С.Б.Гашков В.Н.Чубариков

АРИФМЕТИКА. АЛГОРИТМЫ. СЛОЖНОСТЬ ВЫЧИСЛЕНИЙ

ИЗДАНИЕ ВТОРОЕ, ПЕРЕРАБОТАННОЕ

Рекомендовано
Министерством образования
Российской Федерации
в качестве учебного пособия
для студентов вузов

Москва
«Высшая школа» 2000

УДК 511
ББК 22.1
Г 24

Рецензенты: кафедра математической кибернетики факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова (зав. кафедрой докт. физ.-мат. наук, профессор В.Б. Алексеев); докт. физ.-мат. наук, профессор. Г.И. Архипов (МИАН им. В.А. Стеклова)

Гашков С.Б., Чубариков В.Н.

Г 24 Арифметика. Алгоритмы. Сложность вычислений: Учеб. пособие для вузов/Под ред. В.А. Садовничего.— 2-е изд., перераб.— М.: Высш. шк., 2000.— 320 с.

ISBN 5-06-003613-8

В книге (1-е изд.— 1986) впервые в отечественной литературе рассматривается связь вопросов арифметики с современными проблемами кибернетики. Она представляет собой сборник задач по арифметике и теории сложности арифметических алгоритмов, позволяющий получить систематические знания в этих областях математики. Рассматриваются классические проблемы, из которых возникли новые направления исследований, и задачи олимпиадного характера.

Для студентов вузов. Может быть полезна студентам университетов и педагогических вузов, а также для самостоятельной и научной работы на разных уровнях обучения.

УДК 511
ББК 22.1

Учебное издание

Гашков Сергей Борисович
Чубариков Владимир Николаевич

АРИФМЕТИКА. АЛГОРИТМЫ. СЛОЖНОСТЬ ВЫЧИСЛЕНИЙ.

Редактор *Ж.И. Яковлева.*
Художественный редактор *Ю.Э. Иванова.*
Технический редактор *Л.А. Овчинникова.*
Корректор *В.В. Кожуткина.*
Компьютерная верстка авторов

ЛР № 010146 от 25.12.96. Изд. № ФМ-197. Подп. в печать 06.08.99
Формат 60x90 1/16. Бумага газетная. Гарнитура "Литературная". Печать офсетная
Объем 20,00 усл. печ. л. + 0,75 усл. печ. л. форз., 20,75 усл. кр.-отт., 17,67 уч.-изд. л. + + 0,43 уч.-изд. л. форз. Тираж 7000 экз. Заказ № 2330

Издательство «Высшая школа», 101430, Москва, ГСП-4, Неглинная ул., д. 29/14

Отпечатано в ГУП ИПК "Ульяновский Дом печати"
432601, г. Ульяновск, ул. Гончарова, 14

ISBN 5-06-003613-8

ПРЕДИСЛОВИЕ

В России исторически сложилось так, что представление об образовании включает в себя органичное единство школы как системы приобретения знаний, фундаментальной науки как показателя уровня подготовки специалистов и гуманитарной культуры как основы духовного богатства человека.

Формулируя задачи образования, академик А. Н. Крылов говорил: "Школа не может дать вполне законченного знания; главная задача школы — дать общее развитие, дать необходимые навыки, одним словом... главная задача школы — научить учиться, и для того, кто в школе *научится учиться*, практическая деятельность всю его жизнь будет наилучшей школой."

Отметим, что особенность отечественной школы состоит в сочетании четкости рассуждений с глубиной содержания и простотой, доступностью, конкретностью изложения материала, которые всегда предпочитаются формальным конструкциям. Практическое воплощение данных идей подразумевает наличие высококвалифицированных и творчески мыслящих преподавателей.

Математическое образование и математическая культура составляют стержень научного знания и значение математики как основы фундаментальных исследований постоянно возрастает.

Для решения этих задач требуются учебники, отражающие в определенной полноте современное состояние исследований и мировоззренческие принципы данной области науки.

Предлагаемые к публикации избранные учебники по математике реализуют указанный выше подход. Они написаны, в основном, профессорами Московского государственного университета им. М. В. Ломоносова.

Книга С. Б. Гашкова, В. Н. Чубарикова "Арифметика. Алгоритмы. Сложность вычислений" посвящена изучению свойств целых чисел, связанных с делимостью. Арифметика является первым математическим предметом, с которого начинается обучение в школе. Этот процесс обучения по существу в дальнейшем продолжается, так как идеи, рассуждения и утверждения арифметического характера

пронизывают всю математику. Поэтому арифметика представляет интерес для всех, кто занимается математикой, от школьников до специалистов.

Книга состоит из 17 параграфов, тесно связанных целью, поставленной авторами — ознакомить читателя с материалом, который скорейшим путем приводит к современным проблемам теории чисел и теории сложности арифметических алгоритмов. Задачи в каждом параграфе сгруппированы по единству идей и содержания, иногда их объединяют связанные между собой сходные методы решения или просто схожесть формулировки. Часто группы задач заканчиваются красивой и очень трудной задачей. Но если прорешать все задачи подряд, то и она не покажется трудной. Каждый параграф сопровождается указаниями и решениями.

Этот задачник отличается от многочисленных пособий для поступающих в вузы и различных дидактических материалов по школьной математике тем, что в нем нет задач тренировочного и экзаменационного характера, нужных лишь для усвоения и закрепления некоторых стандартных приемов и навыков. Авторы предполагают, что основные навыки у читателя имеются, а недостающие он приобретет, работая с этой книгой. Хочется надеяться, что после ее прочтения у вас появится привычка самостоятельно размышлять над решением нетривиальных (не значит обязательно чрезмерно трудных) задач. В книге имеется достаточное количество и несложных задач.

Отметим также, что задачник отличается и от многочисленных изданий по занимательной математике. Истинная занимательность заключается, скорее, в содержании задач, чем во внешнем "оформлении" их условий.

По-настоящему интересные задачи часто неизбежно оказываются довольно трудными, а иногда и чрезвычайно трудными. Это в полной мере относится и к задачам, помещенным в данной книге. Многие из них предлагались на различных математических олимпиадах. Но пугаться этих задач не следует — в отличие от участников олимпиады у читателя достаточно времени для их решения, к тому же можно заглянуть в указания. Но не делайте этого, не потратив несколько часов на попытку самостоятельно решить задачу, — даже в случае неудачи в этом случае будет легче понять указание.

В отличие от сборников олимпиадных задач эта книга содержит сравнительно мало слишком искусственных задач, хотя и носящих арифметический характер, но не имеющих арифметического содержания. Зато в ней довольно много классических теорем и задач, взятых из разных областей теории чисел, которые мало известны школьникам (и не только им), но безусловно, заслуживают более широкой популярности.

Надеюсь, что книга послужит вам долго и с ее помощью вы

научитесь решать трудные задачи. Если же вы изберете профессию, связанную с математикой, она пригодится вам и в студенческие годы, и позже, ведь последние разделы задачника представляют интерес не только для студентов, но и для специалистов.

Уже вышли в свет следующие учебники и учебные пособия: Архипов Г. И., Садовничий В. А., Чубариков В. Н. "Лекции по математическому анализу", Виноградов И. М. "Элементы высшей математики (Аналитическая геометрия. Дифференциальное исчисление. Основы теории чисел)", Привалов И. И. "Введение в теорию функций комплексного переменного", Садовничий В. А. "Теория операторов", Нечаев В. И. "Элементы криптографии (основы теории защиты информации)".

Надеюсь, что данные книги положат начало новой серии базовых учебников по высшей математике для вузов с повышенным уровнем математической подготовки.

Кроме практической ценности эта серия призвана подвести некоторые итоги работы российских ученых и педагогов-математиков по созданию базовых учебников по математике на рубеже второго и третьего тысячелетий. Серия не ограничивается указанными книгами. В дальнейшем предполагается продолжить отбор и издание как современных, так и классических учебников, которые отвечают изложенной выше концепции, не потеряли своей новизны и актуальности и пользуются заслуженной популярностью и авторитетом у студентов и педагогов.

Академик
Российской академии наук
В. А. Садовничий

ВВЕДЕНИЕ

В книге содержатся задачи о числах натуральных, целых, рациональных — короче говоря, о дробях. На первый взгляд, она посвящена довольно узкой теме, но удивительно, сколь обширной она оказалась. Причина этого в том, что именно дробные числа составляют "сердцевину" элементарной теории чисел и служат конструктивной основой для коммутативной алгебры и математического анализа. От рациональных чисел естественно совершается переход к иррациональным числам, последовательностям рациональных чисел и построению теории вещественных чисел. Это делается в исторической последовательности их возникновения, опираясь на естественное предназначение вещественных чисел для измерения длин отрезков, и приводит к построению вещественных чисел, исходя из понятия бесконечных десятичных дробей. При этом авторы исходили из представления о числе, которое дает школьная программа, а затем постепенно углубляли это понятие, уточняя только те моменты, которые нуждаются в большей ясности.

Начинается книга с параграфа о дробных и целых частях чисел, содержащего кроме большой подборки олимпиадных задач и ряд классических результатов. Далее рассматривается представление рациональных чисел дробями специального вида, истоки многих задач которого находятся в глубокой древности. Следующие параграфы содержат задачи о рядах Фарея и задачи, связанные с так называемой китайской теоремой об остатках.

В §5 содержатся задачи о делимости целых чисел. Разумеется, задачи о делимости в определенном смысле являются задачами о дробях. Теория делимости — основной раздел элементарной теории чисел. Авторы умышленно не пользуются терминологией теории сравнений (несмотря на ее очевидное удобство) с целью сделать формулировки задач понятными даже школьникам средних классов. В этом параграфе содержатся много олимпиадных задач, не зависимых друг от друга, и большой цикл задач, объединенных единым методом решения, основанным на применении мало известного варианта формулы Лежандра для максимальной степени простого числа, делящего заданный факториал. В конце параграфа помещен цикл задач, по-

священный постулату Бертрана (как известно, впервые доказанному П.Л.Чебышевым). Доказательство разбито на много вспомогательных и в основном несложных задач и следует схеме С.Рамануджана.

Учитывая важность вопроса о представлении рациональных чисел периодическими дробями и его связь с интересными задачами элементарной теории чисел и то обстоятельство, что этот вопрос недостаточно освещается в школе, авторы посвятили ему большую подборку задач, многие из которых мало известны или вообще не известны широкой публике. Начиная с задач о периодических дробях, читатель в этом параграфе доберется до первообразных корней, квадратичных вычетов и квадратичного закона взаимности — "золотой теоремы" Гаусса.

При выполнении операций с рациональными числами и в вопросе о соизмеримости отрезков естественно появляется алгоритм Евклида, который, в свою очередь, ведет к цепным дробям. Цепные дроби очень важны для математики, и поэтому мы посвятили им большой раздел, содержащий также задачи о различных применениях алгоритма Евклида.

На практике иррациональные числа приходится заменять на приближающие их рациональные, и в §7 содержится большая подборка задач о приближении иррациональных чисел рациональными. Здесь имеется много задач, являющихся классическими теоремами, принадлежащими выдающимся математикам (в скобках указаны их фамилии) или фрагментов этих теорем (эти фрагменты появились по причине, указанной в предисловии). Тем не менее в этом и других параграфах даже искушенный читатель, возможно, найдет много не известных ему фактов и доказательств.

С параграфами о диофантовых приближениях и цепных дробях связан §10 о диофантовых уравнениях, в котором, правда, собраны только задачи о так называемом уравнении Пелля. Здесь изложен классический метод решения уравнения Пелля, рассмотрены многочисленные частные случаи, указана элементарная (но довольно точная) оценка величины минимального решения произвольного уравнения Пелля, установлена связь между решениями уравнения Пелля и наилучшими рациональными приближениями квадратичных иррациональностей, приведены разнообразные приложения. Подборка задач этого параграфа, по-видимому, является самой обширной в популярной литературе на эту тему.

Геометрии чисел посвящен §12. В нем приведено много интересных олимпиадных задач и классических результатов. Здесь даны два новых геометрических доказательства теоремы Маркова – Гурвица.

В последние сорок лет широко распространяется подход, связанный с рассмотрением сложности конструктивных математических объектов и сложности вычислений. Поэтому в книгу включена подборка

задач о сложности представления рациональных чисел арифметическими формулами разных видов, цепными дробями и их обобщениями. Эти задачи оказались тесно связанными с задачей об оптимальном конструировании электрических цепей из единичных сопротивлений и задачей об оптимальном разбиении прямоугольника на квадраты. Здесь мы использовали некоторые идеи, постановки задач и неопубликованные результаты О. М. Касим-заде, которому мы выражаем нашу искреннюю благодарность.

Естественным продолжением § 12 является § 14 о сложности приближения иррациональных чисел рациональными. В нем, в частности, имеется теорема, в определенном смысле двойственная к теореме Маркова – Гурвица.

Отметим, что в решениях задач §§ 10 – 14 часто используются задачи из предыдущих параграфов, например, о числах Фибоначчи. В подготовке этих параграфов использована кандидатская диссертация Марзука эль Овейхана, выполненная под руководством авторов этой книги.

Сложностной подход использован также в параграфе о построениях рациональных чисел циркулем и линейкой. Здесь получены довольно точные оценки наименьшего числа прямых и окружностей, которые нужно провести для разделения отрезка на n равных частей, и других подобных задач, указана связь этих задач с оценками сложности вычисления значений многочленов и так называемыми аддитивными цепочками. Хотя постановка задачи о нахождении наиболее экономных построений известна с прошлого века (она принадлежит Лемуану), по-видимому, упомянутые результаты являются оригинальными.

Вопросам сложности выполнения арифметических операций над числами и многочленами посвящен § 17. Прорешав содержащиеся в нем задачи, читатель узнает, как можно выполнять эти операции существенно быстрее, чем традиционным образом. Результаты этого параграфа получены сравнительно недавно (самый старый из них — в 1962 г. А. А. Карацубой, который тогда был аспирантом МГУ) и излагались лишь в небольшом количестве специальных монографий. По сравнению с известными изложениями внесены усовершенствования, приведшие к упрощениям в доказательствах и улучшению констант в оценках.

Параграфы, о которых только что шла речь, вводят читателя в круг идей современной математики, но являются элементарными, хотя и довольно трудными. Более трудным и совсем не элементарным является § 16, содержащий задачи о равномерном распределении дробных частей последовательностей вещественных чисел. Теория равномерного распределения составляет важный раздел современной аналитической теории чисел и находит применение как в самой теории чисел (например, в доказательстве И.М.Виноградова гипотезы Гольд-

баха о представлении нечетного числа в виде суммы трех простых чисел), так и в вычислительной математике и теории вероятностей (метод Монте-Карло, компьютерные датчики случайных чисел) и теории информации (криптология и криптография). В решениях этих задач читатель найдет ряд оригинальных идей, отсутствующих, например, в известной книге Кейперса и Нидеррейтера. Имеются в этом параграфе и новые задачи. Несмотря на более высокий в среднем уровень трудности задач § 16, в нем имеется достаточное количество несложных задач, намеренно сформулированных совершенно элементарным образом.

Образцом при написании этой книги был знаменитый задачник Г.Полиа и Г.Сеге. Поэтому имеются пересечения с ним и по темам, и по конкретным задачам. Но в отличие от упомянутого задачника авторы посвятили свою книгу более узкой, главным образом, теоретико-числовой и смежной с ней тематике. Причиной явились (кроме неуместности конкуренции с замечательной книгой венгерских математиков) личные вкусы и интересы авторов, а также бедность литературы по избранной теме. Поскольку, если не считать стандартных вузовских задачников по алгебре и теории чисел, она ограничивается в основном задачником В.Серпинского "Двести пятьдесят задач по элементарной теории чисел" и разделом задач в "Основах теории чисел" И.М.Виноградова, а также "Избранными задачами и теоремами арифметики и алгебры" Д.О. Шклярского, Н.Н. Ченцова и И.М.Яглома.

Другое отличие от книги Г. Полиа и Г. Сеге — ориентация в первую очередь на школьника, а потом уже на студента. Следуя Г.Полиа и Г.Сеге и И.М.Виноградову, авторы старались выстраивать задачи в циклы, прорешав которые, читатель сможет самостоятельно находить доказательства трудных теорем.

Надеемся, что книга будет полезной не только в изучении, но и в преподавании математики.

Из-за нежелательности чрезмерного увеличения объема книги часть задач оставлена без решений, а к некоторым даны только краткие указания, впрочем, достаточные для того, чтобы читатель восстановил по ним полные решения. К наиболее трудным задачам, как правило, даются подробные указания или полные решения. Задачи, к которым не приведено указаний, можно использовать для проведения олимпиад, экзаменов и контрольных работ. После номеров задач, предлагавшихся на олимпиадах, в скобках указано название олимпиады (например, IMO — международная олимпиада, ВМО — всесоюзная олимпиада, AMM — заочный конкурс американского математического ежемесячника) и год ее проведения. Некоторые задачи могут использоваться для курсовых работ и студенческих семинаров.

Задачи дифференцированы по уровню сложности. Предполагаемой

сложности соответствуют символы *, **, или ***.

Авторы выражают благодарность своим учителям — профессорам В. Б. Алексееву, Г. И. Архипову, А. А. Карацубе, чл.-корр. РАН О.Б.Лупанову и коллегам по механико-математическому факультету Московского университета и специализированной физико-математической школе-интернату №18 при МГУ (ныне СУНЦ МГУ), а также С. А. Богатому, В. В. Вавилову, М. З. Гараеву, Ф. М. Малышеву и всем друзьям и коллегам.

§ 1. ЦЕЛАЯ И ДРОБНАЯ ЧАСТИ ЧИСЛА

Целой частью числа x называется такое целое число $n = [x]$, которое удовлетворяет неравенствам $n \le x < n+1$. **Дробной частью** числа x называется число $\{x\} = x - [x]$. Целое число $m =]x[$ такое, что $m - 1 < x \le m$ называется **верхней целой частью.** Число

$$||x|| = \min(x - [x],]x[- x)$$

называется **расстоянием до ближайшего целого числа,** а само это ближайшее целое число обозначается $((x))$.

1.1. Докажите, что функции $\{x\}$, $||x||$, периодичны с наименьшим периодом единица, и постройте их графики. Проверьте, что

$$]x[= -[-x],\ ((x)) = [2x] - [x] \quad (\text{при} \quad x \ne n + 1/2, n \in \mathbb{Z}),$$

$$||x|| = |x - (x)| \quad (\text{при} \quad x \ne n + 1/2, n \in \mathbb{Z}),$$

$$||x|| = \min(\{x\}, 1 - \{x\}) = \frac{1}{2} - |\{x\} - \frac{1}{2}|.$$

1.2. Докажите, что $\left[x + \frac{1}{2}\right] = [2x] - [x], [x] + [y] + 1 \ge [x+y] \ge [x] + [y]$,

$$0 \le [2x] - 2[x] \le 1, [2x] + [2y] \ge [x] + [y] + [x+y], [[x]/n] = [x/n].$$

1.3. Докажите, что $]x - \frac{1}{2}[=]2x[-]x[,]x[+]y[- 1 \le]x + y[\le]x[+]y[$,

$$0 \le 2]x[-]2x[\le 1,]2x[+]2y[\le]x[+]y[+]x + y[,]]x[/n[=]x/n[.$$

1.4 Выразить количество целых чисел, находящихся на промежутке $(a, b]$, т. е. удовлетворяющих неравенствам $a < x \le b$, через функцию целая часть числа.

1.5. *(Эрмит)* Докажите, что

$$[x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \cdots + \left[x + \frac{n-1}{n}\right] = [nx].$$

1.6. Докажите, что

$$\left(\left\{x + \frac{1}{n}\right\} - \frac{1}{2}\right) + \left(\left\{x + \frac{2}{n}\right\} - \frac{1}{2}\right) + \cdots + \left(\left\{x + \frac{n}{n}\right\} - \frac{1}{2}\right) = \{nx\} - \frac{1}{2}.$$

1.7. *(IMO,68)* Докажите,что

$$\left[\frac{n+1}{2}\right] + \left[\frac{n+2}{4}\right] + \left[\frac{n+4}{8}\right] + \cdots + \left[\frac{n+2^k}{2^{k+1}}\right] + \cdots = n.$$

1.8*. *(AMM)* Докажите,что

$$\left[\frac{n}{2}\right]+\left[\frac{n+1}{4}\right]+\left[\frac{n+3}{8}\right]+\cdots+\left[\frac{n+2^k-1}{2^{k+1}}\right]+\cdots=n-1.$$

1.9*. *(AMM)* Докажите,что при любых x и m

$$\sum_{n=1}^{m}\left(\left\{2^n x+\frac{1}{2}\right\}-\frac{1}{2}\right)\le 1.$$

1.10*. *(США,75)* Докажите, что

$$[5x]+[5y]\ge[x]+[y]+[3x+y]+[x+3y],$$

и выведите отсюда, что для неотрицательных x и y

$$[5x]+[5y]\ge[3x+y]+[x+3y].$$

1.11*. Пусть $p,q\in\mathbb{N}$ — взаимно простые числа. Докажите путем подсчета целых точек в области $1\le x\le p-1, 1\le y\le qx/p$, что

$$\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\cdots+\left[\frac{(p-1)q}{p}\right]=(p-1)(q-1)/2.$$

1.12*. *(Эйзенштейн)* Пусть $p,q\in\mathbb{N}$ — взаимно простые числа, $p'=\frac{p-1}{2}$, $q'=\frac{q-1}{2}$. Докажите путем подсчета целых точек в области $1\le x\le p', 1\le y\le q'$, что

$$\left(\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\cdots+\left[\frac{p'q}{p}\right]\right)+\left(\left[\frac{p}{q}\right]+\left[\frac{2p}{q}\right]+\cdots+\left[\frac{q'p}{q}\right]\right)=p'q'.$$

В задачах 1.13 – 1.20 достаточно знать, что $[\sqrt{n}]=k$, если и только если $k^2\le n<(k+1)^2$.

1.13. Докажите,что

$$\left[\sqrt{[x]}\right]=[\sqrt{x}],\ \left]\sqrt{]x[}\right[=]\sqrt{x}[\quad\text{при}\quad x\ge 0,$$

$$[\log_n[x]]=[\log_n x]\quad\text{при}\quad x\ge 1,\quad\ ]\log_n]x[[=]\log_n x[\quad\text{при}\quad x>1/n,$$

если $n>1$ — целое.

Следующая задача обобщает предыдущую.

1.14*. *(Мак-Элис)* Пусть $f(x)$ — непрерывная строго возрастающая на отрезке I функция, и если x лежит в I, то и $[x]$ и $]x[$ — тоже лежат в этом отрезке.

Тогда равенства

$$[f([x])] = [f(x)] \text{ и }]f(]x[)[=]f(x)[$$

равносильны друг другу и выполняются тогда и только тогда, когда функция обладает следующим свойством: если $f(x)$ — целое число, то и x — тоже целое число.

Следующая задача обобщает одно из утверждений задачи 1.2.

1.15. Докажите,что при любых целых m и $n, n > 0$, и любом действительном x справедливы равенства

$$[(x+m)/n] = [([x]+m)/n],](x+m)/n[=](]x[+m)/n[,]m/n[= [(n+m-1)/n].$$

1.16. Докажите, что

$$\left[\sqrt{1}\right] + \left[\sqrt{2}\right] + \cdots + \left[\sqrt{n^2-1}\right] = n(n-1)(4n+1)/6,$$

$$\left[\sqrt{1}\right] + \left[\sqrt{2}\right] + \cdots + [\sqrt{n}] = [\sqrt{n}]\left(n - \frac{(2[\sqrt{n}]+5)([\sqrt{n}]-1)}{6}\right).$$

1.17. *(Австрия,74)* Докажите при любом натуральном n, что

$$[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+2}].$$

1.18*. Докажите, что $n = ((n/2))+((n/4))+((n/8))+((n/16))+\dots$.

1.19. *(ВМО,78)* Докажите, что

$$2n = 1/((\sqrt{1})) + 1/((\sqrt{2})) + \cdots + 1/((\sqrt{n(n+1)})).$$

1.20. *(Москва,66)* Дано, что $a_1 = 1, a_k = [\sqrt{a_1 + \cdots + a_{k-1}}]$ при $k > 1$. Найдите a_{1000}.

1.21. Докажите, что:

а)

$$T(n) = \tau(1) + \cdots + \tau(n) = [n/1] + [n/2] + \dots + [n/n],$$

где $\tau(k)$ — число всех натуральных делителей числа k;

б)* *(Дирихле)*

$$T(n) = 2\sum_{k \le \sqrt{n}} [n/k] - [\sqrt{n}]^2;$$

в)* *(Дирихле)* $T(n) = n(\ln n + 2\gamma - 1) + R_n$, где $|R_n/\sqrt{n}| \le C$, $C > 0$ — некоторая постоянная, а $\gamma = 0,577\dots$ — постоянная Эйлера ($\gamma = \lim\limits_{n\to\infty}(1 + 1/2 + \dots + 1/n - \ln n)$).

В 1903 г. для величины остатка R_n Г. Ф. Вороной получил оценку $|R_n/n^{1/3}\ln n| \le C, C > 0$ — некоторая постоянная. В настоящее время

в оценке Вороного показатель степени $1/3$ улучшен до $7/22$. Харди показал, что этот показатель не может быть меньше $1/4$. Существует предположение, что он в точности равен $1/4$.

г)* *(Марджанишвили)* При любых целых $l \geq 1$, $n \geq 1$, $k \geq 2$ выполняется неравенство

$$n^{-1} \sum_{1 \leq m \leq n} \tau_k^l(m) < A(\ln n + k^l - 1)^{k^l - 1},$$

где $\tau_k(m)$ — число решений $(x_1, \ldots, x_k)$ уравнения $x_1 \ldots x_k = m$ в натуральных числах и $A = k^l (k!)^{-(k^l-1)/(k-1)}$.

1.22*. Докажите, что $\sigma(1) + \ldots + \sigma(n) = [n/1] + 2[n/2] + \cdots + n[n/n]$, где $\sigma(k)$ — сумма всех натуральных делителей числа k.

1.23*. Найдите целую часть числа

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n^2}}.$$

1.24*. Найдите целую часть числа $4^{-1/3} + 5^{-1/3} + \cdots + (n^3)^{-1/3}$.

1.25. Докажите, что $\left[\sqrt{n(n+1)(n+2)(n+3)}\right] = n^2 + 3n$.

1.26. *(В. Тебо)* Докажите, что $\left[(n(n+1)\ldots(n+7))^{1/4}\right] = n^2 + 7n + 6$.

1.27. Докажите, что $\left[\sqrt{[\sqrt{x}]}\right] = \left[\sqrt{\sqrt{x}}\right]$.

1.28. Докажите, что $[(1+\sqrt{3})^{2n+1}] = (1+\sqrt{3})^{2n+1} + (1-\sqrt{3})^{2n+1}$.

1.29. Докажите, что $[(2+\sqrt{3})^n]$ — нечетно.

1.30. Найти наивысшую степень двойки, на которую делится число $[(1+\sqrt{3})^n]$.

1.31*. Докажите, что сумма чисел $[(n/x)^{1/m}]$, взятая по всем x, $1 \leq x \leq n$, не делящимся ни на какие m-е степени натуральных чисел, равна $[n]$.

1.32*. *(Болгария, 83)* а) Докажите, что если при любом натуральном n имеем равенство $[na] + [nb] = [nc]$, то хотя бы одно из чисел a, b — целое.

б) Докажите, что равенство $[na_1] + \cdots + [na_k] = [nb]$ справедливо при любом натуральном n тогда и только тогда, когда все числа a_i, кроме, быть может, одного, целые, а число $b = a_1 + \cdots + a_k$.

1.33*. *(США, 81)* Докажите, что при любом $x \geq 0$ и натуральном n справедливо равенство

$$[nx] \geq [x]/1 + [2x]/2 + \cdots + [nx]/n.$$

1.34*. Последовательности $[\alpha], [2\alpha], [3\alpha], \ldots$ и $[\beta], [2\beta], [3\beta], \ldots$ содержат в совокупности все натуральные числа, причем каждое число

принадлежит только одной из них, тогда и только тогда, когда $\alpha > 1$ и иррациональное и $1/\alpha + 1/\beta = 1$.

1.35. *(С.-Петербург, 1992)* Докажите, что если натуральное m не является точным квадратом, то найдется такое натуральное n, что $m = [n + \sqrt{n} + 1/2]$.

1.36. Докажите, что при натуральном n справедливо тождество

$$[\sqrt{9n-1}] = [\sqrt{n-1} + \sqrt{n} + \sqrt{n+1}].$$

1.37. *(Москва, 57)* Решите уравнение $x^3 - [x] = 3$.

1.38. *(Киев, 72)* Решите уравнение $[x]^3 + [x]^2 + [x] = \{x\} - 1$.

1.39. *(Москва, 55)* При любом натуральном N найти все a, такие, что все числа $[a], [2a], \ldots, [Na]$ различны и все числа $[1/a], \ldots, [N/a]$ тоже различны.

1.40*. Докажите, что при любых целых m и $n, n > 0$, и любом действительном x справедливы равенства

$$\sum_{k=0}^{n}[(x+mk)/n] = (m-1)(n-1)/2 + (d-1)/2 + d[x/d] = \sum_{k=0}^{m}[(x+nk)/m],$$

где d — наибольший общий делитель чисел m и n.

1.41. *(Турнир городов)* Докажите тождество

$$[n^{1/2}] + [n^{1/3}] + \cdots + [n^{1/n}] = [\log_2 n] + [\log_3 n] + \ldots [\log_n n].$$

УКАЗАНИЯ

1.2. Для доказательства последнего равенства заметьте, что чисел, не больших x и кратных n будет $[x/n]$, а чисел, кратных n и не больших $[x]$, будет $[[x]/n]$.

1.3. Воспользуйтесь тождеством "двойственности" $]x[= -[-x]$.

1.5. При $0 \le x < 1/n$ равенство очевидно. Если x увеличить на $1/n$, то обе части равенства возрастают на 1.

1.6. Выведите из 1.4.

1.7. Примените равенство $[x + 1/2] = [2x] - [x]$.

1.8. Пусть $n - 1 = \sum_{r=0}^{s} 2^r \alpha_r$, тогда

$$\left[\frac{n + 2^k - 1}{2^{k+1}}\right] = \alpha_{k-1} + \sum_{m=k}^{s} 2^{m-k}\alpha_m.$$

1.9. Примените равенства $\{2^n x + 1/2\} - 1/2 = \{2^{n+1}x\} - \{2^n x\}$.

1.10. Учитывая периодичность и симметричность, можно предполагать, что $0 \le x \le y < 1$; рассмотрите возможные случаи

$$x \in [k/5, (k+1)/5), y \in [p/5, (p+1)/5), m \le 3x + y < m + 1, n \le x + 3y < n + 1.$$

1.11. Выписанная сумма равна количеству целых точек внутри прямоугольника с вершинами $(0,0),(p,0),(p,q),(0,q)$, лежащих под диагональю, а значит половине всех целых точек внутри прямоугольника.

1.12. Подсчитайте отдельно число точек выше и ниже прямой $y = qx/p$.

1.14. Если, например, $[f([x])] < [f(x)]$, то согласно непрерывности и монотонности $f(x)$ существует y, такое, что $[x] < y \leq x$ и $f(y)$ — целое, но y при этом целым быть не может.

1.15. Примените 1.14.

1.16. Воспользуйтесь формулой Абеля

$$\sum_{k=1}^{n} a_k = na_n - \sum_{k=1}^{n-1} k(a_{k+1} - a_k).$$

1.17. Докажите, что $\sqrt{n} + \sqrt{n+1} < \sqrt{4n+2}$. Предположите, что для целого m имеют место неравенства

$$\sqrt{n} + \sqrt{n+1} < m \leq \sqrt{4n+2},$$

и выведите отсюда, что

$$4n(n+1) < (m^2 - 2n - 1)^2 \leq 4n(n+1) + 1,$$

откуда $m^2 = 2(2n+1)$, что невозможно.

1.18. Количество нечетных чисел, меньших n, равно $((n/2))$, количество четных чисел, меньших n и не делящихся на 4, равно $((n/4))$ и т.д.

1.19. Заметьте, что

$$\frac{1}{((\sqrt{n}))} = \frac{1}{k} \Longleftrightarrow k^2 - k < n \leq k^2 + k,$$

и сгруппируйте в соответствии с этим слагаемые.

1.21. Заметьте, что $T(N)$ равно числу точек с натуральными координатами, лежащих не выше гиперболы $xy = N$. В силу симметричности гиперболы относительно прямой $y = x$ справедливо равенство

$$T(N) = 2T_0(N) - \left[\sqrt{N}\right]^2,$$

где $T_0(N)$ — число упомянутых точек, лежащих не выше гиперболы и не правее прямой $x = \sqrt{N}$. Подсчитывая эти точки "по вертикалям", имеем

$$T_0(N) = \sum_{1 \leq n \leq \sqrt{N}} [N/n] = \sum_{1 \leq n \leq \sqrt{N}} N/n + O(\sqrt{N}),$$

где через $O(f(N))$ здесь и далее обозначаем величину, модуль которой не превосходит $Cf(N)$, где $C > 0$ — не зависящая от N константа. Отсюда следует, что

$$T(N) = 2N \sum_{1 \leq n \leq \sqrt{N}} 1/n - N + O(\sqrt{N}).$$

Остается воспользоваться формулой Эйлера

$$\sum_{1 \leq n \leq X} 1/n = \ln X + \gamma + O(1/X),$$

где γ — константа Эйлера, равная $\lim\limits_{X\to\infty}\left(\sum\limits_{1\le n\le X} 1/n - \ln X\right)$, а $\ln X$ — функция, равная площади, ограниченной прямыми $x=1, x=X, y=0$ и гиперболой $xy=1$ (эта функция называется натуральным логарифмом). Для доказательства формулы Эйлера заметим, что площадь, ограниченная прямыми $x=Y, x=X, y=0$, где $0<Y<X$, и гиперболой $xy=1$, равна $\ln X/Y$ и при целых Y и X заключена между

$$A=\sum_{Y+1\le n\le X} 1/n \quad \text{и} \quad \sum_{Y\le n\le X-1} 1/n = A + 1/Y - 1/X.$$

Отсюда следует, что при целых X и Y, $X>Y$, справедливы неравенства

$$\gamma_X = \sum_{1\le n\le X-1} 1/n - \ln X = \gamma_Y + \sum_{Y\le n\le X-1} 1/n - \ln X/Y < \gamma_Y + 1/Y,$$

$$\gamma_X > \gamma_Y.$$

Устремляя X к бесконечности, получите, что при любом целом Y

$$\gamma_Y < \gamma < \gamma_Y + 1/Y.$$

Значит,

$$\sum_{1\le n\le x} 1/n = \ln x + 1/x + \gamma_x = \ln x + \gamma + O(1/x),$$

а при нецелом x также имеем

$$\sum_{1\le n\le x} 1/n = \sum_{1\le n\le [x]} 1/n = \ln[x] + \gamma + O(1/[x]) =$$

$$= \ln x - \ln x/[x] + \gamma + O(1/x) = \ln x + \gamma + O(1/x),$$

так как

$$0 < \ln x/[x] < \ln(([x]+1)/[x]) < 1/[x] = O(1/x).$$

1.32. Докажем утверждение б). Сначала проверьте, что имеет место равенство $b = a_1 + \cdots + a_k$. Для этого заметьте, что если бы, например, $b < a_1 + \cdots + a_k$, то при достаточно большом n было бы справедливо неравенство

$$[na_1] + \cdots + [na_k] > n(a_1 + \cdots + a_k) - k > nb \ge [nb].$$

Пользуясь равенством $b = a_1 + \cdots + a_k$, замените тождество задачи на тождество

$$\{na_1\} + \cdots + \{na_k\} = \{nb\}$$

и заметьте, что в нем можно полагать, что $0 \le a_i < 1$, и даже, что всегда $0 < a_i < 1$ (так как нулевые слагаемые можно вычеркнуть).

Осталось показать, что при $k>1$ это тождество невозможно. Для этого проверьте, что при некоторых n имеет место неравенство

$$\{na_1\} + \cdots + \{na_k\} \ge 1.$$

В случае, когда все a_i рациональны, это вытекает из центральной симметричности множества всех наборов длины k вида $(\{na_1\}, \ldots, \{na_k\})$. Действительно, $\{-na_i\} = 1 - \{na_i\}$, поэтому для N, равного наименьшему общему знаменателю всех

дробей a_i, справедливы равенства $\{(N-1)na_i\} = 1 - \{na_i\}$, из которых следует, что для некоторого натурального n имеем $\{na_1\} + \cdots + \{na_k\} \geq k/2 \geq 1$.

Пусть теперь, например, a_k — иррациональное число. Можно считать, что $a_1 + \cdots + a_k < 1$, иначе достаточно взять n равным 1. Во множестве всех чисел вида

$$n_1 a_1 + \cdots + n_{k-1} a_{k-1} + a_k,$$

где n_i — натуральные, выберем такое наибольшее c, которое будет все же меньше 1 (это возможно, так как наше множество конечно и не пусто). Тогда

$$a_1 + \cdots + a_{k-1} + a_k \leq c < 1.$$

В силу всюду плотности на отрезке $[0,1]$ последовательности $\{na_k\}$ (которая будет доказана в §16) найдется такое n, что $c < \{na_k\} < 1$. Рассуждая от противного, предположите, что при всех n имеем $\{na_1\} + \cdots + \{na_k\} < 1$, откуда следует, что при всех $i < k$ справедливо неравенство $\{na_i\} < 1 - c$.

Из определения c вытекает, что при всех $i < k$ имеем $a_i \geq 1 - c$. Отсюда следует, что

$$a_i \geq 1 - c > \{na_i\} = \{(n-1)a_i\} + a_i - 1 \geq 0,$$

значит,

$$\{(n-1)a_i\} \geq 1 - a_i,$$

а так как $a_k < c < \{na_k\}$, то

$$\{(n-1)a_k\} = \{na_k\} - a_k > c - a_k,$$

поэтому

$$\{(n-1)a_1\} + \cdots + \{(n-1)a_k\} > k - 1 + c - a_1 - \cdots - a_k \geq k - 1 \geq 1,$$

противоречие.

1.35. Рассмотрите $m - [\sqrt{m}]$.

1.37. *Ответ.* $x = 4^{1/3}$.

1.38. *Ответ.* $x = -1$.

1.39. *Ответ.* $1 - 1/N < a < 1 + 1/(N-1)$.

1.40. Задача сводится к вычислению суммы

$$\sum_{k=0}^{n-1} \{(x + mk)/n\}.$$

Так как при любом целом s имеем

$$\{(x + mk)/n\} = \{(x' + m'k)/n'\} = \{(x' + m'(k + sn'))/n'\},$$

где $x' = x/d$, $n' = n/d$, $m' = m/d$, то

$$\sum_{k=0}^{n-1} \{(x + mk)/n\} = d \sum_{k=0}^{n'} \{(x' + m'k)/n'\}.$$

Вычисление последней суммы сводится к вычислению суммы

$$\sum_{k=0}^{n'} [(x' + m'k)/n'],$$

которую, согласно задаче 1.14, достаточно уметь вычислять при целом x'. Поэтому при вычислении суммы

$$\sum_{k=0}^{n'-1} \{(x' + m'k)/n'\}$$

можно считать, что x' целое и применить задачу 4.13.

1.41. Докажите, что обе части тождества, увеличенные на число n, равны количеству точек с натуральными координатами (x, y), удовлетворяющих неравенствам

$$x^y \leq n, x \leq n, y \leq n.$$

§ 2. ЗАДАЧА ПИСЦА АХМЕСА

Сорок веков назад египтяне уже умели ловко обращаться с обыкновенными дробями. Правда, они предпочитали простейшие дроби вида $\frac{1}{n}$, а более сложные разлагали в сумму простейших. Представление об этом дает задача, имеющаяся в папирусе, хранящемся ныне в музее изобразительных искусств им.А.С.Пушкина в Москве: "Раздели семь хлебов между восьмью людьми". Ответ дан такой: $\frac{1}{2} + \frac{1}{4} + \frac{1}{8}$.

Чтобы у читателя не сложилось мнение о легкости древнеегипетских задач, приведем задачу из папируса Райнда, хранящегося в Британском Музее: найдите натуральное n, такое, что

$$\frac{2}{73} = \frac{1}{60} + \frac{1}{219} + \frac{1}{292} + \frac{1}{n}.$$

Эта задача в 1997 году предлагалась на Московской олимпиаде для шестиклассников, и решили ее отнюдь не все участники.

Следующий цикл задач посвящен вопросам, связанным с разложением чисел в сумму простейших дробей.

2.1. Представьте дробь вида $m/2^n, 0 < m < 2^n$, в виде суммы различных дробей вида $1/2^k$.

Следующая задача обобщает предыдущую.

2.2. Представьте дробь вида m/p^n, $0 < m < p^n$, в виде суммы различных дробей вида a/p^k, $1 \leq a < p$.

2.3. Всегда ли можно представить правильную дробь со знаменателем mn, где m и n — взаимно простые числа в виде: а) суммы; б) суммы или разности двух правильных дробей со знаменателями m и n?

2.4. Докажите, что для любого $k \geq 3$ единицу можно представить в виде суммы k различных дробей вида $\frac{1}{n}$.

2.5. Докажите, что для любого нечетного $k \geq 9$ единицу можно представить в виде суммы k различных дробей вида $1/n$ с нечетными знаменателями. Докажите, что единицу нельзя представить в

виде суммы четного числа различных дробей вида $1/n$ с нечетными знаменателями.

2.6. *(Серпинский)* Докажите, что любое рациональное число можно лишь конечным числом способов представить в виде суммы k дробей вида $1/n$.

2.7.** *(Венгрия, 1980)* Докажите, что дробь $4/n$ при нечетном n представима в виде суммы дробей $1/a$ и $1/b$ тогда и только тогда, когда $n = m(4k-1)$, $m, k \in \mathbb{N}$.

2.8*. Докажите, что дробь $1/n$ при простом n представима в виде суммы дробей $1/a$ и $1/b$ двумя, а при составном n — более чем двумя способами.

2.9*. *(Венгрия, 1931)* Докажите, что дробь $2/n$ при простом n представима в виде суммы дробей $1/a$ и $1/b$ единственным образом.

2.10*. *(Австрия - Польша, 1980)* Докажите, что число n является суммой всех дробей вида $\frac{1}{i_1 \dots i_k}$, где $1 \leq i_1 < \dots < i_k \leq n$.

2.11. *(Фибоначчи)* Докажите, что любое рациональное число из интервала $(0,1)$ можно однозначно представить в виде

$$\frac{1}{a_1} + \dots + \frac{1}{a_n},$$

где a_i — натуральное, $a_{i+1} > a_i^2 - a_i, a_i \geq 2$, причем в таком виде представляются только рациональные числа из интервала $(0,1)$.

2.12*. *(Алгоритм Остроградского)* Докажите, что любое рациональное число из интервала $(0,1)$ можно однозначно представить в виде

$$\frac{1}{a_1} + \frac{1}{a_1 a_2} + \dots + \frac{1}{a_1 \dots a_n},$$

где a_i — натуральное, $a_{i+1} \geq a_i, a_i \geq 2$, причем в таком виде представляются только рациональные числа из интервала $(0,1)$.

Сформулированную задачу можно рассматривать как обобщение задачи 2.1.

2.13. Убедитесь, что алгоритмы 2.11 и 2.12 иногда дают различные разложения в сумму аликвотных дробей, т.е. дробей с числителем, равным 1.

2.14. Обозначим для любого n число $n+1$ через $P_0(n)$, а число $n(n+1)$ — через $P_1(n)$. Докажите индукцией по s равенство

$$1 = \sum_{k=1}^{s} \sum_{a_1=0}^{1} \dots \sum_{a_k=0}^{1} \frac{1}{P_{a_k}(\dots(P_{a_1}(n))\dots)} +$$

$$+(n-s) \sum_{a_1=0}^{1} \dots \sum_{a_s=0}^{1} \frac{1}{P_{a_s}(\dots(P_{a_1}(n))\dots)}$$

и выведите из него, что

$$1 = \sum_{k=1}^{n} \sum_{a_1=0}^{1} \cdots \sum_{a_k=0}^{1} \frac{1}{P_{a_k}(\ldots(P_{a_1}(n))\ldots)}.$$

2.15*. Докажите, что в представлении, указанном в 2.14, все дроби различны.

2.16. Докажите, что любое натуральное n представимо в виде суммы различных аликвотных дробей.

2.17. Докажите, что любое положительное рациональное число представимо в виде суммы различных аликвотных дробей (некорректное доказательство этого факта приведено в книге Ч.Тригга "Задачи с изюминкой").

Из задачи 2.17, в частности, следует, что сумма $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ неограниченно возрастает — как говорят, гармонический ряд расходится.

2.18*. Докажите, что сумма $\frac{1}{2^2} + \cdots + \frac{1}{n^2}$, меньше $2/3$, и выведите отсюда, что любое рациональное число, не меньшее $2/3$, нельзя представить в виде суммы различных дробей, обратных натуральным квадратам.

На самом деле в 2.18 можно заменить $2/3$ на $\pi^2/6 - 1$ (это следует из того, что, согласно Эйлеру, сумма ряда обратных квадратов равна $\pi^2/6$). Эрдеш доказал, что любое положительное рациональное число, меньшее $\pi^2/6 - 1$, можно представить в виде суммы различных дробей, обратных натуральным квадратам.

2.19*. Докажите, что $1/2$ можно представить в виде суммы различных дробей, обратных натуральным квадратам.

2.20. Докажите, что любое положительное рациональное число, меньшее 1, однозначным образом представляется в виде

$$a_1/2! + a_2/3! + \cdots + a_{n-1}/n!,$$

где a_i — целые числа, $0 \leq a_i \leq i$.

2.21. *(BMO,69)* Докажите, что $1/2$ равна сумме всех дробей вида $1/pq$, где $0 < p < q \leq n, p + q > n, p$ и q взаимно просты.

Следующая задача дает еще одно решение задачи 2.4.

2.22. *(Ленинград,85)* Пусть F_n — последовательность Фибоначчи, т.е. $F_{n+1} = F_n + F_{n-1}, F_1 = F_2 = 1$. Докажите, что

$$1/F_1F_3 + 1/F_2F_4 + \cdots + 1/F_{n-2}F_n + 1/F_{n-1}F_n = 1.$$

2.23. *(IMO,79)* Пусть $\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots - \frac{1}{1318} + \frac{1}{1319}$. Докажите, что p делится на 1979.

УКАЗАНИЯ

2.1. Найдите наибольшую дробь вида $1/2^k$, меньшую, чем $m/2^n$, также поступите с "остатком" $m/2^n - 1/2^k = m_1/2^n < 1/2^k$ и т.д. В итоге дробь $m/2^n$ представится в виде суммы не более чем n разных дробей вида $1/2^k$. Можно воспользоваться также разложением числа m в двоичной системе счисления.

2.2. Действуйте аналогично решению предыдущей задачи.

2.3. а) Нет, например $1/mn$ так представить нельзя.

б) Представьте произвольное натуральное число k в виде $k = ma - nb$, где a и b — натуральные числа. Для этого достаточно рассмотреть случай $k = 1$. В этом случае a и b можно найти, определяя остатки от деления на n последовательности чисел $m, 2m, \ldots, (n-1)m$. Они все будут различными, и среди них встретится 1. Пользуясь равенством $k = ma - nb$, представьте дробь k/mn в виде $a/n - b/m$. Если целые части дробей a/n и b/m совпадают, то искомое представление в виде разности правильных дробей имеет вид $k/mn = \{a/n\} - \{b/m\}$. Если же $[a/n] = [b/m] + 1$, то $k/mn = \{a/n\} + \{1 - b/m\}$.

2.4. Воспользуйтесь равенствами

$$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}, \frac{1}{n} = \frac{1}{2n} + \frac{1}{3n} + \frac{1}{6n}$$

и примените индукцию.

2.5. Воспользуйтесь равенствами

$$1 = \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \frac{1}{11} + \frac{1}{15} + \frac{1}{35} + \frac{1}{45} + \frac{1}{231}, \frac{1}{3m} = \frac{1}{5m} + \frac{1}{9m} + \frac{1}{45m}$$

и примените индукцию.

2.6. Примените индукцию по k.

2.7. Если $n = m(4k-1)$, то, очевидно, что

$$\frac{4}{n} = \frac{1}{km} + \frac{1}{km(4k-1)}.$$

Пусть теперь $4/n = 1/a$ и $1/b$. Представим a и b в виде $a = 2^q a_1, b = 2^r b_1$, где a_1 и b_1 — нечетны. Проверьте, что если $r \neq q$, то $n = \frac{4ab}{a+b}$ будет четным, что противоречит условию. Поэтому $r = q$, и так как

$$n = \frac{2^q \cdot 4a_1 b_1}{a_1 + b_1},$$

нечетно, то $q = 0$ и $a_1 + b_1$ кратно 4, значит, a_1 и b_1 имеют разные остатки при делении на 4. Но тогда какое-то простое число p вида $4k-1$ входит в разложения чисел a_1 и b_1 на простые множители в разных степенях, т.е. $a_1 = p^u a_2$ и $b_1 = p^v b_2$, где $u \neq v$, и a_2 и b_2 не кратны p. Считая,что,например, $u > v$, получите тогда равенство

$$n = \frac{4p^v a_2 b_2}{a_2 + p^{v-u} b_2} = p^v c = (4k-1)m.$$

2.8. Если $1/n = 1/a + 1/b$, то $(a-n)(b-n) = n^2$. В случае простого n это уравнение имеет три решения (дающие два разных представления в виде суммы дробей), а в случае составного n — не менее пяти решений.

2.9. Если $2/n = 1/a + 1/b$, то $(2a-n)(2b-n) = n^2$. В случае простого n это уравнение имеет три решения, дающие два разных представления в виде суммы дробей, в том числе при разных a и b — только одно такое представление.

2.10. Пусть

$$S_n = \sum_{1 \le i_1 < \cdots < i_k \le n} \frac{1}{i_1 \dots i_k}.$$

Воспользуйтесь равенством

$$S_n - S_{n-1} = \sum_{1 \le i_1 < \cdots < i_k = n} \frac{1}{i_1 \dots i_k} =$$

$$= \frac{1}{n} + \sum_{1 \le i_1 < \cdots < i_{n-1} \le n-1} \frac{1}{i_1 \dots i_{n-1} n} = \frac{1}{n} + \frac{S_{n-1}}{n}$$

и примените индукцию.

2.11. Пусть $r = m/n$ — рациональное число, $0 < r < 1$. Выберем a_1 так, что $\frac{1}{a_1} \le r < \frac{1}{a_1 - 1}$, тогда

$$r_1 = r - \frac{1}{a_1} = (ma_1 - n)/na_1 = m_1/n_1$$

удовлетворяет неравенствам

$$0 \le r_1 < \frac{1}{a_1(a_1 - 1)}, \quad 0 < ma_1 - n = m_1 < m.$$

Поэтому, выбирая a_2 так, что $\frac{1}{a_2} \le r_1 < \frac{1}{a_2 - 1}$, получаем, что $a_2 > a_1^2 - a_1$, и полагаем

$$r_2 = r_1 - \frac{1}{a_2} = (m_1 a_2 - n_1)/n_1 a_2 = m_2/n_2,$$

тогда $0 < m_1 a_2 - n_1 = m_2 < m_1$. Далее по r_2 определяем a_3 и т. д. Так как последовательность числителей m_i убывает, то при некотором $i < m$ получим, что $r_i = 1/n_i = 1/a_i$.

2.12. Пусть $r = m/n$ — рациональное число, $0 < r < 1$. Выберем a_1 так, что $\frac{1}{a_1} \le r < \frac{1}{a_1 - 1}$, тогда

$$r_1 = r - \frac{1}{a_1} = (ma_1 - n)/na_1$$

удовлетворяет неравенствам

$$0 \le a_1 r_1 = (ma_1 - n)/n = m_1/n < \frac{1}{a_1 - 1}, 0 < ma - n = m < m.$$

Поэтому, выбирая a_2 так, что $\frac{1}{a_2} \le a_1 r_1 < \frac{1}{a_2 - 1}$, получаем, что $a_2 \ge a_1$, и полагаем

$$r_2 = a_1 r_1 - \frac{1}{a_2} = (m_1 a_2 - n)/na_2 = m_2/na_2,$$

тогда

$$0 \le a_2 r_2 = (m_1 a_2 - n)/n = m_2/n < \frac{1}{a_2 - 1}, 0 < m_1 a_2 - n = m_2 < m_1,$$

$$r = r_1 + \frac{1}{a_1} = \frac{1}{a_1} + \frac{1}{a_1 a_2} + \frac{r_2}{a_1}.$$

Далее по r_2 определяем a_3 и т.д. Так как последовательность числителей m_i убывает, то при некотором $k < m$ получим, что

$$a_{k-1} r_{k-1} = \frac{1}{n_{k-1}} = \frac{1}{a_k}, r = \frac{1}{a_1} + \frac{1}{a_1 a_2} + \cdots + \frac{1}{a_1 \dots a_k},$$

где $a_{i+1} \geq a_i, a_1 \geq 2, i = 1, \ldots, k-1$.

2.13. Возьмите, например, число $1 - 2^{-n}$.

2.14. Заметьте, что $1 = \frac{1}{n} + \cdots + \frac{1}{n}$, $\frac{1}{n} = \frac{1}{P_0(n)} + \frac{1}{P_1(n)}$.

2.15. Пусть s — такое наименьшее число, что для некоторых разных наборов $a_1, \ldots, a_s$ и $b_1, \ldots, b_q$ справедливо равенство

$$P_{a_s}(\ldots(P_{a_1}(n))\ldots) = P_{b_q}(\ldots(P_{b_1}(n))\ldots),$$

тогда $a_s \neq b_q$ и без ограничения общности можно считать, что

$$a_s = \cdots = a_{r+1} = 0, a_r = 1 = b_q,$$

тогда $k + f(f+1) = g(g+1)$, где $1 \leq k \leq n, f \geq n, g \geq n, f, g, k$ — натуральные числа, что невозможно.

2.16. Воспользуйтесь 2.15 и примените индукцию по n.

2.17. Примените задачу 2.16.

2.18. Заметьте, что $1/n^2 < 1/(n-1/2) - 1/(n+1/2)$.

2.19. *Ответ.* $1/2 = 2^{-2} + 3^{-2} + 4^{-2} + 6^{-2} + 7^{-2} + 9^{-2} + 12^{-2} + 14^{-2} + 21^{-2} + 36^{-2} + 45^{-2} + 60^{-2}$.

2.20. Примените индукцию.

2.21. Примените индукцию. Для обоснования шага индукции заметьте, что при $p + q = n$ справедливо равенство

$$1/pq = 1/pn + 1/qn$$

и поэтому сумма всех дробей вида $1/pq$, где $p+q = n, 0 < p < q < n, p$ и q взаимно просты, равна сумме всех дробей вида $1/pq$, где $p + q > n, 0 < p < q = n, p$ и q взаимно просты.

2.22. Примените индукцию. Для обоснования шага индукции заметьте, что

$$1/F_{n-1}F_{n+1} + 1/F_{n+1}F_n - 1/F_{n-1}F_n =$$

$$= 1/F_{n-1}F_{n+1} + (F_{n-1} - F_{n+1})/(F_{n+1}F_nF_{n-1}) =$$

$$= 1/(F_{n-1}F_{n+1}) - 1/(F_{n+1}F_{n-1}) = 0.$$

§ 3. ОТКРЫТИЕ АНГЛИЙСКОГО ГЕОЛОГА

В 1816 г. мистер Фарей расположил в неубывающем порядке все правильные дроби со знаменателями, не большими N, и получил то, что сейчас называют последовательностью Фарея F_N. Например, F_3 — это $\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$.

3.1. Докажите, что в ряде F_N при $N > 1$ нет двух соседних дробей с одинаковыми знаменателями.

3.2. Дробь $\frac{a+c}{b+d}$ называется **медиантой** дробей a/b и c/d. Докажите, что медианта двух дробей заключена по величине между ними.

И вообще, если m — минимальная, а M — максимальная из дробей a_i/b_i, то дробь

$$(a_1 + \cdots + a_n)/(b_1 + \cdots + b_n)$$

заключена между m и M.

3.3. *(Фарей – Коши – Харош)* Пусть a/b и c/d — соседние члены ряда F_N. Докажите, что $ad - bc = +1$.

Эта задача неоднократно предлагалась на различных математических олимпиадах.

3.4. Докажите, что сумма знаменателей соседних дробей в ряде F_N больше N.

3.5. Докажите, что средняя из трех соседних дробей из F_N является медиантой остальных двух.

3.6. Докажите, что дроби из ряда F_{N+1}, не входящие в F_N, являются медиантами своих соседей из ряда F_N.

3.7. *(Евклид)* Докажите, что наибольший общий делитель чисел a и b представляется в виде $ax + by$, где x, y — целые числа.

Далее для наибольшего общего делителя чисел a и b используем стандартное обозначение (a, b).

3.8. Пусть $(m, n) = 1$.

а) Чему равно $(m + n, m - n)$?

б) Чему равно $(mn, m^2 + n^2)$?

Дробь m/n назовем **несократимой,** если $(m, n) = 1$. Обозначим число всех несократимых дробей со знаменателем n через $\varphi(n)$. По определению имеем $\varphi(1) = 1$.

3.9. а) *(Гаусс)* Пусть d пробегает все делители числа n. Тогда справедлива формула

$$\sum_{d|n} \varphi(d) = n.$$

б) *(Лиувилль)* Пусть n — четное число. Тогда

$$\sum_{d|n} (-1)^d \varphi\left(\frac{n}{d}\right) = 0.$$

в) *(Лиувилль)* Пусть d_1 пробегает все нечетные делители числа n, а d_2 — все четные делители числа n. Тогда имеем

$$\sum_{d_1|n} \varphi\left(\frac{n}{d_1}\right) = \sum_{d_2|n} \varphi\left(\frac{n}{d_2}\right) = \frac{n}{2}.$$

г) *(Дирихле)* Имеет место формула

$$\sum_{s=1}^{n} \left[\frac{n}{s}\right] \varphi(s) = \frac{1}{2}(n^2 + n).$$

3.10. Пусть a/b и c/d — соседние дроби Фарея. Докажите, что дроби $\frac{a+c}{b+d}$ и $\frac{a+b}{c+d}$ несократимы.

3.11. Докажите, что в последовательности F_N количество чисел равно

$$\sum_{n=1}^{N} \varphi(n) + 1.$$

Следующая задача предлагалась на Московской математической олимпиаде в 1973 г.

3.12*. *(Последовательность Штерна-Броко).* Между двумя единицами вставляем двойку и далее между любыми двумя соседними числами вставляем их сумму. Докажите, что число n будет выписано ровно $\varphi(n)$ раз.

Следующий трудный цикл задач посвящен доказательству некоторых теорем Эйлера и Дирихле. Они также связаны с рядами Фарея.

3.13*. Обозначим длину последовательности F_N через $F(N)$. Докажите, что

$$\sum_{n=1}^{N} F([N/n]) = N(N+3)/2.$$

Определим функцию Мёбиуса $\mu(n)$, равную нулю для любого числа, содержащего среди своих делителей хоть один квадрат целого числа, и равную в противном случае $(-1)^k$, где k — число всех простых делителей числа n. Положим $\Phi(N) = \sum_{n=1}^{N} \varphi(n)$ и обозначим через $\Psi(N)$ число точек с взаимно простыми натуральными координатами в квадрате с вершинами $(1,1), (1,N), (N,1), (N,N)$.

3.14. Докажите, что: а)* Сумма $\mu(d)$ по всем натуральным d, делящим n, равна 0 при $n > 1$ и равна 1 при $n = 1$.

б)* *(Формула Мёбиуса - Чебышёва)* Если при любом $x \geq 1$ имеем

$$g(x) = \sum_{n=1}^{[x]} f(x/n),$$

то

$$f(x) = \sum_{n=1}^{[x]} \mu(n) g(x/n).$$

в)* Справедлива формула

$$\Psi(N) = \sum_{n=1}^{N} [N/n]^2 \mu(n).$$

г)** *(Дирихле)* Справедливы формулы

$$\Psi(N) = N^2 \sum_{n=1}^{\infty} \mu(n)/n + C(N)N \log N,$$

$$F(N) = (N^2/2) \sum_{n=1}^{\infty} \mu(n)/n^2 + C(N)N \log N,$$

$$\Phi(N) = (N^2/2) \sum_{n=1}^{\infty} \mu(n)/n^2 + C(N)N \log N,$$

где $C(N)$ ограничена по модулю, а

$$\sum_{n=1}^{\infty} \mu(n)/n^2 = \lim_{N\to\infty} \sum_{n=1}^{N} \mu(n)/n^2.$$

Для получения окончательной формулировки теоремы Дирихле осталось доказать формулы Эйлера

$$\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6, \sum_{n=1}^{\infty} \mu(n)/n^2 = 6/\pi^2.$$

Докажем их, хотя это и уведет нас несколько в сторону.

3.15. Докажите, что:

а)* *(Виет)*

$$\sin na =$$

$$= \binom{1}{n} \sin a \cos^{n-1} a - \binom{3}{n} \sin^3 a \cos^{n-3} a + \binom{5}{n} \sin^5 a \cos^{n-5} a - \ldots,$$

$$\cos na =$$

$$= -\binom{2}{n} \sin^2 a \cos^{n-2} a + \binom{4}{n} \sin^4 a \cos^{n-4} a - \binom{6}{n} \sin^6 a \cos^{n-6} a + \ldots;$$

б)* уравнение

$$\binom{1}{2n+1} x^n - \binom{3}{2n+1} x^{n-1} + \binom{5}{2n+1} x^{n-2} - \cdots + (-1)^n = 0$$

имеет корни $\operatorname{ctg} \pi/(2n+1), \operatorname{ctg} 2\pi/(2n+1), \ldots, \operatorname{ctg} n\pi/(2n+1)$;

в)* справедливы равенства

$$\operatorname{ctg} \pi/(2n+1) + \operatorname{ctg} 2\pi/(2n+1) + \cdots + \operatorname{ctg} n\pi/(2n+1) = m(2m-1)/3;$$

г) $\operatorname{cosec}^2 \pi/(2n+1) + \operatorname{cosec}^2 2\pi/(2n+1) + \cdots + \operatorname{cosec}^2 n\pi/(2n+1) = m(2m+2)/3$;

д)* при $0 < a < \pi/2$ верно неравенство $\operatorname{cosec} a > 1/a > \operatorname{ctg} a$;

е)* справедлива формула Эйлера

$$\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6.$$

3.16. а)* *(Коши)* Пусть существуют пределы

$$A = \lim_{N\to\infty} \sum_{n=1}^{N} a_n,\ \lim_{N\to\infty} \sum_{n=1}^{N} |a_n|,\ B = \lim_{N\to\infty} \sum_{n=1}^{N} b_n,\ \lim_{N\to\infty} \sum_{n=1}^{N} |b_n|.$$

Докажите, что при $c_n = \sum_{i=1}^{n} a_i b_{n+i-1}$ справедливо равенство

$$\lim_{N\to\infty} \sum_{n=1}^{N} c_n = AB.$$

б)* *(Коши)* Если существует предел

$$\lim_{N\to\infty} \sum_{n=1}^{N} |a_n|,$$

то существует предел

$$\lim_{N\to\infty} \sum_{n=1}^{N} a_n.$$

в)* *(Эйлер)* Докажите равенство

$$\sum_{n=1}^{\infty} \mu(n)/n^2 = 6/\pi^2.$$

3.17. *(Дирихле)* Докажите, что для среднего значения функции Эйлера

$$\Phi(N)/N = \sum_{n=1}^{N} \varphi(n)/N$$

справедливо равенство $\Phi(N)/N = 3N/\pi^2 + C(N)\log N$, где $C(N)$ ограничена по модулю.

Формула Эйлера дает значение в точке 2 так называемой дзета-функции Римана. Эйлер вычислил ее значения во всех четных натуральных точках. Все они выражаются рациональным образом через

число π, и поэтому, как стало ясно после работ Линдемана, решившего проблему "квадратуры круга", они являются трансцендентными числами, т. е. не удовлетворяют никакому алгебраическому уравнению с рациональными коэффициентами. До сих пор неизвестно, рациональны или иррациональны значения дзета-функции в нечетных точках, больших 3. Иррациональность значения дзета-функции в точке 3 была недавно доказана (см. задачи 11.65 – 11.68).

Вопрос о распределении нулей дзета-функции оказался тесно связан с вопросом о распределении простых чисел. Из до сих пор не доказанной гипотезы Римана о нулях дзета-функции вытекают очень сильные и также до сих пор не доказанные утверждения о плотности распределения простых чисел в натуральном ряду. Наиболее сильные доказанные к настоящему времени результаты о распределении простых получаются с помощью метода И.М.Виноградова в теории дзета-функции Римана.

Следующие три задачи, посвященные приближению иррациональных чисел рациональными, помещены в этот параграф потому, что могут быть решены с помощью рядов Фарея. Другие решения этих задач появятся в нескольких далее идущих параграфах.

3.18*. Докажите теорему Дирихле: для любого вещественного числа a и натурального числа N найдется такая рациональная дробь p/q, что $q \leq N$ и

$$|a - p/q| \leq 1/q(N+1).$$

3.19**. Пусть $\frac{a}{b} \leq \alpha \leq \frac{c}{d}$, $\frac{a}{b}$ и $\frac{c}{d}$ — соседние числа в ряде Фарея F_N. Тогда справедливо хотя бы одно из трех неравенств:

$$|\alpha - a/b| < 1/(\sqrt{5}b^2), |\alpha - c/d| < 1/(\sqrt{5}d^2), |\alpha - \frac{a+c}{b+d}| < 1/(\sqrt{5}(b+d)^2).$$

3.20**. Докажите **теорему Маркова – Бореля – Гурвица:** *для любого иррационального числа α найдется бесконечно много рациональных дробей p/q таких, что $|\alpha - p/q| \leq 1/(\sqrt{5}q^2)$.*

Последний цикл задач связан с рядами Фарея через "основную теорему арифметики" (задача 3.21) и задачу 3.7. В нем помещено несколько задач, связанных с простыми числами. Много других задач о простых числах читатель найдет в других параграфах.

3.21. Докажите, что любое натуральное число единственным образом представляется в виде произведения простых чисел (с точностью до порядка сомножителей).

3.22*. *(Россия,65)* Пусть натуральные числа p и q взаимно просты. Целое число n назовем **"хорошим"**, если оно представимо в виде $px + qy$, где x и y — целые неотрицательные числа, и **"плохим"** в противном случае. Докажите, что наибольшим "плохим" числом

будет $c = pq - p - q$, и всегда, если n — "хорошее", то $c - n$ — "плохое" и наоборот.

3.23. Если p — простое и $8p^2 + 1$ — также простое число, то число $8p^2 - p + 2$ — простое.

3.24. Докажите, что: а) если $2^n - 1$ — простое, то n — также простое число (такие числа называются **простыми числами Мерсенна – Люка**);

б) если $2^n + 1$ — простое, то n — степень двойки (такие числа называются **простыми числами Ферма**);

в) при каких натуральных n числа $2^n - 1$ и $2^n + 1$ оба простые?

г) *(ГДР,67)* Найдите последнюю цифру десятичной записи n-го числа Ферма $2^{2^n} + 1$ при $n \geq 2$.

3.25. Все простые числа, не превосходящие простого p, разбиты на две группы $a, b, \ldots, c$ и $d, e, \ldots, f$ так, что разность $q = ab \ldots c - de \ldots f$ заключается между 1 и p. Докажите, что q — простое число.

3.26. *(Софи Жермен)* При каких натуральных n и m число $n^4 + 4m^4$ — простое?

3.27. *(А.Монковский)* При каких n число $n^4 + 4^n$ — простое?

Предыдущие две задачи неоднократно предлагались на математических олимпиадах.

3.28. *(Эрдеш)* а) Среди первых n натуральных чисел выбрано более, чем $(n+1)/2$ различных. Докажите, что одно из них делится на другое.

б) Среди первых n натуральных чисел выберите $[(n+1)/2]$ различных так, что ни одно из них не делится на другое.

3.29. *(США,83)* Докажите, что для любого a имеется не более $(n+1)/2$ дробей p/q из ряда Фарея F_n таких, что $a \leq p/q < a + 1/n$.

УКАЗАНИЯ

3.1. Если $\frac{a}{b} < \frac{c}{b}$ — "соседи" в F_N, то

$$a/b < a/(b-1) < (a+1)/b \leq c/b,$$

откуда следует противоречие.

3.2. Так как $mb_i \leq a_i \leq Mb_i$, то

$$m(b_1 + \cdots + b_n) \leq a_1 + \cdots + a_n \leq M(b_1 + \cdots + b_n).$$

3.3. Примените индукцию по N. Пусть $\frac{a}{b} < \frac{k}{l} < \frac{c}{d}$ — "соседи" в F_{N+1}, $l = N+1$, и максимальное из чисел $kb - al$ и $cl - kd$ больше 1. Согласно 3.1 и 3.2 справедливы неравенства

$$b \leq N, d \leq N, \frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d},$$

а согласно предположению индукции — равенство $bc - ad = 1$. Докажите тогда, что

$$\frac{1}{bd} = \frac{c}{d} - \frac{a}{b} = \frac{c}{d} - \frac{k}{l} + \frac{k}{l} - \frac{a}{b} > \frac{1}{dl} + \frac{1}{bl} = \frac{b+d}{bdl},$$

$$l > b + d, \frac{a+c}{b+d} \neq \frac{k}{l}, \frac{a+c}{b+d} \in F_N,$$

и получите противоречие.

3.4. Примените 3.2.

3.5. Выведите из 3.3.

3.6. Примените 3.1 и 3.5.

3.7. Рассмотрите соседнюю дробь с дробью a/b в соответствующем ряде Фарея и примените 3.3.

3.8. *Ответы.* а) 1 или 2; б) 1.

3.10. Примените 3.3 и докажите, что

$$(a+c)b - (b+d)a = +1, (a+b)c - (c+d)a = +1.$$

3.11. Дробей со знаменателем n в ряду F_N ровно $\varphi(n)$ штук.

3.12. Начиная с дробей $\frac{0}{1}, \frac{1}{1}$, вставляйте между соседними дробями их медианту. Используя 3.2, 3.5 и 3.6, докажите для любого N, что все дроби из ряда F_N рано или поздно будут построены.

3.13. Положим $\Phi(N) = \sum_{n=1}^{N} \varphi(n)$ и обозначим через $\Psi(N)$ — число точек с взаимно простыми натуральными координатами в квадрате с вершинами $(1,1), (1,N), (N,1), (N,N)$. Тогда $2\Phi(N) - 1 = \Psi(N)$ ввиду того, что квадрат разрезается диагональю на два равных треугольника, а на диагонали $x = y$ только вершина $(1,1)$ имеет взаимно простые координаты. Так как всего целых точек в этом квадрате N^2, а для любого $d \leq N$ число точек с координатами (m,n), имеющими общий наибольший делитель d, равно $\Psi([N/d])$ (в силу взаимно однозначного соответствия $(m,n) \longleftrightarrow (m/d, n/d)$ между упомянутым множеством точек и множеством точек с взаимно простыми натуральными координатами в квадрате с вершинами $(1,1), (1,[N/d]), ([N/d],1), ([N/d],[N/d])$), то

$$\sum_{n=1}^{N} \Psi([N/n]) = N^2.$$

3.14. а) Воспользуйтесь тем, что сумма $\mu(d)$ по всем натуральным d, делящим n, равна 0, если $n > 1$, и равна 1, если $n = 1$. Для доказательства этого утверждения примените равенство

$$0 = (1-1)^m = 1 - \binom{1}{m} + \binom{2}{m} - \cdots + (-1)^m \binom{m}{m}.$$

б) Замените в равенстве

$$f(x) = \sum_{n=1}^{[x]} \mu(n) g(x/n)$$

функцию $g(x/n)$ на

$$g(x/n) = \sum_{n=1}^{[x/n]} f(x/nm),$$

сгруппируйте вместе члены, для которых $nm = k$, и примените а).

в) Примените формулу пункта б) к равенству задачи 3.12.

г) Заменяя в формуле пункта в) $[N/n]$ на $N/n - \theta$, где $0 \leq \theta < 1$, и пользуясь доказанным в первом параграфе равенством

$$\sum_{n=1}^{N} 1/n = \log N + C(N),$$

$C(N)$ — ограничена, получите равенство

$$\Psi(N) = N^2 \sum_{n=1}^{N} \mu(n)/n^2 + C(N)N\log N.$$

Остается заметить, что

$$\sum_{n=1}^{N} \mu(n)/n^2 = \sum_{n=1}^{\infty} \mu(n)/n^2 - \sum_{n=N+1}^{\infty} \mu(n)/n^2,$$

$$\left| \sum_{n=N+1}^{\infty} \mu(n)/n^2 \right| \le \sum_{n=N+1}^{\infty} 1/n^2 < \sum_{n=N+1}^{\infty} 1/n(n+1) =$$

$$= \sum_{n=N+1}^{\infty} (1/n - 1/(n+1)) = 1/(N+1).$$

3.15. а) Примените индукцию, формулы для синуса и косинуса суммы углов и тождество $\binom{k}{n+1} = \binom{k}{n} + \binom{k-1}{n}$, которое тоже докажите по индукции.

б) Обе части первой из формул а) разделите на $\cos^n \alpha$.

в) Примените теорему Виета о сумме корней уравнения.

г) Примените в) и тождество, связывающее косеканс с котангенсом.

д) Докажите неравенства $\sin\alpha < \alpha < \operatorname{tg}\alpha$. Первое из них выведите из того, что длина дуги больше длины стягивающей ее хорды. Второе выведите из того, что площадь треугольника с катетами 1 и $\operatorname{tg}\alpha$ больше площади сектора единичного круга с углом α.

е) Примените в), г), д).

3.16. а) Положим

$$A' = \sum_{i=1}^{\infty} |a_i|,\ A'_n = \sum_{i=1}^{n} |a_i|,\ B' = \sum_{i=1}^{\infty} |b_i|,\ B'_n = \sum_{i=1}^{n} |b_i|,\ C_n = \sum_{i=1}^{n} c_i,$$

$$A_n = \sum_{i=1}^{n} a_i,\ B_n = \sum_{i=1}^{n} b_i.$$

Проверьте, что

$$|A_nB_n - C_n| \le A'(B'_n - B'_{[n/2]}) + B'(A'_n - A'_{[n/2]})$$

(для этого воспользуйтесь неравенством

$$|x_1 + \cdots + x_m| \le |x_1| + \cdots + |x_m|,$$

и тем, что если $i + j \ge n + 2$, то или $i > [n/2]$ или $j > [n/2]$).

Далее заметьте, что при $n \to \infty$ имеем

$$B'_n - B_{[n/2]} \to 0, A'_n - A_{[n/2]} \to 0$$

(так как $B'_n \to B', A'_n \to A'$), поэтому

$$A'(B'_n - B'_{[n/2]}) + B'(A'_n - A'_{[n/2]}) \to 0,$$

значит, $|A_nB_n - C_n| \to 0, A_nB_n - C_n \to 0$, откуда

$$\lim_{N\to\infty} C_N = \lim_{N\to\infty} A_NB_N = \lim_{N\to\infty} A_N \lim_{N\to\infty} B_N = AB.$$

б) Воспользуйтесь существованием предела у монотонной ограниченной последовательности.

в) Воспользуйтесь задачами 3.13 а), 2.20, пунктами а) и б) настоящей задачи и пунктом е) предыдущей.

3.17. Примените задачи 3.13 и 3.15.

3.18. В качестве p/q возьмите подходящую дробь из F_N, сложенную с $[a]$, и примените 3.3 и 3.4.

3.19. Можно считать, что $\alpha > \frac{a+c}{b+d}$. В противном случае заменим α на $1-\alpha$, дробь a/b — на $1-c/d$ и т. д. Предположите, что ни одно из неравенств задачи неверно, тогда

$$\alpha - a/b \geq 1/(\sqrt{5}b^2), c/d - \alpha \geq 1/(\sqrt{5}d^2), \alpha - \frac{a+c}{b+d} \geq 1/(\sqrt{5}(b+d)^2).$$

Складывая первые два неравенства, получите, что согласно 2.1

$$1/db = c/d - a/b \geq 1/(\sqrt{5}b^2) + 1/(\sqrt{5}d^2),$$

а последние два при сложении дадут неравенство

$$\frac{1}{d(b+d)} = \frac{c}{d} - \frac{a+c}{b+d} \geq 1/(\sqrt{5}d^2) + 1/(\sqrt{5}(b+d)^2).$$

Переписывая эти неравенства в виде

$$\sqrt{5}db \geq b^2 + d^2, \sqrt{5}d(b+d) \geq d^2 + (b+d)^2$$

и складывая их, получите неравенство

$$\sqrt{5}d(2b+d) = \sqrt{5}d(b+(b+d)) \geq d^2 + (b+d)^2 + b^2 + d^2 = 2b^2 + 3d^2 + 2db,$$

которое перепишите в виде

$$0 \geq (3-\sqrt{5})d^2 + 2b^2 - 2(\sqrt{5}-1)db = \frac{1}{2}((\sqrt{5}-1)d - 2b)^2.$$

Но это неравенство возможно лишь когда $(\sqrt{5}-1)d - 2b = 0$, а так как b и d — целые, то последнее равенство возможно лишь при нулевых значениях b и d (иначе $\sqrt{5}$ окажется рациональным числом, что неверно). Так как на самом деле они ненулевые, то получено противоречие.

3.20. Примените 3.16 и воспользуйтесь тем, что в ряде Фарея F_n расстояния между соседними дробями стремятся к нулю при растущем n.

3.21. Примените индукцию по числу сомножителей, предварительно доказав с помощью 3.7, что если ab кратно c и $(a,c) = 1$, то b кратно c.

3.22. Из 3.7 выведите, что любое целое n представимо в виде $px+qy$, где x и y — целые числа, $0 \leq x < q$, причем это представление однозначно. Заметьте, что если $n = px + qy$ — хорошее, то $c - n = (q-1-x)p + q(-1-y)$ — плохое, и наоборот.

3.23. Если p не кратно 3, то $8p^2+1$ кратно 3, что противоречит его простоте. Значит, $p = 3$, так как число $8 \cdot 2^2 + 1$ составное.

3.24. а) Воспользуйтесь тождеством

$$a^n - 1 = (a-1)(1 + a + \cdots + a^{n-1}).$$

б) Воспользуйтесь тождеством

$$a^{2n+1} + 1 = (a+1)(a^{2n} - a^{2n-1} + a^{2n-2} - \cdots + a^2 - a + 1).$$

в) Оба условия выполнены лишь при $n = 2$. г) *Ответ.* 7.

3.25. Заметьте, что q не делится ни на одно из простых чисел, не превосходящих p.

3.26. *Ответ.* При $n = 1$ и $m = 1$. Заметьте, что

$$n^4 + 4m^4 = n^4 + 4m^4 + 4n^2m^2 - 4n^2m^2 =$$

$$= (n^2 + 2m^2 + 2nm)(n^2 + 2m^2 - 2nm).$$

3.27. *Ответ.* При $n = 1$. При четном n число $n^4 + 4^n$ кратно 16 и поэтому не простое. При $n = 2k + 1$ число

$$n^4 + 4^n = n^4 + 4 \cdot 4^{2k} = (n^2 + 2 \cdot 4^k)^2 - (n \cdot 2^{k+1})^2 =$$

$$= (n^2 + 2 \cdot 4^k - n \cdot 2^{k+1})(n^2 + 2 \cdot 4^k + n \cdot 2^{k+1})$$

тоже составное.

3.28. а) Сопоставьте каждому числу его наибольший нечетный делитель. Тогда каким-то двум числам сопоставятся одинаковые делители. Большее из них делится на меньшее.

б) Рассмотрите все числа, большие $n/2$.

3.29. Заметьте, что если знаменатель одной дроби из F_n делит знаменатель другой, то их разность не меньше $1/n$, и примените предыдущую задачу.

§ 4. ЧТО ЗНАЛИ И ЧЕГО НЕ ЗНАЛИ В ДРЕВНЕМ КИТАЕ

4.1. Найдите наименьшее натуральное число, которое при делении на n дает остаток $n - 1$, а при делении на $n + 1$ — остаток n.

4.2. *(Китайская теорема об остатках)* По остатку от деления произвольного числа на mn можно однозначно определить остатки от его деления на m и n. Если $(m, n) = 1$, то по остаткам от деления на m и n можно однозначно восстановить остаток от деления на mn, причем всегда найдется число, имеющее заданные остатки от деления на числа m и n.

Следующая задача обобщает предыдущую и указывает эффективный способ ее решения.

4.3. Пусть m_i, $1 \le i \le n$, — попарно взаимно простые числа, M_i — произведение всех этих чисел, кроме m_i. Согласно 3.7 найдется такое натуральное число a_i, что a_iM_i при делении на m_i дает в остатке 1. Докажите, что для любых n_i, $0 \le n_i < m_i$, число $\sum_{i=1}^{n} n_i a_i M_i$ при делении на m_i дает остаток n_i.

4.4. Докажите, что любую правильную дробь вида $\frac{n}{m_1 \cdots m_n}$ можно представить в виде алгебраической суммы правильных дробей вида n_i/m_i, если числа m_i попарно взаимно просты.

4.5*. Докажите, что при $(m,n) = 1$ остаток от деления на mn взаимно прост с mn тогда и только тогда, когда соответствующие ему (согласно 4.2) остатки от деления на m и n взаимно просты с m и n соответственно. Обобщите это утверждение на случай n попарно взаимно простых чисел.

Следующий цикл объединяет задачи, решение которых облегчается применением китайской теоремы об остатках.

4.6*. Генерал-аншеф Раевский хочет построить для парада своих солдат в несколько равных квадратных каре, но он не знает, сколько солдат (от одного до двадцати) находится в лазарете. Докажите, что у генерала могло быть такое количество солдат, что он, независимо от заполнения лазарета, смог бы выполнить свое намерение.

4.7.** *(Серпинский)* Докажите, что существует конечная арифметическая прогрессия произвольной длины, состоящая из различных чисел, являющихся степенями натуральных чисел.

4.8*. Пусть $f(x)$ — многочлен с целыми коэффициентами. Обозначим $N_f(m)$ количество натуральных чисел x, таких, что $1 \leq x \leq m$ и $f(x)$ делится на m.

а) Докажите, что при взаимно простых $m_1, ..., m_n$ имеем

$$N_f(m_1, ..., m_n) = N_f(m_1)...N_f(m_n).$$

б) *(Лагранж)* Докажите, что при простом m число $N_f(m)$ не превосходит степени многочлена f.

4.9*. *(С.-Петербург, 1990)* Многочлен $F(n)$ с целыми коэффициентами при любом целом n делится на одно из чисел $a_1, ..., a_m$. Докажите, что для некоторого a_i при любом целом n число $F(n)$ делится на a_i.

Следующий цикл задач принадлежит петербургскому академику Леонарду Эйлеру, так же как и задача 4.2. Сунь Цю, живший около 2000 лет назад, сформулировал только частный случай этой задачи. Интересно, что примерно в то же время тот же самый частный случай был найден древнегреческим математиком Никомахом, что дало основание Акритасу, автору известного учебника по компьютерной алгебре, назвать в нем китайскую теорему об остатках греко-китайской теоремой.

4.10. Докажите, что при взаимно простых m и n справедливо равенство

$$\varphi(mn) = \varphi(m)\varphi(n).$$

4.11. Докажите, что при простом p справедливо равенство

$$\varphi(p^n) = p^n - p^{n-1}.$$

4.12. Докажите, что если $p_1^{\alpha_1} \dots p_n^{\alpha_n}$ — разложение числа m на простые множители, то

$$\varphi(m) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \dots (p_n^{\alpha_n} - p_n^{\alpha_n - 1}) = m(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_n}).$$

Предыдущая формула была открыта Эйлером и носит, так же как и сама функция $\varphi(n)$, его имя.

4.13. Докажите равенство $\varphi(m^k) = m^{k-1}\varphi(m)$.

4.14. Пусть $[m, n]$ — наименьшее общее кратное чисел m и n, а (m, n) — их наибольший общий делитель. Докажите тождества

$$mn = (m, n)[m, n], \ \varphi(m)\varphi(n) = \varphi((m, n))\varphi([m, n]),$$

$$\varphi(mn)\varphi((m, n)) = \varphi(m)\varphi(n)(m, n).$$

4.15*. Докажите, что сумма $\varphi(d)$, взятая по всем натуральным d, делящим n, равна n.

В следующих задачах полезно применить функцию Эйлера.

4.16*. На каждой из бесконечного числа карточек написано натуральное число, причем для любого n имеется ровно n карточек, на которых написаны его делители. На скольких карточках написано число 1995?

4.17. Окружность разделена n точками на n равных частей. Сколько различных замкнутых ломаных можно составить из n равных звеньев с вершинами в этих точках (ломаные, получающиеся друг из друга поворотом, считаются одинаковыми)?

4.18. Используя формулу Эйлера, докажите, что простых чисел бесконечно много.

4.19. Найдите сумму всех правильных несократимых дробей со знаменателем n.

4.20. Докажите, что число всех правильных несократимых дробей со знаменателем n четно.

4.21*. Докажите, что число всех правильных несократимых дробей со знаменателем $a^n - 1$ кратно n.

4.22*. Пусть $(a, m) = 1$. Докажите, что для любого целого b имеем

$$\sum_{x=0}^{m-1} \{(ax + b)/m\} = (m - 1)/2.$$

4.23*. Пусть $(a, m) = 1$. Докажите, что

$$\sum_{\substack{1 \le \xi \le m \\ (\xi, m) = 1}} \{a\xi/m\} = \varphi(m)/2.$$

4.24. При каких целых n дробь $(n^4+3n^2+1)/(n^3+2n)$ сократима?

4.25. *(IMO,59)* Докажите, что дробь $\frac{21n+4}{14n+3}$ несократима при всех натуральных n.

4.26. *(Россия, 64)* При каких целых n число $(n-1)!/n^2$ не является целым?

4.27. *(IMO,64)* При каких натуральных n несократимы дроби $(2^n \pm 1)/7$?

Предыдущая задача является частным случаем одной из задач следующего параграфа.

Следующий цикл задач посвящен мультипликативным функциям и совершенным и дружественным числам.

4.28.** Функция $f(n)$ монотонна и обладает тем же свойством, что и $\varphi(n)$, а именно, при $(m,n)=1$ имеем $f(mn)=f(m)f(n)$. Докажите, что $f(n)=n^a$, где a — константа.

Назовем функцию **мультипликативной**, если она обладает упомянутым в предыдущей задаче свойством функции Эйлера.

4.29. а) Докажите, что мультипликативными являются: функция $d(n)$ — число всех различных натуральных делителей числа n, функция $\sigma(n)$ — сумма всех этих делителей, функция $\sigma_k(n)$ — сумма k-х степеней этих делителей, функция Мёбиуса $\mu(n)$, равная нулю для любого числа, содержащего среди своих делителей хоть один квадрат целого числа, и равная в противном случае $(-1)^k$, где k — число всех простых делителей числа n.

б) Докажите, что мультипликативная функция однозначно определяется своими значениями на степенях простых чисел.

в) Если $f(n)$ — мультипликативна, то функция $g(n)$, равная сумме $f(d)$ по всем натуральным d, делящим n, тоже мультипликативна.

4.30*. *(Формула Мёбиуса – Чебышёва)* В обозначениях пункта в) докажите, что $f(n)$ равна сумме $\mu(n/d)g(d)$ по всем натуральным d, делящим n.

4.31*. Докажите, что дробь $\varphi(n)/n$ равна сумме дробей $\mu(d)/d$ по всем натуральным d, делящим n.

4.32. *(Эйлер)* Докажите, что если $p_1^{\alpha_1}\dots p_n^{\alpha_n}$ — разложение числа m на простые множители, то

$$\sigma_k(m)=\frac{p_1^{(\alpha_1+1)k}-1}{p_1^k-1}\dots\frac{p_n^{(\alpha_n+1)k}-1}{p_n^k-1}.$$

Число n называется **совершенным**, если $2n=\sigma(n)$, т. е. оно равно сумме всех своих собственных делителей.

4.33. *(Евклид)* Пусть $2^{n+1}-1$ — простое число. Докажите, что число $2^n(2^{n+1}-1)$ — совершенное.

4.34*. *(Эйлер)* Докажите, что каждое четное совершенное число евклидово, т.е. имеет вид, указанный в предыдущей задаче.

Нечетные совершенные числа до сих пор не найдены. Неизвестн конечно или бесконечно множество совершенных чисел. Одно из самы больших известных совершенных чисел получается при $n = 86242$.

Числа n и m называются **дружественными**, если $\sigma(n) = m + n$ $= \sigma(m)$, т. е. сумма всех собственных делителей одного равна сум всех собственных делителей другого. Следующую теорему получи в IX в. арабский математик Сабит ибн Корра. В Европе она был переоткрыта в XVII в. Ферма и Декартом.

4.35. *(Сабит ибн Корра)* Пусть числа $p = 3 \cdot 2^{n-1} - 1, q = 3 \cdot 2^n -$ и $r = 9 \cdot 2^{2n-1} - 1$ — простые. Докажите, что числа $2^n pq$ и $2^n r$ — дружественные.

Проверьте, что числа 220 и 284 — дружественные: они получаютс при $n = 2$. Следующие две пары получаются при $n = 4$ и $n =$ Известно, что до $n = 20000$ больше таких пар нет.

Для дружественных чисел неизвестно единого метода их порожде ния. Много пар дружественных чисел открыл Эйлер. До сих пор неизвестно, конечно или бесконечно множество пар дружественных чисел.

Следующий цикл задач посвящен пифагоровым треугольникам, которые, вероятно, имеют еще большую древность, чем китайская теорема об остатках. Будем говорить, что натуральные числа (x, y, z) образуют пифагорову тройку, если $x^2 + y^2 = z^2$, т. е. треугольник со сторонами x, y, z — прямоугольный. Пифагорову тройку чисел называем **примитивной**, если ее числа не имеют общего делителя, большего единицы.

4.36. Любая пифагорова тройка чисел кратна некоторой примитивной пифагоровой тройке.

4.37. Задача поиска всех пифагоровых троек равносильна задаче поиска на единичной окружности с центром в начале координат всех точек с рациональными координатами.

4.38. Используя тригонометрические формулы, выражающие $\sin x$ и $\cos x$ через $\operatorname{tg} x/2$, докажите, что на единичной окружности с центром в начале координат имеется бесконечно много точек с рациональными координатами.

4.39. Докажите, что квадрат целого числа или кратен 4, или при делении на 8 дает остаток 1.

4.40. Пусть натуральные x, y, z, n удовлетворяют следующим условиям $x^n = yz$, $(y, z) = 1$. Докажите, что при некоторых натуральных u и v имеем $y = u^n, z = v^n$.

4.41*. Докажите, что все примитивные пифагоровы тройки задаются формулами:

$$x = 2mn, y = m^2 - n^2, z = m^2 + n^2, (m, n) = 1, m > n.$$

Эти формулы были, вероятно, известны в Древнем Шумере более 3500 лет назад. Во всяком случае, на одной из глиняных клинописных табличек, хранящихся в археологической коллекции Колумбийского университета, наряду с тройкой чисел $(3,4,5)$ записана и тройка чисел $(4961, 6480, 8161)$.

4.42*. *(Ферма)* Докажите, что не существует пифагоровой тройки, в которой первые два числа являются квадратами целых чисел. Другими словами, уравнение $x^4+y^4=z^2$ неразрешимо в натуральных числах.

Из этой задачи следует неразрешимость в натуральных числах уравнения Ферма при $n=4$: $x^n+y^n=z^n$. Случай $n=4$, — вероятно, единственный, в котором сам Ферма доказал свою теорему. Трудами Эйлера, Лежандра, Дирихле, Ламе и, главным образом, Куммера теорема Ферма была доказана в прошлом веке для всех натуральных $n \leq 100$.

В XX в. количество показателей, для которых доказана эта теорема, насчитывает многие тысячи. Последние сообщения из США о доказательстве теоремы Ферма в общем виде обнадеживают.

4.43**. *(Ферма)* Докажите, что не существует пифагоровой тройки, в которой первое и последнее числа являются квадратами целых чисел. Другими словами, уравнение $x^4-y^4=z^2$ неразрешимо в натуральных числах.

4.44. Докажите, что если n — сумма двух квадратов целых чисел, то n при делении на 4 дает в остатке 0, 1 или 2.

Полное описание чисел, являющихся суммами двух квадратов, нашел Ферма, а доказательство первым получил Эйлер. Изложение этих результатов имеется в § 11.

4.45. Докажите, что если n — сумма трех квадратов целых чисел, то n при делении на 8 не может давать в остатке 7.

Полное описание чисел, являющихся суммами трех квадратов, получил Гаусс. Доказательство его теоремы весьма сложное. Лагранж доказал, что любое натуральное число есть сумма четырех квадратов целых чисел.

4.46. Докажите, что $16^n \cdot 31$ нельзя представить в виде суммы 15 четвертых степеней целых чисел.

Г. Дэвенпорт доказал, что любое достаточно большое число является суммой 16 четвертых степеней целых чисел. Его доказательство очень сложно. Г. Харди и Д. Литтлвуд определили функцию $G(k)$ как такое наименьшее число, что любое достаточно большое натуральное число можно представить в виде суммы k-х степеней неотрицательных целых чисел в количестве $G(k)$ слагаемых. Им удалось доказать, что $G(k) < 2^k k$ при больших k. И.М.Виноградов доказал, что $G(k) < Ck \log k$. Для этого ему пришлось развить новый метод в теории чисел — метод тригонометрических сумм. Некоторое

представление об этом методе можно получить, читая § 16 задачника.

4.47*. Докажите, что $G(k) > k$.

Математики иногда ошибаются. Ошибался и великий Пьер Ферма — среди его предположений встречаются неверные. Следующий цикл задач связан с ошибочной попыткой обратить так называемую малую теорему Ферма, которая утверждает, что при любом простом p и любом целом a число $a^p - a$ кратно p. Но сам Ферма не совершал этой ошибки. Поразительно, что ее совершили китайские математики около 2000 лет назад. Они предположили, что если число $2^n - 2$ кратно n, то оно простое. Сейчас такие числа называются **псевдопростыми по базе 2. Псевдопростыми по базе** a называются такие числа n, для которых $a^n - a$ делится на n. Числа псевдопростые по любой базе называются **абсолютно псевдопростыми.** Такие числа играют важную роль в некоторых современных алгоритмах распознавания простоты.

4.48*. *(Чиполла)* Для любого a существует бесконечно много псевдопростых по базе a чисел, являющихся составными. Такими являются все числа из последовательности $(a^{2p} - 1)/(a^2 - 1)$, где p — такие простые p, что $p > 2$ и $(p, a^2 - 1) = 1$.

Из этой задачи следует, что 341 — псевдопростое по базе 2. Известно, что это число — наименьшее, опровергающее "теорему китайцев". Доказано также, что имеется бесконечно много четных псевдопростых по базе 2. Недавно появилось сообщение о бесконечности количества абсолютно псевдопростых составных чисел.

4.49. Пусть $n = p_1 p_2, p_1 \neq p_2$. Тогда $m - 1$ не делится на одно из чисел $p_i - 1$.

4.50. Пусть n делится на p^2. Тогда для числа $a = 1 + n/p$ разность $a^{n-1} - 1$ не делится на n.

4.51*. *(Кармайкл)* Число n — абсолютно псевдопростое и составное если и только если $n = p_1 \ldots p_k, k \geq 3$, где p_i — различные простые такие, что $n - 1$ делится на $p_i - 1$ при всех i.

Из этой задачи следует, что абсолютно псевдопростыми и составными являются числа $561 = 3 \cdot 11 \cdot 17$ (оно наименьшее среди них), $5 \cdot 29 \cdot 73, 7 \cdot 13 \cdot 31, 7 \cdot 23 \cdot 31, 7 \cdot 31 \cdot 73, 13 \cdot 17 \cdot 61$. Известно и много других таких чисел.

И, наконец, мы опять возвращаемся к китайской теореме об остатках. В последнее время китайская теорема об остатках нашла интересные применения в криптологии — науке об организации хранения и передачи секретной информации. Расскажем об одном из простейших таких применений. Допустим, что вам поручили организовать доступ к секретной информации на компьютере для трех сотрудников банка так, чтобы они только собравшись втроем, смогли получить ее. Каждому вы сообщаете ключ — некоторое большое (например, стозначное) число, которое он хранит в секрете от остальных

ных. Паролем, который открывает секретную информацию, является не известное никому из них число, которое, однако можно быстро определить (разумеется, с помощью компьютера) по трем упомянутым ключам. В случае же отсутствия одного из них для определения пароля придется (даже зная алгоритм определения пароля по ключам) перебрать $9 \cdot 10^{99}$ вариантов возможного значения неизвестного ключа (а это пока недоступно даже суперЭВМ). Кроме того, для надежности вы можете периодически менять ключи. Это смогут сделать даже сами работники банка (договорившись только о размерах ключей, чтобы гарантировать их отличие друг от друга, и выбирая в качестве ключей, например, числа вида $2^{2^n}+1$) и сохранить пароль в тайне даже от вас.

4.52*. Предложите алгоритм определения пароля по ключам, основанный на применении китайской теоремы об остатках.

УКАЗАНИЯ

4.1. Прибавьте 1.

4.2. Если a и b имеют одинаковые остатки при делении на n и одинаковые остатки при делении на m, то $a-b$ кратно mn, значит a и b имеют одинаковые остатки при делении на mn. Так как разных пар остатков от деления на m и n будет ровно mn, то каждой такой паре соответствует один и только один остаток от деления на mn.

4.3. Проверьте, что $n_i a_i \mathrm{M}_i$ делится на a_j при $j \neq i$, а при делении на m_i дает остаток n_i.

4.7. Пусть p_k — различные простые числа, $P = p_1 \ldots p_n$. Согласно 4.3 найдутся такие натуральные числа a_k, кратные P/p_k и дающие остаток $p_k - 1$ при делении на p_k. Положим $Q = 2^{\alpha_2} \ldots n^{\alpha_n}$ и рассмотрим арифметическую прогрессию $Q, 2Q, \ldots, nQ$. Согласно выбору чисел a_k число

$$Q = k^{\frac{\alpha_k+1}{p_k}} \prod_{\substack{m=1 \\ m \neq k}}^{n} m^{\frac{\alpha_m}{p_k}}$$

будет натуральным, и $kQ = Q_k^{p_k}$.

4.11. Число взаимно просто с p^n тогда и только тогда, когда оно не кратно простому числу p.

4.14. Разложите m и n на простые множители и примените формулу Эйлера.

4.15. Всего правильных (но возможно сократимых) дробей со знаменателем n ровно n штук. После сокращения этих дробей получается для каждого d, делящего n, ровно $\varphi(d)$ дробей со знаменателем d.

4.16. Воспользуйтесь индукцией и предыдущей задачей и докажите, что число n встречается ровно $\varphi(n)$ раз.

4.17. Ответ. $\varphi(n)$.

4.18. Пусть $p_1, \ldots, p_k$ — все различные простые числа и $n = p_1 \ldots p_k$. Тогда $\varphi(n) = 1$, что противоречит формуле Эйлера.

4.19-20. Если m/n — несократима, то $(n-m)/n$ — тоже несократима.

4.21. Если дробь m/n является несократимой, то дроби вида $\{am/n\}$, $\{a^2 m/n\}, \ldots, \{a^n m/n\}$ — тоже несократимы, причем построенные таким образом

последовательности для разных m/n либо не имеют общих членов, либо получаются друг из друга циклическим сдвигом.

4.26. Ответ. При простом n и при $n = 9$.

4.27. Заметьте, что остатки от деления 2^n на 7 периодически повторяются. Более подробно об этом явлении см. § 6.

4.28. Проверьте, что $f(1) = 1, f(n) > 0$. Без ограничения общности считаем, что $f(n)$ возрастает и $f(2) = 2$. Докажите, что $f(n) = n$. Допустим, что при некотором $k > 2$ справедливо неравенство $f(k) > k$. Докажите индукцией неравенства

$$2^{n-1} \le f(2^n - 1) \le f(2^n) \le f(2^n + 1) \le f(3) \cdot 2^{n-1},$$

$$f(k-1) \cdot f(k)^{n-1} \le f(k^n - 1) \le f(k^n) \le f(k^n + 1) \le f(k+1) \cdot f(k)^{n-1}.$$

Для любого n выберите m так, чтобы $2^m \le k^n < 2^{m+1}$, тогда

$$f(k-1)2^{m \log_k f(k)} f(k)^{-1} \le f(k-1)f(k)^{n-1} \le f(k^n) \le$$

$$\le f(2^{m+1}) \le f(3)2^m,$$

что невозможно при достаточно больших m. Аналогично получается противоречие в случае $f(k) < k$.

4.29. Примените основную теорему арифметики.

4.30. Воспользуйтесь тем, что сумма $\mu(d)$ по всем натуральным d, делящим n, равна 0, если $n > 1$, и равна 1, если $n = 1$. Для доказательства этого утверждения примените равенство

$$0 = (1-1)^m = 1 - \binom{1}{m} + \binom{2}{m} - \ldots + (-1)^m \binom{m}{m}.$$

4.31. Примените задачи 4.15 и 4.30 при $f(n) = \varphi(n), g(n) = n$.

4.32. Примените 4.30 и формулу суммирования геометрической прогрессии.

$$1 + p_i^k + p_i^{2k} + \ldots + p_i^{\alpha_i k} = (p_i^{(\alpha_i+1)k} - 1)(p_i^k - 1)^{-1}.$$

4.33. Воспользуйтесь предыдущей задачей. Тогда для $m = \sigma(2^n(2^{n+1} - 1)$ справедливо равенство

$$\sigma(m) = \sigma(2^n)\sigma(2^{n+1} - 1) = (2^{n+1} - 1)2^{n+1} = 2m.$$

4.34. Пусть $N = 2^n M$ — совершенное число, M — нечетно. Тогда в силу 4.32 имеем

$$2^{n+1}M = 2N = \sigma(N) = \sigma(2_n)\sigma(M) = (2^{n+1} - 1)\sigma(M),$$

значит, M кратно $2^{n+1} - 1$, т. е. $M = (2^{n+1} - 1)K$. Отсюда

$$\sigma(M) = 2^{n+1}M/(2^{n+1} - 1) = 2^{n+1}K = M + K,$$

значит, $K = 1$ и M — простое.

4.35. Примените 4.32. Тогда

$$\sigma(2^n pq) = (2^{n+1} - 1)(p+1)(q+1) = 9 \cdot 2^{2n-1}(2^{n+1} - 1) =$$

$$= (2^{n+1} - 1)(r+1) = 2 \cdot 9 \cdot (2^{2n} - 2^{n-1}) = 2^n(2r - p - q) =$$

$$= 2^n(r + pq) = 2^n r + 2^n pq, \sigma(2^n r) = (2^{n+1} - 1)(r+1).$$

4.36. Вынесите общий делитель из всех чисел тройки.

4.37. Равенство $x^2 + y^2 = z^2$ равносильно равенству

$$(x/z)^2 + (y/z)^2 = 1.$$

4.38. Подставьте в формулы

$$\sin x = \frac{2\,\mathrm{tg}\,(x/2)}{1 + \mathrm{tg}^2\,(x/2)}, \quad \cos x = \frac{1 - \mathrm{tg}^2\,(x/2)}{1 + \mathrm{tg}^2\,(x/2)}$$

вместо $\mathrm{tg}\,(x/2)$ несократимую дробь m/n.

4.39. Заметьте, что $(2n+1)^2 = 4n(n+1) + 1$ и $n(n+1)$ — четно.

4.40. Разложите числа x, y, z на простые множители и примените основную теорему арифметики.

4.41. Учитывая 4.39, без ограничения общности считайте, что x — четно, а y и z — нечетны. Так как $(x/2)^2 = ((y+z)/2)((z-y)/2)$, то согласно 4.39, 4.40 имеем $y + z = 2m^2, z - y = 2n^2, m > n, (m, n) = 1$, значит,

$$x = 2mn, y = m^2 - n^2, z = m^2 + n^2.$$

4.42. Воспользуемся рассуждением от противного. Пусть x, y, z — такая тройка натуральных решений уравнения $z^2 = x^4 + y^4$, в которой число z наименьшее возможное. Из предыдущей задачи следует, что без ограничения общности можно считать, что

$$x^2 = 2mn, y^2 = m^2 - n^2, z = m^2 + n^2.$$

Так как $y^2 + n^2 = m^2$, то из нее же следует, что m — нечетно, а значит, n — четно, и

$$n = 2ab, y = a^2 - b^2, m = a^2 + b^2, a > b, (a, b) = 1.$$

Поэтому

$$(x/2)^2 = ab(a^2 + b^2),$$

а так как в силу $(a, b) = 1$ имеем, что $(ab, (a+b)) = 1$, то согласно 4.39 и 4.40 числа ab и $a^2 + b^2$ являются квадратами целых чисел. Опять применяя 4.40, получаем, что $a = X^2, b = Y^2$, следовательно

$$X^4 + Y^4 = Z^2$$

для некоторых натуральных X, Y, Z, причем

$$Z^2 = X^4 + Y^4 = a^2 + b^2 = m < (m^2 + n^2)^2 = z^2 = x^4 + y^4.$$

Получено противоречие с предположением, что число z — минимально. Значит, уравнение натуральных решений не имеет.

4.43. Рассуждаем от противного. Пусть x, y, z — такая тройка натуральных решений уравнения $z^2 = x^4 - y^4$, в которой число z наименьшее возможное. Без ограничения общности считаем, что $(x, y) = 1$, так как в противном случае тройку чисел (x, y, z) можно будет сократить на (x, y) и получить натуральное решение с меньшим числом z. Поэтому числа x и y имеют разную четность, а значит, числа $x^2 + y^2$ и $x^2 - y^2$ нечетны и согласно 3.8 взаимно просты. Согласно 4.40 из равенства

$$z^2 = (x^2 + y^2)(x^2 - y^2)$$

следуют равенства

$$x^2 + y^2 = u^2, x^2 - y^2 = v^2, u > v, (u, v) = 1,$$

причем числа u и v нечетны. Поэтому числа $p = (u - v)/2, q = (u + v)/$ натуральные и согласно 3.8 взаимно простые. Так как

$$pq = (u^2 - v^2)/4 = y^2/2,$$

то в силу 4.39 число y четно и $pq/2 = (y/2)^2$.

Значит, числа p и q имеют разную четность в силу их взаимной простоты, поэтому согласно 4.40 четное из них, скажем p, является удвоенным квадрато а нечетное - квадратом, т. е. $q = Z^2$, где Z — натуральное число. Так как

$$p^2 + q^2 = (u - v)^2/4 + (u + v)^2/4 = (u^2 + v^2)/2 = x^2, (p, q) = 1,$$

то согласно 4.41 для некоторых взаимно простых m и $n, m > n$, справедли равенства

$$p = 2mn, q = m^2 - n^2, x = m^2 + n^2.$$

Так как mn — квадрат целого числа, и $(m, n) = 1$, то в силу 4.36 име $m = X^2, n = Y^2$, где X, Y — натуральные. Следовательно,

$$Z^2 = X^4 - Y^4,$$

причем так как $x > y$ натуральные, то

$$Z^2 = q < p^2 + q^2 = x^2 < (x^2 + y^2)(x^2 - y^2) = z^2.$$

Противоречие. Значит, уравнение натуральных решений не имеет.

4.44 - 4.45. Примените задачу 4.39.

4.46. Проверьте с помощью 4.39, что остаток от деления a^4 на 16 рав 0, если a — четно, и 1, если нечетно. Поэтому число, кратное 16, мож представить в виде суммы 15 четвертых степеней целых чисел, лишь когда в они четны. Разделите все эти числа на 2 и проведите индукцию.

4.47. Положим $N = P^k + P^{k-1} + ... + P + 1$, тогда $P^k < N < (P+1)^k$ и поэто имеется ровно P k-х степеней натуральных чисел, не больших N. Из них мож составить не более $P^k + P^{k-1} + ... + P$ различных сумм, состоящих не более че из k слагаемых.

Поэтому найдется такое натуральное $n \leq N$, которое не представимо в ви суммы не более чем k k-х степеней натуральных чисел.

4.48. Положите

$$y_p = (a^{2p} - 1)/(a^2 - 1),$$

где p — такие простые p, что $p > 2$ и $(p, a - 1) = 1$. Тогда

$$y_p - 1 = ((a^p - 1)/(a - 1))((a^p + 1)/(a + 1))$$

— составное целое число. Кроме того, $a^{2p} - 1$ делится на y_p, а число

$$y_p - 1 = (a^{2p} - 1)/(a^2 - 1) - 1 = a^2(a^{p-1} + 1)(a^{p-1} - 1)/(a^2 - 1)$$

делится на $2p$, так как $a(a^{p-1} - 1)$ делится на p согласно малой теореме Ферм $(p, a^2 - 1) = 1$, и число $a^2(a^{p-1} + 1)$ четно, а число $(a^{p-1} - 1)/(a^2 - 1)$ — цел в силу нечетности p. Поэтому число

$$a^{y_p - 1} - 1 = a^{2p(y_p - 1)/2p} - 1$$

делится на y_p и, значит, число y_p — псевдопростое по базе a.

4.49. Пусть $n-1$ делится на $p_i-1, i=1,2$. Тогда $p_2-1=m-1-p_2(p_1-1)$ делится на p_1-1 и, аналогично, p_1-1 делится на p_2-1, что невозможно, так как одно из чисел больше второго.

4.50. Проверьте, что для любых целых k и k' числа $(1+kn/p)(1+k'n/p)$ и $1+(k+k')n/p$ имеют одинаковые остатки при делении на n и поэтому $(1+n/p)^s-1$ кратно n тогда и только тогда, когда s кратно p.

4.51. Примените две предыдущие задачи и задачу 6.40.

4.52. Выберем три больших попарно взаимно простых числа, например числа Ферма $a_1=2^{2^n}+1, a_2=2^{2^{n+1}}+1, a_3=2^{2^{n+2}}+1$. Пусть i-й "компаньон" в качестве ключа выбирает произвольное число k_i в пределах от 1 до a_i-1. Тогда, собравшись вместе, они могут выработать пароль k, взяв в качестве него такое число в пределах от 1 до $a-1, a=a_1a_2a_3$, которое при делении на a_i дает в остатке k_i. Как было показано в этом параграфе, число k можно вычислить по формуле $k=k'-[k'/a]a$, где

$$k'=k_1n_1+k_2n_2+kn_3, n_im_i-a_iq_i=1, m_i=a_ja_k, j\neq k\neq i\neq j.$$

Для вычисления n_i можно, как будет показано в § 8, применить алгоритм Евклида. Нетрудно написать программу для компьютера, которая будет вычислять пароль k, после того как "компаньоны", таясь друг от друга, введут в него свои ключи. Положим $N=2^n$. Если двое, в тайне от третьего, захотят найти ключ k, то им придется перебрать все возможные варианты выбора третьего ключа (потому что разным способам выбора ключей соответствуют разные значения k), т.е. перебрать не менее 2^N вариантов. С помощью результатов § 17 о сложности умножения и деления с остатком многозначных чисел и оценки числа шагов алгоритма Евклида, указанной в § 8, можно оценить сложность алгоритма вычисления общего ключа по порядку как $N\cdot M(N)$, где $M(N)$ — сложность умножения N разрядных чисел. Применение оценки Карацубы дает оценку $N^{\log_2 6}$. Использование более совершенных алгоритмов умножения и решения линейных уравнений с двумя неизвестными в целых числах позволяет получить оценку по порядку $N\log N\log\log N$. Поэтому даже при больших N вычисление общего ключа можно провести достаточно быстро.

§ 5. ДЕЛИТСЯ ИЛИ НЕ ДЕЛИТСЯ ?

5.1. *(Формула Лежандра)* Наибольшее k, при котором число $n!/p^k$, где p — простое, $p\leq n$, будет целым и равно

$$[n/p]+[n/p^2]+\ldots+[n/p^m]+\ldots.$$

5.2. При каких n число $(n-1)!/n$ — целое?

5.3. Докажите, что число $(2n)!/(n!)^2$ — натуральное и делится на $n+1$.

5.4. Докажите, что число $n!/a!b!\ldots k!$ — целое, если только

$$a+b+\ldots+k\leq n.$$

5.5*. *(Каталан)* Докажите, что для любых натуральных m, n число $(2n)!(2m)!/(n!m!(n+m)!)$ — натуральное.

5.6*. *(США, 75)* Докажите, что для любых натуральных m, n число $(5n)!(5m)!/(n!m!(3n+m)!(3m+n)!)$ —натуральное.

5.7*. Докажите, что для любых натуральных m, n число

$$\frac{1}{n}+\ldots+\frac{1}{m} \text{ — нецелое.}$$

5.8*. Докажите, что для любых натуральных m, n число $\frac{1}{2n+1}+\frac{1}{2n+3}+\ldots+\frac{1}{2m+1}$ — нецелое.

5.9. *(Чехословакия, 1971)* Докажите, что при простом $p \geq 5$ числитель несократимой дроби, равной $1+\frac{1}{2}+\ldots+\frac{1}{p-1}$, делится: а) на число p; б)* на число p^2.

5.10*. Докажите, что при простом $p \geq 5$ числитель несократимой дроби, равной $1+\frac{1}{2}+\ldots+\frac{1}{(p-1)p}$, делится на p.

5.11. Будет ли целым число $\frac{1}{1\cdot 2}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{(2n-1)2n}$? А число

$$\frac{1}{2\cdot 1}+\frac{1}{3\cdot 2}+\cdots+\frac{1}{(n+1)n}?$$

5.12. При каких целых m число $m/3+m^2/2+m^3/6$ — целое?

5.13. Докажите, что если $\frac{2^n-2}{n}$ — целое, то $\frac{2^{2^n-1}-2}{2^n-1}$ — также целое число.

5.14*. Найдите наибольшее k, при котором:

а) число $\left(3^{2^n}-1\right)/2^k$ — целое;

б) число $\left(2^{3^n}+1\right)/3^k$ — целое.

5.15*. Докажите, что $(4^m-4^n)/3^{k+1}$ целое тогда и только тогда, когда $(m-n)/3^k$ - целое.

5.16*. При каких натуральных n число $\left(n^{2^m}-1\right)/2^{m+2}$ целое при всех натуральных m?

5.17. *(AMM)* При каких натуральных m и n число $\frac{2^m+1}{2^n-1}$ — целое?

5.18*. При каких натуральных m, n и k число $\frac{k^m+1}{k^n-1}$ целое ? А когда $\frac{k^m-1}{k^n+1}$ — целое?

5.19*. *(BMO, 82)* Докажите, что если a делится на 2^n-1, то в двоичной записи a не менее n единиц.

5.20*. *(AMM)* Докажите, что если $p>3$ — простое число и $n=\frac{2^{2p}-1}{3}$, то $\frac{2^n-2}{n}$ — целое число.

5.21. При каких натуральных m и n число $(2^n-1)^{1/m}$ — целое?

5.22*. Является ли целым число $(2^{1093}-2)/1093^2$? А число $(2^{3511}-2)/3511^2$?

5.23. Докажите, что при простом $p > 2$ число

$$\frac{[(2+\sqrt{5})^p] - 2^{p+1}}{p}$$

— целое.

5.24*. а) При каких целых x будет целым число $\sqrt{(1+x+x^2)}$? Другими словами, нужно найти все целые решения уравнения $y^2 = 1 + x + x^2$.

б) *(BMO,67)* Решите в целых числах уравнение

$$y^2 + y = 1 + x + x^2 + x^3 + x^4.$$

в)** *(AMM)* Решите в целых числах уравнение

$$y^2 = 1 + x + x^2 + x^3 + x^4.$$

г)*** *(Ферма)* Решите в целых числах уравнение

$$y^2 = 1 + x + x^2 + x^3.$$

Следующий цикл задач посвящен, главным образом, делимости биномиальных коэффициентов. Решать их нужно в той последовательности, в какой они приведены, тогда не будет никаких затруднений. В противном случае многие из этих задач заслуживают "звездочек", а то и двух.

5.25. *(Лежандр)* Докажите, что

$$[n/2] + [n/2^2] + \ldots + [n/2^m] + \ldots = n - \nu(n),$$

где $\nu(n)$ — сумма цифр двоичной позиционной записи числа n.

5.26. Докажите, что число $(2n)!/(n!)^2$ натуральное и делится на $n+1$ и на $2^{\nu(n)}$, но не делится на $2^{\nu(n)+1}$.

5.27. Докажите, что число $(2n)!/n!$ делится на 2^n, но не на 2^{n+1}.

5.28. Докажите, что число $n!/2^n$ - нецелое. При каком натуральном m число $n!/2^{n-m}$ будет целым при всех натуральных n?

5.29. *(Лежандр)* а) Докажите, что

$$[n/p] + [n/p^2] + \ldots + [n/p^m] + \ldots = (n - \nu_p(n))/(p-1),$$

где $\nu_p(n)$ — сумма цифр p-ичной позиционной записи числа n, а p — произвольное (не обязательно простое) натуральное число.

б) Пусть $u_k = (p^{k+1} - 1)/(p-1)$, $h = p_m u_m + \ldots + p_1 u_1 + p_0$,

$$p_m = [h/u_m],\ h_{m-1} = h - p_m u_m,\ p_{m-1} = [h_{m-1}/u_{m-1}], \ldots,$$

$$h_1 = h_2 - p_2 u_2,\ p_1 = [h_1/u_1].$$

Тогда простое p входит в разложение $n!$ в степени h тогда и только тогда, когда $n = p_m p^{m+1} + \ldots + p_1 p^2 + p_0 p + p'$, где все $p_m, \ldots, p_0$ p' — целые неотрицательные и меньше p.

5.30. *(Киев, 71)* Может ли $n!$ оканчиваться ровно 1971 нулем в десятичной записи?

Обозначим для краткости наименьший показатель степени p, делящей число n, через $ord_p(n)$, целое число $\frac{n!}{k!(n-k)!}$ (биномиальный коэффициент) — через $\binom{n}{k}$, а через p — произвольное простое число.

5.31. *(Куммер)* Докажите, что:

а) $ord_p\binom{n}{k} = (\nu_p(n-k) + \nu_p(k) - \nu_p(n))/(p-1)$;

б) последнее число равно количеству переносов в следующий разряд при сложении чисел k и $n-k$ в p-ичной системе счисления, причем и при составном p.

5.32. Докажите, что при простом p

а)* *(Вильсон - Лейбниц)* число $(p-1)! + 1$ кратно p.

б)** *(Беббидж - Вустенхольм)* число $\binom{2p-1}{p} - 1$ кратно p^3, если $p > 2$. Неизвестно, верно ли обратное утверждение.

Следующая теорема обобщает предыдущую и уточняет теорему Лежандра.

5.33.** *(Штикельбергер)* Пусть p — простое и $\mu = ord_p n!$, где

$$n = p_m p^m + \cdots + p_1 p + p_0,\ 0 \le p_i < p, 0 \le i \le m.$$

Докажите, что число $n!/p^\mu - (-1)^\mu p_0! \ldots p_m!$ кратно p.

5.34. *(Болгария,68)* Докажите, что биномиальный коэффициент $\binom{n}{k}$ нечетен тогда и только тогда, когда в двоичной записи числа k единицы не стоят в тех разрядах, где в числе n стоят нули.

5.35. Докажите, что биномиальный коэффициент $\binom{n}{k}$ не кратен простому числу p тогда и только тогда, когда в p-ичной записи числа k все разряды не превосходят соответствующих разрядов числа n.

5.36. Докажите, что в ряду биномиальных коэффициентов

$$\binom{n}{0}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$$

все числа нечетны тогда и только тогда, когда $n = 2^k - 1$.

5.37. *(Люксембург,80)* Докажите, что в ряду биномиальных коэффициентов $\binom{n}{0}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$ все числа не кратны заданному простому p тогда и только тогда, когда $n = mp^k - 1$, где натуральное $m < p$.

5.38. Докажите, что в ряду биномиальных коэффициентов

$$\binom{n}{0}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$$

все числа, кроме первого и последнего, кратны заданному простому p тогда и только тогда, когда $n = p^k$.

5.39. Докажите, что в ряду биномиальных коэффициентов

$$\binom{n}{0}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$$

количество нечетных чисел равно степени двойки.

5.40. Докажите, что в ряду биномиальных коэффициентов

$$\binom{n}{0}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$$

не может быть поровну четных и нечетных чисел.

5.41. Докажите, что в ряду биномиальных коэффициентов

$$\binom{n}{0}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$$

количество не кратных p чисел равно $(a_1 + 1) \ldots (a_m + 1)$, где числа $a_1, \ldots, a_m$ — разряды p-ичной записи числа n, а число $m =]\log_p n[$.

5.42. Докажите, что в первых $p^n - 1$ строках треугольника Паскаля (т.е. среди ряда биномиальных коэффициентов $\binom{m}{k}$, $0 \leq k \leq m \leq p^n - 1$) количество некратных p чисел равно $(p(p+1)/2)^n$.

5.43. *(Ленинград, 77)* Пусть p — простое число, n, k — натуральные числа. Докажите, что среди биномиальных коэффициентов $\binom{n}{k}, \binom{n+1}{k}, \ldots, \binom{n+k}{k}$ хотя бы один не делится на p.

5.44. Докажите, что для любого натурального k найдется бесконечно много таких чисел n, что все биномиальные коэффициенты $\binom{n}{k}, \binom{n+1}{k}, \ldots, \binom{n+k-1}{k}$ делятся на p.

5.45*. Докажите, что в ряду биномиальных коэффициентов $\binom{n}{0}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$ при $n = 2^m - 2$ в точности $]n/4[$ чисел имеет вид $4l + 2$.

5.46*. Докажите, что в ряду биномиальных коэффициентов $\binom{n}{0}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$ ни одно из чисел не делится на $p^{[\log_p n]+1}$.

5.47. Докажите, что $\nu_p(n-k) + \nu_p(k) - \nu_p(n) \leq (p-1)[\log_p n]$, причем строгое неравенство, вообще говоря, поставить нельзя.

5.48. Докажите предыдущее неравенство и при составном p.

5.49. а) Докажите, что в ряду биномиальных коэффициентов $\binom{n}{0}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$ при $n = p^m$, где p — простое, кратны n только коэффициенты $\binom{n}{k}$, где k не кратно p. При k, не кратном p^s и кратном p^{s-1}, коэффициенты $\binom{n}{k}$ делятся на p^{m-s+1} и не делятся на p^{m-s+2}.

б) Докажите, что наибольший общий делитель всех биномиальных коэффициентов $\binom{n}{1}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n-1}$ равен p при $n = p^m$, где p — простое, и равен единице во всех остальных случаях.

в) Докажите, что наибольший общий делитель всех биномиальных коэффициентов $\binom{n}{1}, \binom{n}{3}, \ldots, \binom{n}{2k+1}, \ldots$ равен $2^{1+ord_2 n}$

5.50. *(Польша, 70)* Докажите, что все биномиальные коэффициенты $\binom{n}{1}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n-1}$ делятся на n тогда и только тогда, когда n — простое.

Пункт г) следующей задачи усиливает в одном частном случае утверждение задачи 5.35, а пункт д) — задачи 5.37.

5.51. *(Люка)* Пусть p — простое, $k \leq n$ — натуральные. Докажите, что

а)* $ord_p \binom{n}{k} = ord_p \binom{np}{kp}$ и $\binom{np}{kp} - \binom{n}{k}$ кратно p.

б)* $\binom{p}{n} - [n/p]$ кратно p.

в)** $\binom{np+m}{kp+s} - \binom{n}{k}\binom{m}{s}$ кратно p при неотрицательных n, m, k, s, и m и s меньших p (биномиальный коэффициент, очевидно, равен нулю, если нижний индекс меньше верхнего, а коэффициент $\binom{0}{0}$ по определению равен 1).

г)** $\binom{k}{n} - \binom{k_m}{n_m} \ldots \binom{k_0}{n_0}$ кратно p при

$$n = n_m p^m + \ldots + n_1 p + n_0, k = k_m p^m + \ldots + k_1 p + k_0,$$

$$0 \leq n_i, k_i < p, 0 \leq i \leq m.$$

д)** $\binom{k}{p^n - 1} - (-1)^{\nu_p(k)}$ кратно p.

е)*** $\binom{np}{kp} - \binom{n}{k}$ кратно p^2, а при $p \geq 5$ — кратно и p^3.

Следующий цикл задач посвящен доказательству замечательной теоремы П.Л.Чебышёва — постулату Бертрана. Здесь уместно повторить все, сказанное перед предыдущим циклом.

5.52*. Докажите, что

$$4^n/2\sqrt{n} < \binom{2n}{n} < 4^n/\sqrt{2n+1}.$$

5.53. Докажите, что число $\binom{2n+1}{n}/S_n$, где S_n — произведение всех простых чисел, заключенных в пределах от $n+2$ до $2n+1$, является целым.

5.54. Докажите, что $S_n < 4^{n+1}/2\sqrt{2n+3}$.

5.55. Докажите, что P_n — произведение всех простых чисел, не превосходящих n, меньше $4^{n-1}/n$ при $n \geq 4$.

5.56. Пусть $\lambda_p(n) = ord_p \binom{2n}{n}$. Докажите, что

$$\lambda_p(n) = [2n/p] - 2[n/p] + [2n/p^2] - 2[n/p^2] + \ldots + [2n/p^m] - 2[n/p^m] \leq \mu_p(n),$$

где $m = \mu_p(n) = [\log_p 2n]$, при $2n/3 \geq p \geq \sqrt{2n}$ и $2n \geq p > n$ справедливо равенство $\lambda_p(n) = 1$, а при $n \geq p > 2n/3$ — равенство $\lambda_p(n) = 0$.

5.57. Докажите, что число $\text{НОК}(2,\dots,2n)/\binom{2n}{n}$ — целое, и что

$$\text{НОК}(2,\dots,2n) = \text{НОК}(n+1, n+2,\dots,2n).$$

5.58. Докажите, что $\text{НОК}(2,\dots,2n) \leq (2n)^k$, где k — число простых, не превосходящих $2n$.

5.59. Докажите, что при некотором $a > 0$ число простых, не превосходящих n больше, чем $an/\log_2 n$.

5.60. Докажите, что последовательность $4^{2n/3}/n$ монотонна.

5.61. Докажите, что произведение чисел $p^{\lambda_p(n)}$ по всем простым $p < \sqrt{2n}$ меньше $(2n)^k$, где k — число простых, меньших $\sqrt{2n}$, а произведение всех простых чисел из отрезка от $\sqrt{2n}$ до $2n/3$ при $n \geq 6$ меньше

$$\frac{3 \cdot 4^{2n/3}}{8n \cdot 2^k}.$$

5.62. Докажите, что число простых, не превосходящих n, не больше $(n+1)/2$.

5.63*. Докажите, что P_{2n}/P_n — произведение всех простых из отрезка от $n+1$ до $2n$ — при $n \geq 6$ больше $4^{n/3}/n^{\sqrt{n/2}}$.

5.64*. Докажите,что при $n \geq 24$ справедливо неравенство

$$4^{n/3} > n^{\sqrt{n/2}},$$

а при $n \geq 98$ — неравенство

$$4^{n/3}/n^{\sqrt{n/2}} > 2n.$$

5.65. Докажите, что между n и $2n-2$ всегда есть простое число.

5.66. Докажите, что между $n+1$ и $2n$ всегда есть два простых.

5.67. Докажите, что при некотором $b > 0$ число простых, не превосходящих n, меньше, чем $bn/\log_2 n$.

Отметим в заключение, что для любого n и любого $m \geq 4n^2$ между m и $2m$ найдется не менее n простых чисел, однако доказательства этой теоремы мы здесь не приводим.

УКАЗАНИЯ

5.3. Числа $n+1$ и n взаимно просты, а число $(2n)!/((n-1)!(n+1)!)$ — натуральное.

5.7. Привести к общему знаменателю и обратить внимание на дробь, в знаменатель которой двойка входит в наибольшей степени.

5.8. Обратить внимание на дробь, в знаменатель которой тройка входит в наибольшей степени.

5.9. а). Сгруппируйте равноудаленные от концов слагаемые; б) найдется такая перестановка $x_1, \ldots, x_{p-1}$ чисел $1, \ldots, p-1$, что при всех k число $kx_k - 1$ делится на p, значит, так как

$$\frac{2}{p}\left(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\right)=\frac{1}{1(p-1)}+\frac{1}{2(p-2)}+\cdots\frac{1}{(p-1)1},$$

то числитель этой дроби при делении на p дает тот же остаток, что и число

$$-((p-1)!)^2(x_1^2+\ldots+x_{p-1}^2)=-((p-1)!)^2(1^2+\ldots+(p-1)^2)=$$

$$=-((p-1)!)^2p(p-1)(2p-1)/6,$$

а оно делится на p.

5.10. Представьте дробь в виде

$$\frac{2}{p}\left(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\right)+\left(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\right)+$$

$$+\left(\frac{1}{p+1}+\cdots+\frac{1}{2p-1}\right)+\ldots$$

и примените 5.9.

5.18. Докажите, что

$$(k^n\pm1,k^m\mp1)=(k^{(m,n)}\pm1,k^{(m,n)}\mp1),$$

в частности, $(k^n-1,k^m-1)=k^{(m,n)}-1$,

$$(k^n-(-1)^{n/(m,n)},k^m-(-1)^{m/(m,n)})=k^{(m,n)}+1,$$

а в остальных случаях при нечетном k имеем

$$(k^{(m,n)}\pm1,k^{(m,n)}\mp1)=2,$$

а при четном k

$$(k^{(m,n)}\pm1,k^{(m,n)}\mp1)=1.$$

5.20. Записать в двоичной системе n и p и доказать с помощью 5.13, что $n-1$ делится на $2p$.

5.24. а) *Ответ:* $(x,y)=(-1,-1),(-1,1),(0,-1),(0,1)$. Уравнение равносильно следующему $(2y)^2-(2x+1)^2=3$. Разлагая левую часть на множители, получим, что

$$2y-2x-1=\pm3, 2y+2x+1=\pm1,$$

или

$$2y-2x-1=\pm1, 2y+2x+1=\pm3.$$

б) *Ответ:* $(x,y)=(-1,-1),(-1,0),(0,-1),(0,0),(2,-6),(2,5)$. Уравнение равносильно следующему $(2y+1)^2=4+4x+4x^2+4x^3+4x^4$. Проверьте, что при $x>2$ или $x<-1$ правая часть этого уравнения заключена между $(2x^2+x)^2$ и $(2x^2+x+1)^2$ и поэтому не может быть квадратом целого числа. Перебирая $x=-1,0,1,2$, получите ответ.

в) *Ответ:* $(x,y)=(-1,-1),(-1,1),(0,1),(0,-1),(3,11),(3,-11)$. Уравнение равносильно следующему

$$(x^2+x/2)^2=y^2-(x+2)^2/4-x^2/2<y^2,$$

из которого, учитывая, что при целых x число $x^2+x/2>0$, вытекает неравенство $x^2+x/2<|y|$. Так как при целых x число $x^2+x/2$ целое или "полуцелое", а y — целое, то, на самом деле, $x^2+x/2+1/2\le|y|$, откуда, учитывая, что

$$y^2=1+x+x^2+x^3+x^4,$$

получаем неравенство

$$y^2\ge(x^2+x/2+1/2)^2=y^2+(x^2-2x-3)/4,$$

а значит, и неравенства

$$(x+1)(x-3)=x^2-2x-3\le 0,-1\le x\le 3.$$

Значения $x=1$ и $x=2$ отбрасываются при проверке.

г) *Ответ.* Все решения уравнения таковы:

$$(x,y)=(-1,0),\ (0,1),\ (0,-1),\ (1,2),\ (1,-2),\ (7,20),\ (7,-20).$$

Уравнение равносильно следующему: $y=(1+x)(1+x^2)$. Тогда $x\ge-1$. Решения $x=-1, x=0$ и $x=1$ находятся сразу, поэтому далее $x>1$. Так как число x^2-1 кратно $x+1$, то $(1+x,1+x^2)\le 2$. Заметьте, что если $y^2=mn,(m,n)=1$, то m и n — квадраты целых чисел (это вытекает из основной теоремы арифметики). Так как число x^2+1 не может быть целым квадратом, ведь при $x>0$, очевидно, $x^2<x^2+1<(x+1)^2$, то равенство $(1+x,1+x^2)=1$ невозможно. Поэтому $(1+x,1+x^2)=2$, и

$$1+x=2u^2,1+x^2=2v^2$$

при целых взаимно простых u и v. Отсюда имеем, что

$$u^4+(u^2-1)^2=(x+1)^2/4+(x-1)^2/4=v^2,$$

т.е. (u^2,u^2-1,v) — примитивная пифагорова тройка. Если u — нечетно, то

$$u^2=p^2-q^2,u^2-1=2pq,v=p^2+q^2,(p,q)=1,p>q.$$

Тогда $p-q=t^2$, где t — натуральное, и

$$1=(p-q)^2-2q^2=t^2-2q^2,(q^2+1)^2=t^4+q^4.$$

Но последнее равенство невозможно, так как уравнение

$$x^4+y^4=z^2$$

неразрешимо в натуральных числах. Поэтому u — четно. Тогда

$$u^2=2pq,u^2-1=p^2-q^2,v=p^2+q^2,(p,q)=1,p>q.$$

Заметьте, что p — четно. Действительно, при нечетном p будет обязательно четно q, тогда остаток от деления p^2-q^2 на 4 был бы равен 1, и, значит, число u^2 при делении на 4 давало бы в остатке 2, что невозможно. Из того, что p — четно, $(p,q)=1$ и $u^2=2pq$, следует равенство $p=2m^2$, где m — натуральное. Поэтому

$$1=2pq-(p^2-q^2)=(p+q)^2-2p^2,$$

$$8m^4 = 2p^2 = (p+q)^2 - 1 = (p+q+1)(p+q-1),$$

$$2m^4 = ((p+q+1)/2)((p+q-1)/2) = (a+1)a.$$

Так как a и $a+1$ натуральные и взаимно простые, то нечетное из них является четвертой степенью натурального числа, а четное — удвоенной четвертой степенью. Отсюда следует, что при некоторых натуральных взаимно простых b и c справедливо одно из равенств

$$b^4 - 2c^4 = \pm 1.$$

Положим $g = c^2$, тогда при знаке + это равенство переписывается в виде

$$(g^2+1)^2 = g^4 + b^4.$$

Но это равенство невозможно так как уравнение

$$x^4 + y^4 = z^2$$

неразрешимо в натуральных числах. Поэтому в рассматриваемом равенстве может стоять лишь знак −, и тогда оно переписывается в виде

$$(g^2-1)^2 = g^4 - b^4.$$

Но уравнение

$$x^4 - y^4 = z^2$$

имеет в целых числах лишь тривиальные решения $x = \pm y, z = 0$ и $y = 0, z = x^2$. Так как $b > 0$ и $g = c^2 > 0$, получаем равенство $c^2 = b$. Но b и c взаимно просты, значит, это равенство возможно лишь при $b = c = 1$. Поэтому справедлива следующая цепочка равенств: $a = b^4 = 1, a+1 = 2c^4 = 2, p+q = 2a+1 = 3, p = 2$ (ввиду четности p), $q = 1, u^2 = 2pq = 4, x = 2u^2 - 1 = 7$.

5.25. Для доказательства равенства проверьте по индукции, что показатель наибольшей степени двойки, делящей $n!$, равен $n - \nu(n)$, и примените 5.1. Другое доказательство основано на тождестве

$$\sum_{i=1}^{m} [k/2^i] = \sum_{i=1}^{m} k/2^i - \sum_{i=0}^{m} (2^{i-1}a_{i-1} + \ldots + 2a_1 + a_0)/2^i =$$

$$k - k/2^n - \sum_{i=0}^{m-1} a_i(1 - 2^{-m+i}) = k - \sum_{i=0}^{m-1} a_i = k - \nu(k),$$

где $k = \sum\limits_{i=0}^{m-1} a_i 2^i, a_i = 0, 1$.

5.29. а) Действуйте также, как в 4.24. Утверждение а) вытекает также и утверждения б).

б) Представьте n в виде

$$n = q_m p^{m+1} + \ldots + q_1 p^2 + q_0 p + q',$$

где все q_i и q' целые неотрицательные и меньше p. Применяя 4.21, и учитывая что $u_k = 1 + p + \ldots + p^k$, получите, что

$$h = q_m u_m + \ldots + q_1 u_1 + q_0.$$

Так как при всех k справедливо неравенство

$$q_k u_k + \ldots + q_1 u_1 + q_0 \leq (p-1)(u_k + \ldots + u_1 + 1) = p^{k+1} + \ldots + p - k - 1 <$$

$$< 1 + p + \ldots + p^{k+1} = u_{k+1},$$

то

$$q_m = [h/u_m] = p_m, h_{m-1} = h - p_m u_m, q_{m-1} = [h_{m-1}/u_{m-1}] = p_{m-1}, \ldots,$$

$$h_1 = h_2 - p_2 u_2, q_1 = [h_1/u_1] = p_1, q_0 = h_1 - q_1 u_1 = h_1 - p_1 u_1 = p_0..$$

5.31. а) Примените 5.29.

б) Примените пункт а). Если переносов не происходило, то величина $\nu_p(n-k) + \nu_p(k) - \nu_p(n)$ равна нулю. Каждый перенос уменьшает один разряд в числе n на p и увеличивает следующий разряд на 1, в результате рассматриваемая величина возрастает на $p-1$, а значит, величина $(\nu_p(n-k) + \nu_p(k) - \nu_p(n))/(p-1)$ возрастает на 1.

5.32. Воспользуйтесь тем, что для каждого $m, 1 < m < p-1$, найдется такое не равное ему число n, что $mn - 1$ кратно p.

5.33. Проведите индукцию по длине p-ичной записи числа n. Для этого среди чисел от 1 до n, не кратных p, выделите $[n/p]$ наборов по $p-1$ последовательному числу в каждом. Произведение чисел в каждом наборе согласно 4.31 имеет остаток $p-1$ при делении на p. Кроме того, остается еще p_0 сомножителей, произведение которых равноостаточно с $p_0!$ при делении на p. Поэтому произведение всех не кратных p чисел из отрезка от 1 до n равноостаточно с $(-1)^{[n/p]} p_0!$. Если взять числа, кратные p, то после их деления на p, применив предположение индукции, получите, что их произведение, деленное на $p^{\mu'}$, равноостаточно с

$$(-1)^{\mu'} p_1! \ldots p_m!,$$

где $\mu' = ord_p[n/p]!$. Так как $\mu = \mu' + [n/p]$, то

$$n!/p^{\mu} = (n!/p^{[n/p]})/p^{\mu'}$$

равноостаточно с

$$(-1)^{[n/p]} p_0!(-1)^{\mu'} p_1! \ldots p_m! = (-1)^{\mu} p_0! \ldots p_m!.$$

5.48. Проведите индукцию по длине p-ичной записи числа n.

5.49. а) Примените 5.35 и 5.29.

б) Воспользуйтесь задачей 5.4 и пунктом а).

в) Заметьте, что сумма всех биномиальных коэффициентов

$$\binom{n}{1}, \binom{n}{3}, \ldots, \binom{n}{2k+1}, \ldots$$

равна 2^{n-1}, поэтому общий делитель есть степень двух. Далее примените теорему Куммера при $p = 2$.

5.51. а) Воспользуйтесь 5.29 и 5.32. Второе утверждение является частным случаем пункта в).

б) Утверждение является частным случаем пункта в).

в) Воспользуйтесь 5.32.

г) Примените индукцию. База и шаг индукции обосновываются в пункте в) Можно также воспользоваться 5.31 и рассмотреть поэтому только случай $n_i \geq k_i < p, 0 \geq i \geq m$. В этом случае утверждение вытекает из формулы для биномиальных коэффициентов и теоремы 5.33. Пункт в) тогда следует из пункта г) (хотя и не всегда является его частным случаем!).

д) Примените г) и тот факт, что $\binom{k}{p-1} - (-1)^k$ кратно p.

е) Представьте $\binom{kp}{np}$ в виде $\binom{k}{n}a/b$, где a и b есть произведения k сомножителей вида $(cp+1)\dots(cp+p-1)$. Для краткости используйте обозначение $x \equiv y$, если $x-y$ кратно p^n. Проверьте, что если $x \equiv y$, $u \equiv v$, то $xu \equiv yv, x+u \equiv y+v$. Раскрывая скобки в произведении $(cp+1)\dots(cp+p-1)$, получите, что оно равноостаточно при делении на p^3 с числом

$$(p-1)!(1+cp\sum_{0<i<p} 1/i + c^2p^2 \sum_{0<i<j<p} 1/ij).$$

Из задачи 5.9 следует, что при $p \geq 5$ число

$$(p-1)! \sum_{0<i<p} 1/i$$

кратно p^2, а при $p=3$ кратно p. Заметьте, что для любого $i, 0 < i < p$, найдется лежащее в том же интервале такое число i', что $ii'-1$ кратно p, причем разным i соответствуют разные числа i'. Поэтому равноостаточны при делении на p числа $(p-1)!/ij$ и $(p-1)!i'j'$, ведь

$$((p-1)!/ij - (p-1)!i'j')ij \equiv (p-1)! - (p-1)! \equiv 0,$$

$$(p-1)!/ij - (p-1)!i'j' \equiv ((p-1)!/ij - (p-1)!i'j')iji'j' \equiv 0,$$

а значит, и числа

$$(p-1)! \sum_{0<i<j<p} 1/ij,\ (p-1)! \sum_{0<i<j<p} i'j' = (p-1)! \sum_{0<i<j<p} ij.$$

Но

$$2\sum_{0<i<j<p} ij = \left(\sum_{0<i<p} i\right)^2 - \sum_{0<i<p} i^2 = (p(p-1)/2)^2 - p(p-1)(2p-1)/6,$$

значит, при $p \geq 5$ число

$$(p-1)! \sum_{0<i<j<p} 1/ij.$$

кратно p, и поэтому

$$c^2p^2(p-1)! \sum_{0<i<j<p} 1/ij$$

кратно p^3. Из полученных результатов следует, что при любом натуральном c число $(cp+1)\dots(cp+p-1)$ равноостаточно при делении на p^3 с числом $(p-1)!$. Поэтому введенные выше числа a и b равноостаточны при делении на p^3, и не кратны p. Значит, разность

$$\binom{k}{n}a/b - \binom{k}{n} = \binom{k}{n}(a-b)/b$$

кратна p^3, т.е. $\binom{kp}{np} - \binom{k}{n}$ кратно p^3.

5.52. Индукционный переход основан на неравенствах

$$4^{n+1}/\sqrt{2n+3} = (4^n/\sqrt{2n+1})(4\sqrt{2n+1}/\sqrt{2n+3}) >$$

$$> \binom{2n}{n}(4\sqrt{2n+1}/\sqrt{2n+3}) =$$

$$= \binom{2n+2}{n+1}(2n+2)/(\sqrt{(2n+3)(2n+1)}) >$$

$$> \binom{2n+2}{n+1} = \binom{2n}{n}2(2n+1)/(n+1) >$$

$$> 4(2n+1)/(\sqrt{n}(n+1)) > 4^{n+1}/2\sqrt{n+1}.$$

5.53. Воспользуйтесь равенством $\binom{2n+1}{n} = (2n+1)\dots(n+2)/n!$ и основной теоремой арифметики.

5.54. Примените 5.52, 5.53 и равенство $\binom{2n+1}{n} = \binom{2n+2}{n+1}/2$.

5.55. База индукции очевидно справедлива при $n = 4$ и 5. Индукционный переход основан на неравенствах :

$$P_{n+1} = P_n \le 4^{n-1}/n < 4^n/(n+1) \quad \text{при нечетном } n > 3,$$

$$P_{n+1} \le P_{n-1}(n+1) \le (n+1)4^{n-2}/(n-1) < 4^n/(n+1)$$

при $6 \le n = 2k \le 12$ (ведь при $n \le 12$ имеем, что $(n+1)^2 < 16(n-1)$, так как $n(n-14)+17 < 0$),

$$P_{2n+1} = P_{n+1}S_n < P_{n+1}4^{n+1}/2\sqrt{2n+3} \le (4^n/(n+1))4^{n+1}/2\sqrt{2n+3} \le$$

$$\le 4^{2n}/(2n+1),$$

последнее из которых справедливо при $n \ge 7$ ввиду неравенства

$$\sqrt{2n+3} > 4 > (4n+2)/(n+1).$$

5.56. Воспользуйтесь формулой Лежандра 5.1 и задачей 1.2.

5.57. Согласно основной теореме арифметики

$$\mathrm{HOK}(2,\dots,2n)/\binom{2n}{n} = \prod_{p\le 2n} p^{\mu_p(n)-\lambda_p(n)}$$

— целое число, так как ввиду 5.56 при всех простых $p \le 2n$ имеем $\lambda_p(n) \le \mu_p(n)$.

5.58. Согласно основной теореме арифметики

$$\mathrm{HOK}(2,\dots,2n) = \prod_{p\le 2n} p^{\mu_p(n)} \le (2n)^k,$$

так как $p^{\mu_p(n)} \le 2n$ в силу определения $\mu_p(n) = [\log_p 2n]$.

5.59. В силу задач 5.52, 5.57, 5.58 имеем

$$4^n/2\sqrt{n} < \binom{2n}{n} \le \mathrm{HOK}(2,\dots,2n) \le (2n)^k,$$

откуда $k > (2n - 1 - \frac{1}{2}\log_2 n)/\log_2 2n$.

5.60. Очевидно, что

$$4^{2n/3}/n < (4^{2n/3}/n)16^{1/3}/(1+1/n) = 4^{2n+2/3}/(n+1).$$

5.61. Первое неравенство следует из неравенства

$$p^{\lambda_p(n)} \le p^{\mu_p(n)} \le 2n$$

подобно задаче 5.58. Второе следует из задач 5.55, 5.60 и очевидного неравенства

$$\prod_{p<\sqrt{2n}} p \ge 2^k.$$

5.62. Четные числа, кроме двойки, составные и единица тоже не простое.

5.63. Из 5.56, 5.52 и 5.61 следует, что

$$P_{2n}/P_n = \binom{2n}{n} \Big/ \left(\prod_{p<\sqrt{2n}} p^{\lambda_p(n)} \prod_{2n/3\ge p\ge\sqrt{2n}} p \right) >$$

$$> (4^n/2\sqrt{n}) \left((2n)^k (4^{2n/3}) \right) / (2\cdot 8n/3)) = 4^{n/3}(4\sqrt{n}/3)/n^k >$$

$$> 4^{n/3}/n^{\sqrt{n/2}},$$

так как согласно 5.62 имеем $k < \sqrt{n/2} + 1/2$.

5.64. Заменой $n = 2x^2$ получаются неравенства

$$2^{4x/3} > 2x^2 \quad \text{при } x \ge \sqrt{12},$$

$$2^{4x^2/3} > 4x^2(2x^2)^x \quad \text{при } x > 7.$$

Первое из них верно при $x = \sqrt{12}$, так как $4^2 > (2,3)^2 3$ и $2^8 > 3^5$, то $8/\sqrt{3} > 4,6$ и $8 > (3/2)^5$, значит, $2^{8/\sqrt{3}} > 2^{4,6}$ и $2^{0,6} > 1,5$, откуда

$$2^{8/\sqrt{3}} > 2^{4,6} = 2^{0,6}16 > 1,5\cdot 16 = 24.$$

При почленном двукратном дифференцировании в точке $x = \sqrt{12}$ неравенство сохраняется, так как его левая часть умножается на $(4\ln 2)/3 > 2/3$ и потом еще раз на то же число, а левая часть сначала умножается на $2/x$, а потом на $1/x$ при $x = \sqrt{12} > 3$, и принимает вид

$$(16\ln 2)/9)2^{4x/3} > 4.$$

В силу монотонности оно будет справедливо и при всех $x \ge \sqrt{12}$, значит, согласно теореме о возрастании функции с положительной производной при всех $x \ge \sqrt{12}$ справедливы неравенства

$$((4\ln 2)/3)2^{4x/3} > 4x \quad \text{и } 2^{4x/3} > 2x^2.$$

Тем самым первое из наших неравенств доказано. Для доказательства второго достаточно установить, что при $x \ge 7$

$$2^{x^2/3} > 4x^2 \quad \text{и } 2^x \ge 2x^2.$$

Заменой $y = x^2/3$ первое из них сводится к неравенству $2^y > 12y$, которое вытекает из неравенства $2^n > 12(n+1)$, верного при $n = 7$ и всех следующих натуральных n в силу очевидной индукции. Второе неравенство вытекает из неравенства $2^n \geq 2(n+1)^2$, также верного при $n = 7$ и всех следующих натуральных n в силу очевидной индукции.

5.65. Примените 5.64 при $n \geq 24$, а при $n < 23$ проверьте непосредственно.

5.66. Примените 5.64 при $n \geq 97$, а при $n < 97$ проверьте непосредственно.

5.67. Из 5.54 выведите, что количество простых чисел, заключенных в пределах от n до $2n$, не превосходит $\log_n 4^n = 2n/\log_2 n$. Отсюда следует, что при $2^{k-1} < n \leq 2^k$ количество простых чисел, не превосходящих n, само не превосходит

$$\sum_{m=1}^{k-1} 2^{m+1}/m < (2^k/(k-1))(1 + 3/4 + \ldots + (3/4)^{k-3}) + 4 < 2^{k+2}/(k-1) + 4 <$$

$$< bn/\log_2 n.$$

§ 6. ОТ ДЕСЯТИЧНЫХ ДРОБЕЙ К "ЗОЛОТОЙ ТЕОРЕМЕ"

Научиться свободно обращаться с дробями - не такое простое дело. В средние века людей, умеющих это делать, можно было пересчитать по пальцам. Заметим, что трудности в действиях с обыкновенными дробями имеют объективную причину: две графически неравные дроби могут оказаться равными по величине, как, например, $\frac{116690151}{427863887}$ и $\frac{3}{11}$ (пример заимствован из книги Ч.Тригга "Задачи с изюминкой"). По этой же причине по-настоящему строгое построение числовой системы рациональных чисел осуществляется только в университетском курсе математики, и каждый, кто хочет вполне овладеть искусством обращения с дробями, вынужден знакомиться с такими понятиями как наименьшее общее кратное (НОК), наибольший общий делитель (НОД), простые и составные числа и т.д. При этом он узнает, например, что для нахождения НОД имеется простой и эффективный способ — алгоритм Евклида, а для разложения чисел на простые множители такого способа пока не известно. На этом факте, кстати, основана одна из описанных далее криптосистем для передачи по публичным каналам связи секретной информации, которую невозможно достаточно быстро расшифровать, не зная ключа.

В этом параграфе речь пойдет о десятичных дробях. Они были введены в практику нидерландским ученым Симоном Стевином, преподававшим на рубеже XVI-XVII в.в. в Лейденской инженерной школе.

6.1. Докажите, что обыкновеная дробь m/n представима в виде конечной десятичной дроби тогда и только тогда, когда n не делится на простые числа, отличные от 2 и 5.

6.2. Если m/n — правильная несократимая дробь и $n \neq 2, 5, 10$, то первая цифра в десятичном разложении этой дроби равна $[10m/n]$.

Десятичные дроби имеют один недостаток, правда не сказывающийся на их применении, и поэтому остающийся в тени, имен некоторые обыкновенные дроби невозможно точно выразить в ви конечных десятичных дробей, а лишь в виде бесконечных перио дических дробей, причем период может начинаться не сразу после запятой, отделяющей целую и дробную части, а после так называемого предпериода.

Правильная десятичная дробь называется **чисто периодической**, если период начинается сразу после запятой. Остальные дроби называются **смешанно-периодическими**, а часть десятичной запис между запятой и началом первого периода называется предпериодом Так, дробь $1/7 = 0,142857142857... = 0,(142857)$ — чисто периодическая с периодом длины 6, а дробь

$$\frac{13931}{70000} = 0,1990142857142857\cdots = 0,1990(142857)$$

смешанно-периодическая с предпериодом длины 4 и периодом 6.

Вычисление периода и предпериода на практике не всегда просто дело. Попробуйте-ка вычислить период у безобидной с виду дроби $1/49$. Теоретически этот вопрос тоже не прост, и не случайно в школьных учебниках, как правило, отсутствует доказательство пери одичности десятичных дробей, представляющих рациональные числа и тем более какие-нибудь факты о длине периода.

6.3. Пусть n делится на простое число, не равное 2 или 5, и r — остаток от деления $10m$ на n. Тогда, если $0, c_1c_2c_3...$ — десятичная запись числа m/n, то $0, c_2c_3c_4...$ — десятичная запись числа r/n.

6.4. Докажите, что любая обыкновенная дробь представима в виде конечной или периодической десятичной дроби.

6.5. Найдите длины периодов дробей $\frac{1}{10^n-1}$ и $\frac{k}{10^n-1}$, $1 < k < 10^n$.

6.6. Докажите, что обыкновенная правильная дробь m/n предста вима в виде чисто периодической десятичной дроби тогда и только тогда, когда n не делится ни на 2, ни на 5.

6.7. Докажите, что длина периода этой дроби равна наименьшему натуральному числу t, для которого n делит $10^t - 1$.

6.8. Докажите, что для произвольной дроби m/n длина периода ее десятичной записи равен наименьшему числу t, для которого найдется натуральное k такое, что n делит $10^k(10^t - 1)$. При этом наименьшее k, удовлетворяющее предыдущему условию, будет длиной предпериода. Докажите, что длина предпериода десятичного разложения правильной дроби со знаменателем n не превосходит $\log_2(n/3)$. Равенство достигается для несократимых дробей со знаменателем $3 \cdot 2^k$ и только для них.

6.9. Превратить обыкновенную дробь в десятичную можно делением столбиком. Используя 6.5, укажите простой способ превращения периодической десятичной дроби в обыкновенную.

6.10. Докажите, что сумма длин периода и предпериода десятичной записи дроби m/n меньше n.

Проверьте, что дробь $1/7$ имеет период 6, дробь $1/17$ — период 16, а дробь $1/29$ — период 28.

В следующем цикле задач читатель научится доказывать малую теорему Ферма и теорему Эйлера.

6.11. Докажите, что сумма длин периода и предпериода десятичного разложения любой правильной дроби со знаменателем n не превосходит $\varphi(n)$ — числа всех несократимых правильных дробей со знаменателем n. Равенство возможно лишь для дробей с чисто периодическим разложением. Проверьте, что дробь $1/49$ имеет период $\varphi(49) = 42$.

Из предыдущей задачи следует, что длина периода десятичной записи дроби со знаменателем n не превосходит $n-1$ и равенство возможно лишь при простом n. Примерами таких n служат, как уже отмечалось, $7, 17, 29$ и, кроме того, еще, например, 1913, однако неизвестно, конечно или бесконечно их количество. Гаусс предположил, что число таких простых n бесконечно, а позднее Артин высказал более общую гипотезу, которую в 1967 г. доказал Хооли, правда с помощью одной до сих пор не доказанной гипотезы о нулях дзета-функции Римана.

6.12. Пусть $(n, 10) = 1$. Докажите, что период дроби m/n будет делителем числа $\varphi(n)$.

6.13. Докажите, что для n, взаимно простого с 10, число $10^{\varphi(n)} - 1$ делится на n, а для простого n число $10^{n-1} - 1$ делится на n.

Далее иногда используем знак $|$ для обозначения отношения делимости: $n \mid m$ означает, что n делит m.

6.14*. Докажите, что при $(a, n) = 1$ имеем $n \mid a^{\varphi(n)} - 1$ (*теорема Эйлера*), и для произвольного a и простого p имеем $p \mid a^p - a$ (*теорема Ферма*).

В следующей задаче излагается математическое содержание *криптосистемы RSA (Райвеста, Шамира, Эдлемана).*

Обозначим для краткости через $\mathbb{Z}_n^*$ множество всех чисел a, таких что $1 \leq a < n, (a, n) = 1$, а для любого целого m остаток от его деления на n обозначим через $m \bmod n$.

6.15*. Пусть $n = pq$, где p, q — различные простые, и число $t \in \mathbb{Z}_n^*$ таково, что st при делении на $\varphi(n)$ дает в остатке 1.

а) Докажите, что отображения

$$x \to f(x) = x^s \bmod n \quad \text{и} \quad x \to g(x) = x^t \bmod n$$

взаимно однозначно отображают множество $\mathbb{Z}_n^*$ в себя и взаимно обратны друг другу, т. е. при любом $x \in \mathbb{Z}_n^*$ имеем

$$f(g(x)) = x.$$

Докажите, что сказанное выше будет верно и тогда, когда st дает в остатке 1 при делении на НОК$(p-1, q-1)$. Проверьте, что имеет место неравенство НОК$(p-1, q-1) \leq \varphi(n)/4$.

б)* Докажите, что утверждение а) справедливо и для всего множества $\mathbb{Z}_n$. Для этого установите следующий факт (*криптографическая лемма*): для любых целых x и k и для n, равного произведению двух разных простых чисел, справедливо равенство

$$x^{k\varphi(n)+1} \bmod n = x \bmod n.$$

в)* Докажите, что отображение $x \to f(x) = x^s \bmod n$ всегда имеет 4 "неподвижных точки" во множестве $\mathbb{Z}_n^*$ и девять "неподвижных точек" во множестве $\mathbb{Z}_n$ ("неподвижная точка" отображения — это такое число a, которое переходит в себя при этом отображении).

г)* Докажите, что если $s-1$ будет общим кратным чисел $p-1$ и $q-1$, то отображение $x \to f(x) = x^s \bmod n$ будет тождественным.

Отображение $x \to x^s$ множества $\mathbb{Z}_n^*$ в себя можно использовать для так называемого "открытого шифрования". Шифрование производится очень быстро с помощью компьютера,а числа s и n можно сообщить всем желающим. Дешифрование также проводится быстро, если известен "ключ" t.

Атакующему эту систему для нахождения числа t, исходя из равенства $st \equiv 1 \pmod{\varphi(n)}$, надо знать число $\varphi(n) = (p-1)(q-1) = n+1-p-q$, т.е. p и q. Вы выбираете p и q очень большими, сообщаете всем число $n = pq$ и произвольное s такое, что $(s, \varphi(n)) = 1$, и можете быть уверенными, что пока не будет изобретен алгоритм быстрого разложения на простые сомножители, ваша секретная система будет надежной.

Заметим, однако, что для предотвращения очевидных атак на систему все же рекомендуется:

а) не выбирать числа p и q слишком близкими друг к другу (рекомендуется, чтобы их двоичные записи отличались по длине на несколько разрядов), так как тогда облегчается возможность факторизации числа n;

б) следить за тем, чтобы число $p-1$ не было делителем числа $q-1$ и наоборот, и вообще чтобы эти числа не имели бы большого общего делителя, так тогда может возникает возможность найти ключ t перебором;

в) не допускать того, чтобы в разложении $\varphi(n)$ на множители встречались только малые простые числа (по той же причине).

Для надежности можно было бы использовать только так называемые "безопасные" простые числа, т.е. такие числа p, для которых и число $(p-1)/2$ тоже простое. К сожалению, проблема генерации таких чисел трудна, и до сих пор неизвестно, конечно или бесконечно их количество.

Заметим еще, что не рекомендуется использовать слишком малые числа s и t (так как тогда опять появляется возможность нахождения ключа перебором, но в случае малого s для этого, правда, нужно суметь перехватить одинаковое сообщение, посланное многим разным получателям), а также такие числа s, что $s-1$ будет общим кратным чисел $p-1$ и $q-1$, например, $s=\varphi(n)/2+1$, так как тогда зашифрованный текст всегда просто совпадает с незашифрованным. Кроме того, во всех случаях надо следить, чтобы случайно не попасть в "неподвижную точку".

Возвращаемся к задачам про периоды дробей.

6.16. Число 142857 обладает забавным свойством: при умножении на числа $2,3,4,5,6$ его цифры переставляются в циклическом порядке. Используя 6.10, объясните его и приведите пример еще одного числа с подобным же свойством.

Если расставить в вершинах правильного девятиугольника числа от 1 до 9, стереть числа $3,6,9$, и оставшиеся числа $1,4,2,8,5,7$ соединить отрезками в этом циклическом порядке (7 следует соединить с 1), то получится рисунок, которому известный эзотерик Г.И.Гюрджиев придавал магический смысл, утверждая, что в некоторой эзотерической традиции он был известен с незапамятных времен.[1)]

6.17. Используя 6.13 и 4.6, докажите, что период дроби $1/59$ равен 58, не вычисляя самого десятичного разложения. Как найти все цифры периода с помощью калькулятора?

6.18*. Еще одно свойство числа 142857 : число, составленное его первыми тремя цифрами, в сумме с числом, записанным последними тремя цифрами, дает 999. Докажите, что таким же свойством обладает число, составленное цифрами периода любой дроби k/p, где p — простое, если, конечно, период имеет четную длину.

6.19*. (*Москва, 82*) При каких n числа $\frac{1}{n}$ и $\frac{1}{n+1}$ выражаются конечными десятичными дробями?

6.20*. Докажите, что дробь $\frac{1}{n}+\frac{1}{n+1}+\frac{1}{n+2}$ при любом натуральном n смешанно-периодическая.

6.21. Докажите, что у любой дроби k/p, где p — простое, отличное от 2 и 5, среднее арифметическое цифр периода равно $4,5$ (если длина

[1)] См. об этом книгу его последователя П. Д. Успенского "В поисках чудесного". Как подозревают знающие люди, Гюрджиев получил посвящение в одной из семи "Башен Сатаны", вероятно в той, что находится в Туркестане (упоминание о них можно найти у Рене Геннона).

периода четна) и не равно 4,5 (если она нечетна.)

6.22. Докажите, что в десятичной записи любой правильной дроби $n/73$ нет двух одинаковых цифр подряд.

6.23. Пусть $a \mid k^m - 1$ и n — наименьшее такое число, что $a \mid k^n - 1$. Докажите, что $n \mid m$.

В следующем цикле задач вы вплотную подойдете к понятию, которое в теории чисел называется первообразным корнем по модулю, равному степени простого числа. Для малых простых оно оказывается существенно проще, чем понятие первообразного корня по простому модулю.

6.24*. Докажите, что при простом p, не равном 2 и 5, длины периодов несократимых дробей $a_1/p, \ldots, a_n/p^n, \ldots$ будут каждый раз увеличиваться в p раз, начиная с некоторого места.

6.25. Найдите периоды дробей $1/3^n, 1/7^n, 1/17^n$.

6.26*. Докажите аналог задачи 6.23 для двоичных дробей и с помощью его найдите периоды двоичных разложений дробей $1/3^n, 1/5^n, 1/7^n$ и троичных разложений дробей $1/2^n, 1/5^n$.

6.27. Докажите, что:

а) наименьшее k, для которого $3^n \mid 2^k - 1$, равно $\varphi(3^n) = 2 \cdot 3^{n-1}$;

б) наименьшее k, для которого $5^n \mid 2^k - 1$, равно $\varphi(5^n) = 4 \cdot 5^{n-1}$;

в) наименьшее k, для которого $7^n \mid 2^k - 1$, равно $\frac{1}{2}\varphi(7^n) = 3 \cdot 7^{n-1}$;

г) наименьшее k, для которого $2^n \mid 3^k - 1$, равно $\frac{1}{2}\varphi(2^n) = 2^{n-2}$ при $n > 2$, равно 2 при $n = 2$ и равно 1 при $n = 1$;

д) наименьшее k, для которого $2^n \mid 5^k - 1$, равно $\frac{1}{2}\varphi(2^n) = 2^{n-2}$ при $n > 2$, равно 1 при $n = 2$ и 1;

е) наименьшее k, для которого $5^n \mid 3^k - 1$, равно $\varphi(5^n) = 4 \cdot 5^{n-1}$.

6.28. Выведите из 6.27 решения задач 5.16 и 5.15.

6.29*. Докажите, что все нечетные числа вида $4k+1$, заключенные между 1 и $2^n - 1$, можно расставить по кругу так, что для любых трех соседних чисел a, b, c разность $b^2 - ac$ будет делиться на 2^n. Все нечетные числа так расставить нельзя, однако все числа вида $4k + 3$ — можно.

Теперь попробуем разобраться, что такое *первообразный корень по простому модулю* и что такое *первообразный корень по модулю, равному степени простого числа*. Отметим, что следующий цикл задач несколько труднее предыдущих.

Множество всех чисел от 1 до $n - 1$, взаимно простых с числом n, обозначаем, как и раньше, $\mathbb{Z}_n^*$.

6.30. Докажите, что все числа из множества M, содержащегося в $\mathbb{Z}_n^*$, можно расставить по кругу так, что для любых трех соседних чисел a, b, c разность $b^2 - ac$ будет делиться на n тогда и только тогда, когда при некоторых натуральных числах f и g i-е от начала число равно остатку от деления $f \cdot g^{i-1}$ на n при любом i (начало

направление нумерации — по часовой или против часовой стрелки — берутся произвольными, но фиксированными для данного круга), при этом g^m при делении на n дает в остатке единицу, где m — количество чисел во множестве M.

Число m назовем *порядком числа g по модулю n*, а расстановку чисел по кругу, о которой шла речь — *циклом порядка m*.

6.31. Если цикл содержит единицу, то при соответствующем выборе начала нумерации элементы цикла совпадают с остатками от деления чисел $1, g, \ldots, g^{m-1}$ на n, причем остаток от деления g^m на n равен единице.

Элемент g тогда называется *порождающим элементом* цикла.

6.32. Докажите, что число g имеет порядок m по модулю n тогда и только тогда, когда g-ичная дробь, изображающая $1/n$, имеет период длины m.

6.33*. Докажите, что если элементы множества M можно расположить по циклу, то это можно сделать ровно $\varphi(m)$ различными способами (способы, отличающиеся только началом и направлением нумерации, считаются одинаковыми).

6.34. Докажите, что все элементы множества $\mathbb{Z}_n^*$ можно расположить по циклу тогда и только тогда, когда это множество имеет порождающий элемент (называемый *первообразным корнем по модулю n*). Докажите, что если первообразные корни по модулю n существуют, то их ровно $\varphi(\varphi(n))$ штук.

6.35*. Докажите, что множество $\mathbb{Z}_n^*$ содержит $\varphi(n)$ чисел и при простом n совпадает с множеством всех чисел от 1 до $n-1$.

Поставим в соответствие каждому числу i из $\mathbb{Z}_n^*$ остаток r_i от деления ig на n. Полученную перестановку множества $\mathbb{Z}_n^*$ можно изобразить графически, поставив в соответствие числам из $\mathbb{Z}_n^*$ точки плоскости, и упорядоченным парам (i, r_i) — стрелки, ориентированные от точки i к точке r_i.

6.36*. Докажите, что полученное изображение (граф) перестановки является объединением непересекающихся циклов равной длины.

6.37. Докажите, что порядок любого числа по модулю n делит $\varphi(n)$ и выведите отсюда теоремы Ферма и Эйлера.

6.38. Докажите,что если порядок числа g по простому модулю p равен m, то множество всех чисел из $\mathbb{Z}_p^*$, порядок которых делит m, совпадает со множеством остатков от деления чисел $1, g, g^2, \ldots, g^{m-1}$ на p.

Далее в этом цикле задач p всегда обозначает простое число.

6.39. Докажите,что если порядок некоторого числа по простому модулю равен m, то во множестве $\mathbb{Z}_p^*$ имеется ровно $\varphi(m)$ чисел, порядок которых равен m.

6.40*. *(Гаусс)* Докажите,что для любого m, делящего $p-1$, суще-

ствует в $\mathbb{Z}_p^*$ ровно $\varphi(m)$ чисел, порядок которых равен m. В частности существует ровно $\varphi(p-1)$ чисел, порядок которых равен $p-1$ (такие числа называются *первообразными корнями по модулю p*.

6.41. Докажите,что если $a-b$ кратно m, то число

$$\frac{a^n-b^n}{a-b}-na^{n-1}$$

тоже кратно m.

6.42. Если $a-1$ кратно m, то число

$$\frac{a^n-1}{a-1}-n$$

тоже кратно m и

$$m \mid \frac{a^n-1}{a-1} \Longleftrightarrow m \mid n.$$

6.43. *(Серпинский)* Докажите, что

$$\left(\frac{a^n-1}{a-1}, a-1\right) = (a-1, n).$$

6.44*. Существует целое g такое, что $g^{p-1}-1$ не делится на p и порядок g по модулю p равен $p-1$.

6.45*. *(Ван-дер-Варден)* Если $n>1$ или $p>2$, то

$$p \mid a-1 \Longleftrightarrow p \mid \frac{a^{p^n}-1}{a^{p^{n-1}}-1}$$

и $(a^{p^n}-1)/(a^{p^{n-1}}-1)$ не кратно p^2.

6.46*. Если $a-1$ кратно $p>2$, то

$$ord_p \frac{a^n-1}{a-1} = ord_p n.$$

6.47. Если $a-1$ кратно $p>2$, то

$$ord_p\left((1+a)(1+a+a^2)\cdot(1+a+\cdot+a^{n-1})\right) = \frac{n-\sigma_p(n)}{p-1}.$$

6.48*. Докажите, что для числа g из 6.43 и любого натурального n число

$$g^{\varphi(p^n)}-1$$

кратно p^n и не кратно p^{n+1} и для любого натурального $m<\varphi(p^n)$ число g^m-1 не кратно p^n.

Будем говорить, что подмножество M, содержащееся в $\mathbb{Z}_n^*$, является *циклическим*, если все его числа можно расставить по кругу так, что для любых трех соседних чисел a, b, c разность $b^2 - ac$ будет делиться на n.

6.49. Если p — простое число, $p > 2$, то множество $\mathbb{Z}_{p^n}^*$ — циклическое. Множество $\mathbb{Z}_{2p^n}^*$ — тоже циклическое.

6.50. Докажите, что разность $5^{2^k} - 2^{k+2} - 1$ кратна 2^{k+3}.

6.51. Множество $\mathbb{Z}_{2^n}^*$ — циклическое при $n \leq 2$ и нециклическое при $n > 2$. При $n > 2$ подмножество всех его чисел вида $4k + 1$ — циклическое и подмножество всех его чисел вида $4k + 3$ — тоже.

6.52. Докажите, что все остальные множества $\mathbb{Z}_m^*$ нециклические.

Пусть далее до конца этого цикла $m = p^n$ или $m = 2 \cdot p^n, p > 2$, $\alpha \in \mathbb{Z}_n^*$ — **первообразный корень** (в другой терминологии - *порождающий* или **образующий элемент**) циклического множества $\mathbb{Z}_m^*$.

Индексом числа x из $\mathbb{Z}_m^*$ по основанию α назовем минимальное положительное n, такое, что остаток от деления α^n на m равен x, и обозначим его $ind_\alpha x$ или просто $ind\, x$. Назовем произведением чисел a и b из $\mathbb{Z}_m^*$ такое число c из $\mathbb{Z}_m^*$, что $ab - c$ кратно m, и обозначим его $a * b$.

Следующие теоремы принадлежат Гауссу.

6.53*. Докажите, что для любых чисел a и b из $\mathbb{Z}_m^*$ существует такое число c из $\mathbb{Z}_m^*$, что $a = c * b$. Далее его называем *частным от деления* a на b.

6.54. Для любых x, y из $\mathbb{Z}_m^*$ индекс их произведения равен остатку от деления на $\varphi(m)$ суммы их индексов, а индекс частного равен остатку от деления на $\varphi(m)$ разности индексов.

6.55*. Пусть $d = (n, \varphi(m))$. Если $d \mid ind\, a$, то во множестве $\mathbb{Z}_m^*$ имеется ровно d чисел b таких, что $b^n - a$ кратно m. Если d не делит $ind\, a$, то таких чисел нет.

6.56*. Во множестве $\mathbb{Z}_m^*$ имеется ровно $\varphi(m)/d$ чисел a, для которых существуют такие числа b, что $b^n - a$ кратно m. Множество таких чисел a совпадает со множеством таких чисел в $\mathbb{Z}_m^*$, порядок которых делит $\varphi(m)/d$.

6.57*. Порядок любого числа x из $\mathbb{Z}_m^*$ равен $\varphi(m)/(\varphi(m), ind\, x)$. В частности, x будет первообразным корнем в $\mathbb{Z}_m^*$ тогда и только тогда, когда $(ind\, x, \varphi(m)) = 1$. Число всех элементов в $\mathbb{Z}_m^*$, имеющих порядок δ, равно $\varphi(\delta)$. В частности, число первообразных корней в $\mathbb{Z}_m^*$ равно $\varphi(\varphi(m))$.

Нахождение индекса произвольного элемента из $\mathbb{Z}_p$ относительно заданного первообразного корня a (называемое коротко **дискретным логарифмированием**) требует весьма громоздких вычислений и при p, состоящем из нескольких сотен цифр, не под силу и суперЭВМ.

Лишь в случае, когда $p-1$ имеет только малые простые множит ли, известен сравнительно быстро работающий алгоритм дискретно логарифмирования (принадлежащий Полигу и Хеллману).

На предположении о труднорешаемости задачи дискретного ло гарифмирования основана следующая система Диффри и Хеллман **открытого распределения ключей**. Допустим, что A и B хо тят, пользуясь публичными каналами связи (например, электронно почтой), выработать общую секретную информацию (**общий ключ**) Противник[1)] знает о затеях A и B и может перехватывать весь и обмен информацией.

6.58*. Предложите протокол выработки общего ключа, роль ко торого играет некоторый элемент из $\mathbb{Z}_p^*$, причем для его выработк требуется обменяться двумя элементами из $\mathbb{Z}_p^*$. Каждый из партнеро вычисляет свой элемент, пользуясь своим ключом (секретным элемен том), а потом, получив вычисленный партнером элемент, с помощь того же ключа вычисляет общий ключ (он, разумеется, должен по лучиться одинаковым у обоих). Алгоритм вычисления общего ключа должен быть простым, а алгоритм взлома этой системы (конечно, при отсутствии информации о ключах партнеров) — очень трудоемким.

Следующий (и самый трудный) в этом параграфе цикл задач посвящен квадратичным вычетам и закону взаимности.

Число a называется *квадратичным вычетом по модулю* p, если оно не кратно p и существует такое b, что b^2-a кратно p, и *квадратичным невычетом по модулю* p, — если оно не кратно p и такого b не существует.

6.59. *(Эйлер)* Во множестве $\mathbb{Z}_p^*$, $p>2$, поровну квадратичных вычетов и невычетов. Произведение вычетов есть вычет, произведение двух невычетов — опять вычет, а произведение вычета на невычет — невычет. Число $p-1$ является вычетом тогда и только тогда, когда $p=4k+1$.

По определению *символ Лежандра* $\left(\frac{a}{p}\right)$ равен 1, если a — вычет, и равен минус 1, если a — невычет, $\left(\frac{a}{p}\right)=0$, если a кратно p.

6.60. *(Эйлер)* Докажите, что $\left(\frac{a}{p}\right)$ и $a^{\frac{p-1}{2}}$ имеют равные остатки при делении на p и $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$.

6.61***. *(Гаусс)* Докажите, что:

а) для любых a и x, не кратных p, остаток от деления ax на p равен остатку от деления $\epsilon_x r_x$ на p, где

$$1 \le r_x \le (p-1)/2, \epsilon_x = (-1)^{[2ax/p]},$$

[1)] Например, нанятый конкурентами агент, занимающийся экономическим шпионажем — это обычное дело на Западе и, вероятно, скоро станет обычным делом и у нас.

б) для любого a, не кратного p, справедливо равенство

$$\left(\frac{a}{p}\right) = (-1)^s,$$

где

$$s = \sum_{x=1}^{(p-1)/2} [2ax/p].$$

6.62***. *(Эйлер – Гаусс)* Докажите, что

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}.$$

6.63***. *(Эйлер – Лежандр – Гаусс)* Докажите, что для любых простых нечетных p и q имеем

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Выполнять арифметические действия с периодическими десятичными дробями очень удобно, если требуется сделать это приближенно, и очень неудобно, если нужно это сделать точно. В последнем случае иногда лучше перейти от них к обыкновенным дробям, выполнить действие, и результат опять перевести в десятичную дробь. НОК(a, b) далее означает наименьшее общее кратное чисел a и b, т. е. такое наименьшее число, которое делится и на a, и на b. Для краткости иногда его обозначаем $[a, b]$.

Однако отметим, что можно складывать, вычитать и умножать периодические дроби, не переводя их в обыкновенные. При этом возникает вопрос об оценке предпериода и периода суммы, разности и произведения двух дробей. Для краткости будем писать период t вместо период длины t и аналогично поступать с предпериодом.

6.64*. Докажите, что сумма и разность периодических дробей имеет предпериод, не больший максимума их предпериодов, и период, не больший НОК их периодов и и укажите способ выполнения этих действий без перехода к обыкновенным дробям.

Для того,чтобы показать точность оценок этой задачи, решите следующую задачу.

6.65*. Дроби $1/10^{k_i}(10^{t_i} - 1) = 0,0\ldots0(0\ldots01), i = 1, 2$, имеют предпериоды k_i и периоды t_i, а их сумма и разность имеют предпериод $\max(k_1, k_2)$ и период НОК(t_1, t_2).

Результат задачи 6.64 можно уточнить. Пусть числа p_i — суть все простые, входящие в разложения чисел m и n в различных степенях α_i

и $\beta_i, \alpha_i \neq \beta_i, 1 \leq i \leq k$. Обозначим через $]m,n[$ произведение $p_1^{\gamma_1} \cdots p_k^{\gamma_k}$, где $\gamma_i = \max(\alpha_i, \beta_i), 1 \leq i \leq k$.

6.66*. Докажите, что сумма и разность дробей с периодами m и n имеют период, делящийся на $]m,n[$ и делящий $[m,n]$, и предпериод, равный максимуму их предпериодов, если они различны.

6.67*. Пусть $]m,n[$ делит t, а $[m,n]$ делится на t, и $0 \leq \delta \leq d$. Докажите, что для некоторых дробей с периодами m и n и предпериодом d сумма (разность) имеет период t и предпериод δ.

Рассмотрим вопрос о предпериоде и периоде произведения дробей.

6.68*. *(Москва, 90)* Докажите, что если дробь имеет период t и предпериод k, то ее квадрат имеет период не более $t(10^t - 1)$ и предпериод не более $2k$.

6.69*. Докажите, что дробь $1/(10^k(10^t - 1))$ имеет период t и предпериод k, а ее квадрат имеет период $t(10^t - 1)$ и предпериод $2k$.

Следующая задача обобщает задачу 6.68.

6.70**. Докажите, что если дроби имеет периоды t и d и предпериоды k и s, то их произведение имеет период не более $\frac{dt}{(t,d)}(10^{(t,d)} - 1)$ и предпериод не более $k + s$. Дроби $1/(10^k(10^t - 1))$ и $1/(10^s(10^d - 1))$ имеют периоды t и d и предпериоды s и k, а их произведение имеет период $\frac{dt}{(t,d)}(10^{(t,d)} - 1)$ и предпериод $s + k$.

Из утверждения задачи 6.70 следует, в частности, что если периоды дробей взаимно просты, то период их произведения не превосходит удевятеренного НОК их периодов, но если периоды имеют большой НОД, то период произведения может их значительно превосходить.

В следующем цикле задач речь пойдет о *распознавании простоты* больших чисел. Этот цикл также довольно труден для начинающих.

Пусть m - число, простоту которого мы хотим распознать. Рассмотрим множество $\mathbb{Z}_m^*$, состоящее из всех чисел a, b, взаимно простых с m и лежащих в пределах от 1 до m. Это множество образует *группу* относительно умножения по $\mathrm{mod} m$. Число s из $\mathbb{Z}_m^*$ назовем *свидетелем простоты* для числа m, если последовательность степеней

$$s^{(m-1)2^{-i}} \bmod m, \quad i = 0, 1, \ldots, r, \quad m - 1 = 2^r t,$$

t — нечетно, состоит только из единиц, либо с них начинается, после чего продолжается минус единицей (или $m - 1$, что равносильно) и может быть, другими числами. Множество всех свидетелей простоты числа m обозначим S.

Заметим, что проверку того, является или нет случайно выбранное число $a < m$ свидетелем простоты числа m можно выполнить очень быстро даже для больших чисел m, так как она сводится к возведению данного числа в заданную степень по модулю m, а для этого известен быстрый алгоритм (который описан в одном из следующих параграфов).

6.71. Если число $a < m$ не является свидетелем простоты числа m, то m— составное.

Докажем следующую теорему, лежащую в основе вероятностного алгоритма распознавания простоты (вероятностного теста) Миллера—Рабина.

Теорема. *Множество всех свидетелей простоты составного числа m, не кратного 6, содержит не более четверти элементов из $\mathbb{Z}_m^*$.*

Из этой теоремы следует, что если k случайно выбранных чисел оказались свидетелями простоты числа m, то вероятность непростоты этого числа не превосходит 4^{-k}. Поэтому для случайно выбранного числа m достаточно не более 20 проверок на свидетельства простоты, чтобы либо доказать (после первой же неудачной проверки), что оно составное, либо заявить, что с вероятностью, практически равной единице, оно является простым (и предоставить абсолютно надежную проверку этого утверждения другим, уже не вероятностным, алгоритмам).

Доказательство теоремы разбивается на последовательность задач.

Как и ранее, символ p с индексом или без него обозначает простое число.

6.72. Пусть m делится на p^2. Тогда множество чисел

$$1 + km/p, k = 0, \ldots, p-1,$$

образует подгруппу в $\mathbb{Z}_m^*$ порядка p и все её неединичные элементы имеют порядок p.

Назовем *лжесвидетелем* любое число a из $\mathbb{Z}_m^*$ такое, что либо $a^{m-1} \bmod m \neq 1$, либо при любом целом k справедливо $a^k \bmod m \neq -1$ и для некоторого простого делителя p числа m порядок числа a по $\bmod p$ равен $p-1$ (напомним, что порядок числа a по $\bmod m$ — это наименьшая натуральная степень, при возведении числа a в которую остаток по $\bmod m$ будет равен 1). Обозначим через A множество всех лжесвидетелей.

6.73.** Если a— лжесвидетель, а s— свидетель, то $as \bmod m$ не является свидетелем, другими словами, пересечение множеств S и aS пусто.

6.74. Пусть $a \neq b \in \mathbb{Z}_m^*$. Множества Sa и Sb не пересекаются тогда и только тогда, когда не пересекаются множества S и $Sab^{-1} \bmod m$.

В частности, для любой подгруппы G группы $\mathbb{Z}_m^*$ справедливо следующее: множества Sg при всех $g \in G$ попарно не пересекаются тогда и только тогда, когда не пересекаются множества S и Sg при любом неединичном $g \in G$.

Множества S и Sa при любом $a \in \mathbb{Z}_m^*$ состоят из одинакового числа элементов и целиком содержатся в $\mathbb{Z}_m^*$

Отображение $x \to xa$ задает взаимно однозначное соответствие между S и Sa.

6.75*. Пусть m делится на p^2. Тогда число элементов в S не превосходит $1/p$-й доли числа элементов в $\mathbb{Z}_m^*$.

6.76*. Пусть $m = p_1p_2, p_1 \neq p_2$. Тогда число элементов в S не превосходит $\varphi(m)/4$.

6.77*. Пусть m делится на три разных простых числа $p_i, i = 1, 2,$ но не делится на их квадраты. Тогда число элементов в S не превосходит $\varphi(m)/4$.

Доказательство теоремы теперь непосредственно следует из утверждений трех последних задач, так как для любого непростого m выполняется условие хотя бы одной из них.

УКАЗАНИЯ

6.4. При разложении $\frac{m}{n}$ в десятичную дробь методом деления столбиком будем записывать под каждым очередным десятичным знаком остаток от той операции деления, частным от которой является упомянутый знак; последовательность остатков будет периодической.

6.8. Докажем последнее утверждение задачи. Представим n в виде 2^a5^bs, где $(s, 10) = 1$. Тогда $s \geq 3$ и $\max(a, b) = k$, потому что n делит $10^k(10^t - 1)$ тогда и только тогда, когда 2^a5^b делит 10^k и s делит $10^t - 1$, ведь $(s, 10) = 1 = (10, 10^t - 1)$. Значит, $n \geq 2^k3$ и равенство возможно лишь при $s = 3, a = k, b = 0$.

6.12. Рассмотрите период остатков, о котором говорилось в указании к задаче 6.4; если какое-то число $k, 1 \leq k < n, (k, n) = 1$, не входит в него, то рассмотрите соответствующий период для k/n и если найдется число $k', 1 \leq k' < n, (k', n) = 1$, не входящее в оба периода, то с ним поступите так же, как и с k; при этом множество всех чисел m, таких, что $1 \leq m < n$ и $(m, n) = 1$, разобьется на несколько периодов одинаковой длины (почему?).

6.14. Повторите рассуждения 6.12 для двоичных, троичных и вообще m-ичных дробей, так же как в 6.13.

6.18. Пусть A и B — l-значные числа, являющиеся "половинками" периода; проверьте, что

$$p \mid 10^l + 1,\ 10^l - 1 \mid A + B < 2(10^l - 1).$$

6.24. Если $k < l$ — такие наименьшие числа, что $p^n \mid 10^k - 1$ и $p^{n+1} \mid 10^l - 1$, то $l = km$ (согласно 6.23) и

$$p \mid (10^l - 1)/(10^k - 1) = 1 + 10^k + 10^{2k} + \ldots + 10^{k(m-1)},$$

а так как 10^{kt} при делении на $10^k - 1$ (а, значит, и при делении на p) дает остаток 1, то последнее возможно лишь при $p \mid m$; примените так же 6.7.

6.41. Используя известное тождество, получаем, что

$$\frac{a^n - b^n}{a - b} - na^{n-1} = a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1} - na^{n-1}$$

кратно m, ибо $a^{n-k}b^{k-1} - a^{n-1}$ кратно m согласно условию задачи.

6.42. Первое утверждение следует из 6.40, а второе — из первого.

6.44. Из 6.40 следует, что порядок некоторого целого a равен $p-1$. Допустим, что $a^{p-1}-1$ кратно p^2 и выберем $g=a+p$. Из задачи 6.41 следует, что число

$$\frac{g^{p-1}-a^{p-1}}{g-a}-(p-1)a^{p-2}$$

кратно p, откуда следует, что

$$g^{p-1}-a^{p-1}=p\frac{g^{p-1}-a^{p-1}}{g-a}$$

не кратно p^2, значит, $g^{p-1}-1$ не кратно p^2, ибо $a^{p-1}-1$ кратно p^2.

6.45. Из 6.42 с помощью индукции следует, что если $p \mid a-1$, то

$$p \mid \frac{a^{p^n}-1}{a^{p^{n-1}}-1}, p^{n+1} \mid a^{p^n}-1, p^n \mid \frac{a^{p^n}-1}{a-1}.$$

Воспользовавшись равенством

$$\frac{a^{p^n}-1}{a^{p^{n-1}}-1}=\left(a^{p^{n-1}(p-1)}-1\right)+\left(a^{p^{n-1}(p-2)}-1\right)+\left(a^{p^{n-1}}-1\right)+p$$

и делимостью на p^n каждого слагаемого, кроме последнего, получите, что рассматриваемая дробь при делении на p^n дает остаток p, т.е. при $n>1$ не делится на p^2.

6.46. Пусть $p^\alpha \mid n$ и $(n/p^\alpha, p)=1$. Тогда, как показано в задаче 6.45,

$$p^\alpha \mid \frac{a^{p^\alpha}-1}{a-1},$$

значит,

$$p^\alpha \mid \frac{a^n-1}{a^{p^\alpha}-1}\frac{a^{p^\alpha}-1}{a-1}=\frac{a^n-1}{a-1}.$$

Из 6.43 следует, что первый сомножитель здесь не кратен p. Индукцией с помощью второго утверждения задачи 6.44 докажите, что

$$p^n \mid \frac{a^{p^n}-1}{a-1}$$

а p^{n+1} — нет. Отсюда следует, что $p^{\alpha+1}$ не делит

$$\frac{a^n-1}{a-1}.$$

6.47. Примените 6.46 и формулу Лежандра.

6.48. Индукция по n. База ($n=1$) доказана в 6.44. Шаг индукции: $n=l+1$. Пусть g^m-1 кратно p^{l+1}, тогда согласно предположению индукции $\varphi(p^l)$ кратно m, откуда с помощью 6.42 получаем цепочку эквивалентных соотношений

$$p \mid \frac{g^m-1}{g^{\varphi(p^n)}-1},\ p \mid \frac{m}{\varphi(p^n)},\ \varphi(p^{n+1}) \mid m,$$

а так как согласно предположению индукции

$$p^l \mid g^{\varphi(p^l)}-1 \quad \text{и} \quad p^{l+1} \nmid g^{\varphi(p^n)}-1,$$

то

$$p^{l+1} \mid g^m - 1,\ \varphi(p^{l+1}) \mid m,$$

значит, число $g^{\varphi(p^{l+1})} - 1$ кратно p^{l+1} и при любых $m > 0$ и $m < \varphi(p^{l+1})$ числ $g^m - 1$ не кратно p^{l+1}. Осталось проверить, что $g^{\varphi(p^{l+1})} - 1$ не кратно p^{l+2}. Дл этого достаточно установить, что $\frac{g^{\varphi(p^{l+1})}-1}{g^{\varphi(p^l)}-1} - p$ кратно p^{l+1}, откуда следует, чт число $\frac{g^{\varphi(p^{l+1})}-1}{g^{\varphi(p^l)}-1}$ кратно p и не кратно p^2, значит, число

$$p^{l+1} \mid g^{\varphi(p^{l+1})} - 1 = (g^{\varphi(p^l)} - 1)\frac{g^{\varphi(p^{l+1})} - 1}{g^{\varphi(p^l)} - 1}$$

не кратно p^{l+2}. Полагая $a = g^{\varphi(p^l)}$ и учитывая, что $p^l \mid (a-1)$, получаем

$$\frac{g^{\varphi(p^{l+1})} - 1}{g^{\varphi(p^l)} - 1} - p = \frac{a^p - 1}{a - 1} - p = 1 + a + \cdots + a^{p-1} - p =$$

$$= (a-1)\left(1 + \frac{a^2 - 1}{a-1} + \cdots + \frac{a^{p-1} - 1}{a-1}\right)$$

откуда согласно 6.42 имеем, что число

$$\frac{a^p - 1}{a-1} - p - (a-1)(1 + 2 + \cdots + p - 1) = \frac{a^p - 1}{a-1} - p - (a-1)\frac{p(p-1)}{2}$$

кратно p^{l+1}, ибо $\frac{a^k-1}{a-1} - k$ кратно p, что и требовалось доказать.

В случае $n \geq 2$ требуемое утверждение следует из более простого сравнения $\frac{a^p-1}{a-1} \equiv p \pmod{p^n}$, сразу вытекающего из задачи 6.42.

6.49. Примените 6.48 и 6.34. Для доказательства второго утверждения заметьте, что числа из $\mathbb{Z}^*_{2p^n}$ либо принадлежат $\mathbb{Z}^*_{p^n}$, либо получаются из них прибавлением p^n и это соответствие сохраняется при перемножении их "по модулю" $2p^n$, и примените первое утверждение.

6.50. Индукция по k. База ($k = 1$) очевидна. Шаг индукции обосновывается равенствами:

$$5^{2^{k+1}} = \left(5^{2^k}\right)^2 = \left(1 + 2^{k+2}(2s+1)\right)^2 = 1 + 2^{k+3} + d2^{k+4}.$$

6.51. При $n \leq 2$ утверждение очевидно. Пусть $n > 2$. Из 6.50 следует, что элемент 5 из $\mathbb{Z}^*_{2^n}$ порождает циклическое подмножество M, состоящее из всех чисел вида $4k+1$. А так как любое число из $\mathbb{Z}^*_{2^n}$, не принадлежащее M, имеет вид $2^n - a$, где a принадлежит M, то последнее утверждение задачи следует из предпоследнего.

6.52. Пусть $m = p_1^{a_1} \ldots p_n^{a_n}$ — каноническое разложение на простые множители числа m. Можно считать, что все p_i больше 2, или $p_1 = 2$, то тогда или $n \geq 3$, или $a_1 \geq 2$. Согласно 6.14 порядок по модулю p_i любого элемента g из $\mathbb{Z}^*_m$ при $p_i > 2$ делит число

$$\varphi(p_i^{a_i}) = p_i^{a_i - 1}(p_i - 1),$$

а так как эти числа — четные, а порядок g по модулю m делит **НОК** этих чисел, то он, очевидно, не превосходит половины их произведения, т.е. $\varphi(m)/2$. Если бы множество $\mathbb{Z}^*_m$ было циклическим, то оно содержало бы порождающий элемент g, который имел бы порядок $\varphi(m)$, что невозможно.

6.53. Последовательность $c * b$, где c пробегает все числа из $\mathbb{Z}_m^*$, является перестановкой последовательности $\mathbb{Z}_m^*$.

6.58. Обозначим ключи партнеров через x_A и x_B, а через a — некоторый первообразный корень из $\mathbb{Z}_p^*$. Партнер A вычисляет с помощью быстрого алгоритма возведения в степень остаток y_A от деления числа a^{x_A} на p, и аналогичным способом партнер B вычисляет остаток y_B. Получив число y_B, партнер A находит остаток от деления $y_B{}^{x_A}$ на p, и аналогично поступает A. В результате оба получают одно и то же число, равное остатку от деления на p числа $a^{x_B x_A}$. Противник, зная y_A, y_B и a, для нахождения x_a и x_B должен уметь быстро выполнять дискретное логарифмирование.

6.61. а) Очевидно, что утверждение верно при $\varepsilon_x = +1$ в зависимости от того, меньше или больше $1/2$ число $\{ax/p\}$. Так как при любом b число $[2b] = [2[b] + 2\{b\}] = 2[b] + [2\{b\}]$ четно или нечетно в зависимости от того, меньше или больше $1/2$ его дробная часть $\{b\}$, то

$$\varepsilon_x = (-1)^{[2ax/p]}.$$

б) Так как для любого $x, 1 \le x \le p_1 = (p-1)/2$, числа ax и $\varepsilon_x r_x$ равноостаточны при делении на p, то и числа

$$a \cdot 2a \cdots p_1 a = a^{p_1} p_1! \text{ и } r_1 \ldots r_{p_1} \varepsilon_1 \cdots \varepsilon_{p_1} = \varepsilon_1 \cdots \varepsilon_{p_1} p_1!$$

тоже (учитываем, что числа r_x попарно различны, так как иначе $a(x \pm y)$ при разных x и y было бы кратно p, что невозможно, так как a не кратно p, и $0 < |x \pm y| < p$, поэтому последовательность $r_1, \ldots, r_p$ является перестановкой последовательности $1, \ldots, p_1$). Значит, числа a^{p_1} и $\varepsilon_1 \cdots \varepsilon_{p_1}$ также равноостаточны, так как иначе число $p_1!(a^{p_1} - \varepsilon_1 \cdots \varepsilon_{p_1})$ не было бы кратным p. Согласно 6.59 число a^{p_1} равноостаточно с $\left(\frac{a}{p}\right)$, следовательно, $\left(\frac{a}{p}\right)$ равноостаточно с произведением

$$\varepsilon_1 \cdots \varepsilon_{p_1} = (-1)^s,$$

где

$$s = \sum_{x=1}^{(p-1)/2} [2ax/p]$$

(используем пункт а). Но так как рассматриваемые числа равны ± 1, то их равноостаточность возможна только при их равенстве.

6.62. Заметьте, что для любого нечетного a согласно 6.59 справедливы равенства (учитываем, что тогда $a + p$ — четно)

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{(a+p)/2}{p}\right) =$$

$$= \left(\frac{2}{p}\right)^2 \left(\frac{(a+p)/2}{p}\right) = \left(\frac{(a+p)/2}{p}\right).$$

Согласно 6.60 последний символ равен $(-1)^s$, где

$$s = \sum_{x=1}^{(p-1)/2} [(a+p)x/p] = \sum_{x=1}^{(p-1)/2} [ax/p] + \sum_{x=1}^{(p-1)/2} x =$$

$$= \sum_{x=1}^{(p-1)/2} [ax/p] + (p^2-1)/8.$$

Подставив в полученные равенства $a = 1$, найдите, что

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}.$$

6.63. Утверждение следует из формулы задачи 6.61 б) и теоремы 1.12.

6.64. Сначала рассмотрим случай одинаковых по длине периодов и предп
риодов обеих дробей. Пусть

$$a = 0, a_1 \dots a_k(A_1 \dots A_t) = 0, a_1 \dots a_k + \sum_{i=0}^{\infty} 0, A_1 \dots A_t \cdot 10^{-it-k},$$

$$b = 0, b_1 \dots b_k(B_1 \dots B_t) = 0, b_1 \dots b_k + \sum_{i=0}^{\infty} 0, B_1 \dots B_t \cdot 10^{-it-k}.$$

Очевидно, если

$$0, a_1 \dots a_k + 0, b_1 \dots b_k = c_0, c_1 \dots c_k,$$

$$0, A_1 \dots A_t + 0, B_1 \dots B_t = 0, C_1 \dots C_t,$$

то

$$a + b = c_0, c_1 \dots c_k + \sum_{i=0}^{\infty} 0, C_1 \dots C_t \cdot 10^{-it-k}.$$

Если же

$$0, A_1 \dots A_t + 0, B_1 \dots B_t \geq 1,$$

то для некоторой дроби $0, C_1 \dots C_t$ имеем

$$0, A_1 \dots A_t + 0, B_1 \dots B_t = 0, C_1 \dots C_t + 0, \underbrace{9 \dots 9}_{t},$$

а так как $\sum\limits_{i=0}^{\infty} 0, \underbrace{9 \dots 9}_{t} \cdot 10^{-it} = 1$, то

$$a + b = c_0, c_1 \dots c_k + \sum_{i=0}^{\infty} (0, C_1 \dots C_t + 0, \underbrace{9 \dots 9}_{t}) \cdot 10^{-it-k}$$

$$= c_0, c_1 \dots c_k + 0, \underbrace{0 \dots 01}_{k} + \sum_{i=0}^{\infty} 0, C_1 \dots C_t 10^{-it-k}.$$

Случай вычитания рассматривается аналогично: если

$$0, A_1 \dots A_t - 0, B_1 \dots B_t < 0,$$

то для некоторой дроби $0, C_1 \dots C_t$ справедливо равенство

$$0, A_1 \dots A_t - 0, B_1 \dots B_t = 0, C_1 \dots C_t - 0, \underbrace{9 \dots 9}_{t},$$

а так как $\sum_{i=0}^{\infty} 0,\underbrace{9\ldots9}_{t}\cdot 10^{-it} = 1$, то

$$a - b = c_0, c_1 \ldots c_k + \sum_{i=0}^{\infty}(0, C_1 \ldots C_t - 0,\underbrace{9\ldots9}_{t})\cdot 10^{-it-k}.$$

$$= c_0, c_1 \ldots c_k - 0,\underbrace{0\ldots01}_{k} + \sum_{i=0}^{\infty} 0, C_1 \ldots C_t 10^{-it-k}.$$

Теперь можно рассматривать обе дроби как дроби с одинаковыми по длине предпериодами и одинаковыми по длине периодами (длина предпериода тогда будет равна максимуму длин их минимальных предпериодов, а длина периода — НОК длин их минимальных периодов) и применить предыдущие рассуждения. Согласно им, одним из периодов суммы и разности будет НОК длин их минимальных периодов. Но минимальный период всегда является делителем любого другого периода той же дроби. Если бы это было неверно, то, укладывая в большом периоде минимальный период до тех пор, пока это возможно, мы получили бы: так как периодический остаток дроби не меняется при сдвигах на большой и минимальный периоды, то он не меняется и при сдвиге на часть большого периода, не вошедшую в уложенные в него минимальные, значит дробь имеет еще меньший период, что невозможно по предположению.

6.65. Для краткости обозначаем НОК u и v через $[u, v]$, а НОД — через (u, v). Предположим, что $k_2 \geq k_1$, и сложим дроби

$$\frac{1}{10^{k_1}(10^{t_1} - 1)},$$

применяя для нахождения НОК знаменателей формулу

$$(10^{t_1} - 1, 10^{t_2} - 1) = 10^{(t_1, t_2)} - 1,$$

вытекающую из одной из задач следующего параграфа. Получим дробь со знаменателем

$$10^{k_2}(10^{t_1} - 1)(10^{t_2} - 1)/(10^{(t_1,t_2)} - 1)$$

и с числителем

$$10^{k_2-k_1}(10^{t_2} - 1)/(10^{(t_1,t_2)} - 1) + (10^{t_1} - 1)/(10^{(t_1,t_2)} - 1).$$

Последняя цифра числителя равна 1 при $k_2 > k_1$ и 2 при $k_2 = k_1$, поэтому числитель не делится ни на 2, ни на 5. Так как числа

$$n_1 = (10^{t_1} - 1)/(10^{(t_1,t_2)} - 1), n_2 = (10^{t_2} - 1)/(10^{(t_1,t_2)} - 1)$$

не имеют общих делителей, то числитель не имеет общих делителей ни с n_1, ни с n_2, значит, после сокращения рассматриваемой дроби ее знаменатель будет кратен числу $n = 10^{k_2} n_1 n_2$. Эта дробь представляется десятичной дробью с периодом t и предпериодом k, если и только если $10^k(10^t - 1)$ делится на n, причем k и t — наименьшие натуральные числа, удовлетворяющие этому условию. Значит, $k = k_2 = \max(k_1, k_2)$ и числа n_1 и n_2 делят число $10^t - 1$.

Предположим, что $t_1 > t_2 > (t_1, t_2)$. Заметим, что согласно 6.22 для любого m, делящего $10^v - 1$, число v делится на наименьшее u, для которого $10^u - 1$

кратно m. Отсюда следует,что наименьшее u, такое, что $10^u - 1$ кратно n_i, рав t_i, так как

$$n_i = (10^{t_i} - 1)/(10^{(t_1,t_2)} - 1) \geq (10^{t_i} - 1)/(10^{t_i/2} - 1) > 10^{t_i/2} - 1,$$

и поэтому t делится на t_i, а значит, t не меньше $[t_1, t_2]$. Если же $t_2 = (t_1, t_2)$, все равно $t \geq t_1 = [t_1, t_2]$. Случай вычитания дробей рассматривается аналогичн

6.66. Пусть периоды дробей r, s и $r + s$ равны m, n, t, а предпериоды равн τ, δ, d. Из 6.64 следует, что

$$t \mid [m, n], d \leq \max(\delta, \tau).$$

Применяя 6.64 к равенству $s = (r + s) - r$, получите, что

$$n \mid [m, t], \delta \leq \max(d, \tau),$$

а применяя 6.64 к равенству $r = (r + s) - s$, получите, что

$$m \mid [n, t], \tau \leq \max(d, \delta).$$

Если $\delta \neq \tau$, то из этих соотношений следует равенство $d = \max(\delta, \tau)$.

Пусть числа p_i — суть все простые, входящие в разложения чисел m и в различных степенях α_i и $\beta_i, \alpha_i \neq \beta_i, 1 \leq i \leq k$, тогда

$$]m, n[= p_1^{\gamma_1} \dots p_k^{\gamma_k},$$

где $\gamma_i = \max(\alpha, \beta), 1 \leq i \leq k$. Обозначим через δ максимальный показатель степени p_i, делящей t. Тогда из полученных соотношений следует, что

$$\beta_i \leq \max(\alpha_i, \delta_i), \ \alpha_i \leq \max(\beta, \delta_i),$$

а так как $\alpha_i \neq \beta_i$, то отсюда имеем $\delta_i \geq \max(\alpha_i, \beta_i) = \gamma_i$, и поэтому

$$t \mid]m, n[= p_1^{\gamma_1} \cdots p_k^{\gamma_k}.$$

Для разности дробей утверждение доказывается аналогично.

6.67. Пусть числа p_i — суть все простые, входящие в разложения чисел m и n в различных степенях α_i и $\beta_i, \alpha_i \neq \beta_i, 1 \leq i \leq k$, тогда

$$]m, n[= p_1^{\gamma_1} \cdots p_k^{\gamma_k}, m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} u, n = p_1^{\beta_1} \cdots p_k^{\beta_k} u,$$

где $\gamma_i = \max(\alpha_i, \beta_i), \alpha_i, \beta_i, u$ не делится на $p_i, 1 \leq i \leq k$. Положим

$$m' = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, n' = p_1^{\beta_1} \cdots p_k^{\beta_k},$$

тогда

$$m = m'u, \ n = n'u, \ [m, n] =]m, n[u = [m', n']u, \ (m', u) = (n', u) = 1.$$

Так как $]m, n[\mid t \mid [m, n]$, то

$$t =]m, n[u', \ u' \mid u, \ (m', u') = (n', u') = 1.$$

Рассмотрим дроби

$$a = 1/(10^u - 1) + 1/(10^{u'n'} - 1) \quad \text{и} \quad b = 1/(10^{m'} - 1) - 1/(10^u - 1)$$

(если последняя из них отрицательна, то превратим ее без изменения периода в положительную, прибавив единицу). Тогда

$$a+b=1/(10^{u'n'}-1)+1/(10^{m'}-1)$$

(или на единицу больше). Согласно 6.65 периоды дробей $a, b, a+b$ равны соответственно

$$[u, n'u']=n'u=n, [m', u]=m'u=m, [m', n'u']=[m', n']u'=t.$$

Добавив к чисто периодическим дробям a и b подходящие предпериоды длины d, можно получить у суммы предпериод любой заданной длины $\delta \leq d$, если выбрать их так, чтобы сумма предпериодов заканчивалась на последние $d-\delta$ цифр периода дроби $a+b$, но последние $d-\delta+1$ цифр периода дроби $a+b$ уже не совпадает с последними $d-\delta+1$ цифрами суммы предпериодов.

6.68. Используйте 6.7, 6.8 и указание к 6.24.

6.69. Воспользуйтесь указанием к 6.68.

6.70. Пусть даны две дроби с предпериодами k_i и периодами t_i. Используя задачу 6.8, можно считать, что они имеют знаменатели $10^{k_1}(10^{t_1}-1)$. Перемножая знаменатели и используя опять задачу 6.8, получаем, что предпериод произведения дробей удовлетворяет неравенству $k \leq k_1+k_2$, а период не превосходит наименьшего натурального числа t, такого, что 10^t-1 делится на $(10^{t_1}-1)(10^{t_2}-1)$. Из утверждения задачи 6.23 следует, что $t=t_1 n$, где n целое, так как 10^t-1 делится на $10^{t_1}-1$, а значит, t делится на t_1. Тогда согласно известному тождеству (формуле суммирования геометрической прогрессии)

$$10^t-1=(10^{t_1}-1)\left(1+10^{t_1}+\ldots+10^{(n-1)t_1}\right),$$

и поэтому число $1+10^{t_1}+\ldots+10^{(n-1)t_1}$ должно делится на $10^{t_2}-1$.

Рассмотрим последовательность $r_1, r_2, r_3, \ldots$ остатков от деления чисел последовательности $t_1, 2t_1, 3t_1, \ldots$ на число t_2. Согласно задаче 6.23 последовательность остатков от деления чисел $10^{t_1}, 10^{2t_1}, 10^{3t_1}, \ldots$ на число $a=10^{t_2}-1$ есть $10^{r_1}, 10^{r_2}, 10^{r_3}, \ldots$

Докажем,что последовательность $r_1, r_2, r_3, \ldots$ периодическая с длиной периода $d=t_2/(t_1, t_2)$ и ее период $r_1, r_2, r_3, \ldots r_d$ состоит из всех различных чисел из промежутка от 0 до t_2-1, делящихся на $b=(t_1, t_2)$, и заканчивается нулем. Последнее очевидно, так как dt_1 делится на t_2, откуда с помощью задачи 6.23 следует также периодичность с периодом d. Делимость остатков $r_1, \ldots, r_d$ на b следует из того, что согласно задаче 6.23 числа $10^{nt_1}-1$ и $10^{t_2}-1$ делятся на $10^{(t_1, t_2)}-1$, а, значит, и число $10^{r_n}-1$ тоже, откуда, опять в силу 6.23, имеем, что r_n делится на число $(t_1, t_2)=b$.

Остается проверить, что все остатки разные, откуда вытекает также, что d — минимальный период. Допустим противное, например $r_i=r_j$, тогда число $(j-i)t_1$ делится на t_2 и $0<j-i<d$, что противоречит известному следствию основной теоремы арифметики.

Из доказанного имеем, что последовательность остатков от деления чисел последовательности $10^{t_1}, 10^{2t_1}, 10^{3t_1}, \ldots$ на число a будет периодической с длиной периода $d=t_2/(t_1, t_2)$ и ее период $10^{r_1}, 10^{r_2}, \ldots, 10^{r_n}$ состоит из переставленных в каком-то порядке чисел

$$1, 10^b, 10^{2b}, \ldots, 10^{(d-1)b}.$$

Поэтому остаток от деления числа

$$s=1+10^{t_1}+\cdots+10^{(n-1)t_1}$$

на a равен при $n = dm$ остатку от деления на a числа

$$m\left(1 + 10^b + 10^{2b} + \cdots + 10^{(d-1)b}\right) = m\frac{10^{db} - 1}{10^b - 1} = m\frac{10^{t_2} - 1}{10^b - 1}.$$

Следовательно, при $n = (10^b - 1)d$ число s делится на a, а при меньш натуральных n — нет. Вспоминая доказанное выше, выводим отсюда, ч наименьшее натуральное t, при котором число $10^t - 1$ делится на чис $\left(10^{t_1} - 1\right)\left(10^{t_2} - 1\right)$, есть

$$t_1 n = (10^b - 1)dt_1 = (10^b - 1)t_1 t_2/(t_1, t_2) = [t_1, t_2]\left(10^{(t_1,t_2)} - 1\right),$$

откуда и следует вторая верхняя оценка задачи.

Рассмотрим теперь дроби $1/(10^{k_i}(10^{t_i} - 1)), i = 1, 2$. Из утверждений задач 6.8 следует, что предпериод их произведения равен $k_1 + k_2$, а период рав минимальному натуральному t, такому, что $10^t - 1$ делится на $\left(10^{t_1} - 1\right)\left(10^{t_2} - 1\right)$ Но было доказано, что таким числом является

$$t = [t_1, t_2]\left(10^{(t_1,t_2)} - 1\right).$$

6.72. Доказательство основано на тождестве

$$(1 + km/p)(1 + k'm/p) \bmod m = 1 + ((k + k') \bmod p)m/p \bmod m.$$

Из него вытекает изоморфизм этой группы с циклической группой порядка p

6.73. Если $a^{m-1} \bmod m \neq 1$, то $(as)^{m-1} \bmod m \neq s^{m-1} = 1$ при $s \in S$, значит $as \bmod m$ не принадлежит S.

Пусть теперь $a^{m-1} \bmod m = 1$ и при некотором простом делителе p числа m порядок числа a по $\bmod p$ равен $p-1$ и также при любом целом k $a^k \bmod m \neq -1$ Если

$$a^{(m-1)2^{-i}} \bmod m = 1,$$

то

$$a^{(m-1)2^{-i}} \bmod p = 1,$$

значит, $(m-1)2^{-i}$ делится на $p-1$, поэтому $i < r$, так как t — нечетно, а $p-$ — четно, и значит, $a^t \bmod m \neq 1$, и согласно теореме Ферма

$$s^{(m-1)2^{-j}} \bmod p = 1,$$

и, следовательно,

$$s^{(m-1)2^{-j}} \bmod m \neq -1$$

при всех $j, 0 \leq j \leq i$, а так как $s \in S$, то из последнего утверждения имеем, что

$$s^{(m-1)2^{-j}} \bmod m = 1, 0 \leq j \leq i$$

и

$$s^{(m-1)2^{-i-1}} \bmod m = \pm 1.$$

Можно выбрать $i \geq 0$ так, что $a^{(m-1)2^{-j}} \bmod m = 1$ при всех $j, 0 \leq j \leq i$, но $a^{(m-1)2^{-i-1}} \bmod m \neq 1$. Тогда имеем, что

$$(as)^{(m-1)2^{-j}} \bmod m = s^{(m-1)2^{-j}} \bmod m = 1$$

при всех $j, 0 \le j \le i$, но

$$(as)^{(m-1)2^{-i-1}} \bmod m = \pm a^{(m-1)2^{-i-1}} \bmod m \neq \pm 1,$$

так как

$$a^{(m-1)2^{-i-1}} \bmod m \neq 1 \text{ и } a^k \bmod m \neq -1$$

при всех k. Доказанное означает, что $as \bmod m$ не принадлежит S.

6.74. Пусть $c \in Sa \cap Sb$. Тогда $cb^{-1} \bmod m \in Sab^{-1} \cap S$.

6.75. Рассмотрим определенную в задаче 6.72 подгруппу G. Так как p делит m, то оно делит $m-1$, и значит согласно этой задаче и элементарному утверждению теории групп для любого неединичного $a \in G$ имеем $a^{m-1} \neq 1$, значит, $a \in A$ и согласно задаче 6.73 множество $S \cap Sa$ пусто. Применяя предыдущую задачу, отсюда выводим, что все множества $Sg, g \in G$, попарно не пересекаются, и поэтому их объединение состоит из pn элементов, где n— число свидетелей, а так как объединение содержится в $\mathbb{Z}_m^*$, то $n \le \varphi(m)/p$, где $\varphi(m)$ — число элементов в $\mathbb{Z}_m^*$.

6.76. Применяя китайскую теорему об остатках и теорему о первообразном корне, находим такие числа $a_i \in \mathbb{Z}_m^*$, что $a_i \bmod m/p_i = 1$ и порядок вычета $a_i \bmod p_i = p_i - 1$. Так как при любом k имеем $a_i^k \bmod m/p_j = 1$ и, следовательно, $a_i^k \bmod m \neq -1$, и $a_i^k \bmod m = 1$ согласно китайской теореме тогда и только тогда $a_i^k \bmod p_i = 1$, т. е. при k кратном $p_i - 1$, значит, a_i— лжесвидетель и аналогично a_i^{-1} — тоже. Заметим еще, что для произведения $a = a_1 a_2 \bmod m$ согласно китайской теореме равенство $a^k \bmod m = 1$ равносильно системе равенств $a_i^k \bmod p_i = 1$, и значит, делимости k на $p_i - 1, i = 1, 2$. Из задачи 4.49 тогда следует, что $a^{m-1} \bmod m \neq 1$, и, значит, $a \in A$. Аналогично проверяется, что $a_1 a_2^{-1} \in A$. Применяя задачу 6.73 к множествам S, Sa_1, Sa_2, Sa, замечаем, что они попарно не пересекаются и равномощны, значит каждое из них содержит не более четверти элементов из $\mathbb{Z}_m^*$.

6.77. Как и в указании к предыдущей задаче, находим числа $a_i \in \mathbb{Z}_m^*$ такие, что $a_i \bmod m/p_i = 1$ и порядок $a_i \bmod p_i = p_i - 1, i = 1, 2$. Так как тогда $a_i \bmod p_3 = 1$, то

$$a = a_1 a_2 \bmod p_3 = 1, b = a_1 a_2^{-1} \bmod p_3 = 1,$$

и при любом k, как и в решении предыдущей задачи, видим, что

$$a_i^k \bmod m \neq -1, a^k \bmod m \neq -1, b^k \bmod m \neq -1,$$

а также что порядок числа a по $\bmod p_1$ такой же, как и у a_1, т. е. $p_1 - 1$, и тоже самое верно для числа b. Значит $a_i, a, b \in A$, и в силу задачи 6.73 множества S, Sa_1, Sa_2, Sa попарно не пересекаются. Заканчивается доказательство так же, как и в предыдущей задаче.

§ 7. АЛГОРИТМ ЕВКЛИДА, ЦЕПНЫЕ ДРОБИ И ЧИСЛА ФИБОНАЧЧИ

Для выяснения, является ли данная дробь a/b несократимой, или ее можно сократить, заменив на равную дробь с меньшими, чем у исходной дроби, числителем и знаменателем, имеется замечательный

способ, называемый теперь алгоритмом Евклида. Этот алгорит находит (a, b), после чего остается разделить a и b на (a, b). Его работ заключается в последовательном выполнении деления с остатком сначала делим b на a и получаем частное a_1 и остаток r_1, пото делим a на r_1 и получаем частное a_2 и остаток r_2, и т. д., пок не получится остаток $r_n = 0$. Результаты делений можно записать в виде равенств:

$$b = aa_1 + r_1, a = r_1a_2 + r_2, r_1 = r_2a_3 + r_3, \ldots, r_{n-2} = r_{n-1}a_n.$$

Свой знаменитый алгоритм Евклид придумал для решения задачи о соизмеримости двух отрезков. **Общей мерой отрезков с длинами** l_1 **и** l_2 называется такой отрезок длины l, который можно уложить без остатка как в первом отрезке (очевидно, ровно l_1/l раз), так во втором (соответственно l_2/l раз). В этой интерпретации алгорит заключается в следующем. Меньший отрезок l_2 укладывается большем l_1 максимально возможное число, скажем a_1 раз, после че остается отрезок длины $l_1 - a_1l_2$, которую обозначим l_3. Отрезок укладывается, скажем, a_2 раз в отрезке l_2, и получается в остат отрезок l_4. Потом отрезок l_4 укладывается a_3 раз в отрезке l_3, получается в остатке отрезок l_5 и т. д. Как утверждает Д.Кну во втором томе своей энциклопедии "Искусство программирования" сам Евклид индукцию не проводил, а повторил шаг алгоритма тр раза. Работу алгоритм заканчивает на том шаге, скажем с номером когда полученный на предыдущем шаге отрезок l_{n+1} укладывается н отрезке l_n ровно $a_n = l_n/l_{n+1}$ раз. Тогда в качестве l берется отрезо l_{n+1}. В современной терминологии число l называют **наибольшим общим делителем** чисел l_1 и l_2 и обозначают (l_1, l_2).

7.1. Докажите, что $(b, a) = (a, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$.

В этой задаче указана связь между получающимися остатками Связь между частными появляется в следующей задаче.

7.2. Докажите равенство

$$\frac{a}{b} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n}}}.$$

Полученная запись называется **непрерывной или цепной дробью.**

7.3. Проверьте, что произвольную (не обязательно правильную дробь) можно представить в виде цепной дроби (возможно, $a_0 = 0$)

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n}}}.$$

Запись числа в виде цепной дроби неоднозначна, так как

$$\frac{1}{a_n} = \frac{1}{a_n - 1 + \dfrac{1}{1}}.$$

Чтобы сделать ее однозначной, далее используем только запись, в которой последний элемент $a_n \neq 1$. Будем использовать также следующую сокращенную запись цепной дроби:

$$a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\cdots\frac{1}{+a_n}.$$

Если выполнить все действия, указанные в цепной дроби, то ее можно преобразовать в обыкновенную; выражение ее числителя и знаменателя через $a_0, a_1, \ldots, a_n$ обозначим

$$[a_0, \ldots, a_n] \quad \text{и} \quad [a_1, \ldots, a_n].$$

7.4. Выражение $[a_0, \ldots, a_n]$ представляет собой многочлен с переменными $a_0, \ldots, a_n$. Докажите, что

$$[a_0, \ldots, a_n] = a_0[a_1, \ldots, a_n] + [a_2, \ldots, a_n].$$

Можно считать, что это равенство справедливо и при $n = 1$, если последней скобке в этом случае приписать значение 1.

7.5. *(Правило Эйлера)* Докажите индукцией по n, что многочлен $[a_0, \ldots, a_n]$ можно получить следующим образом: берем произведение всех элементов, затем всевозможные произведения, которые можно получить, опустив какую-нибудь пару соседних элементов, затем из этих произведений получаем новые, выбрасывая произвольным образом пары соседних элементов и т. д., и наконец суммируем все различные из получившихся произведений (если $n + 1$ четно, то на последнем шаге получается "пустое" произведение, не содержащее вообще сомножителей; как принято, его значение по определению полагаем равным 1).

7.6. Докажите, что

$$[a_0, \ldots, a_n] = [a_n, \ldots, a_0],$$

т.е. при изменении порядка элементов на противоположный числитель дроби не меняется.

7.7. Докажите, что

$$[a_0, \ldots, a_n] = a_n[a_0, \ldots, a_{n-1}] + [a_0, \ldots, a_{n-2}].$$

Дробь, образованную первыми k этажами назовем **k-й подходящей дробью** для исходной дроби. Ее величина изображается обыкновенной дробью

$$\frac{[a_0, \ldots, a_k]}{[a_1, \ldots, a_k]},$$

которую для краткости далее обозначаем p_k/q_k.

Дробь

$$\frac{[a_{k+1}, \ldots, a_n]}{[a_{k+2}, \ldots, a_n]},$$

назовем **k-м остатком** и обозначим r_k.

7.8. Проверьте, что

$$\frac{[a_0, \ldots, a_n]}{[a_1, \ldots, a_n]} = \frac{[a_0, \ldots, a_{k-1}, r_k]}{[a_1, \ldots, a_{k-1}, r_k]}.$$

7.9. Докажите, что при $k \geq 2$ справедливы равенства

$$p_k = a_k p_{k-1} + p_{k-2}, q_k = a_k q_{k-1} + q_{k-2}.$$

7.10. Докажите равенства

$$\frac{p_{k-1}}{q_{k-1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k q_{k-1}}, \frac{p_{k-2}}{q_{k-2}} - \frac{p_k}{q_k} = \frac{(-1)^{k-1} a_k}{q_k q_{k-2}}.$$

7.11. Докажите равенства $(p_k, q_k) = (p_k, p_{k-1}) = (q_k, q_{k-1}) = 1$.

7.12. Докажите, что

$$\frac{[a_0, \ldots, a_n]}{[a_1, \ldots, a_n]} = \frac{p_{k-1} r_k + p_{k-2}}{q_{k-1} r_k + q_{k-2}}.$$

7.13. Докажите равенства

$$\frac{p_k}{p_{k-1}} = \frac{[a_k, \ldots, a_0]}{[a_{k-1}, \ldots, a_0]}, \qquad \frac{q_k}{q_{k-1}} = \frac{[a_k, \ldots, a_1]}{[a_{k-1}, \ldots, a_1]}.$$

7.14. Докажите, что если дробь

$$a_0 + \frac{1}{a_1 +} \frac{1}{a_2 +} \cdots \frac{1}{+ a_n}$$

симметрическая, т.е. $a_n = a_0, a_1 = a_{n-1}, \ldots$, то справедливо равенство

$$p_{n-1} = q_n.$$

Следующий цикл задач посвящен числам Фибоначчи.

7.15. Последовательность чисел $\{F_n\}$, определенная равенствами $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$, $n = 3, 4, \ldots$, называется **последовательностью Фибоначчи**. Проверьте, что n-этажная цепная дробь

$$1 + \frac{1}{1+} \cdots \frac{1}{+1}$$

равна F_{n+2}/F_{n+1}.

7.16. Докажите, что число одночленов во многочлене $[x_1, \ldots, x_n]$ равно F_{n+1} и что для любой подходящей дроби p_k/q_k справедливо неравенство $q_k \geq F_{k+1}$.

7.17. Докажите, что среди всех правильных дробей n/F_k наибольшую по высоте цепную дробь имеет F_{k-1}/F_k.

7.18. Докажите формулу Бине

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}, \text{ где } \varphi = (\sqrt{5}+1)/2$$

— так называемое золотое сечение, и проверьте, что F_n — ближайшее целое к числу $\varphi^n/\sqrt{5}$, а также, что

$$F_n \leq m \Longleftrightarrow n \leq [\log_\varphi (\sqrt{5}(m + 1/2))].$$

7.19*. *(Ламе)* Докажите, что наибольшее число делений в алгоритме Евклида нахождения (a, b) не превосходит

$$[\log_\varphi (\sqrt{5}(\max(a, b) + 1/2))] - 1.$$

Убедитесь, что оценка точная.

7.20. Докажите, что

$$F_{n+m} = F_m F_{n+1} + F_{m-1} F_n, \; F_{m+1} F_n - F_m F_{n+1} = (-1)^m F_{n-m}.$$

7.21*. Докажите неравенство

$$[x_1, \ldots, x_n] \leq F_{1+x_1+\cdots+x_n},$$

и проверьте, что при $n \geq 2$ равенство возможно лишь когда

$$x_1 \leq 2, x_n \leq 2, x_2 = \cdots = x_{n-1} = 1, \text{ а при } n = 1 \text{ еще и когда } x_1 = 3.$$

7.22*. Докажите, что среди всех несократимых правильных дробей вида n/F_k наименьшую сумму элементов соответствующей цепной дроби имеют только F_{k-2}/F_k и F_{k-1}/F_k. Докажите, что сумма элементов цепной дроби для любого числа m/n, где $(m, n) = 1, m < n$, не меньше

$$[\log_\varphi (\sqrt{5}(n - 1/2))],$$

причем это неравенство бесконечно часто обращается в равенство.

7.23. Докажите, что если $n \mid m$, то $F_n \mid F_m$.

7.24. Докажите, что $(F_n, F_{n+1}) = 1$.

Если продолжить последовательность Фибоначчи в "отрицательную" сторону с сохранением равенства $F_n + F_{n+1} = F_{n+2}$, то будет выполняться равенство $F_{-k-1} = (-1)^k F_k, F_{-1} = 1, F_0 = 0$.

Следующая задача обобщает обе предыдущие.

7.25*. *(Люка)* Докажите, что $(F_n, F_m) = F_{(n,m)}$.

7.26. Докажите, что разложение числа F_{n-3}/F_n в цепную дробь имеет вид

$$\frac{1}{4+} \cdots \frac{1}{+4+a_k},$$

где $k = 1+m, a_k = 0$, если $n = 3m$, $a_k = 1/3$, если $n = 3m+1$, $a_k = 1/$ если $n = 3m+2$.

7.27*. Разложите в цепную дробь число F_{n-5}/F_n.

7.28*. Докажите, что

$$\frac{F_{(2k+1)m}}{F_{(2k+1)(m+1)}} = \frac{1}{a+} \cdots \frac{1}{+a},$$

где число этажей в дроби равно m, а число $a = F_{2k+2} + F_{2k}$.

7.29. Докажите, что 2^{2k} делит сумму

$$\sum_{i=0}^{k} \binom{2k+1}{2i} 5^i,$$

где $\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{1\cdot 2\ldots k}$ — биномиальный коэффициент.

7.30. Докажите, что для цепной дроби $\frac{1}{a+} \cdots \frac{1}{+a}$ справедливо тождество

$$p_n^2 + p_{n+1}^2 = p_{n-1}p_{n+1} + p_n p_{n+2}.$$

7.31. Докажите, что при $k \geq 1$

$$\frac{a^{F_{k+2}} - 1}{a^{F_{k+1}} - 1} = a^{F_k} + \frac{1}{a^{F_{k-1}}+} \cdots \frac{1}{+a^{F_0}},$$

где $F_0 = 0$.

Следующий цикл задач посвящен делимости чисел Фибоначчи.

7.32. Пусть первое число Фибоначчи, делящееся на m, есть F. Докажите, что $m \mid F_n$ тогда и только тогда, когда $k \mid n$.

7.33. Докажите, что

$$2 \mid F_n \iff 3 \mid n,\ 3 \mid F_n \iff 4 \mid n,\ 4 \mid F_n \iff 6 \mid n,$$

$$5 \mid F_n \Longleftrightarrow 5 \mid n,\ 7 \mid F_n \Longleftrightarrow 8 \mid n,\ 8 \mid F_n \Longleftrightarrow 6 \mid n \Longleftrightarrow 4 \mid F_n.$$

7.34. *(С.-Петербург, 92)* Докажите, что ни одно из чисел Фибоначчи не является степенью семерки.

7.35. Докажите, что число $F_{2n}/F_n = F_n + 2F_{n-1}$ делится на 2, но не на 4, если F_n, кратно 4 и F_{2n}/F_n делится на 4, но не на 8, если F_n четно, но не кратно 4.

7.36. а) Докажите, что при $k \geq 3$ справедлива эквивалентность

$$2^k \mid F_n \Longleftrightarrow 3 \cdot 2^{k-2} \mid n.$$

б) Докажите, что при $k \geq 3$ и $m = 3 \cdot 2^{k-2}$

$$2^k \mid F_{m+1} - 1 - 2^{k-1}.$$

Обозначим $d(n)$ — наименьший номер числа Фибоначчи, кратного n. Предыдущие задачи позволяют вычислить $d(n)$ при некоторых n. Обозначим $t(n)$ такое наименьшее t, что $n \mid F_t$ и $n \mid F_{t+1} - 1$.

7.37. Докажите что последовательность остатков от деления чисел Фибоначчи на n — периодическая, с наименьшим периодом $t(n)$ и $d(n) \mid t(n)$.

7.38. *(Москва, 58)* Докажите , что $t(n) \leq n^2$.

7.39*. Докажите, что при нечетном $d(n)$ справедливо равенство $4d(n) = t(n)$, при четном $d(n)$ либо справедливо равенство $2d(n) = t(n)$, либо равенство $d(n) = t(n)$, причем тогда при простом n число $d(n)$ не кратно 4.

7.40. Докажите следующий вариант формулы Бине

$$2^{n-1}F_n = \sum_{i=0}^{[(n-1)/2]} \binom{2i+1}{n} 5^i.$$

7.41*. Докажите, что при простом p, не равном 5, число F_p при делении на p равноостаточно с символом Лежандра $\left(\frac{5}{p}\right)$.

7.42. Докажите равенства:

а) *Кеплер-Кассини* $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$;

б) $F_{n+k}F_{m-k} - F_nF_m = (-1)^n F_{m-n-k}F_k$.

7.43. Докажите, что при простом p, не равном 5, либо F_{p-1}, либо F_{p+1} кратно p.

7.44*. Докажите, что при простом p вида $5k \pm 1$ число $t(p)$ кратно $p-1$, а если к тому же p имеет вид $4m+3$, то $d(p) = t(p)$; при простом p вида $5k \pm 2$ справедливо, что $t(p) \mid 2(p+1)$ и $d(p) \mid (p+1)$, и $2d(p) = t(p)$ при четном $d(p)$ и $4d(p) = t(p)$ при нечетном $d(p)$, причем в последнем случае $d(p) \mid (p+1)/2$.

7.45. Если числа n_i попарно взаимно просты, то при $n = n_1 \dots$

$$d(n) = \text{НОК}(d(n_1), \dots, d(n_m)), t(n) = \text{НОК}(t(n_1), \dots, t(n_m)).$$

Следующая задача использовалась Ю. В. Матиясевичем в е знаменитом доказательстве алгоритмической неразрешимости десят проблемы Гильберта[1)]

7.46. Докажите, что

$$\frac{F_{mn}}{F_n} - mF_{n+1}^{m-1}$$

кратно F_n^2 и что $F_{mn+1} - F_{n+1}^m$ кратно F_n^2.

7.47. Пусть $p \mid F_n$, и p — нечетное простое, тогда F_{mn}/F_n крат p тогда и только тогда, когда $p \mid m$ и

$$\frac{F_{pn}}{F_n} - p$$

кратно p^2.

7.48. Докажите, что при простом нечетном p имеем

$$d(p^n) = p^{n-m}d(p), t(p^n) = p^{n-m}t(p),$$

где m — такое наибольшее число, что $t(p^m) = t(p)$.

Возможно, что всегда $m = 1$.

7.49*. Докажите, что $t(n) \leq 4n, d(n) \leq 2n$, причем равенства в можны лишь для $n = 2 \cdot 3^a$. Если в разложение нечетного n вход не менее трех разных простых чисел, или n четно и еще содержит менее четырех простых множителей, или n кратно 4 и еще содерж не менее трех простых множителей, то $t(n) < n$.

Следующее утверждение усиливает утверждение задачи 7.46.

7.50. Докажите, что

$$F_{mn+1} - F_{n+1}^m - \frac{m(m-1)}{2}F_{n+1}^{m-2}F_n^2$$

кратно F_n^4.

7.51*. Докажите, что для любого нечетного простого p найдут целые числа a_p и b_p, меньшие p, и такие, что при любом натурально n и $t = t(p^n)$ справедливо, что $F_t - p^n a_p$ кратно p^{n+1} и $F_{t+1} - 1 - p^n$ кратно p^{n+1}.

Следующая задача обобщает предыдущую.

[1)] Ю. В. Матиясевич доказал, в частности, что не существует алгоритма, расп знающего по любому алгебраическому уравнению с целыми коэффициентами име ли оно решение в целых же числах.

7.52*. Докажите, что для любого нечетного простого p и любых натуральных k и m число

$$F_{k+tm} - F_k - p^n m(a_p F_{k-1} + b_p F_k)$$

кратно p^{n+1}.

7.53*. Докажите, что записи чисел Фибоначчи в троичной системе счисления могут оканчиваться на любую комбинацию цифр.

7.54*. Докажите, что записи чисел Фибоначчи в пятеричной системе счисления могут оканчиваться на любую комбинацию цифр.

7.55. Для двоичной и десятичной систем счисления и вообще для любой n-ичной системы, где n — четно, аналоги двух предыдущих задач не верны. Если n кратно простому числу вида $5k \pm 1$ или такому простому p вида $5k \pm 2$, что $d(p) \leq (p+1)/2$, то предыдущее утверждение также верно.

В предпоследнем параграфе задачника будет, в частности, доказано, что начинаться числа Фибоначчи могут с любой комбинации цифр в любой системе счисления.

7.56. Пусть $\{u_n\}$ задается по следующему правилу:

$$u_0 = 1,\ u_1 = 2, \quad \text{и} \quad u_n = u_{n-1} + u_{n-2} \quad \text{при} \quad n \geq 2.$$

Показать, что всякое натуральное число N имеет единственное представление в виде

$$N = a_1 u_1 + a_2 u_2 + \cdot + a_N u_N,$$

где $a_r = 0$ или 1 и $a_r a_{r+1} = 0$ при $r \geq 1$.

Заключительный в этом параграфе цикл задач посвящен определению длины периода **линейной конгруэнтной последовательности** по модулю m. Так называется любая последовательность, n-й член которой является остатком от деления на m числа $ax_{n-1} + c$, где x_{n-1} — ее $(n-1)$-й член, а a, c, m — заданные натуральные числа.

Заметим, что линейные конгруэнтные последовательности используются при построении наилучших из известных сегодня датчиков псевдослучайных чисел. Идея такого их применения принадлежит Д.Х.Лемеру.

7.57. Докажите, что линейная конгруэнтная последовательность периодична и длина ее периода не превосходит m.

7.58. Докажите, что подпоследовательность x_{nk} при фиксированном k тоже будет линейной конгруэнтной последовательностью.

7.59. Пусть $m = m_1 \ldots m_k$, числа m_i попарно взаимно просты, x_n — последовательность с периодом λ, состоящая из целых неотрицательных чисел, не больших m, $x_{n,i}$ — последовательность остатков от деления x_n на m_i, а λ_i — ее период. Докажите, что

$\lambda = \text{НОК}(\lambda_1, \ldots, \lambda_k)$, и если x_n — линейная конгруэнтная последовательность, то все последовательности $x_{n,i}$ — тоже.

7.60*. Пусть $1 < a < p^k$, где p — простое число и λ — такое наименьшее натуральное число, что $(a^\lambda - 1)/(a-1)$ кратно p^k. Докажите, что $\lambda = p^k$ тогда и только тогда, когда $a-1$ кратно p при $p > 2$, когда $a-1$ кратно 4 при $p = 2$.

7.61*. *(Халл и Добелл)* Длина периода линейной конгруэнтной последовательности максимальна (т. е. равна m) тогда и только тогда, когда $(c, m) = 1, a-1$ кратно любому простому делителю m, кратно 4, если m кратно 4.

Определим функцию $\lambda(m)$ при $m = p^n$, где p — простое, $p > 2$, и при $m = 2$ или 4 равенством $\lambda(m) = \varphi(m)$, при $m = 2, n \geq 3$ — равенством $\lambda(m) = \varphi(m)/2$, и при произвольном $m = p_1^{a_1} \ldots p_n^{a_n}$, где p_i — простые, — равенством $\lambda(m) = \text{НОК}\,(\lambda(p_1^{a_1}), \ldots, \lambda(p_n^{a_n}))$.

7.62*. *(Кармайкл)* При $c = 0$ максимальный период линейной конгруэнтной последовательности равен $\lambda(m)$.

УКАЗАНИЯ

7.7. Выведите из 7.6 и 7.4.

7.11. Примените 7.8 и 7.9.

7.12. Примените индукцию по k и воспользуйтесь 7.9.

7.16. Примените 7.9 и индукцию.

7.18. Примените индукцию по n. Заметьте, что $\log_\varphi(\sqrt{5}(n+1/2))$ — не целое.

7.20. Примените индукцию.

7.21. Пусть m/n — несократимая правильная дробь и

$$\frac{m}{n} = \frac{1}{a_1+}\,\frac{1}{a_2+}\,\cdots\,\frac{1}{+a_k}.$$

Докажем индукцией по k, что $F_{k+1} \leq [a_1, \ldots, a_k] \leq F_{1+a_1+\cdots+a_k}$, причем равенство $F_{k+1} = n$ справедливо, лишь, когда $a_1 = \ldots = a_k = 1$, а равенство $n = F_{1+a_1+\cdots+a_k}$ — лишь, когда $a_1 = \ldots = a_{k-1} = 1, a_k \leq 2$, или $a_1 = 2, a_2 = \ldots = a_{k-1} = 1, a_k \leq 2$.

База индукции ($k = 1, 2$) очевидна, так как $F_2 = 1 \leq n = a_1 \leq F_{1+a_1}$.

Докажем индукционный переход. Согласно равенствам

$$\frac{m}{n} = \frac{1}{a_1+}\,\frac{1}{a_2+}\,\cdots\,\frac{1}{+a_k} = \frac{[a_1, \ldots, a_k]}{[a_2, \ldots, a_k]},$$

$$[a_1, \ldots, a_k] = a_1[a_2, \ldots, a_k] + [a_3, \ldots, a_k],$$

и предположению индукции справедливо, что

$$F_k \leq [a_2, \ldots, a_k] \leq F_{1+a_1+\ldots+a_k},\ F_{k-1} \leq [a_3, \ldots, a_k] \leq F_{1+a_3+\ldots+a_k},$$

следовательно,

$$F_{k+1} = F_k + F_{k-1} \leq [a_2, \ldots, a_k] + [a_3, \ldots, a_k] \leq [a_1, \ldots, a_k] =$$

$$= a_1[a_2, \ldots, a_k] + [a_3, \ldots, a_k] \leq a_1 F_{1+a_2+\ldots+a_k} + F_{1+a_3+\ldots+a_k} \leq$$

$$\leq F_{a_1+1} F_{1+a_2+\ldots+a_k} + F_{a_1} F_{1+a_3+\ldots+a_k},$$

и равенство $F_{k+1} = [a_1, \ldots, a_k]$ справедливо лишь при $a_1 = \ldots = a_k = 1$. Согласно задаче 7.20 имеем $F_{u+v} = F_{u-1}F_v + F_u F_{v+1}$. Отсюда следует, что

$$[a_1, \ldots, a_k] \leq F_{a_1} F_{1+a_2+\ldots+a_k} + F_{a_1} F_{a_2+\ldots+a_k} = F_{1+a_1+\ldots+a_k},$$

и неравенство доказано. Равенство возможно, лишь когда

$$a_1 \leq 2, a_2 = 1, [a_2, \ldots, a_k] = F_{1+a_2+\ldots+a_k},$$

и, следовательно, согласно предположению индукции, лишь когда

$$a_1 = 2, a_2 = \ldots = a_{k-1} = 1, a_k \leq 2,$$

или $a_1 = a_2 = \ldots = a_{k-1} = 1, a_k \leq 2$. Тем самым шаг индукции сделан.

7.22. Из доказанного в 7.21 неравенства $n \leq F_{1+a_1+\ldots+a_k}$ и задачи 7.19 немедленно следует неравенство задачи. Остальное вытекает из 7.19 и равенств

$$\underbrace{\frac{1}{1+}\cdots\frac{1}{+1}\,\frac{1}{+2}}_{k-1} = \underbrace{\frac{1}{1+}\cdots\frac{1}{+1}\,\frac{1}{+1}}_{k} = \frac{F_k}{F_{k+1}},$$

$$\underbrace{\frac{1}{2+}\,\frac{1}{1+}\cdots\frac{1}{+1}\,\frac{1}{+2}}_{k-2} = \underbrace{\frac{1}{2+}\,\frac{1}{1+}\cdots\frac{1}{+1}\,\frac{1}{+1}}_{k} = 1 + \frac{F_{k-2}}{F_{k-1}} = \frac{F_{k-1}}{F_{k+1}}.$$

7.23. Индукция с помощью 7.20.

7.25. Примените алгоритм Евклида и 7.20, 7.23, 7.24.

7.29. Воспользуйтесь равенством

$$2^{-2k} \sum_{i=0}^{k} \binom{2k+1}{2i} 5^i = F_{2k+2} + F_{2k}.$$

7.34. Согласно 7.33 справедливы следствия

$$7 \mid F_n \Longrightarrow 8 \mid n \Longrightarrow 3 \mid F_n.$$

7.36. а) Примените индукцию. Для обоснования ее шага воспользуйтесь предыдущей задачей.

б) Для обоснования шага индукции примените пункт а) и тождество $F_{2n+1} = F_{n+1}^2 + F_n^2$.

7.37. Докажите по индукции, что для любого $s \geq 1$ остатки от деления на n чисел F_s и $F_{s+t(n)}$ совпадают. Примените также 7.32.

7.38. Допустим, что $t(n) > n^2$. Тогда согласно принципу ящиков Дирихле найдутся такие k и $m, k < m \leq t(n)$, что остатки от деления на n чисел F_k и F_m совпадают, и чисел F_{k+1} и F_{m+1} тоже. Отсюда с помощью индукции получается, что для любого $s \geq k$ остатки от деления на n чисел F_s и F_{s+m-k} совпадают, т. е. последовательность этих остатков периодическая с периодом $m - k < t(n)$, что противоречит 7.37.

7.39. Обозначим остаток от деления $F_{d(n)+1}$ на n через k. Докажите индукцией, что при любом s остаток от деления kF_s на n равен остатку

от деления $F_{s+d(n)}$ и также $(-1)^{F_{d(n)-s}}$ на n. Отсюда следует, что числ $(-1)^{d(n)} = (-1)^{d(n)}F_1$ и $kF_{d(n)-1}$, а, значит, и k^2 равноостаточны при делени на n. Поэтому при четном $d(n)$ число $F_{2d(n)+1}$ равноостаточно с k^2, а значит, с единицей. Отсюда следует, что при $k \neq 1$ справедливо равенство $2d(n) = t(n$ При $k = 1$, очевидно, справедливо равенство $d(n) = t(n)$. Так как при четно $d(n)$ числа $(-1)^{d(n)/2-1}F_{d(n)/2}$ и $kF_{d(n)/2}$ равноостаточны при делении на n то при простом n это возможно лишь при k, равноостаточном с $(-1)^{d(n)/2-}$ (так как $F_{d(n)/2}$ некратно n), поэтому равенство $k = 1$ справедливо лишь пр нечетном $d(n)/2$, а при четном $d(n)/2$ имеем, что $k = -1$. При нечетном $d(n$ число $F_{4d(n)+1}$ равноостаточно с k^4, а, значит, и с единицей. Так как тогд числа $F_{2d(n)+1}$ и $F_{3d(n)+1}$ не равноостаточны с единицей, то согласно 7.37 имее что $4d(n) = t(n)$.

7.40. Раскройте скобки в формуле Бине с помощью формулы бинома.

7.41. Примените 7.40 и воспользуйтесь задачами 6.14 и 6.5 и тем фактом что биномиальные коэффициенты $\binom{k}{p}$ кратны p при $0 < k < p$.

7.42. В пункте а) примените индукцию по n, а в пункте б) проще всег воспользоваться формулой Бине.

7.44. При простом p вида $5k \pm 1$ число $t(p)$ кратно $p-1$, так как согласн задаче 7.40 имеем

$$2^{p-2}F_{p-1} = \sum_{i=0}^{(p-3)/2} \binom{2i+1}{p-1}5^i,$$

откуда, пользуясь тем, что $\binom{2i+1}{p-1} + 1$ кратно p, получаем согласно теореме 6. что число

$$2^pF_{p-1} + 4\sum_{i=0}^{(p-3)/2} 5^i = 2^pF_{p-1} + 5^{(p-1)/2} - 1,$$

а, значит, и число $2^pF_{p-1} + \left(\frac{5}{p}\right) - 1 = 2^pF_{p-1}$, кратны p, а значит, числа F_{p-1} (согласно 7.41) $F_p - \left(\frac{5}{p}\right) = F_p + 1$ — тоже, поэтому согласно 7.37 имеем $t(p) \mid p-1$ Если к тому же p имеет вид $4m+3$, то согласно 7.39 получим $d(p) = t(p)$. Пр простом p вида $5k \pm 2$ справедливо, что число

$$2^pF_{p-1} + \left(\frac{5}{p}\right) - 1 = 2^pF_{p-1} - 2,$$

а согласно теореме 6.14 и число $2F_{p-1} - 2$ кратны p, значит, числа $F_{p-1} -$ (согласно 7.41)

$$F_{p-1} - 1 + F_p - \left(\frac{5}{p}\right) = F_{p-1} - 1 + F_p + 1 = F_{p+1},$$

$$F_{p+1} - 1 + F_p - \left(\frac{5}{p}\right) = F_{p+1} + F_p + 1 = F_{p+2} + 1,$$

тоже, откуда с помощью 7.42 б) получается, что и $F_{2p+3} - 1$ кратно p. Отсюда силу 7.37 следует, что $t(p) \mid 2(p+1)$ и $d(p) \mid (p+1)$. Если бы при этом $d(p) = t($ то согласно 7.37 была бы невозможна одновременная делимость на p чис $F_{p+2} + 1$ и F_{p+1}. Поэтому согласно 7.39 имеем $2d(p) = t(p)$ при четном $d(p)$ $4d(p) = t(p)$ при нечетном $d(p)$, причем в последнем случае $d(p) \mid (p+1)/2$.

7.45. Примените 7.32 и 7.37.

7.46. Положим для краткости $V_{m,n} = F_{mn}/F_n$. Индукцией по m с помощью равенства $F_{n+m} = F_m F_{n+1} + F_{m-1}F_n$ (см. 7.20) докажите, что

$$F_{mn+1} = F_n^2(V_{m-1,n} + V_{m-2,n}F_{n+1} + V_{m-3,n}F_{n+1}^2 + \ldots + F_{n+1}^{m-2}) + F_{n+1}^m.$$

Отсюда вытекает второе утверждение. Индукцией по m с помощью следующего из 7.20 равенства $V_{m,n} = V_{m-1,n}F_{n+1} + F_{(m-1)n+1}$ и доказанного второго утверждения получите первое утверждение.

7.47. Воспользуйтесь 7.24 и 7.46 для доказательства первого утверждения и примените малую теорему Ферма для доказательства второго.

7.48. Примените 7.46 и 7.39 и докажите, что при $n > m$ имеем

$$d(p^n) = pd(p^{n-1}), t(p^n) = pt(p^{n-1}),$$

(для доказательства последнего равенства нужна еще формула бинома), а далее проведите индукцию.

7.49. Разложим n на простые множители:

$$n = 2^\beta 5^\gamma p_1^{\alpha_1} \ldots p_m^{\alpha_m},\ p_i \neq 2, p_i \neq 5.$$

Применяя 7.45, 7.44, 7.48, 7.36, получите,что

$$t(n) \leq \text{НОК}\left(3 \cdot 2^{\beta-1}, 4^{\min(\gamma,1)}5^\gamma, p_1^{\alpha_1-1}2(p_1 \pm 1), \ldots, p_m^{\alpha_m-1}2(p_m \pm 1)\right) \leq$$

$$\leq 3 \cdot 2^{\max(\beta-1,2)}5^\gamma \times$$

$$\times \left(\frac{p_1^{\alpha_1-1}}{2}\left(p_1 - \left(\frac{5}{p_1}\right)\right)\right) \ldots \left(\frac{p_m^{\alpha_m-1}}{2}\left(p_m - \left(\frac{5}{p_m}\right)\right)\right).$$

Пусть n кратно 8, тогда $\beta \leq 3$ и

$$\frac{t(n)}{n} \leq 3\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right) \ldots \left(1 - \frac{\left(\frac{5}{p_m}\right)}{p_m}\right) 2^{-m-1} \leq$$

$$\leq \frac{3\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right)}{4} \leq 1.$$

Пусть $\beta = 2$, тогда

$$\frac{t(n)}{n} \leq 3\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right) \ldots \left(1 - \frac{\left(\frac{5}{p_m}\right)}{p_m}\right) 2^{-m} \leq 2,$$

а при $m \geq 3$ имеем $t(n)/n \leq 3 \cdot 2/3 \cdot 4/7 \cdot 6/13 < 1$. При $\beta = 1$ получим

$$\frac{t(n)}{n} \leq 3\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right) \ldots \left(1 - \frac{\left(\frac{5}{p_m}\right)}{p_m}\right) 2^{-m+1} \leq$$

$$\leq 3\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right) \leq 4.$$

причем равенство возможно лишь при $n = 2 \cdot 3^\alpha$, а при $m \geq 4$ имеем $t(n)/n \leq$ $\leq 6 \cdot (2/3) \cdot (4/7) \cdot (6/13) \cdot (8/17) < 1$. Если же n нечетно, то

$$\frac{t(n)}{n} \leq \left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right) \dots \left(1 - \frac{\left(\frac{5}{p_m}\right)}{p_m}\right) 2^{-m+1} \leq$$

$$\leq 2\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right) \leq \frac{8}{3}.$$

а при $m \geq 3$ имеем $t(n)/n \leq (8/3) \cdot (4/7) \cdot (6/13) < 1$.

Аналогично оцениваем при $\beta \geq 2$

$$\frac{d(n)}{n} \leq 3\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right) \dots \left(1 - \frac{\left(\frac{5}{p_m}\right)}{p_m}\right) 2^{-m-1} \leq$$

$$\leq \frac{3\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right)}{4} \leq 1,$$

при $\beta = 1$ имеем

$$\frac{d(n)}{n} \leq 3\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right) \dots \left(1 - \frac{\left(\frac{5}{p_m}\right)}{p_m}\right) 2^{-m} \leq$$

$$\leq \frac{3\left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right)}{2} \leq 2,$$

причем равенство возможно лишь при $n = 2 \cdot 3^\alpha$, и при нечетном n имеем

$$\frac{d(n)}{n} \leq \left(1 - \frac{\left(\frac{5}{p_1}\right)}{p_1}\right) \dots \left(1 - \frac{\left(\frac{5}{p_m}\right)}{p_m}\right) 2^{-m+1} \leq$$

$$\leq 1 - \frac{\left(\frac{5}{p_1}\right)}{p_1} \leq \frac{4}{3}.$$

7.50. Примените равенство

$$F_{mn+1} = F_n^2(V_{m-1,n} + V_{m-2,n}F_{n+1} + V_{m-3,n}F_{n+1}^2 + \dots + F_{n+1}^{m-2}) + F_{n+1}^m$$

и первое из утверждений 7.46.

7.51. Шаг индукции. Если $F_t - p^n a_p$ и $F_{t+1} - 1 - p^n b_p$ кратны p^{n+1}, согласно 7.47 число $V_{p,t}F_t - p^n a_p p = F_{pt} - p^{n+1}a_p$ кратно p^{n+2}, а согласно 7. число $F_{pt+1} - F_{t+1}^p$ кратно p^{2n+1} и тем более p^{n+2}, откуда на основании форму бинома следует, что $F_{pt+1} - 1 - p^{n+1}b_p$ кратно p^{n+2}.

7.52. Согласно 7.20 имеем $F_{k+tm} = F_{k-1}F_{tm} + F_k F_{tm+1}$, а согласно 7. получим $F_{tm} - mF_{t+1}^{m-1}F_t$ кратно F_t^3, значит, $F_{tm} - mF_t$ кратно p^{n+1} в си 7.51, а потому и $F_{tm} - mp^n a_p$ тоже. С помощью 7.46, 7.51 и формулы бино

получите, что число $F_{tm+1} - F_{t+1}^m$ кратно p^{n+1}, а значит, и $F_{tm+1} - 1 - mp^n b_p$ — тоже. Отсюда следует, что число

$$F_{k+tm} - F_k - p^n m(a_p F_{k-1} + b_p F_k)$$

кратно p^{n+1}.

7.53. Шаг индукции. Пусть для любого целого a от 0 до $3^n - 1$ найдется такое k, что $F_k - a$ кратно 3^n, и $k-2$ не кратно 4. Согласно 7.51 при $t = 8 \cdot 3^n$ числа $F_t - 3^n$ и $F_{t+1} - 1 - 2 \cdot 3^n$ кратны 3^{n+1}. Применяя 7.52, получите, что число

$$F_{k+tm} - F_k - 3^n m(F_{k-1} + 2F_k) = F_{k+tm} - F_k - 3^n m F_{k+2}$$

кратно 3^{n+1}. Так как $k+2$ не кратно 4, то согласно 7.33 число F_{k+2} не кратно 3, значит, для любого $b = 0, 1$ или 2 найдется такое m, равное 0, 1 или 2, что $F_{k+tm} - F_k - 3^n b$, а значит, и $F_{k+tm} - a - 3^n b$ кратно 3^{n+1}. При этом $k + tm - 2$ не кратно 4.

7.54. Шаг индукции. Пусть для любого целого a от 0 до $5^n - 1$ найдется такое k, что $F_k - a$ кратно 5^n. Согласно 7.51 при $t = 4 \cdot 5^n$ числа $F_t - 3 \cdot 5^n$ и $F_{t+1} - 1 - 4 \cdot 5^n$ кратны 5^{n+1}. Применяя 7.52, получите, что число

$$F_{k+tm} - F_k - 5^n m(3F_{k-1} + 4F_k) = F_{k+tm} - F_k - 5^n m(F_{k+4} - F_k)$$

кратно 5^{n+1}. Так как

$$F_{k+8} - 2F_{k+4} + F_k = 15F_{k+1} + 10F_k,$$

то $F_{k+8} - 2F_{k+4} + F_k$ кратно 5, значит, остатки от деления на 5 последовательности $F_{k+4} - F_k$ периодически повторяются с периодом 4. Непосредственно проверяется, что в этой последовательности нет нулей, поэтому для любого $b = 0, 1, 2, 3$, или 4 найдется такое m, равное $0, 1, 2, 3$ или 4 что $F_{k+tm} - F_k - 5^n b$, а значит, и $F_{k+tm} - a - 5^n b$ кратно 5^{n+1}.

7.55. Заметьте, что если для n-ичной системы неверен аналог задач 7.43 и 7.44, то он неверен для любого m, кратного n. То, что этот аналог неверен для $n = 2$, вытекает из 7.33. То, что он неверен для простого n вида $5k \pm 1$, следует из 7.44. То, что он неверен для простых n вида $5k \pm 2$ таких, что $d(n) \leq (n+1)/2$, можно доказать с помощью рассуждений, применявшихся для решения задачи 7.39.

7.57. Найдутся такие k и $s, 0 \leq k < s \leq m$, что числа x_k и x_s равны. Тогда и числа x_{n+k} и x_{n+s} тоже равны при любом целом n. Поэтому последовательность периодическая, наименьший период состоит из разных чисел, и его длина делит $k - s$.

7.58. Докажите формулу

$$x_{n+k} = a^k x_n + \frac{(a^k - 1)c}{a - 1} \pmod{m}.$$

7.59. Применяя китайскую теорему об остатках, заметьте, что всегда x_n однозначно восстанавливается по набору длины k, составленному из остатков $x_{n,i}$, причем разным наборам остатков соответствуют разные числа x_n. Докажите, что период последовательности рассматриваемых наборов равен $\text{НОК}(\lambda_1, \ldots, \lambda_k)$.

7.60. Пусть $\lambda = p^k, p > 2$, и $a - 1$ некратно p. Тогда $a^\lambda - 1$ кратно p^k. Применив k раз малую теорему Ферма, получите, что $a^\lambda - a$ кратно p, значит, и $a - 1$ кратно p, вопреки предположению.

Если же $p=2$ и $a-3$ кратно 4, то при любом $\mu=2^m$ число $(a^\mu-1)/(a^{\mu/2}-$ четно, значит,

$$(a^{\lambda/2}-1)/(a-1)=((a^{\lambda/2}-1)/(a^{\lambda/4}-1))\dots((a^2-1)/(a-1))$$

кратно 2^k.

Для доказательства достаточности условий примените 6.46 и получите, чт $(a^\mu-1)/(a-1)$ кратно p^k и некратно p^{k+1} тогда и только тогда, когда μ крат p^k и некратно p^{k+1}.

7.61. В силу 7.58 достаточно доказать теорему при $m=p^a$. Можно считат что $a>1$. Период имеет длину m тогда и только тогда, когда в нем встречают все числа от 0 до $m-1$. Поэтому можно считать, что $x_0=0$. Тогда x_n рав остатку от деления на m числа

$$c(a^n-1)/(a-1).$$

Если $(c,m)>1$, то всегда $x_n\neq 1$, и поэтому длина периода меньше m. Значи если длина периода равна m, то $(c,m)=1$. Из 7.56 следует, что при $x_0=$ длина периода равна m тогда и только тогда, когда наименьшее положительн n, такое, что $x_n=0$, равно m. При $(c,m)=1$ условие $x_n=0$ равносилы делимости на m числа $(a^n-1)/(a-1)$. Остается применить предыдущую задач

7.62. С помощью 7.58 сведите к случаю $m=p^a$. Примените задачу 6.26.

§8. ПРИМЕНЕНИЯ АЛГОРИТМА ЕВКЛИДА

8.1. При каких целых n дробь $\frac{5n+6}{8n+7}$ несократима? Докажите, чт дробь $\frac{21n+4}{14n+3}$ несократима при всех целых n.

8.2. На миллиметровой бумаге нарисован прямоугольник размеро $a\times b$ так, что стороны его идут по линиям сетки. На какое числ частей делят узлы сетки его диагональ?

8.3. От нарисованного прямоугольника отрезают несколько кв дратов со стороной b до тех пор, пока не останется прямоугольник шириной меньше b, и с ним поступают точно так же, пока не получитс прямоугольник, который целиком разрезается на квадраты. Квадрат какого размера получились? Приведите пример прямоугольника $a\times$ который разрезается ровно на n квадратов.

8.4. Докажите, что число квадратов, получающихся при разрезан прямоугольника $a\times b$, не меньше $[\log_\varphi(\sqrt{5}(\max(a,b)-1/2))]$, причем д $a=F_k$ или F_{k-1} и $b=F_{k+1}$ это неравенство обращается в равенств

Следующий цикл задач посвящен решению линейных уравнений целых числах.

8.5. Пусть $(m,360)=1, 1<m<360$. Докажите, что с помощь одного циркуля можно разделить угол в m градусов на m равны частей.

8.6*. *(Конструкция для наименьших решений в натуральных числа уравнения $ax-by=1$).* Разложим $\frac{a}{b}$ в цепную дробь

$$\alpha_0+\frac{1}{\alpha_1+}\frac{1}{\alpha_2+}\dots\frac{1}{+\alpha_n}.$$

Заменяя в случае необходимости α_n на $(\alpha_n - 1) + \frac{1}{1}$, можно считать, что n нечетно. Докажите, что наименьшее решение в натуральных числах уравнения $ax - by = 1$ есть $x = q_{n-1}, y = p_{n-1}$.

8.7. Найдите все решения в целых числах уравнения $ax - by = 1$.

8.8. Найдите необходимое и достаточное условие разрешимости в целых числах уравнения $ax + by = c$ и вообще уравнения

$$a_1x_1 + \ldots + a_nx_n = c.$$

8.9*. Докажите, что для любых целых m и n разрешима в целых числах система уравнений

$$\begin{cases} 3x + 5y = m, \\ 7x + 5z = n. \end{cases}$$

В следующих задачах речь идет фактически о подгруппах и подполугруппах в множествах целых и натуральных чисел.

8.10. Множество целых чисел обладает следующим свойством: вместе с любыми двумя числами оно содержит их сумму и разность. Докажите, что это множество состоит из всех чисел, кратных некоторому числу d.

8.11*. Множество натуральных чисел разбито на два подмножества A и B так, что $A \cdot B$ (то есть множество всех произведений вида ab, где a — число из A, а b — число из B) содержится в A и $A + B$ (т.е. множество всех сумм вида $a + b$, где a — число из A, а b — число из B) содержится в B. Докажите, что а) $A \cdot A$ содержится в A;

б) A состоит из всех чисел, кратных некоторому числу d.

8.12*. В султанстве Сулейманском была выпущена бесконечная серия монет достоинством в a_1 таньга, a_2 таньга, и так далее. Докажите, что найдется такое n, что любую сумму, которую можно уплатить выпущенными монетами, можно уплатить уже монетами достоинствами в $a_1, \ldots, a_n$ таньга.

8.13*. *(Франция, 79).* Пусть $(a, b) = 1$. Докажите, что любую сумму, начиная с $(a - 1)(b - 1)$ можно уплатить монетами достоинством a и b таньга, а сумму $(a - 1)(b - 1) - 1$ — нельзя.

8.14*. *(IMO, 82).* Пусть a, b, c попарно взаимно просты. Докажите, что любую сумму, начиная с $2abc - ab - ac - bc + 1$, можно уплатить монетами достоинством ab, ac и bc таньга, а сумму $2abc - ab - ac - bc$ — нельзя.

8.15. В султанстве Сулейманском была выпущена бесконечная серия монет достоинством в 1 таньга, 2 таньга, 4 таньга и так далее. Докажите, что любую сумму можно уплатить без сдачи этими монетами, используя каждую из них не более одного раза. Докажите, что тем же свойством, что и $1, 2, 4, \ldots$, обладает последовательность Фибоначчи. Однако $1, 2, 4, \ldots$ единственная последовательность, которая

вместе с упомянутым свойством возможности уплаты обладает еще свойством единственности такой возможности.

8.16. Как расположить по n конвертам сумму в $F_{n+3}-2$ таны так, чтобы любую меньшую сумму также можно было бы уплатит не вскрывая конвертов?

8.17. Стоящие в шеренге школьники передают друг другу слеи направо карточки. Получив от левого соседа карточку с парой чисе (m,n), разрешается передать правому соседу одну из следующи карточек: (n,m), $(m+n,n)$ или $(|m-n|,n)$. Один из школьнико получил карточку $(19,90)$. Может ли у кого-то из стоящих прав оказаться карточка: а) $(31,13)$; б) $(12,21)$?

Новый цикл задач посвящен вопросам о том, как быстро мож но проводить некоторые вычисления (как сейчас стали говорить сложности вычислений).

8.18*. Покажите, как с помощью калькулятора, умеющего зап минать только два числа, можно возвести x в n-ю степень, сдела $l(n)+\lambda(n)-2$ умножений, где $l(n)$ — число разрядов в двоичнс записи n, а $\lambda(n)$ — число единиц в этой записи.

8.19*. На первый взгляд кажется, что в условиях 8.18 быстре вычислить x^n, чем отмечено там, нельзя. Покажите, что однак $x^{2^{F_k}-1}$ можно вычислить с помощью $F_{k+1}+k-4$ умножений.

8.20. *(Бинарный алгоритм Евклида)* Докажите следующие утве ждения: если u и v четны, то $(u,v)=2(u/2,v/2)$; если u четн а v нечетно, то $(u,v)=(u/2,v)$; если u и v нечетны, то $u-$ четно, $|u-v|<\max(u,v)$ и $(u,v)=(|u-v|,\min(u,v))$. Предложит алгоритм, основанный на этих утверждениях, и примените его дл доказательства равенства

$$(2^m-1,2^n-1)=2^{(m,n)}-1.$$

8.21. Докажите, что при любом $a\in\mathbb{N}$ справедливо равенст $(a^m-1,a^n-1)=a^{(m,n)}-1$.

8.22. Проверьте, что при любых m и $n\in\mathbb{N}, m>n$, числ вычитаний, выполняемых бинарным алгоритмом в применении к па чисел

$$u=2^{m+1}-a_{n+2}, v=a_{n+2}, \text{ где } a=(2^n-(-1)^n)/3,$$

равно $m+1$.

8.23*. *(Д.Кнут)* Докажите индукцией по $[\log_2 u]+[\log_2 v]$, что числ вычитаний, выполняемых бинарным алгоритмом в применении к па чисел u,v не больше $1+[\log_2\max(u,v)]$ и равенство возможно лиш когда $[\log_2(u+v)]>[\log_2\max(u,v)]$.

8.24. В результате работы бинарного алгоритма получается цепоч равенств вида $(2u,2v)=2(u,v),(2u,2v+1)=(u,2v+1),(2u+1,2v)$

$= (2u+1, v), (2u+1, 2v+1) = (2|u-v|, 2\min(u,v)+1)$. На первый взгляд кажется, что среди всех цепочек того же вида с данными началом и концом она будет кратчайшей, однако это не так. Пусть $a_1 = 3, a_{k+1} = 8a_k + 3, k \in \mathbb{N}, u = 3a_n + 1, v = 2a_n + 1$. Проверьте, что в применении к u и v бинарный алгоритм делает $6n$ шагов, в том числе, и $3n-2$ вычитаний, а обычный алгоритм — только три шага $(u, v) = (2a_n + 1, a_n) = (1, a_n)$, и еще $2n-1$ вычитание и $3n-2$ деления пополам требуются для получения цепочки, заканчивающейся парой $(1, 1)$.

При выполнении деления больших чисел столбиком возникает такая задача: как найти частное q от деления $n+1$ разрядного числа $u = \overline{u_0 \ldots u_n}$ на n- разрядное число $v = \overline{v_1 \ldots v_n}$ (числа десятичные, старшие разряды -слева)? Это число равно $[u/v]$ и находится обычно подбором. Следующий прием облегчает его нахождение. Положим

$$q^* = \min([(10u_0 + u_1)/v_1], 9).$$

8.25. *(Д.Кнут)* Докажите, что $q^* \geq q$, а при $v_1 \geq 5$ к тому же $q^* - 2 \leq q$. Умножив u и v на $[10/(v_1+1)]$, можно, не изменяя u/v, добиться того, что $v_1 \geq 5$. Покажите, что неравенство $q^* - 2 \leq q$, вообще говоря, усилить нельзя.

8.26. *(Д.Кнут)* Докажите, что: а) если $u_0 = v_1$, то $q = 9$ или 8;

б) $q \geq [(10u_0 + u_1)/(v_1 + 1)]$;

в) если при $r^* = 10u_0 + u_1 - q^* v_1$ справедливо неравенство

$$v_2 q^* > 10r^* + u_2,$$

то $q = q^* - 1$ или $q = q^* - 2$, а если

$$v_2 q^* \leq 10r^* + u_2,$$

то $q = q^*$ или $q = q^* - 1$;

г) если $v_1 \geq 5, v_2 q^* \leq 10r^* + u_2$, но $q^* \neq q$, то $u - qv \geq 7v/10$, (т.е. с вероятностью $0,7$ все же $q^* = q$).

Назовем **обобщенным алгоритмом Евклида** последовательность вычислений вида

$$a = bq_2 + \epsilon_2 r_2, b = r_2 q_3 + \epsilon_3 r_3, r_2 = r_3 q_4 + \epsilon_4 r_4, \ldots,$$

$$r_{k-3} = r_{k-2} q_{k-1} + \epsilon_{k-1} r_{k-1}, r_{k-1} = r_k q_k,$$

где

$$\epsilon_i = \pm 1, 0 < r_i < r_{i-1}, i \geq 1, b = r_1, a = r_0.$$

Число $k-1$ назовем его длиной. Как и в обычном алгоритме Евклида $(a, b) = r_k$ обозначим $L(a, b)$ минимальную длину обобщенного алгоритма Евклида для вычисления (a, b). Назовем алгоритмом Евклида

с выбором минимального остатка обобщенный алгоритм Евклида, котором всегда $2r_i \leq r_{i-1}$, т.е. на каждом шаге из двух возможных вариантов деления

$$r_{i-2} = r_{i-1}q_{i-1} + r_i, \text{ где } 0 < r_i < r_{i-1},$$

и

$$r_{i-2} = r_{i-1}(q_{i-1} + 1) - (r_{i-1} - r_i),$$

выбираем тот, при котором получается минимальный по абсолютной величине остаток (если они равны по модулю, то берем любой из них). Обозначим $L_0(a, b)$ минимальную длину алгоритма Евклида с выбором минимального остатка.

8.27. *(Кронекер)* Докажите, что число всех различных обобщенных алгоритмов Евклида для пары (a, b) взаимно простых чисел равно 1.

8.28*. *(Кронекер)* Докажите, что при $a \geq 2b$ справедливо неравенство

$$L_0(a, b) \leq L_0(a, a - b).$$

8.29*. *(Кронекер)* Докажите, что

$$L_0(a, b) \leq L(a, b).$$

8.30. Докажите для последовательности

$$u_n = 2u_{n-1} + u_{n-2}, u_1 = 1, u_0 = 0$$

формулу

$$u_k = 2^{-3/2}(\sqrt{2} + 1)^k - (1 - \sqrt{2})^k,$$

и соотношение

$$u_k \leq n \Longleftrightarrow k \leq [\log_\alpha (2\sqrt{2}n + \sqrt{2})],$$

где $\alpha = \sqrt{2} + 1$.

8.31*. *(Дюпре).* Докажите, что $L_0(a, b) \leq$

$$\leq \min\{[\log_\alpha (2\sqrt{2}\min(a, b) + \sqrt{2})], [\log_\alpha (2\sqrt{2}(a + b) + \sqrt{2})] - 1\}.$$

и проверьте, что равенство достигается при

$$b = u_n, a = u_n + u_{n-1}.$$

Следующая задача предложена Д.А.Масловым, студентом одного из авторов. Она хорошо дополняет теоремы Дюпре и Кронекера.

8.32*. В предыдущих задачах фактически было показано, что разложение любого рационального числа $\frac{p}{q}$ в цепную дробь с минимальным по модулю остатком не длиннее обычного разложения этого числа в цепную дробь. Докажите, что минимум отношения их длин равен $\frac{1}{2}$ и достигается на $\frac{F_{2n-1}}{F_{2n}}$.

Другими словами, алгоритм Евклида с выбором минимального по модулю остатка на каждом шаге не более чем вдвое короче по числу шагов деления обычного алгоритма Евклида.

УКАЗАНИЯ

8.4. Выведите из 7.22.

8.6. Используйте 7.10.

8.7. Используйте 7.6.

8.10. Заметьте, что это множество содержит нуль и замкнуто относительно сложения. Рассмотрите в нем наименьшее положительное число и докажите, что все числа в нем кратны этому числу. Для этого рассуждайте от противного и, применяя деление с остатком, получите противоречие.

8.11. Докажите, что 1 принадлежит B, и , используя равенство $a(b+1) = ab+a$, докажите методом от противного, что если a и b взяты из A, то и ab принадлежит A. Далее примените указание к задаче 8.10.

8.12. Докажите, что множество A всех сумм, которые можно уплатить выпущенными деньгами, замкнуто относительно сложения и, начиная с некоторого места, содержит все кратные некоторого числа и только их. Пусть x и y такие числа из A, что их разность $d = x - y > 0$ минимальна. Тогда все числа из A кратны d, ибо если $z = qd + v, 0 < v < d$, то $v = z + qy - qx$, и если z принадлежит A, то $z + qy$ и qx тоже, что ведет к противоречию. Считая далее, что $d = 1$ (сократив на d все числа из A в противном случае), заметьте, что любое $n > xy$ представимо в виде

$$n = qx + v = (q - v)x + (x + 1)v = (q - v)x + vy,$$

где $0 \leq v < x, q - v > y - x = 1$, значит, n принадлежит A.

8.18. Пусть

$$n = \sum_{k=0}^{l(n)-1} 2^k \alpha_k,$$

где $\alpha_k = 0$ или 1, причем единиц $\lambda(n)$ штук. Положим n равным сумме последних k ненулевых слагаемых, разделенной на минимальное из них, и число y_k, равным x^{n_k}. Тогда вычисляете последовательно $y_k = y_{k-1}^{2^{m_k}} x$, где $n_k - 1 = 2^{m_k} n_{k-1}$, храня при этом число x в памяти, а y_k сохраняя на индикаторе.

8.19. Примените 7.31.

8.22. Воспользуйтесь тем, что последовательность a_n удовлетворяет рекуррентным соотношениям $a_n = a_{n-1} + 2a_{n-2}, a_n + a_{n+1} = 2^n$.

8.23. Положим $m = [\log_2 u], n = [\log_2 v]$. Пусть $m = n$. Можно считать, что $u > v$. Выполнив шаг деления-сдвига, по индукции получаем, что нужно еще выполнить не более $m + 1$ шагов деления. Если бы понадобилось ровно $m + 1$ шагов, то мы имели бы

$$[\log_2 ((u - v)2^{-r} + v)] > [\log_2 v],$$

где $r \geq 1$ — число уже выполненных сдвигов вправо, что невозможно, так как $(u-v)2^{-r}+v \leq (u-v)+v = u$.

Пусть $m > n$. Выполнив шаг деления, получим пару (u', v), где

$$u' = (u-v)2^{-r}, r \geq 1, [\log_2 u'] = m-k, k \geq 1.$$

Согласно предположению индукции осталось сделать не более $1+\max(m-k, n) \leq m$ шагов. Если требуется ровно m шагов, то согласно предположению индукции $[\log_2 (u'+v)] \geq m$, откуда

$$[\log_2 (u+v)] = [\log_2 2((u-v)/2+v)] >$$

$$> [\log_2 2(u'+v)] \geq m+1 > [\log_2 v].$$

8.25. Можно считать, что $q^* < 9$, тогда

$$q^* = [(10u_0+u_1)/v_1], q^* v_1 \geq (10u_0+u_1) - v_1 + 1,$$

значит,

$$u - q^* v \leq u - 10^{n-1} v_1 q^* \leq$$

$$\leq u_0 10^n + \ldots + u_n - 10^n u_0 - 10^{n-1} u_1 + 10^{n-1} v_1 - 10^{n-1} << 10^{n-1} v_1 \leq v.$$

Отсюда следует, что $q^* \geq q$. Допустим, что $q^* \geq q+3$. Тогда

$$q^* \leq (10u_0+u_1)/v_1 = (10^n u_0 + 10^{n-1} u_1)/(10^{n-1} v_1) \leq$$

$$\leq u/(10^{n-1} v_1) < u/(v - 10^{n-1}),$$

значит,

$$3 \leq q^* - q < u/(v-10^{n-1}) + 1 - u/v = 1 + (u/v)10^{n-1}/(v-10^{n-1}),$$

поэтому

$$u/v \geq 2(v-10^{n-1})/10^{n-1} \geq 2(v_1-1),$$

откуда

$$6 \geq q^* - 3 \geq q = [u/v] \geq 2(v_1-1), v_1 \leq 4,$$

противоречие.

Для доказательства последнего утверждения заметьте, что

$$v[10/(v+1)] < (v+1)[10/(v+1)] \leq 10,$$

и при $v \geq 5$, очевидно, $v[10/(v+1)] \geq v \geq 5$.

Если же $1 \leq v \leq 4$, то $v[10/(v+1)] > v(10/(v+1)-1) \geq 4$, так как $v(10/(v+1)-1) - 4 = v(9-v)/(v+1) \geq 0$.

Пример, когда неравенство $q^* - 2 \leq q$ обращается в равенство, таков: $u = 4100, v = 588$.

8.26. а) $u/v > u_0 10^n/(v_1+1)10^{n-1} \geq 10(1-1/(v_1+1)) > 10(1-1/5) = 8$.

б) $(10u_0+u_1)/(v_1+1) \leq u/10^{n-1}(v+1) < u/v$.

в) В первом случае

$$u - q^* v \leq u - q^* v_1 10^{n-1} - q^* v_2 10^{n-2} = u_2 10^{n-2} + \ldots + u_n + r^* 10^n -$$

$$-q^* v_2 10^{n-2} < 10^{n-2}(u_2 + 1 + 10r^* - q^* v_2) \leq 0,$$

и так как $u - qv \geq 0$, то $q^* > q$.

Во втором случае, предположив, что $q^* - 2 \geq q$, заметьте, что тогда

$$u < (q^* - 1)v < q^*(v_1 10^{n-1} + (v_2 + 1)10n - 2) - v < q^*(v_1 10^{n-1} + v_2 10^{n-2}) +$$

$$+10^{n-1} - v \leq q^* v_1 10^{n-1} + (10r^* + u_2)10^{n-2} + 10^{n-1} - v = u_0 10^n +$$

$$+10^{n-1}u_1 + u_2 10^{n-2} + 10^{n-1} - v \leq u_0 10^n + 10^{n-1}u_1 + u_2 10^{n-2} \leq u,$$

противоречие.

г) Предположив, что $u - qv < 7v/10$, получите, что

$$q^*(v - 10^{n-2}) < q^*(v_1 10^{n-1} + v_2 10^{n-2}) \leq u_0 10^n + 10^{n-1}u_1 + u_2 10^{n-2} \leq u,$$

$$1 = q^* - q < u/(v - 10^{n-2}) - u/v + 0,7,$$

откуда

$$0,3 < (u/v)10^{n-2}/(v - 10^{n-2}) < 10^{n-1}/(v - 10^{n-2}), 10^n + 3 \cdot 10^{n-2} > 3v,$$

что противоречит неравенству $v_1 \geq 5$.

8.27. Воспользуйтесь индукцией. База $(b = 1)$ очевидна. Обозначим $\varphi(a, b)$ число число всех различных обобщенных алгоритмов Евклида для пары (a, b). Первый шаг любого из них имеет вид $a = bq + r$ или

$$a = b(q + 1) - (b - r), 0 < r < b, (r, b) = (b, b - r) = 1, \text{ если } b > 1.$$

Тогда $\varphi(a, b) = \varphi((b, r) + \varphi(b, b - r) = r + b - r = b$.

8.28. Воспользуйтесь индукцией. База $(a = 2)$ очевидна. Для обоснования шага индукции рассмотрите три случая. Пусть $a \geq 3b$,

$$a = bq_2 + \epsilon_2 r_2, 2r_2 \leq b,$$

тогда $a = (a - b) \cdot 1 + b$, так как $2b \leq a - b$, и

$$a - b = b(q_2 - 1) + \epsilon_2 r_2,$$

поэтому $L_0(a, b) = L_0(a, a - b) - 1$.

Пусть теперь $2b \leq a < 5b/2$. Тогда первые два шага алгоритма в применении к паре (a, b) имеют вид

$$a = b \cdot 2 + (a - 2b), b = r_2 q_3 + \epsilon_3 r_3, r_2 = a - 2b,$$

а в применении к паре $(a, a - b)$ имеют вид

$$a = (a - b) \cdot 2 - (a - 2b), a - b = b + r_2 = r_2(q_3 + 1) + \epsilon_3 r_3.$$

Поэтому $L_0(a, b) = L_0(a, a - b)$.

В третьем случае считаем, что $5b/2 \leq a < 3b$. Тогда первый шаг алгоритма в применении к паре (a, b) имеет вид

$$a = b \cdot 3 - (3b - a), r_2 = 3b - a,$$

значит, $L_0(a, b) = L_0(b, r_2) + 1$. а в применении к паре $(a, a - b)$ — следующий вид:

$$a = (a - b) \cdot 2 - (a - 2b) = (a - b) \cdot 2 - (b - r_2),$$

значит, $L_0(a, a-b) = L_0(a-b, b-r_2) + 1$. Так как $a - b = 2b - r_2 = b + (b - r_2)$, то из равенства

$$a - b = (b - r_2)_2 q_3 + \epsilon_3 r_3$$

следует равенство

$$b = (b - r_2)_2 (q_3 - 1) + \epsilon_3 r_3,$$

поэтому

$$L_0(a, b) = L_0(a - b, b - r_2) + 1 = L_0(b - r_2, r_3) + 2 = L_0(b, b - r_2) + 1.$$

Согласно предположению индукции $L_0(b, b - r_2) = L_0(b, r_2)$, откуда

$$L_0(a, b) = L_0(a, a - b).$$

8.29. Примените индукцию и задачу 8.28. Пусть

$$a = bq_2 + \epsilon_2 r_2, 2r_2 \leq b, a = bq_2' + \epsilon_2' r_2'.$$

Если $r_2 = r_2'$, то $\epsilon_2 = \epsilon_2', q_2 = q_2'$ и согласно предположению индукции

$$L_0(a, b) = L_0(b, r_2) + 1 \leq L(b, r_2) + 1 = L(a, b).$$

Если же $r_2 < r_2'$, то $\epsilon_2 = -\epsilon_2', q_2 = q_2' - \epsilon_2, r_2 = b - r_2'$ и согласно предположению индукции и задаче 8.28 имеем

$$L_0(a, b) = L_0(b, r_2) + 1 \leq L(b - r_2, b) + 1 = L(a, b).$$

8.30. Формулу

$$u_k = 2^{-3/2}\left((\sqrt{2}+1)^k - (1-\sqrt{2})\right)$$

докажите по индукции. Выведите из нее, что ближайшее целое к числу $2^{-3/2}(\sqrt{2}+1)^k$ есть u_k, и заметьте, что, так как число $2^{-3/2}(\sqrt{2}+1)^k - 1/2$ нецелое (оно иррационально), то

$$0 < u_k - 2^{-3/2}(\sqrt{2}+1)^k + 1/2 < 1,$$

и значит,

$$u_k \leq n \Longleftrightarrow 2^{-3/2}(\sqrt{2}+1)^k - 1/2 \leq n,$$

откуда следует, что

$$u_k \leq n \Longleftrightarrow k \leq [\log_a (2\sqrt{2}n + \sqrt{2})].$$

8.31. Пусть алгоритм Евклида порождает равенства

$$a = bq_2 + \epsilon_2 r_2, b = r_2 q_3 + \epsilon_3 r_3, r_2 = r_3 q_4 + \epsilon_4 r_4, \ldots, r_{k-3} =$$

$$= r_{k-2} q_{k-1} + \epsilon_{k-1} r_{k-1}, r_{k-1} = r_k q_k,$$

где $2r_i \leq r_{i-1}, i = 2, \ldots, k, r_1 = b$. Тогда

$$r_i = r_{i+1} q_{i+2}' + r_{i+2}' \geq 2r_{i+1} + r_{i+2}, i = 1, \ldots, k-2, r_{k-1} \geq 2r_k,$$

откуда с помощью индукции получается, что $r_{k-i} \geq u_{i+1}, i = 0, \ldots, k-1$, значит $b \geq u_k, a \geq b + r_2 \geq b + u_{k-1}, a + b \geq u_{k-1}$.

Из 8.30 следует теперь, что

$$k \leq [\log_\alpha (2\sqrt{2}\min(a,b)+\sqrt{2})], k \leq [\log_\alpha (2\sqrt{2}(a+b)+\sqrt{2})] - 1.$$

8.32. Для произвольного рационального числа $\frac{p}{q}$ рассмотрим следующие цепные дроби: обычную

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \cfrac{1}{a_n}}}}$$

с длиной разложения n и цепную дробь с минимальным по модулю остатком

$$\frac{p}{q} = A_0 + \cfrac{(-1)^{u_1}}{A_1 + \cfrac{(-1)^{u_1}}{\ldots + \cfrac{(-1)^{u_m}}{A_m}}}$$

длина которой равна m.

Пусть последовательностью подходящих дробей для обычного разложения будет последовательность

$$\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$$

. Выделим из этой последовательности подпоследовательность

$$\left\{\frac{p_{i_s}}{q_{i_s}}\right\}_{s=0}^{m}$$

следующим образом:

$$\frac{p_{i_1}}{q_{i_1}} = \begin{cases} \frac{p_1}{q_1}, & \text{если } a_1 > 1, \\ \frac{p_2}{q_2}, & \text{если } a_1 = 1, \end{cases}$$

и т. д., т. е., если значение $\frac{p_{i_s}}{q_{i_s}}$ мы выбрали равным $\frac{p_k}{q_k}$, то значение $\frac{p_{i_s+1}}{q_{i_s+1}}$ ищется так:

$$\frac{p_{i_s+1}}{q_{i_s+1}} = \begin{cases} \frac{p_{k+1}}{q_{k+1}}, & \text{если } a_{k+1} > 1, \\ \frac{p_{k+2}}{q_{k+2}}, & \text{если } a_{k+1} = 1. \end{cases}$$

Покажем, что построенная таким образом последовательность является последовательностью подходящих дробей для разложения $\frac{p}{q}$ в цепную дробь с минимальным по модулю остатком методом математической индукции.

Предположим, что $\frac{P_s}{Q_s} = \frac{p_{i_s}}{q_{i_s}}$ (равное по построению $\frac{p_k}{q_k}$). Покажем, что $\frac{P_{s+1}}{Q_{s+1}}$ ищется по формулам (1): если $a_{k+1} > 1$ и $k+1 \neq n$, то остаток, получающийся на этом шаге при обычном разложении, будет

$$r = \cfrac{1}{a_{k+1} + \cfrac{1}{a_{k+2} + \cfrac{1}{\ldots + \cfrac{1}{a_n}}}} < \frac{1}{a_{k+1}} \leq \frac{1}{2},$$

т. е., $r < 1/2$, следовательно, r совпадает с остатком при разложении с минимальным по модулю остатком.

И тогда $\frac{P_{s+1}}{Q_{s+1}} = \frac{p_{k+1}}{q_{k+1}}$. Поэтому, если $a_{k+1} > 1$ и $k+1 = n$, то доказательство окончено.

Если же $a_{k+1} = 1$, то $k+1 \neq n$, и получающийся остаток при обычном разложении будет

$$r = \frac{1}{a_{k+1} + \frac{1}{a_{k+1} + \frac{1}{\ldots + \frac{1}{a_n}}}} = \frac{1}{1 + \frac{1}{a_{k+2} + \frac{1}{\ldots + \frac{1}{a_n}}}} > \frac{1}{1+1} = \frac{1}{2},$$

так как

$$\frac{1}{a_{k+2} + \frac{1}{\ldots + \frac{1}{a_n}}} < 1.$$

Таким образом, $r > \frac{1}{2}$. Следовательно, для разложения с минимальным по модулю остатком остаток R полагается равным $1 - r$. Получаем:

$$\begin{cases} A_s = & a_{k+1}, \\ u_{s+1} = & 1, \\ A_{s+1} = & a_{k+2} + 1. \end{cases}$$

Тогда соответствующая часть разложения с минимальным по модулю остатком будет выглядеть следующим образом:

$$A_s + \frac{(-1)^{u_s+1}}{A_{s+1}} = a_k + 1 - \frac{1}{a_{k+2}+1} =$$

$$= a_k + (1 - \frac{1}{a_{k+2}+1}) = a_k + (\frac{a_{k+2}}{a_{k+2}+1}) =$$

$$= a_k + \frac{1}{\frac{a_{k+2}+1}{a_{k+2}}} = a_k + \frac{1}{1 + \frac{1}{a_{k+2}}} = a_k + \frac{1}{a_{k+1} + \frac{1}{a_{k+2}}},$$

и, значит, будет равна соответствующей части обычного разложения, однако короче на одно деление. Из последней серии равенств в частности следует, что $\frac{P_{s+1}}{Q_{s+1}} = \frac{p_{k+2}}{q_{k+2}}$. Тем самым шаг индукции выполнен и утверждение доказано. Из него выводится, что $2m \geq n$.

Рассмотрим два разложения для дроби Фибоначчи $\frac{F_{2n-1}}{F_{2n}}$. Последовательностью подходящих дробей для обычного разложения будет

$$\frac{p_1}{q_1} = 0; \frac{p_2}{q_2} = \frac{F_1}{F_2} = 1; \frac{p_3}{q_3} = \frac{F_2}{F_3} = \frac{1}{2}; \ldots; \frac{p_{2n}}{q_{2n}} = \frac{F_{2n-1}}{F_{2n}}$$

— всего $2n$ элементов.

Последовательностью $\{\frac{p_{i_s}}{q_{i_s}}\}_{s=0}^{m}$, строящейся в соответствии с изложенным выше алгоритмом, является

$$\frac{p_{i_1}}{q_{i_1}} = \frac{p_2}{q_2} = 1; \frac{p_{i_2}}{q_{i_2}} = \frac{p_4}{q_4} = \frac{2}{3}; \ldots; \frac{p_{i_n}}{q_{i_n}} = \frac{p_{2n}}{q_{2n}} = \frac{F_{2n-1}}{F_{2n}}$$

— n элементов.

Значит, наименьшее отношение длин m/n разложений равно $\frac{1}{2}$.

§9. ТАЙНА ПИФАГОРЕЙЦЕВ

Алгоритм Евклида, примененный к паре отрезков, построит отрезок, укладывающийся целое число раз в каждом из них; он является общей

мерой рассматриваемых отрезков. Задолго до Евклида пифагорейцы обнаружили поразительный факт, что существуют несоизмеримые отрезки, не имеющие общей меры. Алгоритм Евклида, будучи применен к таким парам отрезков, никогда не закончит работы.

9.1. Докажите геометрически, что сторона и диагональ квадрата, а также, что основание и боковая сторона равнобедренного треугольника с углами 72° при основании, несоизмеримы.

9.2. Вычислите отношения длин упомянутых пар отрезков и разложите их в цепные дроби (они, конечно, будут бесконечными).

Как отмечалось в параграфе 6, любое положительное рациональное число можно представить в виде бесконечной периодической дроби. Будем рассматривать также бесконечные непериодические дроби. Числа, представляемые ими, называются **иррациональными.**

9.3. Докажите, что следующие числа иррациональны:

$$10^{-1}+10^{-4}+\ldots+10^{-n^2}+\ldots., 10^{-1}+10^{-2}+\ldots+10^{-n!}+\ldots,$$

$$3^{-1}+3^{-3}+\ldots+3^{-n(n-1)/2}+\ldots .$$

9.4. Докажите, что не существует 11 бесконечных десятичных дробей, каждые две из которых совпадают лишь в конечном числе разрядов.

9.5. Докажите, что в каждой бесконечной дроби существует последовательность десятичных знаков произвольной длины, которая в разложении дроби встречается бесконечное число раз.

9.6*. *(BMO, 83)* В бесконечной дроби встречаются все цифры. Пусть u_n — количество различных цифровых отрезков длины n, встречающихся в ней. Докажите, что если дробь изображает иррациональное число, то u_n строго монотонно возрастает и поэтому всегда $u_n \geq n+9$, а если дробь периодична, то последовательность u_n сначала монотонно возрастает, а потом стабилизируется и поэтому начиная с некоторого n выполняется неравенство $u_n < n$.

Следующие задачи указывают путь более строгого построения системы действительных чисел, чем это обычно делается в школе. Далее будем рассматривать бесконечные десятичные дроби, а конечные дроби, если нужно, превращать в бесконечные, добавляя к ним в конце бесконечную последовательность нулей.

9.7. Будем говорить, что одна бесконечная десятичная дробь не меньше другой, если в них несколько начальных цифр совпадают, а следующая цифра в первой дроби больше, чем во второй (или сразу начальная цифра первой дроби больше). Могут ли эти дроби изображать равные числа?

9.8. Докажите, что между любыми двумя числами найдется бесконечно много как рациональных, так и иррациональных чисел (число a лежит между b и c, если $b < a < c$).

9.9. Докажите, что для любой бесконечной возрастающей ограниченной последовательности десятичных дробей найдется дробь, у которой для любого n первые n цифр совпадают с первыми n цифрами любой дроби из этой последовательности, имеющей достаточно большой номер (последовательность ограничена, если все ее дроби меньше некоторой одной и той же дроби). Докажите, что эта дробь определяется по последовательности однозначно (и называется пределом этой последовательности).

9.10. Для каждой дроби, заканчивающейся девяткой в периоде, найдется дробь, заканчивающаяся нулем в периоде, изображающая то же самое рациональное число. Остальные дроби назовем истинно бесконечными. Различные истинно бесконечные дроби изображают различные числа.

9.11. Докажите, что любая дробь является пределом некоторой бесконечной ограниченной возрастающей последовательности дробей, а для истинно бесконечной дроби эту последовательность можно составить из дробей, заканчивающихся нулем в периоде.

Определим сумму двух бесконечных дробей, не заканчивающихся девяткой в периоде, следующим образом. Рассмотрим последовательности из предыдущей задачи, построенные для этих дробей (если дробь заканчивается нулем в периоде, то в качестве такой последовательности берем саму эту дробь, повторенную бесконечное число раз). Складывая члены этих последовательностей, имеющие одинаковые номера, получим последовательность такого же вида. Предел ее и назовем **суммой двух дробей.**

9.12. Докажите, что для любых чисел a, b, c имеем

$$a + b = b + a, a + (b + c) = (a + b) + c$$

(не забудьте, что рациональные числа вида $m \cdot 10^{-n}$ изображаются дробями двумя способами).

9.13*. По аналогии с предыдущей задачей определите умножение дробей и докажите тождества $ab = ba, a(bc) = (ab)c, (a + b)c = ac + bc$.

9.14*. Докажите, что для любой дроби a найдется дробь b, такая что $ab = 1$. Выбрав дробь a_0 так, чтобы $0 < 1 - a_0 a$, можно получить число a как предел последовательности дробей $a_{n+1} = 2a_n - aa_n^2$.

Из 9.14 следует, что для любых дробей a и b найдется дробь c, такая, что $cb = a$; соответствующее ей число обозначают a/b.

Аналогичная задача для сложения имеет решение только если $a \geq b$; тогда через $a - b$ обозначают такое число c, что $c + b = a$. Чтобы она имела решение всегда, введем в рассмотрение отрицательные числа, которые будем изображать дробями со знаком минус перед ними (нулевая дробь пишется без знака: $-0 = 0$). Определим операции над положительными и отрицательными дробями с помощью равенств

$$(-a)b = a(-b) = -ab, (-a)(-b) = ab, (-a) + (-b) = -(a + b),$$

$$(-a)+b=\begin{cases} b-a, & \text{если } b\geq a,\\ -(a-b), & \text{если } b<a,\end{cases}$$

$$a+(-b)=\begin{cases} a-b, & \text{если } a\geq b,\\ -(b-a), & \text{если } a<b.\end{cases}$$

9.15. Докажите, что для дробей со знаками и так определенных операций над ними справедливы все тождества, указанные в задачах 9.12 – 15, а также что для любых дробей a и b найдется дробь c такая, что $c+b=a$.

Соответствующее число обозначается $a-b$ и называется разностью a и b. Разность $0-a$ обозначается просто $-a$.

9.16*. Докажите, что для любого $a\geq 0$ и любого натурального n найдется такое единственное b, что $b^n=a$; оно обозначается $\sqrt[n]{a}$.

Далее предлагаются задачи на доказательство иррациональности некоторых чисел.

9.17. Докажите, что для любого $a\in\mathbb{N}$ либо $\sqrt[n]{a}\in\mathbb{N}$, либо оно иррационально.

9.18. Докажите иррациональность чисел

$$\sqrt{2}+\sqrt{3},\ \sqrt{2}+\sqrt[3]{3},\ \sqrt[3]{2}+\sqrt[3]{3},\ \sqrt{2}+\sqrt{3}+\sqrt{5}.$$

9.19*. Докажите иррациональность чисел $\sqrt[4]{2}+\sqrt[4]{4}+\sqrt[4]{8}$, $\sqrt[3]{2}+\sqrt[3]{3}+\sqrt[3]{5}$.

9.20. Будет ли иррациональным число $(\sqrt{2}+1)^n-(\sqrt{2}-1)^n$?

9.21. Будет ли иррациональным число $\sqrt{n^3+1}$ при нечетном n? А при четном?

9.22*. *(Материалы жюри IMO)* Будет ли иррациональным число

$$\sqrt[3]{\sqrt{5}+2}-\sqrt[3]{\sqrt{5}-2}?$$

Числа $x_1,\ldots,x_n$ называются рационально независимыми, если для рациональных чисел $q_1,\ldots,q_n$ равенство $q_1x_1+\ldots+q_nx_n=0$ справедливо лишь когда все $q_i=0$.

9.23*. Пусть $b_1,\ldots,b_m$ — разные произведения различных простых чисел из множества $\{p_1,\ldots,p_n\}$, $m\leq 2^n-1$ (произведение может состоять и из одного множителя) . Докажите, что числа $1,\sqrt{b_1},\ldots,\sqrt{b_m}$ являются рационально независимыми и выведите отсюда, что число $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}+\sqrt{11}+\sqrt{13}$ иррационально.

9.24. Пусть $p_1,\ldots,p_n$ — различные простые числа. Докажите, что их логарифмы $\ln p_i$ рационально независимы.

Следующие задачи посвящены понятию предела.

9.25. Докажите, что из любой бесконечной последовательности чисел можно выбрать монотонную бесконечную подпоследовательность (неубывающую или невозрастающую).

9.26. а) *(Вейерштрасс)* Докажите, что монотонная ограниченная последовательность чисел имеет предел.

б)* Докажите, что число

$$e = 2 + 1/2! + ... + 1/n! + ...,$$

равное пределу $\lim\limits_{n\to\infty}(2 + 1/2! + ... + 1/n!)$, иррационально.

9.27. *(Больцано – Вейерштрасс)* Докажите, что из любой ограниченной бесконечной последовательности можно выбрать бесконечную подпоследовательность, имеющую предел.

В последнем цикле задач речь идет о бесконечных цепных дробях.

9.28. Докажите для любой цепной дроби, что подходящие к ней дроби с четными номерами образуют возрастающую, а с нечетными — убывающую последовательность. При этом любая дробь с нечетным номером больше любой дроби с четным номером.

9.29. Докажите, что значение α цепной дроби связано с ее подходящими дробями неравенством $|\alpha - \frac{p_k}{q_k}| \le \frac{1}{q_k q_{k+1}}$.

Наряду с конечными можно рассматривать и бесконечные цепные дроби, причем составленные из произвольных положительных элементов. Для таких дробей верны утверждения 9.25, 27. Дробь называется **сходящейся**, если пределы последовательностей четных и нечетных подходящих к ней дробей равны.

9.30. Докажите, что любая цепная дробь с натуральными элементами сходится.

Можно доказать, что для сходимости произвольной цепной дроби необходимо и достаточно, чтобы сумма первых n ее элементов неограниченно росла с ростом n.

Отметим, что любое рациональное число разлагается в конечную цепную дробь. Если же разложить иррациональное число в цепную дробь, то она окажется бесконечной.

9.31. Докажите, что предел цепной дроби числа равен самому числу.

Тем самым устанавливается взаимно-однозначное соответствие между действительными числами и представляющими их цепными дробями. Рациональным числам соответствуют конечные, а иррациональным — бесконечные дроби.

9.32. Докажите, что

$$\left(\frac{1}{1+}\frac{1}{1+}\right)^3 = \frac{1}{4+}\frac{1}{4+}\ldots, \quad \left(\frac{1}{1+}\frac{1}{1+}\right)^2 = \frac{1}{3-}\frac{1}{3-}\ldots.$$

9.33. И вообще, для произвольных натуральных n, k существуют такие натуральные m, l, s, что

$$\left(\frac{1}{n+}\frac{1}{n+}\ldots\right)^{2k+1} = \frac{1}{m+}\frac{1}{m+}\ldots, \left(\frac{1}{n+}\frac{1}{n+}\ldots\right)^{2k} = \frac{1}{l-}\frac{1}{l-}\ldots,$$

$$\left(\frac{1}{n-}\frac{1}{n-}\dots\right)^k = \frac{1}{s-}\frac{1}{s-}\dots.$$

9.34*. Докажите, что справедливы следующие равенства

$$\left(\frac{1}{1+}\frac{1}{1+}\right)^{2k+1} = \frac{1}{a+}\frac{1}{a+}\dots, \left(\frac{1}{1+}\frac{1}{1+}\right)^{2k} = \frac{1}{b-}\frac{1}{b-}\dots,$$

где $a = F_{2k+2} + F_{2k}, b = F_{2k+1} + F_{2k-1}$, а F_n —последовательность Фибоначчи.

9.35*. В равенствах задачи 9.33 при $n = F_{2r+2} + F_{2r}$ числа m и l равны

$$m = F_{(2k+1)(2r+1)+1} + F_{(2k+1)(2r+1)-1},$$

$$l = F_{2k(2r+1)+1} + F_{2k(2r+1)-1},$$

а если $n = F_{2r+1} + F_{2r-1}$, то $s = F_{2rk+1} + F_{2rk-1}$.

9.36*. (*А. Н. Колмогоров*) Пусть, как и ранее, символ $[x]$ обозначает целую часть числа x. *Положительным вещественным числом* называется однозначная функция

$$m = \varphi(n),$$

определенная для всех натуральных чисел n, принимающая целые значения m и обладающая следующими свойствами:

1) для всех натуральных чисел k справедливо равенство

$$\varphi(n) = \left[\frac{\varphi(kn)}{k}\right];$$

2) для любого натурального числа n существует такое натуральное число k, что

$$\varphi(kn) > k\varphi(n).$$

Положительные вещественные числа будем обозначать малыми греческими буквами, а множество всех положительных вещественных чисел буквой Ф. Отношение порядка и операции сложения и умножения вводятся в множестве Ф следующим образом.

Неравенство $\varphi < \psi$ между вещественными числами φ, ψ обозначает, что существует такое натуральное число n, для которого имеют место соотношения

$$\varphi(n) < \psi(n), \varphi(1) = \psi(1), \dots, \varphi(n-1) = \psi(n-1).$$

Сумма $\chi = \varphi + \psi$ обозначает, что для всех натуральных n

$$\chi(n) = \max_k \left[\frac{\varphi(kn) + \psi(kn)}{k}\right],$$

где максимум берется по всем натуральным k.

Произведение $\chi = \varphi \cdot \psi$ обозначает, что для всех натуральных n

$$\chi(n) = \max_{k,k'} \left[\frac{\varphi(kn)\psi(kn)}{kk'n} \right],$$

где максимум берется по всем парам натуральных чисел k, k'.

Докажите, что множество Φ с определенными выше отношением порядка и операциями сложения и умножения обладает всеми свойствами обычных положительных вещественных чисел, т.е. изоморфно системе положительных вещественных чисел, построенных любым другим общепринятым способом.

УКАЗАНИЯ

9.14. Если $1 - a_n a = \epsilon_n$, то $\epsilon_{n+1} = \epsilon_n^2$.

9.20. *Ответ:* нет.

9.21. Примените индукцию по n.

9.22. *Ответ:* нет, так как оно равно 1.

9.23. Примените индукцию.

9.24. Примените основную теорему арифметики (задача 3.17).

9.26. б) Сначала примените задачу 9.26а), а при доказательстве иррациональности рассуждайте от противного.

9.32-9.35. Положим

$$\rho = \frac{1}{n+} \frac{1}{n+} \ldots,$$

тогда

$$\rho = \frac{1}{n+\rho}, \quad 0 < \rho < 1,$$

значит,

$$\rho = \frac{\sqrt{n^2+4} - n}{2}$$

Обозначим $\rho^{-2k+1} - \rho^{2k-1}$ через y_k, тогда

$$y_0 = -y_1 = -n, y_{k+1} = y_k(\rho^2 + \rho^{-2}) - y_{k-1} = y_k(n^2+2) - y_{k-1} \in \mathbb{N},$$

поэтому ρ^{2k+1} есть корень уравнения

$$x = \frac{1}{x+m}, m = y_{k+1} \in \mathbb{N}.$$

Значит,

$$\rho^{2k+1} = \frac{1}{m + \rho^{2k+1}} = \frac{1}{m+} \frac{1}{m+} \ldots,$$

так как $0 < \rho^{2k+1} < 1$.

Пусть $n = 1$. Докажем, что $y_k = F_{2k-2} + F_{2k}$. Это верно при $k = 1, 2$. Далее по индукции имеем

$$\begin{aligned} y_{k+1} &= 3y_k - y_{k-1} = 3F_{2k} + 3F_{2k-2} - F_{2k-2} - F_{2k-4} = \\ &= 3F_{2k} + 2F_{2k-2} - F_{2k-4} = \\ &= F_{2k} + (2F_{2k} + 2F_{2k-2} - F_{k-2} + F_{2k-3}) = \\ &= F_{2k} + (2F_{2k} + F_{2k-2} + F_{2k-3}) = F_{2k} + (2F_{2k} + F_{2k-1}) = \\ &= F_{2k} + (F_{2k} + F_{2k+1}) = F_{2k+2} + F_{2k}. \end{aligned}$$

Обозначим $\rho^{-2k}+\rho^{2k}$ через z_k, тогда

$$z_0=2,\quad z_1=n^2+2,\quad z_{k+1}=z_kz_1-z_{k-1}=z_k(n^2+2)-z_{k-1}\in\mathbb{N},$$

поэтому ρ^{2k} есть корень уравнения

$$x=\frac{1}{l-x},\quad l=z_{k+1}\in\mathbb{N}.$$

Значит,

$$\rho^{2k}=\cfrac{1}{l-\cfrac{1}{l-\cfrac{1}{\ddots}}},$$

так как $0<\rho^{2k}<1$.

Если $n=1$, то $z_k=F_{2k+1}+F_{2k-1}$, так как

$$z_1=3=F_3+F_1, z_0=2=F_1+F_{-1},$$

$$z_{k+1}=3z_k-z_{k-1}=3F_{2k+1}+3F_{2k-1}-F_{2k-1}-F_{2k-3}=F_{2k+3}+F_{2k+1}.$$

Пусть

$$\lambda=\cfrac{1}{n-\cfrac{1}{n-\cfrac{1}{\ddots}}},$$

тогда $\lambda=\frac{1}{n-\lambda}$, $0<\lambda<1$, значит,

$$\lambda=\frac{-\sqrt{n^2+4}+n}{2}.$$

Обозначим $\lambda^{-k}+\lambda^k$ через x_k, тогда

$$x_0=2, x_1=n, x_{k+1}=x_k(\lambda+\frac{1}{\lambda})-x_{k-1}=x_kn-x_{k-1}\in\mathbb{N},$$

следовательно, λ^k есть корень уравнения

$$x=\frac{1}{s-x},\quad s=x_{k+1}\in\mathbb{N}.$$

Поэтому

$$\lambda^k=\cfrac{1}{s-\cfrac{1}{s-\cfrac{1}{\ddots}}},$$

так как $0<\lambda^k<1$.

9.36. Покажите, что при любом натуральном числе r функция

$$\varphi(n)=\varphi_r(n)=nr-1$$

удовлетворяет условиям 1 и 2, т.е. является положительным вещественным числом.

Это "число" φ_r естественно идентифицировать с натуральным числом r.

Присоединив к множеству Ф функцию $\varphi \equiv 0$, т.е. число *нуль*, условившись, что

$$0 + 0 = 0,\ 0 \cdot 0 = 0$$

и для всех φ из Ф

$$0 < \varphi,\ \varphi + 0 = 0 + \varphi = \varphi,\ \varphi \cdot 0 = 0 \cdot \varphi = 0,$$

получим систему неотрицательных целых чисел.

Для любого φ из Ф положим $[\varphi] = m$ — наибольшему целому числу, не превосходящему φ, т.е.

$$m \leq \varphi < m + 1$$

(целая часть числа φ).

Затем для любого неотрицательного целого числа m и натурального числа n определим операцию деление в Ф как действие, обратное умножению и целое число $[m/n]$, которое совпадает с неполным частным этих чисел, определенным непосредственно.

Наконец, можно доказать, что для любого φ из Ф

$$\varphi(n) = \begin{cases} \varphi n - 1, & \text{если } \varphi \text{ — целое число,} \\ [\varphi n] - 1, & \text{если } \varphi \text{ — нецелое число.} \end{cases}$$

Таким образом $\varphi(n)$ — наибольшее целое число m, для которого

$$\frac{m}{n} < \varphi.$$

§ 10. КВАДРАТНЫЕ КОРНИ, ЦЕПНЫЕ ДРОБИ И УРАВНЕНИЕ ПЕЛЛЯ

10.1. Разложите в цепную дробь числа $\sqrt{3}, \sqrt{5}, \sqrt{6}$.

10.2. Разложите в цепную дробь числа $\sqrt{n^2 + 1}$, где n — натуральное.

10.3. Разложите в цепную дробь числа

$$\sqrt{(nm)^2 + 2m} \quad \text{и} \quad \sqrt{(nm)^2 + m},$$

где m, n — натуральные.

10.4*. Докажите, что среди чисел $\sqrt{N}$ только числа вида, указанного в 10.3, разлагаются в цепные дроби с двучленным периодом.

10.5*. *(Серпинский)* Докажите, что для числа $D = [(4m^2 + 1)n + m]^2 + 4mn + 1$, где m, n — натуральные, цепная дробь для $\sqrt{D}$ начинается с числа $a = (4m^2 + 1)n + m$, и далее является периодической с элементами периода $2m, 2m, 2a$.

Серпинский доказал, что только квадратные корни указанного вида разлагаются в цепные дроби с трехчленным периодом.

Целью этого трудного цикла задач является доказательство теоремы Лагранжа – Галуа о периодичности цепных дробей для квадратичных иррациональностей и оценка длины периода.

Число называется **квадратичной иррациональностью,** если оно является корнем квадратного уравнения с целыми коэффициентами. Это уравнение будет определено однозначно, если потребовать, чтобы его коэффициенты не имели общего делителя, на который их можно было бы сократить, а старший коэффициент был бы положителен.

10.6. Докажите, что квадратичная иррациональность имеет вид $\frac{P\pm\sqrt{D}}{Q}$, где P — целое, а Q и D — натуральные, D не является точным квадратом, а P^2-D делится на Q.

Числа $\frac{P-\sqrt{D}}{Q}$ и $\frac{P+\sqrt{D}}{Q}$ называются **сопряженными.**

Квадратичная иррациональность α представляется в виде $\frac{P\pm\sqrt{D}}{Q}$, указанном в 10.6, не однозначно.

10.7. Докажите, что если из всех представлений числа α выбрать представление с минимальным D, то оно уже будет единственным, причем D будет равно дискриминанту минимального квадратного уравнения для α, определенного в 10.6. Это число называется дискриминантом иррациональности α.

Числа α и β называются эквивалентными (обозначение $\alpha\sim\beta$), если для некоторых целых чисел p,p',q,q' таких, что $|pq'-p'q|=1$, справедливо равенство

$$\alpha=\frac{p\beta+p'}{q\beta+q'}.$$

10.8. Докажите, что $\alpha\sim\alpha,\alpha\sim-\alpha,\alpha\sim\alpha+m$ при всех целых m, $\alpha\sim 1/\alpha$; если $\alpha\sim\beta$, то $\beta\sim\alpha$; если $\alpha\sim\beta,\beta\sim\gamma$, то $\alpha\sim\gamma$; если α разложено в цепную дробь, то все ее остатки $r_n\sim\alpha$.

10.9. Докажите, что если квадратичные иррациональности α и β, эквивалентны, то их дискриминанты равны.

10.10. Докажите, что все числа вида $\alpha_1+\alpha_2\sqrt{D}$, где α_1 и α_2 рациональные, являются квадратичными иррациональностями с дискриминантами, делящимися на D; их множество обозначим $\mathbb{Q}(\sqrt{D})$. Проверьте, что результат арифметической операции над числами из множества $\mathbb{Q}(\sqrt{D})$ принадлежит ему же.

Число $\alpha=\frac{P+\sqrt{D}}{Q}$ называется приведенным, если $\alpha>1$ и для сопряженного числа α' справедливо неравенство $-1<\alpha'<0$.

10.11. Докажите, что

$$0<Q<P+\sqrt{D}<2\sqrt{D},\ \ |\sqrt{D}-Q|<P<\sqrt{D},$$

и, следовательно, существует лишь конечное количество приведенных квадратичных иррациональностей с данным дискриминантом D, которое обозначим через $K(D)$. Проверьте, что

$$K(D) \le [\sqrt{D}]^2 + [\sqrt{D}],$$

и для $Q = 1$ существует лишь одна приведенная иррациональность, а именно $[\sqrt{D}] + \sqrt{D}$, которая среди всех приведенных иррациональностей с данным дискриминантом D наибольшая по величине, а для числа $Q = 2[\sqrt{D}]$ также существует лишь одна приведенная иррациональность, именно,

$$([\sqrt{D}] + \sqrt{D})/2[\sqrt{D}],$$

которая среди всех приведенных иррациональностей с данным дискриминантом D наименьшая по величине.

10.12. Проверьте, что вторая по величине среди приведенных иррациональностей с данным дискриминантом D, равна $([\sqrt{D}] + \sqrt{D})/2$, если D и $[\sqrt{D}]$ одинаковой четности, и равна $([\sqrt{D}] - 1 + \sqrt{D})/2$, если D и $[\sqrt{D}] - 1$ одинаковой четности, причем она является единственной приведенной иррациональностью с $Q = 2$. Проверьте, что третья по величине среди приведенных иррациональностей с данным дискриминантом D, в случае D вида $3k$ равна $(P + \sqrt{D})/3$, где P — то из чисел $[\sqrt{D}] - 2, [\sqrt{D}] - 1, [\sqrt{D}]$, которое кратно 3, (в этом случае имеется одна приведенная иррациональность с $Q = 3$), в случае D вида $3k + 1$ равна $(P + \sqrt{D})/3$, где P наибольшее из $[\sqrt{D}] - 2, [\sqrt{D}] - 1, [\sqrt{D}]$, не кратное 3 (в этом случае имеются две приведенные иррациональности с $Q = 3$), в случае D вида $12k + 8$ или $12k + 5$ равна $(P + \sqrt{D})/4$, где P — то из чисел $[\sqrt{D}], [\sqrt{D}] - 1$, которое имеет одну четность с D (в этом случае не имеется ни одной приведенной иррациональности с $Q = 3$), а в оставшихся случаях она не больше $([\sqrt{D}] + \sqrt{D})/5$, так как тогда нет ни одной приведенной иррациональности с $Q = 3, 4$.

10.13*. Обозначим $K(D, Q)$ число таких $P = 1, 2, ..., Q$, что $D - P^2$ делится на Q. Докажите, что

$$K(D) \le K(D, 1) + K(D, 2) + ... + K(D, 2[\sqrt{D}]) \le \sqrt{\frac{512}{27}} D^{3/4} + \sqrt{\frac{8}{3}} D^{1/4}.$$

Проверьте, что при всех D справедливо неравенство

$$K(D) < D.$$

10.14*. Докажите, что чисто периодическая цепная дробь равна квадратичной иррациональности α такой, что $\alpha > 1, -1 < \alpha' = -\frac{1}{\beta} < 0$, где β определяется цепной дробью, период которой записывается теми же числами, что и α, только в обратном порядке.

10.15. *(Эйлер)* Докажите, что любая (смешанно) периодическая цепная дробь изображает квадратичную иррациональность.

10.16*. *(Лагранж – Галуа)* Докажите, что любая квадратичная приведенная иррациональность с дискриминантом D разлагается в чисто периодическую цепную дробь с периодом, не превосходящим $K(D)$.

Согласно 10.8 все приведенные квадратичные иррациональности с дискриминантом D разбиваются на непересекающиеся классы, состоящие из всех попарно эквивалентных чисел каждый.

10.17*. Докажите, что для каждой приведенной иррациональности длина периода соответствующей дроби равна количеству чисел в классе, содержащем эту иррациональность, и, следовательно, сумма периодов попарно не эквивалентных приведенных иррациональностей с дискриминантом D не больше $K(D)$.

10.18*. Докажите, что все элементы цепной дроби из 10.16 не превосходят $2[\sqrt{D}]$, причем на периоде это число встречается не более одного раза, а все остальные элементы периода не превосходят наибольшего из чисел $[\sqrt{D}]$ и $[\sqrt{D}]-1$, имеющего одинаковую четность с D, причем это число встречается на периоде не более одного раза. Если на периоде цепной дроби для иррациональности с дискриминантом D встречается число $2[\sqrt{D}]$, то эта иррациональность эквивалентна $\sqrt{D}$.

10.19*. Докажите, что $\sqrt{N}+[\sqrt{N}]$ представляется чисто периодической цепной дробью, причем период начинается числом $2[\sqrt{N}]$, а оставшаяся его часть состоит из чисел, не превосходящих $[\sqrt{N}]$, и не меняется, если ее записать в обратном порядке, причем числа $[\sqrt{N}]$ или $[\sqrt{N}]-1$ могут стоять только в ее середине.

10.20*. *(Теорема Лагранжа)* Докажите, что любая квадратичная иррациональность с дискриминантом D разлагается в периодическую цепную дробь с периодом, не превосходящим $K(D)$.

Следующий цикл задач посвящен уравнению Пелля, которое, возможно правильнее называть уравнением Архимеда – Брахмагупты – Бхаскары – Ферма. Пусть N не является квадратом натурального числа. Уравнению $x^2-Ny^2=1$, которое надо решить в натуральных числах, Эйлер по недоразумению приписал имя Пелля (в случае, когда N — квадрат, оно не имеет таких решений, — разложите на множители).

10.21. Проверьте, что если (x_1,y_1) и (x_2,y_2) — решения этого уравнения, то натуральные x и y такие, что

$$x+y\sqrt{N}=(x_1+y_1\sqrt{N})(x_2+y_2\sqrt{N}),$$

тоже будут его решениями.

10.22. Докажите, что если два числа представимы в виде $x^2 - Ny^2$, где x и y — натуральные, то их произведение тоже представимо в таком виде.

10.23. Пусть

$$x_1^2 - Ny_1^2 = x_2^2 - Ny_2^2 = k,$$

k — натуральное число, пары (x_1, y_1) и (x_2, y_2) различны и имеют одинаковые остатки при делении на k. Докажите, что пара натуральных x и y таких, что

$$x + y\sqrt{N} = (x_1 + y_1\sqrt{N})/(x_2 - y_2\sqrt{N}) =$$

$$= (x_1 + y_1\sqrt{N})(x_2 + y_2\sqrt{N})/(x_1^2 - Ny_1^2),$$

является решением уравнения $x^2 - Ny^2 = 1$.

10.24. Докажите, что если пара натуральных чисел (x, y) — решение уравнения $x^2 - Ny^2 = 1$, то пары натуральных чисел (x_n, y_n) такие, что

$$x_n + y_n\sqrt{N} = (x_1 + y_1\sqrt{N})^n,$$

являются также его решениями.

10.25*. Пусть пара натуральных чисел (x, y) — решение уравнения $x^2 - Ny^2 = 1$ с наименьшим $x + y\sqrt{N}$. Докажите, что все решения уравнения получаются из x, y так, как указано в 10.24.

В следующих задачах речь идет о решении отдельных типов уравнения Пелля.

10.26. Решите уравнение $x^2 - (n^2 + 1)y^2 = 1$.

10.27. Решите уравнение $x^2 - ((nm)^2 + m)y^2 = 1$.

10.28. Решите уравнение $x^2 - ((nm)^2 + 2m)y^2 = 1$.

10.29. Решите уравнение $x^2 - (n^2 - 1)y^2 = 1$.

10.30. Решите уравнение $x^2 - (n^2 - 2)y^2 = 1$.

10.31. Решите уравнение $x^2 - ((nm)^2 - m)y^2 = 1$.

10.32. Решите уравнение $x^2 - ((nm)^2 - 2m)y^2 = 1$.

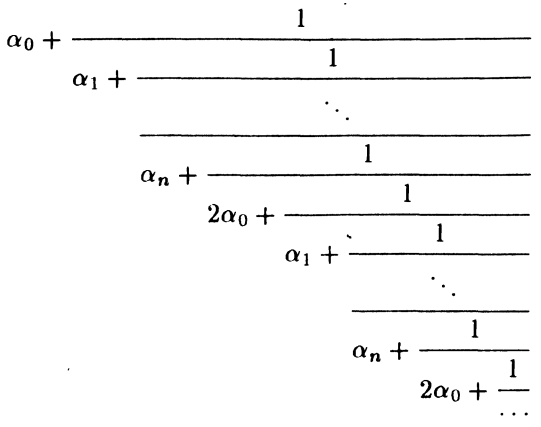
Далее предлагается доказать разрешимость уравнения Пелля в общем виде.

10.33. Разложим $\sqrt{N}$ в цепную дробь.Докажите, что

$$0 < p_{2n}^2 - Nq_{2n}^2 < 2\sqrt{N} + 1.$$

10.34*. *(Лагранж)* Докажите, что уравнение Пелля $x^2 - Ny^2 = 1$ имеет бесконечно много решений в натуральных числах.

10.35*. *(Метод лорда Браункера)* Пусть разложение $\sqrt{N}$ в цепную дробь имеет вид



(а это верно согласно 10.19). Тогда числитель и знаменатель n-й подходящей дроби p_n/q_n удовлетворяют уравнению

$$x^2 - Ny^2 = (-1)^{n-1}.$$

Если n нечетно, то получается решение уравнения Пелля. Если n четно, то его решением будет $x = p_{2n+1}, y = q_{2n+1}$.

Можно доказать, что метод Браункера в действительности дает минимальные решения;однако, видимо, неизвестно, как охарактеризовать числа N, для которых получается четное n.

10.36*. Применяя метод Браункера, найдите решения уравнений Пелля для $N = [(4m^2 + 1)n + m]^2 + 4mn + 1$, где m, n — натуральные.

В следующем цикле задач рассматривается так называемое уравнение "минус Пелль".

10.37*. В отличие от уравнения Пелля уравнение $x^2 - Ny^2 = -1$ не всегда имеет решение. Докажите, что если N делится на 4 или какое-нибудь простое число вида $4k + 3$, то это уравнение решений не имеет.

Условие, указанное в 10.37, не является необходимым, так как оно не выполняется для $N = 34$, а уравнение $x^2 - 34y^2 = -1$ неразрешимо в целых числах. В тех случаях, когда уравнение $x^2 - Ny^2 = M$ разрешимо, его решения можно отыскать с помощью подходящих дробей к цепной дроби для $\sqrt{N}$.

10.38*. *(Лежандр)* Докажите, что если p — простое число вида $4k+$

$+1$, то уравнение $x^2 - p^m y^2 = -1$ при $m \in \mathbb{N}$ разрешимо в натуральных числах.

10.39*. Докажите, что если длина периода дроби для $\sqrt{N}$ нечетна, то N можно представить в виде суммы квадратов натуральных чисел. То же самое верно, если найдутся две приведенные квадратичные иррациональности, у которых периоды взаимно обратны, то есть один из них получается из второго, если его числа переставить в противоположном порядке.

10.40. Докажите, что если уравнение $x^2 - Ny^2 = M$ разрешимо в целых числах, то оно имеет бесконечно много таких решений.

10.41*. Пусть длина периода цепной дроби для $\sqrt{N}$ равна n. Докажите, что последовательность $p_k^2 - Nq_k^2$ периодическая с периодом n, если n четно и антипериодическая с антипериодом n, если n нечетно, а, следовательно, периодическая с периодом $2n$. Период начинается с $k = 1$ (последовательность называется антипериодической, если ее член меняет знак при прибавлении к ее номеру длины антипериода).

Несколько задач на применение уравнения Пелля.

10.42. Сколько существует прямоугольных треугольников с целочисленными сторонами (пифагоровых треугольников), у которых длины катетов отличаются на 1?

10.43. Решите в целых числах уравнение $(x+1)^3 - x^3 = y^2$.

10.44. Докажите, что если уравнение $x^2 - 2y^2 = n$ разрешимо в целых числах, то существует его решение, для которого имеем неравенства $0 < x \leq \sqrt{2n}, 0 < y \leq \sqrt{n/2}$.

Два примера радикалов с длинными периодами цепных дробей.

10.45*. Докажите, что разложение $\sqrt{n^2+n+1}$ при $n = 3^k$ имеет период

$$1, 1, \frac{2n}{3} - 1, 1, 5, \frac{2n}{3^2} - 1, 1, ..., 1, 2\cdot 3^{s-1} - 1, \frac{2n}{3^s} - 1, 1, ..., 1, 2\cdot 3^{k-1} - 1, 1, 2n$$

и его длина с точностью до нескольких единиц равна $\frac{3}{2}\log_3 D$, где

$$D = n^2 + n + 1.$$

10.46*. Докажите, что разложение числа $\sqrt{D}$ при $D = n^2 - \alpha$, $n = (2\alpha^k + \alpha + 1)/2$ и нечетном $\alpha > 1$ имеет период

$$1, 2\alpha^{k-1}, \alpha, 2\alpha^{k-2}, \alpha^2, \ldots,$$

$$2\alpha, \alpha^{k-1}, 2, n-1, 2, \alpha^{k-1}, 2\alpha, \ldots, \alpha, 2\alpha^{k-1}, 1, 2n-2$$

и его длина с точностью до нескольких единиц равна $2\log_\alpha D$.

10.47**. *(М. З. Гараев)* Докажите, что уравнение

$$x^3 + y^3 = (xy)^2 + (x+y)^2$$

не имеет решений в натуральных числах x, y.

10.48**. *(М. З. Гараев)* Докажите, что уравнение

$$x^3 + y^3 = (3xyz - 1)^2$$

не имеет решений в натуральных числах x, y, z.

10.49**. *(М. З. Гараев)* Пусть m, n — натуральные числа, $n \geq 2$. Докажите, что уравнение

$$2^{n-1}(x^n + y^n) = (x - y)^{mn}$$

не имеет решений в натуральных числах x, y.

10.50**. Докажите, что: а) уравнение Л. Эйлера

$$t^2 = 4xyz - x - y$$

не имеет решений в натуральных числах t, x, y, z.

б) ** *(М. З. Гараев)* Обобщенное уравнение Л. Эйлера

$$t^2 = 4xyzuv - xu^2 - yv^2$$

не имеет решений в натуральных числах t, x, y, z, u, v.

10.51**. *(В. Серпинский)* Докажите, что: а) уравнение

$$x^4 + 9x^2y^2 + 27y^4 = z^2$$

не имеет решений в целых числах x, y, z.

б) **. *(М. З. Гараев)* Уравнение

$$x^3 + y^3 + 4y^3 = 6xyz$$

имеет в ненулевых целых числах x, y, z единственное решение $(1, 1, 1)$ с точностью до пропорциональности общему множителю чисел x, y, z.

10.52**. *(Д. Д. Сильвестр)* Пусть A, B, C, D — произвольные вещественные числа, (α, β, γ) — произвольное решение уравнения

$$Ax^3 + By^3 + Cz^3 = Dxyz.$$

Тогда, докажите, что

$$ABCf^3 + g^3 + h^3 = Dfgh,$$

где

$$h = A^2B\alpha^6\beta^3 + B^2C\beta^6\gamma^3 + C^2A\gamma^6\alpha^3 - 3ABC\alpha^3\beta^3\gamma^3,$$

$$g = AB^2\alpha^3\beta^6 + BC^2\beta^3\gamma^6 + CA^2\gamma^3\alpha^6 - 3ABC\alpha^3\beta^3\gamma^3,$$

$$f = \alpha\beta\gamma(A^2\alpha^6 + B^2\beta^6 + C^2\gamma^6 - AB\alpha^3\beta^3 - AC\alpha^3\gamma^3 - BC\beta^3\gamma^3).$$

10.53**. *(М. З. Гараев)* а) Пусть n — целое число и уравнение

$$x^3 + y^3 + y^3 = nxyz$$

разрешимо в ненулевых целых (натуральных) числах.

Тогда докажите, что для любого натурального числа N существует такой набор $(x(N), y(N), z(N))$ ненулевых целых (натуральных) чисел, являющийся решением этого уравнения, который удовлетворяет условиям

$$(x(N), y(N)) = (y(N)z(N), N) = 1.$$

б) Пусть n — натуральное число, x, y, z — попарно взаимно простые натуральные числа, удовлетворяющие уравнению

$$x^3 + y^3 + y^3 = nxyz.$$

Пусть, далее, $d = (x + y, z)$, т.е. $x + y = da$, $z = db$, $(a, b) = 1$.

Тогда докажите, что существует натуральное число α, такое, что n^3 дает остаток 27 при делении на число α, $(\alpha, a) = (\alpha, b) =$ наибольший общий делитель чисел α и $nb - a$ является делителем числа 4, кроме того, выполняются равенства

$$\alpha(4d^2b^2 + n(x - y)^2) = a(n^2ab - na^2 + 12b^2),$$

$$\alpha(d^2b^2 + n(x - y)^2) = (nb - a)(na^2 - 3b^2).$$

в) Пусть натуральное число n имеет вид $4k$ или $8k - 1$ или $2^{2m+1}(2k - 1) + 3$, где k и m — натуральные числа. Тогда уравнение

$$x^3 + y^3 + z^3 = nxyz$$

не имеет решений в натуральных числах x, y, z.

г) При значениях n, указанных в п. в) этой задачи уравнение

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = n$$

не имеет решений в натуральных числах x, y, z.

10.54**. *(М. З. Гараев)* Пусть функции $f(n, m)$, $g(n, m)$ натуральных аргументов n, m, принимающие неотрицательные целые значения, таковы, что система неравенств

$$\begin{cases} n \leq & f(n, m) + 2g(n, m) + 5, \\ m \leq & 2f(n, m) + g(n, m) + 5, \end{cases}$$

имеет конечное число решений в натуральных числах n, m.

Тогда докажите, что уравнение

$$x^3 + f(x,z)x^2 + g(x,z)x + y + 1 = xyz$$

также имеет конечное число решениий в натуральных числах x, y, z.

10.55**. *(Х. Хессами Пилеруд)* а) Пусть k — не делящееся на 3, нечетное число. Тогда докажите, что уравнение

$$x^2 = y^3 - (4x^2 - 1)$$

не имеет решений в натуральных числах x, y.

б) Докажите, что уравнение

$$x^2 = y^3 - 10$$

не имеет решений в натуральных числах x, y.

10.56*. *(М. З. Гараев)* Пусть при целых x, y число $k = \frac{4x^2-1}{4x^2-y^2}$ — целое. Тогда $k = 1$.

10.57**. *(Х. Хессами Пилеруд)* а) При $N = 205,12317 = 109 \cdot 113,505$ уравнение $x^2 - Ny^2 = -1$ неразрешимо в целых числах.

б) Пусть уравнение $x^2 - Ny^2 = -1$ разрешимо в целых числах. Тогда существует представление числа N в виде $N = A^2 + B^2$, где A и B — натуральные числа, $(A, B) = 1$, причем A является нечетным числом и квадратичным вычетом по модулю N.

в) Пусть p — простое число, $p \equiv 5 \pmod 8$. Тогда уравнение

$$x^2 - 2py^2 = -1 \qquad (*)$$

разрешимо в целых числах.

г) Пусть $p \equiv 1 \pmod 8$, т.е. $p = A^2 + 16B^2$, где A, B — натуральные числа. Тогда если $p \equiv 1 \pmod{16}$, B — нечетное число, то уравнение (*) не имеет решений в целых числах; если $p \not\equiv 1 \pmod{16}$, B — четное число, то это уравнение также не имеет решений в целых числах.

Одной из классических задач теории диофантовых уравнений является задача о разрешимости уравнения

$$x^3 + y^3 = az^3$$

в целых ненулевых числах x, y, z. Здесь a — целое число. Фундаментальный вклад в исследование подобного рода уравнений был внесен Б. Н. Делоне и Д. К. Фаддеевым.

Ряд важных результатов, касающихся этого уравнения, приведен в известной монографии Л. Д. Морделла "Diophantine equations", Academic Press (London), 1969. Там же доказано следующее утверждение.

Теорема. (см. стр. 127) *Пусть* p_1, p_2, p, q — *простые числа*, $p_1, p_2, p \equiv 5 \pmod{18}$, $q \equiv 11 \pmod{18}$. *Тогда, если*

$$a \in \{p, 2p, 9p, p^2, 9p^2, 4p^2, pq, p_1p_2^2, q, 4q, 9q, 2q^2, q^2, 9q^2, q_1q_2^2, p^2q^2\},$$

то уравнение $x^3 + y^3 = az^3$ *не имеет решений в ненулевых целых числах* x, y, z.

Ниже через $\mathbb{Z}[\rho]$ будем обозначать кольцо целых чисел $a + b\rho$, где $a, b \in \mathbb{Z}$, $\rho^2 + \rho + 1 = 0$. Для чисел z_1, z_2, c из этого кольца будем писать $z_1 \equiv z_2 \pmod{c}$, если $\frac{z_1 - z_2}{c} \in \mathbb{Z}[\rho]$.

10.58. *(Х. Хессами Пилеруд)* Пусть a, b — целые числа, $s-$ простое число, $a^2 + 3b^2 \not\equiv 0 \pmod{s}$. Тогда $(a + b\sqrt{-3})^{s^2-1} \equiv 1 \pmod{s}$.

10.59**. *(Нагель)* Пусть q — простое число, $q \equiv 1 \pmod{3}$, $q = \frac{q_1^2 + 27q_2^2}{4}$, где q_1, q_2 — натуральные числа. Тогда все делители числа q_1q_2 являются кубическими вычетами по модулю q.

10.60**. *(Х. Хессами Пилеруд)* Пусть p, q — простые числа, $p \equiv 1 \pmod{3}$, $q \equiv 1 \pmod{3}$, $4q - p^2 \not\equiv 3 \pmod{9}$. Пусть, далее, p не является кубическим вычетом по модулю q. Тогда уравнение

$$x^3 + y^3 = pqz^3$$

не имеет решений в ненулевых целых числах x, y, z.

10.61. Пусть $A \in \mathbb{N}, A \neq 1$, и пусть для каждого $t \in \mathbb{N}$ величины $u_t \in \mathbb{N}$, $v_t \in \mathbb{N}$ определены из соотношения $u_t + v_t\sqrt{A^2 - 1} = (A + \sqrt{A^2 - 1})^t$. Тогда при $n \in \mathbb{N}, m \in \mathbb{N}$ и $(n, m) = 1$ имеем

$$(u_n, v_m) = \begin{cases} A, & \text{если } n - \text{нечетное}, \quad m - \text{четное}, \\ 1, & \text{в остальных случаях}, \end{cases}$$

$$(u_n, u_m) = \begin{cases} A, & \text{если } n - \text{нечетное}, \quad m - \text{нечетное}, \\ 1, & \text{в остальных случаях}. \end{cases}$$

10.62. Пусть $A \in \mathbb{N}$, $A \neq 1$, t — нечетное натуральное число. Тогда натуральные числа X, U однозначно определяются из равенства

$$\sqrt{\frac{A+1}{2}}X + \sqrt{\frac{A-1}{2}}U = \left(\sqrt{\frac{A+1}{2}} + \sqrt{\frac{A-1}{2}}\right)^t.$$

При этом имеем

$$\sqrt{\frac{A+1}{2}}X - \sqrt{\frac{A-1}{2}}U = \left(\sqrt{\frac{A+1}{2}} - \sqrt{\frac{A-1}{2}}\right)^t$$

и

$$\frac{A+1}{2}X^2 - \frac{A-1}{2}U^2 = 1.$$

В 1963 г. В. Серпинский и А. Шинцель нашли все решения уравнения

$$(x^2-1)(y^2-1) = (z^2-1)^2, \quad x,y,z \in \mathbb{Z}, \quad |x| \neq |y|, \quad |z| \neq 1,$$

с условием $x - y = 2z$. З.-Ф.Као и Я. -Б. Ван доказали, что это уравнение не имеет решений, удовлетворяющих условию $x - y = kz$, $k \in \mathbb{N}$, $k \leq 30$, $k \neq 2$. Для произвольных значений параметра $k \in \mathbb{N}$ подобный результат был получен в работе Х. М. Ву и М. Х. Ле, но при условии, что неизвестные x, y являются четными натуральными числами.

10.63. Докажите, что рассматриваемое выше уравнение не имеет решений в целых (x, y, z), удовлетворяющих условию $x - y = kz$, где $k \in \mathbb{N}$, $k \neq 2$.

УКАЗАНИЯ

10.4. Воспользуйтесь задачей 10.11.

10.9. Если $a\beta^2 + b\beta + c = 0, D = b^2 - 4ac$, то число $\alpha = \frac{p\beta+p'}{q\beta+q'}$ удовлетворяет уравнению $A\alpha^2 + B\alpha + C = 0$,

$$B^2 - 4AC = D(pq' - p'q)^2 = D,$$

поэтому дискриминант числа α не больше дискриминанта числа β; меняя α и β местами и применяя 10.8, получаем обратное неравенство.

10.13. Применяя 4.10, проверьте, что

$$K(D,Q) = K(D,p_1^{\alpha_1})...K(D,p_n^{\alpha_n}),$$

где $Q = p_1^{\alpha_1}...p_n^{\alpha_n}$ — каноническое разложение на простые множители числа Q; заметьте, что $K(D,p_m^{\alpha_m})$ равно или 0, или его можно оценить сверху числом таких $P = 1,...,p_m^{\alpha_m}$, что $A^2 - P^2$ делится на $p_m^{\alpha_m}$, где A — одно из чисел $1,..,p_m^{\alpha_m}$, такое, что $D - A^2$ делится на $p_m^{\alpha_m}$; если $(A, p_m) = 1, p_m > 2$, то искомая оценка равна 2 и то же верно в случае, когда A^2 не делится на $p_m^{\alpha_m}$, а если $p_m = 2$, то искомая оценка равна 4, и в оставшихся случаях оценка равна $p_m^{[\alpha_m/2]}$; в итоге получается, что $K(D,Q) \leq 4\sqrt{Q/3}$ и остается воспользоваться неравенством

$$1 + \sqrt{2} + ... + \sqrt{x} < \frac{2}{3}x^{3/2} + \frac{1}{2}x^{1/2}.$$

10.14. Примените 7.6 и 7.8.

10.16. Докажите индукцией по n, что все остатки этой цепной дроби будут приведенными квадратичными иррациональностями и примените 10.8, 10.9, 10.11; заметьте, что если $r_n = r_m$, то $r_n' = r_m'$ и, положив $\beta_n = -\frac{1}{r_{n+1}'}$, выведите из равенства $r_n = \alpha_n + \frac{1}{r_{n+1}}$, что $\beta_{n+1} = \alpha_n + \frac{1}{\beta_n}$, + где α_{n-1} — целая часть числа

β_n, а так как $r_n = r_m$, то $r_{n+1} = r_{m+1}, r'_{n+1} = r'_{m+1}, \beta_n = \beta_m, \alpha_{n-1} = \alpha_{m-1}$; значит,

$$r_{n-1} = \alpha_{n-1} + \frac{1}{r_n} = \alpha_{m-1} + \frac{1}{r_m} = r_{m-1}.$$

10.20. Проверьте, что при достаточно больших n остаток r_n — приведенная квадратичная иррациональность и примените 10.16.

10.26. Наименьшее решение есть $x = 2n^2 + 1, y = 2n$; действительно, при $0 < y < 2n$ имеем

$$n^2y^2 < (n^2+1)y^2 + 1 < n^2 + 2ny + 1 = (ny+1)^2.$$

10.27. Наименьшее решение есть $x = 2n^2m + 1, y = 2n$; действительно, при $0 < y < 2n$ имеем

$$(nmy)^2 < ((nm)^2 + m)y^2 + 1 < (nmy+1)^2.$$

10.28. Наименьшее решение есть $x = n^2m + 1, y = n$; действительно, при $0 < y < n$ имеем

$$(nmy)^2 < ((nm)^2 + 2m)y^2 + 1 < (nmy+1)^2.$$

10.29. Наименьшее решение есть $x = n, y = 1$.

10.30. Наименьшее решение есть $x = n^2 - 1, y = n$.

10.31. Наименьшее решение есть $x = 2n^2m - 1, y = 2n$.

10.32. Наименьшее решение есть $x = n^2m - 1, y = n$.

10.33. Примените 10.29 и заметьте, что

$$p_{2n} + \sqrt{N}q_{2n} = 2\sqrt{N}q_{2n} + p_{2n} - \sqrt{N}q_{2n} <$$

$$< 2\sqrt{N}q_{2n} + \frac{1}{q_{2n+1}} < (2\sqrt{N}+1)q_{2n+1}$$

10.35. Так как $r_{n+1} = \sqrt{N} + \alpha_0$, и согласно 7.12 имеем

$$\sqrt{N} = \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}},$$

то ввиду иррациональности $\sqrt{N}$ получим

$$p_{n-1} = Nq_n - \alpha_0 p_n, q_{n-1} = p_n - \alpha_0 q_n;$$

далее примените 7.10.

10.37. Если $x^2 - Ny^2 = -1, x, y \in \mathbb{Z}$, и N делится на простое $p = 4k+3$, то $x^{p-1} + 1$ делится на p вопреки малой теореме Ферма.

10.38. Пусть a и b — минимальное решение уравнения $x^2 - p^m y^2 = 1$, тогда a — нечетно, $a^2 - 1$ делится на $p^m b^2$ и 4, значит, $a \pm 1 = 2u^2$, $a \mp 1 = 2p^m v^2$, где $2uv = b$, откуда $u^2 - p^m v^2 = \mp 1$, но равенство $u^2 - p^m v^2 = 1$ невозможно, так как $|u| < a, |v| < b$.

10.39. Найдется такой остаток r этой дроби, у которого период будет симметричным, тогда согласно 10.14, 10.8, 10.9 для некоторых P, Q имеем $r = \frac{P+\sqrt{N}}{Q}, r' = \frac{P-\sqrt{N}}{Q} = -\frac{1}{r}$, откуда $P^2 + Q^2 = N$.

10.41. Проверьте, что $\frac{p_{k+n}}{q_{k+n}} = \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}}$, где $r_{n+1} = \alpha_0 + \frac{p_k}{q_k}$, и воспользуйтесь тем, что $p_{n-1} = Nq_n - \alpha_0 p_n, q_{n-1} = p_n - \alpha_0 q_n$ согласно указанию к 10.35 и тем, что $p_n^2 - Nq_n^2 = (-1)^{n-1}$.

10.42. Решите в целых числах уравнение $(2x+1)^2 - 2y^2 = -1$.

10.43. Сведите его к уравнению $(2y)^2 - 3(2x+1)^2 = 1$.

10.44. Если x, y — решение уравнения, то $|3x-4y|$, $|2x-3y|$ тоже его решение, причем, если $x, y \in \mathbb{N}$, $x > \sqrt{2n}$, то $x < 2y$ и $|3x-4y| < x, |2x-3y| < y$.

10.47. Рассуждаем от противного. Пусть $x+y=u$, $xy=v$. Тогда

$$v^2 + 3uv - u^2(u-1) = 0,\ (2v+3u)^2 = u^2(4u+5).$$

Отсюда следует, что существует натуральное число t, такое, что

$$4u+5 = (2t+1)^2,\ u = t^2+t-1,$$

$$2v + 3t^2 + 3t - 3 = (t^2+t-1)(2t+1),\ v = (t^2+t-1)(t-1).$$

Итак, имеем

$$x+y = t^2+t-1,\ xy = (t^2+t-1)(t-1),\ t \geq 2.$$

Поэтому

$$(x-y)^2 = (t^2+t-1)(t^2+t-1-4(t-1)).$$

Числа t^2+t-1 и $t^2+t-1-4(t-1)$ — взаимно просты, стало быть, число t^2+t-1 — полный квадрат. Но при $t \geq 2$ имеем, что

$$t^2 < t^2+t-1 < (t+1)^2.$$

Противоречие.

10.48. Рассуждаем от противного. Пусть x, y, z — решение уравнения. Тогда его можно переписать в виде

$$(x+y)((x+y)^2 - 3xy) = (3xyz-1)^2.$$

Поскольку $x+y$ не делится на 3 и $(x,y)=1$, то $x+y$ и $(x+y)^2-3xy$ — взаимно просты. Поэтому существует натуральное число u, такое, что $x+y=u^2$. Перепишем первоначальное уравнение в виде

$$9z^2(xy)^2 - (6z-3u^2)xy - (u^6-1) = 0.$$

Отсюда имеем

$$xy = \frac{2z-u^2 \pm \sqrt{(2z-u^2)^2 + 4z^2(u^6-1)}}{6z^2}.$$

Подкоренное выражение в последней формуле должно быть полным квадратом, поэтому $4z^2u^4 - 4z + u^2$ — полный квадрат. Так как $u \geq 2$,

$$(2zu^2-1)^2 < 4z^2u^4 - 4z + u^2 < (2zu^2+1)^2,$$

то $x+y = u^2 = 4z$.

Используя это, из первоначального уравнения получим, что $z=1$, и

$$\begin{cases} x+y = 4, \\ xy = \frac{-2 \pm \sqrt{6}}{6}, \end{cases}$$

что для натуральных чисел x, y невозможно.

10.49. Рассуждаем от противного. Пусть x, y — решение уравнения. Тогда x, y имеют одинаковую чётность, причём $x \neq y$. Будем считать, что $x >$ Обозначив $x + y = 2u$, $x - y = 2v$, имеем

$$2^{n-1}((u+v)^n - (u-v)^n) = 2^{nm}v^{nm},$$

$$u^n + \binom{n}{2}u^{n-2}v^2 + \cdots = 2^{n(m-1)}v^{nm}.$$

Пусть $(u, v) = d$, т.е. $u = du_1$, $v = dv_1$, $(u_1, v_1) = 1$. Тогда получим

$$u_1^n + \binom{n}{2}u_1^{n-2}v_1^2 + \cdots = 2^{n(m-1)}d^{n(m-1)}v_1^{nm}.$$

Отсюда следует, что u_1^n делится на v_1. Ввиду $(u_1, v_1) = 1$ из последнего утверждения имеем $v_1 = 1$. Таким образом, получим $u = vu_1$. Следовательно,

$$2^{n-1}v^n((u_1+1)^n - (u_1-1)^n) = 2^{nm}v^{nm},$$

т.е. $(u_1+1)^n - (u_1-1)^n = 2t^n$, где $t = 2^{m-1}v^{m-1}$.

Отсюда и из очевидных неравенств $(n \geq 2)$

$$2u_1^n < (u_1+1)^n + (u_1-1)^n < 2(u_1+1)^n$$

приходим к противоречию.

10.50. Рассуждаем от противного.

а). Пусть t, x, y, z — решение уравнения Эйлера. Тогда Тогда число $t^2 +$ делится на число $4yz - 1$. Положим $y = 2^k y_1$, где y_1 — нечётное число. Тогда по свойствам символа Якоби имеем

$$1 = \left(\frac{-y}{4yz-1}\right) = -\left(\frac{2^k y_1}{2^{k+2}y_1 z - 1}\right) = -(-1)^n\left(\frac{y_1}{2^{k+2}y_1 z - 1}\right) =$$

$$= -\left(\frac{y_1}{2^{k+2}y_1 z - 1}\right) = -(-1)^{(y_1-1)/2}\left(\frac{-1}{y_1}\right) = -1.$$

Противоречие.

б). Без ограничения общности можно предположить, что $(u, v) = 1$, где u — нечетное число. Сначала сводим уравнение к случаю $(y, v) = 1$. Затем, используя свойства символа Якоби, покажем, что система сравнений

$$\begin{cases} t^2 \equiv -yv^2 \pmod{u}, \\ t^2 \equiv -yv^2 \pmod{(4yzv - u)}, \end{cases}$$

не имеет решений.

10.51. Рассуждаем от противного.

а) Пусть (x, y, z) — решение уравнения. Среди всех решений (x, y, z) выберем то, для которого значение y — минимально. Имеем $(x, y) = (y, z) = (z, x) = 1$. Число y — четное, а число xz — нечетное. Полагая $y = 2y_1$, будем иметь

$$\frac{z - (x^2 + 18y_1^2)}{2} \cdot \frac{z + (x^2 + 18y_1^2)}{2} = 27y_1^4.$$

Числа $\frac{z-(x^2+18y_1^2)}{2}$ и $\frac{z+(x^2+18y_1^2)}{2}$ — взаимно просты.

Далее, существуют натуральные числа σ, l, t, $0 \le \sigma \le 3$, такие, что

$$\frac{z-(x^2+18y_1^2)}{2} = 3^\sigma l^4,$$

$$\frac{z+(x^2+18y_1^2)}{2} = 3^{3-\sigma} t^4,$$

$$y_1 = lt,$$

т.е. $x^2 + 18l^2t^2 = 3^{3-\sigma}t^4 - 3^\sigma l^4$, откуда $\sigma = 3$.

Из предыдущего равенства имеем

$$\frac{|t^2-9l^2|-x}{2} \cdot \frac{|t^2-9l^2|+x}{2} = 27l^4.$$

Числа $\frac{|t^2-9l^2|-x}{2}$ и $\frac{|t^2-9l^2|+x}{2}$ — взаимно просты. Стало быть, существуют натуральные числа n, m, δ, $0 \le \delta \le 3$, такие, что

$$\frac{|t^2-9l^2|-x}{2} = 3^\delta n^4, \quad \frac{|t^2-9l^2|+x}{2} = 3^{3-\delta} m^4,$$

$$l = nm, \quad |t^2-9l^2| = 3^\delta n^4 + 3^{3-\delta} m^4.$$

Достаточно рассмотреть случай $\delta = 0$. Имеем

$$|t^2-9l^2| = n^4 + 3^3 m^4.$$

Отсюда получим, что числа n, t делятся на 3, если $t^2 - 9l^2 = n^4 + 3^3 m^4$. Следовательно, на 3 делятся и x, y, но $(x, y) = 1$. Противоречие.

Если же $9l^2 - t^2 = n^4 + 3^3 m^4$, то по выбору решения (x, y, z) должно выполняться соотношение $2nmt = y \le m$. Противоречие, что и требовалось доказать.

б) Рассуждаем от противного. Тогда существуют целые ненулевые числа x, y, z, $x \ne y$, такие, что

$$x^3 + y^3 + 4z^3 = 6xyz.$$

Отсюда имеем тождество

$$3(x+y+2z)(x-y)^2 = (2z-(x+y))((x+y)^2 - 4z(x+y) - 8z^2).$$

Введём обозначения:

$$u = \frac{4z-2(x+y)}{3}, \quad v = 2z+x+y, \quad w = 2(x-y).$$

Тогда предыдущее равенство примет вид

$$\left(\frac{w}{u}\right)^2 = -\frac{3v}{2u} - \frac{9}{2} + \frac{9u}{8v},$$

причём $uvw \ne 0$. Следовательно,

$$\left(\left(\frac{w}{u}\right)^2 + \frac{9}{2}\right)^2 = \left(\frac{9u}{8v} + \frac{3v}{2u}\right)^2 - \frac{27}{4},$$

откуда имеем

$$w^4 + 9w^2u^2 + 27u^4 = \left(\frac{9u^3}{8v} + \frac{3uv}{2}\right)^2.$$

Противоречие с утверждением пункта а).

10.53. а) Пусть (x_1, y_1, z_1) — решение уравнения, $n \neq 3$, n — целое число. Определим следующие функции:

$$f(x,y,z) = xyz(x^6 + y^6 + z^6 - x^3y^3 - y^3z^3 - z^3x^3),$$

$$g(x,y,z) = x^3y^6 + y^3z^6 + z^3x^6 - 3x^3y^3z^3,$$

$$h(x,y,z) = x^6y^3 + y^6z^3 + z^6x^3 - 3x^3y^3z^3.$$

Рассмотрим последовательности наборов (x_k, y_k, z_k), определяемые соотношениями $(k \geq 1)$:

$$x_{k+1} = \frac{f_k}{(f_k, g_k, h_k)},\ y_{k+1} = \frac{g_k}{(f_k, g_k, h_k)}, z_{k+1} = \frac{h_k}{(f_k, g_k, h_k)},$$

где

$$f_k = f(x_k, y_k, z_k),\ g_k = g(x_k, y_k, z_k),\ h_k = h(x_k, y_k, z_k),$$

и выражение (f_k, g_k, h_k) обозначает наибольший общий делитель чисел f_k, g_k, h_k.

Согласно задаче 10.51 набор (x_k, y_k, z_k) является решением нашего уравнения для любого числа k и $(x_k, y_k) = (y_k, z_k) = (z_k, x_k) = 1$.

Если (x_1, y_1, z_1) — натуральные числа, то (x_k, y_k, z_k) — также натуральные числа. При $l > k$ имеем, что x_l делится на (x_k, y_k, z_k). Поэтому $(y_l z_l, y_k z_k) = 1$, откуда следует справедливость утверждения задачи.

б) Из уравнения имеем

$$d^2(a^3 + b^3) = (3a + nb)xy.$$

Далее, так как $(x, y) = 1$, то $(d^2, xy) = 1$. Поэтому существует натуральное число α, такое, что

$$2a + nb = \alpha d^2, \quad a^3 + b^3 = \alpha xy.$$

В силу условия $(a, b) = 1$ имеем, что $(\alpha, a) = (\alpha, b) = 1$, число $n^3 - 27$ делится на α и $(4a, \alpha) = (nb - a, \alpha)$, т.е. число $(\alpha, nb - a)$ является делителем 4.

в) Рассуждаем от противного. В силу пункта а) в качестве решения можно взять набор (x, y, z), который удовлетворяет условиям $(x, y) = (yz, 2n) = 1$. Используя свойства символа Якоби и квадратичный закон взаимности, при условиях и обозначениях пункта б) получим, что система сравнений

$$\begin{cases} \alpha(4d^2b^2 + n(x-y)^2) \equiv & 0 \pmod{a}, \\ \alpha(d^2b^2 + n(x-y)^2) \equiv & 0 \pmod{(nb-a)}, \end{cases}$$

не имеет решений при n, имеющих одну из следующих форм

$$4k,\ 8k-1,\ 2^{2m+1}(2k-1)+3.$$

г) Используя утверждение задачи 10.51, сведите задачу к пункту в).

10.55. Рассуждаем от противного. а) Пусть (x, y) — решение уравнения

$$x^2 = y^3 - (4k^2 - 1).$$

Очевидно, что y — нечетное число. Следовательно, число x — четное. Далее имеем

$$x^2 + 4k^2 = (y+1)(y^2 - y + 1).$$

Положим $(x,k)=d$. Тогда из четности x и нечетности k получим $x=2dx_1$, $k=dk_1$, $(x_1,k_1)=1$,

$$4d^2(x_1^2+k_1^2)=(y+1)(y^2-y+1).$$

Поскольку y^2-y+1 — нечетное число, то число $y+1$ делится на 4. Тогда число y^2-y+1 при делении на 4 дает в остатке число 3. Следовательно, существуют простое число $p\equiv 3 \pmod 4$ и натуральное число n такие, что

$$y^2-y+1\equiv 0 \pmod{p^{2n-1}},\ y^2-y+1\not\equiv 0 \pmod{p^{2n}}.$$

Так как k не делится на 3, то x^2+4k^2 не делится на 3. Значит, $(y+1,y^2-y+1)=1$. Но в этом случае получаем, что

$$d^2(x_1^2+k_1^2)\equiv 0 \pmod{p^{2n-1}},\ d^2(x_1^2+k_1^2)\not\equiv 0 \pmod{p^{2n}}.$$

Учитывая то, что $p\equiv 3 \pmod 4$, $(x_1,k_1)=1$, приходим к соотношениям

$$d^2\equiv 0 \pmod{p^{2n-1}},\ d^2\not\equiv 0 \pmod{p^{2n}}.$$

Противоречие.

б) Рассуждаем от противного. Пусть (x,y) — решение в натуральных числах уравнения

$$x^2=y^3-10.$$

Тогда xy — нечетное число. Имеем

$$x^2+9=(y-1)(y^2+y+1).$$

В силу того, что $x^2+9\equiv 2 \pmod 4$, имеем $y\equiv 3 \pmod 4$. Следовательно, $y^2+y+1\equiv 1 \pmod 4$. Если $x\equiv 0 \pmod 3$, то $y\equiv 1 \pmod 3$, $y^2+y+1\equiv 0 \pmod 3$. Поэтому натуральное число $(x/3)^2+1$ делится на $(y^2+y+1)/3$. Но это невозможно, так как

$$\frac{y^2+y+1}{3}\equiv 3 \pmod 4.$$

Если же $x\not\equiv 0 \pmod 3$, то переписав уравнение в виде

$$x^2+2=(y-2)(y^2+2y+4),$$

получим, что $\frac{-2}{y-2}=1$.

При этом $y-2\equiv 1 \pmod 4$. Из свойств символа Якоби выводим, что $y-2\equiv 1 \pmod 8$, т.е. $y\equiv 3 \pmod 8$.

С другой стороны, имеем

$$x^2+18=(y+2)(y^2-2y+4).$$

Учитывая то, что $y+2\not\equiv 0 \pmod 3$, получим $\frac{-2}{y+2}=1$. Но это противоречит тому, что $y\equiv 3 \pmod 8$.

10.56. Если $x=0$, то $y=\pm 1$. Следовательно, $k=1$. Поэтому можно предполагать, что x,y — натуральные числа и $k\neq 1$. Перепишем уравнение в виде

$$((2k-2)x+ky)^2-(k^2-k)(2x+y)^2=1.$$

Так как $k\neq 0$, то k^2-k, k^2-k+1 не равны полным квадратам. Основной единицей уравнения Пелля

$$X^2-(k^2-k)Y^2=1$$

будет $\varepsilon = 2k - 1 + 2\sqrt{k^2 - k}$. Следовательно, существует натуральное число n такое, что

$$((2k-2)x + ky) - \sqrt{k^2 - k}(2x + y) = \varepsilon^n.$$

Отсюда имеем, что $2x + y$ — четное число. Значит, число y — четное. Но последнее невозможно, поскольку $k(4x^2 - y^2) = 4x^2 - 1$ — нечетное число.

10.57. а) Непосредственно из уравнения

$$x^2 - Ny^2 = -1, \tag{1}$$

следует, что необходимым условием разрешимости его в целых числах является представимость N в виде суммы двух квадратов взаимно простых чисел. Уравнение (1) разрешимо в целых числах тогда и только тогда, когда длина периода цепной дроби числа $\sqrt{N}$ равна нечетному числу. Тогда для $N = 12317 = 109 \cdot 113 = (3^2 + 10^2)(7^2 + 8^2) = 101^2 + 46^2 = 59^2 + 94^2$ имеем

$$\left(\frac{59}{109}\right) = \left(\frac{2}{59}\right) = -1, \quad \left(\frac{101}{109}\right) = \left(\frac{109}{101}\right) = \left(\frac{8}{101}\right) = -1.$$

При $N = 505 = 19^2 + 12^2$, имеем $\left(\frac{19}{5}\right) = \left(\frac{19}{101}\right) = 1$, но уравнение $x^2 - 505y^2 = -1$ неразрешимо в целых числах x, y, так как

$$\sqrt{505} = 22 + \cfrac{1}{2 + \cfrac{1}{8 + \cfrac{1}{2 + \cfrac{1}{22 + \sqrt{505}}}}}$$

и период цепной дроби $\sqrt{505}$ имеет четную длину равную 4 (см. 10.57 б)).

б) Пусть x, y являются решением уравнения (1). Тогда имеем $(x+i)(x-i) = Ny^2$.

Если N — нечетное число, то числа $x + i, x - i$, будут взаимно простыми в кольце $\mathbb{Z}[i]$.

Если же N — четное число, то x — нечетное, и в этом случае числа $\frac{x+i}{1+i}$, $\frac{x-i}{1-i}$ будут целыми взаимно простыми числами кольца $\mathbb{Z}[i]$.

Отсюда следует, что в обоих случаях найдутся целые числа A, B, s, t, такие что

$$N = A^2 + B^2, \quad x + i = (B + iA)(s + it)^2, \quad 1 = A(s^2 - t^2) + 2Bst,$$

а это значит, что число A нечетное и выполняется равенство $(As+Bt)^2 - Nt^2 = 1$.

Теперь утверждение теоремы следует из того, что числа A и $-A$ являются квадратичными вычетами по модулю N одновременно (все нечетные простые делители числа N сравнимы с 1 по модулю 4).

в) Если p — простое число, $p \equiv 5 \pmod 8$, то уравнение

$$x^2 - 2py^2 = -1 \tag{2}$$

разрешимо в целых числах.

Действительно, пусть (u, v) — решение уравнения Пелля $x^2 - 2py^2 = 1$ в натуральных числах с наименьшим значением v. Тогда

$$(u-1)(u+1) = 2pv^2.$$

Следовательно, существуют натуральные числа α, β, x, y, такие, что $u-1 = 2\alpha x^2$, $u+1 = 2\beta y^2$, $v = 2xy$, $\alpha\beta = 2P$, $\beta y^2 - \alpha x^2 = 1$. Ввиду минимальности числа v имеем $\alpha \neq 2p$. Поскольку $\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = -1$, то $\beta = 2p$, $\alpha = 1$, т.е. $x^2 - 2py^2 = -1$.

г) Для случая $p \equiv 1 \pmod 8$ воспользуемся п. б). Число $2p$ допускает единственное представление в виде суммы двух квадратов натуральных чисел: $2p = (A+4B)^2 + (A-4B)^2$

Если предположить, что уравнение (2) разрешимо в натуральных числах x, y, то либо $\left(\frac{A+4B}{p}\right) = 1$, либо $\left(\frac{A-4B}{p}\right) = 1$. Замечая, что

$$\left(\frac{A+4B}{p}\right)\left(\frac{A-4B}{p}\right) = \left(\frac{A^2-16B^2}{p}\right) = \left(\frac{2A^2}{p}\right) = 1,$$

имеем

$$\left(\frac{A+4B}{p}\right) = \left(\frac{A-4B}{p}\right) = 1.$$

Пусть $B = 2^k B_1$, где $k \geq 0$ — целое, B_1 — нечетное число. Тогда

$$1 = \left(\frac{A+4B}{A^2+16B^2}\right) = \left(\frac{A^2+16B^2}{A+4B}\right) = \left(\frac{-8AB}{A+4B}\right) =$$

$$= (-1)^{\frac{A-1}{2}+\frac{(A+4B)^2-1}{8}\cdot(k+1)}\left(\frac{A}{A+4B}\right)\left(\frac{B_1}{A+4B}\right) =$$

$$= (-1)^{\frac{A-1}{2}+\frac{(A+4B)^2-1}{8}\cdot(k+1)+\left(\frac{A-1}{2}\right)^2+\frac{B_1-1}{2}\cdot\frac{A-1}{2}}\left(\frac{A+4B}{A}\right)\left(\frac{A+4B}{B_1}\right) =$$

$$= (-1)^{\frac{A^2-1}{8}\cdot(k+1)+AB(k+1)+\frac{B_1-1}{2}\cdot\frac{A-1}{2}+\frac{A^2-1}{8}\cdot k+\frac{A-1}{2}\cdot\frac{B_1-1}{2}} =$$

$$= (-1)^{\frac{A^2-1}{8}+(k+1)AB} = (-1)^{\frac{p-1}{8}+(k+1)AB},$$

т.е. $(-1)^{\frac{p-1}{8}+(k+1)AB} = 1$, откуда следует требуемое.

10.58. При $s = 2$ утверждение очевидно. Пусть простое число $s > 2$. Тогда очевидным образом имеем

$$(a+b\sqrt{-3})^s \equiv a^s + b^s\sqrt{-3}^s \equiv a + b(-3)^{\frac{s-1}{2}}\cdot\sqrt{-3} \pmod s,$$

$$(a+b\sqrt{-3})^{s^2} \equiv a^s + b^s(-3)^{\frac{s(s-1)}{2}}\cdot(-3)^{\frac{s-1}{2}}\sqrt{-3} \equiv a + b\sqrt{-3} \pmod s,$$

т.е.

$$(a+b\sqrt{-3})^{s^2} \equiv a + b\sqrt{-3} \pmod s,$$

откуда, ввиду того, что $a+b\sqrt{-3}$ и s являются взаимно простыми числами в кольце $\mathbb{Z}[\rho]$, где $\rho^2+\rho+1=0$, следует требуемое.

10.60. Доказательство проведем методом "от противного". Пусть при условиях теоремы уравнение $x^3+y^3 = pqz^3$ разрешимо в ненулевых целых числах x, y, z. Среди всех наборов (x, y, z) являющиеся решением этого уравнения выберем тот, для которого $|z|$ имеет наименьшее значение. Очевидно, что тогда $(x, y) = (y, z) = (z, x) = 1$. Ввиду того что число $x^2 - xy + y^2$ не имеет простых делителей вида $2 \pmod 3$, то имеем $x + y \equiv 0 \pmod p$. Будем считать число z натуральным.

Возможны несколько случаев, в зависимости от того делится ли число $x+y$ на q или нет.

1) $x + y = \alpha^2 pqu^3$.

Тогда

$$\frac{(x+y)^2 + 3(x-y)^2}{4} = \alpha v^2,$$

где $\alpha \in \{1,3\}$, $z = \alpha uv$, uv — натуральные числа.

Следовательно,

$$\frac{\alpha^2 p^2 q^2 u^6 + \frac{3}{\alpha}(x-y)^2}{4} = v^3.$$

Ясно, что $(v, pq) = 1$.

Рассмотрим сначала возможность а): $\alpha = 1$.

Поскольку в кольце $\mathbb{Z}[\rho]$ имеет место основная теорема арифметики, то и последнего уравнения следует, что существуют целые числа a, b такие, что

$$\frac{pqu^3 + \sqrt{-3}(x-y)}{2} = \zeta\left(\frac{a+b\sqrt{-3}}{2}\right)^3, \qquad (*$$

где $\zeta \in \left\{1, \frac{1\pm\sqrt{-3}}{2}\right\}$. При этом $v = \frac{a^2+3b^2}{4}$, $(a,b) \in \{1,2\}$.

Поскольку $4q - p^2 \not\equiv 3 \pmod 9$, то либо $\frac{p^2-1}{3} \not\equiv 0 \pmod 3$, либо $\frac{q^2-1}{3} \not\equiv$ (mod 3).

Если $p \neq 2$, то беря за s ту из чисел p, q, для которой $\frac{s^2-1}{3} \not\equiv 0 \pmod 3$ возведя обе части равенства (*) в степень $\frac{s^2-1}{3}$, согласно задаче 10.58 получи

$$\left(\sqrt{-3}(x-y)\right)^{\frac{s^2-1}{3}} \equiv \zeta^{\frac{s^2-1}{3}} \pmod s.$$

Здесь мы учли, что $(a^2+3b^2, pq) = (v, pq) = 1$.

Поэтому

$$\zeta^{\frac{s^2-1}{3}} \equiv w \pmod s,$$

где w — некоторое целое рациональное число.

Учитывая, что $\zeta^3 = 1, \frac{s^2-1}{3} \not\equiv 0 \pmod 3$ имеем единственно возможный случа $\zeta = 1$.

Следовательно,

$$a(a-3b)(a+3b) = 4pqu^3.$$

При этом $(a,b) \in \{1,2\}, a \not\equiv 0 \pmod 3$. Напомним также, что $z = uv = \frac{a^2+3b^2}{4} \cdot$ Далее, имеем

$$a = \sigma_1 X^3, \quad a - 3b = \sigma_2 Y^3, \quad a + 3b = \sigma_3 Z^3,$$

где $\sigma_1, \sigma_2, \sigma_3, X, Y, Z$ — целые числа, $\sigma_1\sigma_2\sigma_3 = 4p \cdot q \cdot 2^{3\beta}$, где $\beta \in \{0,1$ $u = 2^\beta XYZ$. Все это означает, что

$$\sigma_2 Y^3 + \sigma_3 Z^3 = 2\sigma_1 X^3$$

Перебирая всевозможные варианты для $\sigma_1, \sigma_2, \sigma_3, \beta$ мы легко приходим к противоречию либо с тем, что p не является кубическим вычетом по модулю q либо с минимальностью значения z в первоначальном уравнении для которого уже имеем

$$z = \frac{a^2+3b^2}{4} \cdot 2^\beta XYZ.$$

Пусть теперь $p = 2$. Докажем, что $\zeta = 1$. Если $\zeta = \frac{1\pm\sqrt{-3}}{2}$, то возведя обе част (*) в степень $\frac{q^2-1}{3}$ как и выше, убеждаемся в том, что $q \equiv 1 \pmod 9$. кром того, из (*) имеем

$$16qu^3 = a^3 - 9ab^2 \pm 9b(a^2 - b^2),$$

откуда, ввиду $q \equiv 1 \pmod 9$, получим $a^3 \equiv -2u^3 \pmod 9$, т.е. $a \equiv u \equiv 0 \pmod 3$. Противоречие с условиями $(x,y) = (y,z) = (z,x) = 1$.

Таким образом $\zeta = 1$. Из (*) имеем

$$a(a-3b)(a+3b) = 8qu^3,$$

откуда противоречие получается вышеописанным способом.

Пусть теперь имеет место б): $\alpha = 3$. Тогда

$$\frac{x - y + 3\sqrt{-3}pqu^3}{2} = \zeta\left(\frac{a+b\sqrt{-3}}{2}\right)^3,$$

При этом $(a,b) \in \{1,2\}$, $a \not\equiv 0 \pmod 3$. Напóмним также, где a, b — некоторые целые числа, $\zeta \in \left\{1, \frac{1\pm\sqrt{-3}}{2}\right\}$.

Проведя дальнейшие рассуждения в точности также, как и в пункте а) мы приходим к противоречию.

Теперь рассмотрим случай 2) $x + y = \alpha^2 pu^3$, $\frac{(x+y)^2+3(x-y)^2}{4} = \alpha q v^3$, где $\alpha \in \{1,3\}$, u, v — целые числа, $z = \alpha uv$. Имеем

$$\frac{\alpha^3 p^2 u^6 + \frac{3}{\alpha}(x-y)^2}{4} = qv^3.$$

Пусть сначала имеет место а): $\alpha = 1$. Тогда существуют целые ненулевые числа q_1, q_2, a, b такие, что

$$\frac{pu^3 + \sqrt{-3}(x-y)}{2} = \frac{q_1 + \sqrt{-3}q_3}{2} \cdot \left(\frac{a+b\sqrt{-3}}{2}\right), \qquad (**)$$

$$q = \frac{{q_1}^2 + 3{q_3}^2}{4}$$

Тогда

$$8pu^3 = q_1(a^3 - 9ab^2) - 9q_3(a^2b - b^3),$$

откуда ${q_1}^2 \equiv p^2 \pmod 9$. Это означает, что

$$3{q_3}^2 = 4q - {q_1}^2 \equiv 4q - p^2 \not\equiv 3 \pmod 9,$$

т.е.

$${q_3}^2 \not\equiv 1 \pmod 3$$

Следовательно $q_3 \equiv 0 \pmod 3$. Положим $q_3 = 3q_2$, где q_2 — целое число. Тогда

$$q = \frac{{q_1}^2 + 27{q_2}^2}{4}$$

Из (**) имеем

$$\frac{pu^3 + \sqrt{-3}(x-y)}{2} = \frac{q_1 + 3\sqrt{-3}q_2}{2} \cdot \left(\frac{a+b\sqrt{-3}}{2}\right)^3.$$

Умножим обе части последнего соотношения на $27{q_2}^3$ и рассмотрим полученное равенство как сравнение по модулю $q = \frac{{q_1}^2+27{q_2}^2}{4}$. Очевидными преобразованиями получим, что

$$\frac{27{q_2}^3 pu^3 + 27\sqrt{-3}(x-y){q_2}^3}{2} \equiv \frac{q_1 + 3\sqrt{-3}q_2}{2} \cdot \left(\frac{3q_2a + 3q_2b\sqrt{-3}}{2}\right)^3 \equiv$$

$$\equiv \frac{q_1+3\sqrt{-3}q_2}{2}\cdot\left(\frac{3q_2a+q_1b-b(q_1-3\sqrt{-3}q_2)}{2}\right)^3\equiv$$

$$\equiv \frac{q_1+3\sqrt{-3}q_2}{2}\cdot\left(\frac{3q_2a+q_1b}{2}\right)^3 \pmod q,$$

откуда

$$8\cdot 27{q_2}^3u^3\cdot p\equiv q_1(3q_2a+q_1b)^3 \pmod q.$$

Но так как $x+y=pu^3$, $u\not\equiv 0 \pmod q$, то получим, что

$$pX^3\equiv q_1 \pmod q,$$

где X — целое число. Согласно задаче 10.59 существует целое число Y такое что $Y^3\equiv q_1 \pmod q$. Поэтому

$$pX^3\equiv Y^3 \pmod q,\quad (Y,q)=1,$$

откуда следует, что p является кубическим вычетом по модулю q, что противоречит условию теоремы.

Пусть теперь имеет место б): $\alpha=3$. Тогда

$$\frac{(x-y)^2+27p^2u^3}{4}=qv^3.$$

Это означает, что существуют целые числа q_1,q_3,a,b, для которых

$$\frac{x-y+3pu^3\sqrt{-3}}{2}=\frac{q_1+\sqrt{-3}q_3}{2}\cdot\left(\frac{a+b\sqrt{-3}}{2}\right)^3,$$

$$q=\frac{{q_1}^2+3{q_3}^2}{4}.$$

Следовательно,

$$3\cdot 8pu^3=q_1(3a^2b-3b^3)+q_3(a^3-9ab^2),$$

откуда либо $a\equiv 0 \pmod 3$, либо $q_3\equiv 0 \pmod 3$.

Если $a\equiv 0 \pmod 3$, то $x-y\equiv 0 \pmod 3$, что вместе с $x+y\equiv 0 \pmod 3$ противоречит условию $(x,y)=1$.

Поэтому $q_3\equiv 0 \pmod 3$. Пусть $q_3=3q_2$, где q_2 — целое число. Тогда

$$q=\frac{{q_1}^2+27{q_2}^2}{4}$$

$$\frac{x-y+3pu^3\sqrt{-3}}{2}=\frac{q_1+3\sqrt{-3}q_2}{2}\cdot\left(\frac{a+b\sqrt{-3}}{2}\right)^3.$$

Умножим обе части последнего соотношения на ${27q_2}^3$ и рассмотрим полученное равенство как сравнение по модулю $q=\frac{{q_1}^2+27{q_2}^2}{4}$. Так же как и в пункте а) имеем

$$8\cdot 27pu^3\equiv q_2(3aq_2+bq_1)^3 \pmod q$$

откуда, ввиду $(x+y,q)=1$, т.е. $(u,q)=1$, используя лемму 2 получим, что p является кубическим вычетом по модулю q, что противоречит условию теоремы.

Полученные противоречия доказывают утверждение.

10.61. Доказательство проведем методом математической индукции по величине $\max\{n,m\}$. При $n=1$, $m=1$ утверждение очевидно. Пусть при некотором

$s \in \mathbb{N}$ оно верно для всех $n \le s, m \le s$ с условием $(n,m)=1$. Докажем, что оно верно и при $n \le s+1$, $m \le s+1$ с $(n,m)=1$.

Согласно предположению индукции, достаточно считать, что либо $n = s+1$, либо $m = s+1$. Кроме того, $n \ne m$, так как $(n,m)=1$. Очевидно также, что

$$u_k^2 - (A^2-1)v_k^2 = 1 \ , \quad k = 1,2,\dots \tag{1}$$

Возможны два случая: а) $n = s+1$, $m \le s$ и б) $m = s+1, n \le s$. Рассмотрим случай а). Имеем

$$u_n + v_n\sqrt{A^2-1} = (u_m + v_m\sqrt{A^2-1})(u_{n-m} + v_{n-m}\sqrt{A^2-1}),$$

откуда

$$u_n = u_m u_{n-m} + (A^2-1)v_m v_{n-m}. \tag{2}$$

Так как $(n-m,m) = (n,m) = 1$, то из (1), (2) и предположения индукции получим, что

$$(u_n, v_m) = (u_m u_{n-m}, v_m) =$$

$$= (u_{n-m}, v_m) = \begin{cases} A, & \text{если } n-m \equiv 1 \pmod 2, m \equiv 0 \pmod 2, \\ 1, & \text{в остальных случаях,} \end{cases}$$

$$(u_n, u_m) = ((A^2-1)v_m v_{n-m}, u_m) =$$

$$= (u_m, v_{n-m}) = \begin{cases} A, & \text{если } m \equiv 1 \pmod 2, n-m \equiv 0 \pmod 2, \\ 1, & \text{в остальных случаях,} \end{cases}$$

что и требовалось доказать в случае а).

Рассмотрим теперь случай б) $m = s+1, n \le s$. Тогда

$$u_m + v_m\sqrt{A^2-1} = (u_n + v_n\sqrt{A^2-1})(u_{m-n} + v_{m-n}\sqrt{A^2-1}).$$

Имеем

$$u_m = u_n u_{m-n} + (A^2-1)v_n v_{m-n}, v_m = u_n v_{m-n} + v_n u_{m-n}. \tag{3}$$

Так как $(m-n,n) = (n,m) = 1$, то с учетом (1), (3) и предположения индукции получим:

$$(u_n, v_m) = (u_n, v_n u_{m-n}) =$$

$$= (u_n, u_{m-n}) = \begin{cases} A, & \text{если } n \equiv 1 \pmod 2, m-n \equiv 1 \pmod 2, \\ 1, & \text{в остальных случаях,} \end{cases}$$

$$(u_n, u_m) = (u_n, (A^2-1)v_n v_{m-n}) =$$

$$= (u_n, v_{m-n}) = \begin{cases} A, & \text{если } n \equiv 1 \pmod 2, m-n \equiv 0 \pmod 2, \\ 1, & \text{в остальных случаях.} \end{cases}$$

Утверждение доказано полностью.

10.62. Существование таких чисел X, U следует из равенства

$$\left(\sqrt{\frac{A+1}{2}} + \sqrt{\frac{A-1}{2}}\right)^t = \left(\sqrt{\frac{A+1}{2}} + \sqrt{\frac{A-1}{2}}\right)\left(A + \sqrt{A^2-1}\right)^{\frac{t-1}{2}}.$$

Их единственность имеем из иррациональности числа $\sqrt{\frac{A-1}{A+1}}$ при любом $A \in \mathbb{N}$, $A \ne 1$.

§ 11. Диофантовы приближения

В этом параграфе речь пойдет о приближениях иррациональных чисел рациональными. Первый цикл задач посвящен приближениям квадратных радикалов.

11.1. Докажите,что для любого N, не равному квадрату целого числа и любого натурального p справедливо неравенство

$$\left\{p\sqrt{N}\right\} > \frac{1}{2p\sqrt{N}},$$

а для любой дроби q/p — неравенство

$$\left|\sqrt{N} - q/p\right| \geq \frac{1}{(\sqrt{N} + q/p)p^2} > \frac{1}{2\sqrt{N}p^2 + p}.$$

11.2. Докажите, что найдутся бесконечно много несократимых дробей p/q таких, что

$$\left|\sqrt{N} - q/p\right| = \frac{1}{(\sqrt{N} + q/p)p^2} < \frac{1}{2\sqrt{N}p^2 - p}.$$

11.3. Целые числа q и p являются решением уравнения Пелля $x^2 - Ny^2 = 1$ если и только если

$$\left|\sqrt{N} - q/p\right| = \frac{1}{(\sqrt{N} + q/p)p^2} < \frac{1}{2\sqrt{N}p^2 - p}.$$

11.4. *(Румыния, 78)* Докажите, что если $\sqrt{7} - m/n > 0$, m, n — натуральные числа, то $\sqrt{7} - m/n > 1/mn$.

Рациональные приближения, цепные дроби и ряд Фарея.

11.5. Пусть $\{p_k/q_k\}$ — последовательность подходящих дробей к дроби

$$\alpha = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n}.$$

Докажите, что последовательность

$$\frac{p_{k-2}}{q_{k-2}}, \frac{p_{k-2}+p_{k-1}}{q_{k-2}+q_{k-1}}, \frac{p_{k-2}+2p_{k-1}}{q_{k-2}+2q_{k-1}}, \ldots, \frac{p_{k-2}+a_kp_{k-1}}{p_{k-2}+a_kq_{k-1}}, \frac{p_k}{q_k}$$

монотонна.

11.6. Докажите, что

$$\frac{1}{q_k(q_{k+1}+q_k)} < \left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_kq_{k+1}}.$$

Дробь m/n называется **наилучшим приближением** к числу α, если всякая дробь с меньшим знаменателем удалена от α на большее расстояние.

11.7. Докажите,что наилучшее приближение к числу α есть одна из подходящих или одна из промежуточных дробей к цепной дроби для α (*промежуточными* называются дроби из последовательностей, указанных в 11.5).

11.8. Для нахождения наилучшего приближения к числу $\alpha \in [0,1]$ среди дробей со знаменателем, не большим N, надо в последовательности Фарея F_N выбрать одну из двух соседних дробей, заключающих между собой α. Докажите, что отрезок с концами в этих дробях можно получить из отрезка $[0,1]$, разбивая его медиантой концов на два отрезка и выбирая из них тот, который содержит α, и повторяя эту процедуру достаточное число раз.

11.9. Какое наименьшее число участников может быть в математическом кружке, если девочек в нем 43,... % ?

11.10. *(Англия, 78)* Докажите, что в десятичной записи любой дроби со знаменателем, не большим 100, не могут встретиться цифры 1, 6, 7 подряд.

11.11. *(Дирихле)* Докажите, что для любого α найдется бесконечно много дробей p/q таких, что $|\alpha - p/q| < 1/q^2$.

11.12*. *(Усиление теоремы Дирихле, принадлежащее Валену)* Докажите, что для любого α найдется бесконечно много дробей p/q таких, что

$$|\alpha - p/q| < 1/2q^2.$$

Наилучшие приближения второго рода.

Дробь m/n назовем **наилучшим приближением второго рода** к числу α, если для любой другой дроби p/q знаменателем $q \leq n$ справедливо неравенство

$$|q\alpha - p| > |n\alpha - m|.$$

11.13*. Докажите, что всякое наилучшее приближение второго рода есть подходящая дробь.

11.14*. Докажите, что и обратно, любая подходящая дробь $\frac{p_k}{q_k}$ при $k \geq 1$ является наилучшим приближением второго рода к числу α.

11.15*. *(Лежандр)* Докажите, что всякая несократимая дробь $\frac{m}{n}$, удовлетворяющая неравенству

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{2n^2},$$

является подходящей дробью числа α .

11.16. Докажите, что уравнение Пелля при $N = 2, 3$ имеет бесконечно много решений; в случае $N = 2$ все подходящие дроби к $\sqrt{2}$ будут давать решение, а в случае $N = 3$ из каждых двух соседних подходящих дробей хотя бы одна дает решение.

Теоремы Маркова, Гурвица и Бореля.

11.17*. Пусть $\{\frac{p_k}{q_k}\}$ — последовательность подходящих дробей к дроби

$$\alpha = a_0 \frac{1}{a_1+} \frac{1}{a_2+} \dots \frac{1}{a_n+} \dots,$$

r_k — последовательность остатков этой дроби,

$$\varphi_k = \frac{q_k}{q_{k-1}}, \quad \psi_k = \varphi_k + r_k.$$

Докажите, что если $k \geq 2, \psi_k \leq \sqrt{5}, \psi_{k-1} \leq \sqrt{5}$, то $\varphi_k > (\sqrt{5}-1)/2$.

11.18*. *(Борель)* Докажите, что среди трех последовательных подходящих дробей хотя бы одна удовлетворяет неравенству

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{\sqrt{5}q_k^2}.$$

11.19. Докажите, что для любого α найдется бесконечно много дробей p/q таких, что

$$|\alpha - p/q| < 1/\sqrt{5}q^2.$$

Это усиление теоремы Л. Дирихле было доказано А.Гурвицем, а еще ранее (в других терминах) — А.А.Марковым.

11.20*. Докажите, что для числа $\varphi = (\sqrt{5}+1)/2$ и любого $c < 1/\sqrt{5}$ неравенство $|\varphi - p/q| < c/q^2$ имеет лишь конечное число решений.

Одно представление элементов цепной дроби.

11.21. Докажите, что при $n \geq 2$

$$||q_{n-1}\alpha|| = a_{n+1} ||q_n\alpha|| + ||q_{n+1}\alpha||,$$

$$a_{n+1} = \left[\frac{||q_{n-1}\alpha||}{||q_n\alpha||}\right], \quad q_{n-1} ||q_n\alpha|| + q_n ||q_{n-1}\alpha|| = 1.$$

11.22. Докажите, что при $n \geq 1$ и $0 < \alpha < 1$

$$||q_n\alpha|| = \alpha/r_2 \dots r_{n+1}.$$

Эквивалентность цепных дробей и чисел.

Обозначим через G множество всех дробно-линейных функций $\frac{ax+b}{cx+d}$, где a, b, c, d — целые, $|ad-bc|=1$, через G_+ — множество всех дробно-линейных функций $\frac{ax+b}{cx+d}$, где $a, b, c, d \in \mathbb{Z}, ad-bc=1$, а через G_- — множество всех остальных функций из G.

11.23. Проверьте, что если $f(x), g(x) \in G$, то $f(g(x)) \in G$ и для любой функции $f(x) \in G$ найдется такая $g(x) \in G$, что

$$f(g(x)) = g(f(x)) = x,$$

и аналогичные утверждения верны для G_+, а если $f(x), g(x) \in G_-$, то $f(g(x)) \in G_+$. Проверьте, что $f_a(x) = (ax+1)/x \in G$ при любом целом a, и для любой цепной дроби α из 11.17

$$\frac{p_n x + p_{n-1}}{q_n x + q_{n-1}} = f_{a_0}(f_{a_1}(f_{a_2} \dots (f_{a_n}(x)) \dots)) \in G,$$

причем при n нечетном эта функция принадлежит G_+, а при n четном — множеству G_-.

Будем говорить, что α и β эквивалентны, если $\alpha = f(\beta)$ для некоторой $f(x) \in G$.

11.24. Докажите, что значение любой цепной дроби α эквивалентно любому ее остатку α_n, точнее, если n четно, то для некоторой функции $f(x) \in G_+$ имеем $\alpha_n = f(\alpha)$, а если n нечетно, то для некоторой функции $f(x) \in G_-$ справедливо равенство $\alpha_n = f(\alpha)$.

11.25*. Пусть α и β иррациональны, $\alpha = f(\beta)$, причем $f(x) = \frac{ax+b}{cx+d} \in G, c > d > 0, \beta > 1$. Тогда b/d и a/c — последовательные подходящие дроби к α и число β равно некоторому остатку цепной дроби для α.

11.26*. *(Серре)* Докажите, что $\alpha = f(\beta)$, где $f(x) \in G$, тогда и только тогда, когда для некоторых $n, m \in \mathbb{N}$ остатки α_n и β_m цепных дробей для α и β равны, или, что равносильно, для некоторого t при всех достаточно больших n элемент a_n цепной дроби для α равен элементу b_{n+t} цепной дроби для β.

Функция Маркова - Лагранжа

Для иррационального числа α обозначим через $\mu(\alpha)$ такое число что при любом $\nu < \mu(\alpha)$ имеется лишь конечное число дробей p/q, удовлетворяющих неравенству $|\alpha - p/q| < \nu/q^2$, а при любом $\nu > \mu(\alpha)$ неравенство $|\alpha - p/q| < \nu/q^2$ имеет бесконечное число решений. Если при любом $\nu > 0$ неравенство $|\alpha - p/q| < \nu/q^2$ имеет бесконечное число решений, то положим по определению $\mu(\alpha) = 0$.

11.27. Проверьте, что в этом определении неравенство

$$|\alpha - p/q| < \nu/q^2$$

можно заменить неравенством

$$q\,||q\alpha - p|| < \nu.$$

Докажите, что для любого неквадратного натурального N

$$\mu(\sqrt{N}) = 1/2\sqrt{N}$$

и для любого иррационального числа α

$$\mu(\alpha) \leq 1/\sqrt{5},$$

а для $\varphi = (\sqrt{5}+1)/2$

$$\mu(\varphi) = 1/\sqrt{5}.$$

11.28*. Докажите, что если α и β эквивалентны, то $\mu(\alpha) = \mu(\beta)$.

11.29*. *(Первое звено в цепочке теорем А. А. Маркова)* Для любого иррационального α, не эквивалентного числу $\varphi = (\sqrt{5}+1)/2$, справедливо неравенство $\mu(\alpha) \leq 2^{-3/2}$, точнее, найдется бесконечно много дробей p/q таких, что

$$|\alpha - p/q| < 2^{-3/2} q^{-2},$$

причем константу $2^{-3/2}$ заменить на меньшую нельзя.

11.30. Неравенство 11.19 усиливает неравенство

$$\left|\alpha - \frac{p_n}{q_n}\right| < q_n^{-2}$$

хотя и для бесконечно многих, но все же не для всех n. На примере числа $\alpha = \frac{m+1}{(m+2)m}$ покажите, что для любого $\varepsilon > \frac{2}{m+2}$ найдется n такое, что

$$\left|\alpha - \frac{p_n}{q_n}\right| > (1-\varepsilon) q_n^{-2},$$

значит, для всех n существенно усилить неравенство

$$\left|\alpha - \frac{p_n}{q_n}\right| < q_n^{-2}$$

нельзя.

Задача Чебышёва.

11.31. Докажите, что для любых взаимно простых p и q и любых целых t, n найдутся целые x и y такие, что $px - qy = t, n \leq x < n + q$.

11.32*. *(Задача П. Л. Чебышёва).* Докажите, что для любого иррационального α и любого действительного β найдется бесконечно много натуральных x таких, что

$$\|\alpha x - \beta\| < 3/|x|.$$

11.33. Докажите тем же методом, что в неравенстве 11.32 можно заменить 3 на 2, если разрешить x принимать любые целые значения.

11.34*. Докажите, что для любого α и любого целого x, $1 \leq x < q$, где q_n —знаменатель n-й подходящей дроби для α, справедливо, что

$$\{\alpha x\} \geq 1/2q_n.$$

11.35.** *(Уточнение* 11.33 *методом Морделла)* Докажите, что в 11.33 в неравенстве константу 3 можно заменить на $1/2$.

11.36*. Применяя метод Морделла, покажите, что в 11.32 можно константу 3 заменить на 1.

11.37*. Докажите, что если число β представимо в виде $m\alpha+n$, где m, n целые, то неравенство $||\alpha x - \beta|| < 1/(\sqrt{5}\,|x|)$ имеет бесконечно много решений в целых числах.

11.38.** Докажите, что и в случае, когда β не представимо в виде $m\alpha + n$, где m, n целые, то все равно неравенство

$$||\alpha x - \beta|| < 1/(\sqrt{5}\,|x|)$$

имеет бесконечно много решений в целых числах.

Г.Минковский доказал, что в 11.38 можно вместо $\sqrt{5}$ поставить 4, а еще увеличить эту константу уже нельзя.

Односторонние приближения

11.39. Докажите, что если $|p/q - \alpha| < 1/q^2$, то

$$\frac{p}{q} = \frac{rp_{n+1} + p_n}{rq_{n+1} + q_n},\ 0 \leq r \leq a_{n+2},\ n = -1, 0, 1, 2, \ldots,\ p_{-1} = 1,\ q_{-1} = 0.$$

Для иррационального числа α обозначим через $\mu_+(\alpha)$ такое число, что при любом $\nu < \mu_+(\alpha)$ имеется лишь конечное число дробей p/q, удовлетворяющих неравенству $0 < p/q - \alpha < \nu/q^2$, а при любом $\nu > \mu_+(\alpha)$ неравенство $0 < p/q - \alpha < \nu/q^2$ имеет бесконечное число решений. Если же при любом числе $\nu > 0$ неравенство $0 < p/q - \alpha < \nu/q^2$ имеет бесконечное число решений, то положим по определению $\mu_+(\alpha) = 0$. Аналогично определим $\mu_-(\alpha)$, только вместо неравенства $0 < p/q - \alpha$ используем неравенство $0 < \alpha - p/q$.

11.40*. Докажите, что

$$\mu_+(\alpha) = \liminf q_{2n+1}\,||q_{2n+1}\alpha||,$$

$$\mu_-(\alpha) = \liminf q_{2n}\,||q_{2n}\alpha||,$$

где $\liminf a_n$ — наибольшее такое a, что неравенство $a_n < a$ выполняются лишь конечное число раз, а q_n — знаменатели подходящих дробей для α .

11.41. Проверьте, что

$$\mu(\alpha) = \min\{(\mu_+(\alpha), \mu_-(\alpha)\} = \liminf q_n \|q_n\alpha\|.$$

11.42. Выведите 11.20 с помощью 11.41, 6.12 и 6.13.

11.43. Проверьте, что

$$q_n\|q_n\alpha\| = \frac{1}{\psi_{n+1}} = \frac{1}{a_{n+1} + \varphi_{n+1} + r_{n+2}^{-1}}, \varphi_{n+1} = \frac{q_{n-1}}{q_n} = \frac{1}{a_n + \varphi_n},$$

$$r_{n+2}^{-1} = \frac{1}{a_{n+2} + r_{n+3}^{-1}}.$$

11.44. Докажите, что $\mu(\alpha) > 0$ тогда и только тогда, когда все элементы цепной дроби для α ограничены.

11.45*. Докажите, что если $\mu_+(\alpha) = 1$, то $\mu_-(\alpha) = 0$, и если $\mu_-(\alpha) = 1$, то $\mu_+(\alpha) = 0$. Докажите, что всегда справедливы неравенства $\mu_+(\alpha) \leq 1$ и $\mu_-(\alpha) \leq 1$. Проверьте, что для эквивалентных чисел α и β имеем равенства $\mu_+(\alpha) = \mu_+(\beta)$ и $\mu_-(\alpha) = \mu_-(\beta)$ или, наоборот, $\mu_+(\alpha) = \mu_-(\beta), \mu_-(\alpha) = \mu_+(\beta)$.

11.46*. Докажите, что если $\alpha = f(\beta), f(x) \in G_+$, то $\mu_+(\alpha) = \mu_+(\beta)$ и $\mu_-(\alpha) = \mu_-(\beta)$, а если $f(x) \in G_-$, то $\mu_+(\alpha) = \mu_-(\beta)$ и $\mu_-(\alpha) = \mu_+(\beta)$.

11.47. Приведите примеры α таких, что $\mu_+(\alpha) = 1$ или $\mu_-(\alpha) = 1$.

11.48. Проверьте, что

$$\mu_+((\sqrt{5}+1)/2) = 1/\sqrt{5} = \mu_-((\sqrt{5}+1)/2), \mu_+(\sqrt{2}) = 1/\sqrt{8} = \mu_-(\sqrt{2}),$$

$$\mu_+(\sqrt{5}) = 1/(2\sqrt{5}) = \mu_-(\sqrt{5}), \mu_+(\sqrt{3}) = 1/(2\sqrt{3}), \mu_-(\sqrt{3}) = 1/\sqrt{3},$$

$$\mu_+(\sqrt{7}) = 1/(2\sqrt{7}), \mu_-(\sqrt{7}) = 3/(2\sqrt{7}).$$

11.49. Проверьте, что для любого натурального n

$$\mu_+\left(\frac{\sqrt{n^2+4n}-n}{2}\right) = \mu_-\left(\sqrt{\frac{1}{4}+\frac{1}{n}}-\frac{1}{2}\right) = \frac{1}{\sqrt{n^2+4n}},$$

$$\mu_-\left(\frac{\sqrt{n^2+4n}-n}{2}\right) = \mu_+\left(\sqrt{\frac{1}{4}+\frac{1}{n}}-\frac{n}{2}\right) = \frac{1}{\sqrt{n^2+4n}}.$$

Односторонние приближения и уравнение Пелля

11.50*. Докажите, что для любого натурального n минимальное натуральное число, представимое в виде $nx^2 - (n+2)y^2$, где x, y — натуральные числа, равно n.

11.51*. Пусть минимальное натуральное число, представимое в виде $Nx^2 - y^2$, где x, y — натуральные числа, равно k. Докажите, что

$$\mu_-(\sqrt{N}) = k/(2\sqrt{N})$$

и для любой дроби p/q, если $\sqrt{N} - p/q > 0$, то

$$\sqrt{N} - p/q > k/(2\sqrt{N}).$$

11.52. Докажите, что в условиях 11.51 для любых целого P и натурального Q

$$\mu_+\left(\frac{P-Q}{\sqrt{N}}\right) \le \frac{Q}{2\sqrt{N}}, \quad \mu_-\left(\frac{P-Q}{\sqrt{N}}\right) \le \frac{kQ}{2\sqrt{N}},$$

$$\mu_+\left(\frac{P+Q}{\sqrt{N}}\right) \le \frac{Q}{2\sqrt{N}}, \quad \mu_-\left(\frac{P+Q}{\sqrt{N}}\right) \le \frac{kQ}{2\sqrt{N}}.$$

11.53. Докажите, что для любой квадратичной иррациональности α с дискриминантом D числа $\mu_+(\alpha)$ и $\mu_-(\alpha)$ не меньше $1/2\sqrt{D}$.

11.54*. Докажите снова утверждение 10.32, а также то, что уравнение $x^2 - Ny^2 = -1$ разрешимо в натуральных числах тогда и только тогда, когда

$$\mu_+(\sqrt{N}) = \mu_-(\sqrt{N}),$$

а также тогда и только тогда, когда период цепной дроби для $\sqrt{N}$ имеет нечетную длину, и что для любой квадратичной иррациональности α с дискриминантом D

$$\mu_+(\alpha) = \mu_-(\alpha)$$

тогда и только тогда, когда период цепной дроби для $\sqrt{D}$ имеет нечетную длину.

11.55*. Докажите, что решения уравнения Пелля, указанные Браункером (см. 10.32), являются наименьшими возможными.

11.56. Докажите, что простое число вида $4k + 1$ представимо в виде суммы двух квадратов натуральных чисел, причем единственным образом. Вместе с задачей 10.32 это дает конструкцию для такого представления.

11.57*. Пусть k - наименьшее натуральное число, для которого разрешимо уравнение $x^2 - Ny^2 = -k$. Докажите, что $k < 2\sqrt{N}$ и наибольший элемент цепной дроби для $\sqrt{N}$, стоящий на нечетном месте, равен $\left[2\sqrt{N}/k\right]$ или $\left[2\sqrt{N}/k\right] - 1$.

11.58*. Докажите, что оценка из 10.15 точная, и покажите, что для $N = (nm)^2 + 2m, m \le n$, наименьшее k, для которого разрешимо уравнение $x^2 - Ny^2 = -k$, равно $2m$, а для $N = (nm)^2 + m, m \le n$,

оно равно m, тем самым подтверждается, что оценка 11.57 близка к точной.

11.59. Докажите, что в разложении в цепную дробь числа $\sqrt{N}$, $N = n^2 - 1$, период имеет вид $1, 2n-2$ и что $\mu(\sqrt{N}) = (2n-2)/2\sqrt{N}$, $k = 2[\sqrt{N}]$, тем самым подтвердив, что оценка 11.57 точная.

11.60. Докажите, что в разложении в цепную дробь числа $\sqrt{N}$, $N = n^2 - 2$, период имеет вид $1, n-2, 1, 2n-2$ и что

$$\mu(\sqrt{N}) = \frac{2n-3}{2\sqrt{N}}.$$

11.61. Докажите, что наименьшее натуральное k, для которого разрешимо в натуральных числах уравнение $x^2 - Ny^2 = -k$, равно $2n-2$ при $N = n^2 - 1$ и $2n-3$ при $N = n^2 - 2$. Найдите наименьшие решения уравнений

$$x^2 - (n^2-1)y^2 = -2n+2, x^2 - (n^2-2)y^2 = -2n+3.$$

В частности, из 11.61 следует сформулированное в §10 утверждение о том, что уравнение $x^2 - 34y^2 = -1$ неразрешимо.

11.62. Докажите при $|M| < \sqrt{N}$, что если уравнение $x^2 - Ny^2 = M$ разрешимо в натуральных числах, то все его решения имеют вид (p_{k+tn}, q_{k+tn}), где $1 \leq k \leq t$, t — наименьшее четное число, делящееся на период дроби для $\sqrt{N}$, $n \in \mathbb{N}$. Докажите, что если период дроби четен, то при $M \neq 1$ имеется не менее двух серий решений (с различными k), и проверьте, что каждая из них порождается своим минимальным решением (p_k, q_k) по формулам

$$p_{k+tn} + q_{k+tn}\sqrt{N} = (p_k + q_k\sqrt{N})(p_t + q_t\sqrt{N}).$$

Будем говорить, что цепная дробь α с элементами a_n **правоэквивалентна** цепной дроби β с элементами b_n , если для некоторого четного t для всех достаточно больших n

$$a_n = b_{n+t},$$

и **левоэквивалентна**, если это верно для некоторого нечетного t.

11.63. Докажите, что α эквивалентно β тогда и только тогда, когда они право- или левоэквивалентны. Докажите, что если α право-(лево)эквивалентно β , то найдется такая функция $f(x) \in G_+$ $(\in G_-)$, что $\alpha = f(\beta)$. Проверьте, что α и β и право- и левоэквивалентны тогда и только тогда, когда они являются периодическими с одинаковыми периодами нечетной длины.

11.64. Докажите, что если число α правоэквивалентно числу β , то $\mu_+(\alpha) = \mu_+(\beta)$ и $\mu_-(\alpha) = \mu_-(\beta)$, а если α левоэквивалентно β, то $\mu_+(\alpha) = \mu_-(\beta)$ и $\mu_-(\alpha) = \mu_+(\beta)$.

Пусть задано вещественное число α и пусть существуют последовательности $P_n \in \mathbb{Z}$ и $Q_n \in \mathbb{N}$ и арифметическая функция $f(n)$, удовлетворяющие условиям:

а) $|\alpha - \frac{P_n}{Q_n}| \le \frac{1}{q_n f(Q_n)}$, $(P_n, Q_n) = 1$;

б) $Q_n \to +\infty$ при $n \to +\infty$;

б) $f(Q_n) \to +\infty$ при $n \to +\infty$.

Тогда последовательность P_n/Q_n называется **последовательностью хороших приближений вещественного числа** α.

11.65. Докажите, что если α — рациональное число, то не существует последовательности P_n/Q_n его хороших приближений.

11.66. Пусть $r, s \in \mathbb{N} \cup \{0\}$, $r > s$. Докажите, что

а) $\int\limits_0^1 \int\limits_0^1 \frac{x^r y^s}{1-xy}\, dxdy = \frac{P}{Q}$, $(P,Q) = 1$, где $Q \mid dr^2$, $dr = [2, \ldots, r]$;

б) $\int\limits_0^1 \int\limits_0^1 \frac{\ln xy}{1-xy}\, dxdy = \frac{P}{Q}$, $(P,Q) = 1$, где $Q \mid dr^3$;

в) $\int\limits_0^1 \int\limits_0^1 \frac{x^r y^r}{1-xy}\, dxdy = \zeta(2) - 1 - \frac{1}{2^2} - \cdots - \frac{1}{r^2}$;

г) $\int\limits_0^1 \int\limits_0^1 \frac{\ln xy}{1-xy} x^r y^r\, dxdy = \zeta(3) - 1 - \frac{1}{2^3} - \cdots - \frac{1}{r^3}$.

11.67. Докажите, что при достаточно большом r справедливо неравенство

$$[2, \ldots, r] < 3^r.$$

11.68. Докажите, что

а) (*Эйлер*) число $\zeta(2)$ — иррационально;

б) (*Апери*) число $\zeta(3)$ — иррационально.

УКАЗАНИЯ

11.1. Заметьте, что $Np^2 - q^2 \ge 1$, так как $\sqrt{N}$ иррационально и поэтому $Np^2 - q^2 \ne 0$.

11.2. Выведите из 10.22.

11.4. Проверьте, что $7n^2 - m^2 \ne 0, 1, 2$, тогда

$$n\sqrt{7} - m > \frac{3}{n\sqrt{7} + m} > 1/m.$$

11.5. Примените 6.10.

11.6. Выведите из 11.4 и 8.26.

11.9. Разложите $0,44$ в цепную дробь.

11.10. Сведите к случаю, когда дробь начинается с этих цифр и подобно 11.9 докажите, что это невозможно.

11.11. Примените 11.6 или 2.1; третье доказательство можно получить, рассматривая числа $0, 1, \{n\alpha\}$, $n \in N$, $n < q$, и применяя принцип ящиков Дирихле (и не используя ни дробей Фарея, ни цепных дробей).

11.12. Примените 11.6 или 2.1 и заметьте, что

$$\frac{2}{q_k q_{k+1}} \leq q_k^{-2} + q_{k+1}^{-2}$$

согласно неравенству между средним геометрическим и средним арифметическим.

11.13. Пусть m/n — наилучшее приближение к

$$\alpha = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n+}\cdots,$$

если бы $m/n < a_0$ или $m/n > p_1/q_1$, то $a_0/1$ было бы лучшим приближением к α, чем m/n; если бы $m/n \neq p_i/q_i$, то найдется k такое, что $p_{k-1}/q_{k-1} < m/n < p_{k+1}/q_{k+1}$, тогда

$$\left|\frac{m}{n} - \frac{p_{k-1}}{q_{k-1}}\right| \geq \frac{1}{nq_{k-1}}, \quad \left|\frac{m}{n} - \frac{p_{k-1}}{q_{k-1}}\right| < \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_k q_{k-1}},$$

откуда $n > q_k$, а, с другой стороны, согласно 8.25 и 11.6

$$|n\alpha - m| = n\left|\alpha - \frac{m}{n}\right| \geq n\left|\frac{m}{n} - \frac{p_{k+1}}{q_{k+1}}\right| \geq \frac{1}{q_{k+1}} \leq |q_k\alpha - p_k|,$$

причем $|n\alpha - m| = |q_k\alpha - p_k|$, лишь если $\alpha = \frac{m}{n} = \frac{p_{k+1}}{q_{k+1}}$, что невозможно по предположению, значит, $|n\alpha - m| > |q_k\alpha - p_k|$, $n > q_k$, и получается противоречие.

11.14. Примените индукцию по k.

11.17. Используя 6.10, проверьте, что $1/\varphi_{n+1} + 1/r_{n+1} = \psi_n$, и выведите из условий задачи, что

$$(\sqrt{5} - \varphi_k)(\sqrt{5} - \frac{1}{\varphi_k}) \geq 1,$$

откуда

$$5 - \sqrt{5}(\varphi_k + \frac{1}{\varphi_k}) > 0,$$

значит, $(\varphi_k - \sqrt{5/4})^2 < 1/4$, и $\varphi_k > (\sqrt{5} - 1)/2$.

11.18. Выведите из 6.12, что

$$\left|\alpha - \frac{p_k}{q_k}\right| = \frac{1}{\psi_{k+1} q_k^2}$$

и, предположив, что утверждение теоремы неверно, заметьте, что $\psi_{n+1} \leq \sqrt{5}$ при $n = k, k-1, k-2$, потом примените 11.16 и получите, что $a_k = 1/\varphi_{k+1} - \varphi_k < 1$.

11.19. Выведите из 11.18.

11.20. Пусть $\varphi - p/q = c/\sqrt{5}q^2$, $|c| < 1$, тогда

$$\frac{1}{4} - \frac{p}{q} + \frac{p^2}{q^2} = \frac{c^2}{5q^4} - \frac{c}{q^2} + 5/4, \quad -q^2 - pq + p^2 = \frac{c^2}{5q^2} - c > -c > -1,$$

но $-q^2 - pq + p^2$ целое и не равно нулю (иначе число p/q было бы иррациональным), значит,

$$q^2 = \frac{c^2}{5(-q^2 - pq + p^2 + c)} \leq \frac{c^2}{5(1 - |c|)}$$

и поэтому таких дробей конечное число.

11.21. Примените 6.10 и заметьте, что $\|q_n\alpha\| = |q_n\alpha - p_n|$.

11.24. Воспользуйтесь равенством

$$\alpha = \frac{q_{n-1}\alpha_n + q_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}.$$

11.25. Разложите a/c в цепную дробь и выберите ее так, чтобы

$$a = p_{n-1},\ c = q_{n-1},\ p_{n-1}q_{n-2} - q_{n-1}p_{n-2} = ad - bc,$$

тогда $p_{n-1}(d - q_{n-2}) = q_{n-1}(b - p_{n-2})$, значит, q_{n-1} делит $(d - q_{n-2})$, но так как $|d - q_{n-2}| < q_{n-1}$, то $d = q_{n-2}$, откуда $b = p_{n-2}$ и

$$\alpha = \frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}},$$

и поэтому $a/c = p_{n-1}/q_{n-1}$ и $b/d = p_{n-2}/q_{n-2}$ — подходящие дроби к α и n-й остаток цепной дроби для α равен β.

11.26. Пусть $\alpha = f(\beta)$, где

$$f(x) = \frac{ax + b}{cx + d} \in G,$$

и без ограничения общности считаем, что $c\beta + d > 0$; тогда согласно 11.24

$$\alpha = \frac{a'\beta_m + b'}{c'\beta_m + d'},$$

где

$$c' = q_{m-1}\left(c\frac{p_{m-1}}{q_{m-1}} + d\right), \quad d' = q_{m-2}\left(c\frac{p_{m-2}}{q_{m-2}} + d\right),$$

и можно выбрать m таким большим, что $\frac{p_{m-1}}{q_{m-1}}$ и $\frac{p_{m-2}}{q_{m-2}}$ близки к β, тогда c' и $d' > 0$, а если m четно, то и $c' > d'$, кроме того, при $m > 2$ $\beta_m > 1$ и остается применить 11.25.

11.27. Примените 11.1 и 11.2, а потом 11.19 и 11.20.

11.28. Пусть

$$\alpha = \frac{a\beta + b}{c\beta + d},$$

и существует бесконечно много решений неравенства $q\,|q\alpha - p| < \nu$ при некотором ν, тогда

$$q'\beta - p' = \pm\frac{q\alpha - p}{\alpha - c\alpha},$$

где $q' = q(a - c\alpha) + c(q\alpha - p)$, значит,

$$q'\,|q'\beta - p'| \le q\,|q\alpha - p| + \frac{|c|}{|a - c\alpha|}\left|q\alpha\frac{|c|}{|a - c\alpha|}\right| \le$$

$$\le \nu + (\frac{\nu}{q})^2 < \nu'$$

для любого фиксированного $\nu' > \nu$, если q достаточно велико, откуда следует, что неравенство $q'\,|q'\beta - p'| < \nu'$ имеет бесконечно много решений при любом $\nu' > \nu$, т. е. $\mu(\beta) \le \mu(\alpha)$.

11.29. Если α не эквивалентно φ, то в его разложении в цепную дробь для бесконечно многих n справедливо неравенство $a_n \geq 2$; проверим, что для таких n либо

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < 2^{-3/2} q_{n-1}^{-2},$$

либо

$$\left|\alpha - \frac{p_n}{q_n}\right| < 2^{-3/2} q_n^{-2},$$

либо

$$\left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| < 2^{-3/2} q_{n+1}^{-2}.$$

Действительно, иначе

$$\frac{1}{q_{n-1}} = \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| + \left|\alpha - \frac{p_n}{q_n}\right| \geq 2^{-3/2}\left(q_{n-1}^2 + q_n^2\right),$$

откуда $\frac{q_n^2}{q_{n-1}^2} - \frac{\sqrt{8}q_n}{q_{n-1}} + 1 \geq 0$, значит, $\frac{q_n}{q_{n-1}} < \sqrt{2}+1$ (ведь равенство невозможно); аналогично $\frac{q_{n+1}}{q_n} < \sqrt{2}+1$, поэтому

$$a_n + \frac{1}{\sqrt{2}+1} < a_n + \frac{q_n}{q_{n-1}} = \frac{q_{n+1}}{q_n} < \sqrt{2}+1,$$

т. е. $2 \leq a_n < 2$, что невозможно. Константу $2^{-3/2}$ заменить на меньшую нельзя, так как для всех чисел α, эквивалентных $\sqrt{2}$, согласно 11.28, $\mu(\alpha) = 2^{-3/2}$.

11.31. Если $px_0 - qy_0 = 1$, то при любом $k \in \mathbb{Z}$ числа $x = tx_0 + kq$ и $y = ty_0 + kp$ удовлетворяют условию $px - qy = t$; остается подобрать k так, чтобы $n \leq x < n+q$.

11.32. Пусть целые p, q, t таковы, что $|\alpha - p/q| < q^{-2}$ и $|q\beta - t| \leq 1/2$, а целые x и y таковы, что $\frac{q}{2} \leq x < \frac{3q}{2}$ и $px - qy = t$, тогда

$$|\alpha x - y - \beta| \leq \left|\frac{xp}{q} - y + \frac{t}{q}\right| \leq x\left|\alpha - \frac{p}{q}\right| + \left|\beta - \frac{t}{q}\right| \leq \frac{x}{q^2} + \frac{1}{2q} < \frac{3}{x}.$$

11.34. Пусть при некотором x, $1 \leq x < q_n$,

$$\{\alpha x\} = \alpha x - y < 1/2q_n \leq 1/2x,$$

значит, согласно 11.15 при некотором y дробь y/x будет равна некоторой подходящей дроби $\frac{p_k}{q_k}$, $k < n$, для числа α, но

$$\left|\alpha - \frac{p_k}{q_k}\right| > \frac{1}{q_k(q_k + q_{k+1})},$$

тогда $\{\alpha x\} > 1/(2q_n)$ и получаем противоречие.

11.35. Заметьте, применяя принцип Дирихле, что среди множества из $2q$ чисел вида $\{\alpha x\}$, $1 \leq x \leq q$, и вида $\{\alpha x - \beta\}, 1 \leq y \leq q$, найдутся два числа, принадлежащие одному из $2q-1$ отрезков $[(k-1)/(2q-1), k/(2q-1)]$, $1 \leq k \leq 2q-1$; но два числа одного вида, скажем $\{\alpha x\}$ и $\{\alpha x'\}$, не могут при $q = q_n$ принадлежать одному отрезку, так как тогда для некоторого $x \in N, x < q$, будет $\{\alpha x\} < 1/2q$,что противоречит 11.34, поэтому при некоторых x и x' $\{\alpha x'\}$

и $\{\alpha x''-\beta\} \in [(k-1)/(2q-1), k/(2q-1)]$, значит, при $x = x''-x'$ и соответствующем целом y

$$|\alpha x - y - \beta| \le 1/(2q-1) < 1/(2x).$$

11.37. Примените 11.19. Пусть $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}, m > 0$, тогда при $q > m, x = q - m, y = p - n$

$$|\alpha x - y - \beta| < \frac{1}{\sqrt{5}q} < \frac{1}{\sqrt{5}x};$$

случай $m \le 0$ рассматривается аналогично.

11.38. Согласно 11.19 существует бесконечно много p и q таких, что

$$\alpha = 1/q + \delta/q^2\sqrt{5}, \quad |\delta| < 1,$$

тогда, выбрав t так, что $|\beta q - t| \le 1/2$, и x, y так, что $px - qy = t$, $|x| \le q/2$, получим, что

$$|\alpha x - y - \beta| \le \left|\frac{xp}{q} - y + \frac{t}{q}\right| \le x\left|\alpha - \frac{p}{q}\right| + \left|\beta - \frac{t}{q}\right| \le$$

$$\le \frac{x}{\sqrt{5}q^2} + \frac{1}{2q} \le \frac{1}{2\sqrt{5}q} + \frac{1}{2q} \le \frac{1}{4\sqrt{5}|x|} + \frac{1}{4|x|} \le \frac{1}{\sqrt{5}|x|},$$

так как при $|x| \le a$ для некоторого $\varepsilon_a > 0$ справедливо неравенство

$$\varepsilon_a < \|\alpha x - \beta\| \le |\alpha x - \beta - y| \le \frac{1}{2\sqrt{5}q} + \frac{1}{2q},$$

а q можно выбрать сколь угодно большим, то и x при этом будет сколь угодно большим.

11.39. Пусть

$$\frac{P}{Q} = \frac{rp_{n+1} + p_n}{rq_{n+1} + q_n} < \frac{p}{q} < \frac{(r+1)p_{n+1} + p_n}{(r+1)q_{n+1} + q_n} = \frac{P'}{Q'},$$

тогда

$$1/q^2 > p/q - \alpha > p/q - P/Q \ge 1/qQ$$

и

$$1/Q'q \le P'/Q' - p/q < P'/Q' - P/Q = 1/QQ'.$$

11.40. Если

$$|p/q - \alpha| < 1/q^2,$$

то

$$\frac{p}{q} = \frac{rp_{n+1} + p_n}{rq_{n+1} + q_n}, \quad 0 \le r \le a_{n+2},$$

и

$$q\|q\alpha\| = q\,|q\alpha - p| = (rq_{n+1} + q_n)(|q_n\alpha - p_n| - r\,|q_{n+1}\alpha - p_{n+1}|) =$$

$$= (rq_{n+1} + q_n)(\|q_n\alpha\| - r\|q_{n+1}\alpha\|),$$

значит, согласно свойствам квадратного трехчлена

$$q\|q\alpha\| \ge \min\{q_n\|q_n\alpha\|, q_{n+2}\|q_{n+2}\alpha\|\}.$$

11.43. Используйте указание к 11.17.

11.51. Домножить $\sqrt{N} - p/q$ на сопряженное.

11.54. Воспользуйтесь 11.1, 11.2, 11.51, 10.15, 11.43, 11.52.

11.57. Примените 11.51, 11.43, 11.40 и указание к 10.30.

11.58. Примените 10.3, 11.40, 11.43, 11.51 и 10.33. При указанных k решения существуют, так как можно взять $y = 1, x = nm$.

11.65. Предположим противное. Пусть существует последовательность P/Q хороших приближений числа $\alpha = p/q$, $(p, q) = 1$. Очевидно, имеют место неравенства

$$\frac{1}{qQ} \le \left|\frac{p}{q} - \frac{P}{Q}\right| < \frac{1}{Qf(Q)},$$

откуда следует, что $f(Q) < q$. Последнее неравенство противоречит условию неограниченности последовательности $\{f(Q)\}$.

11.66. Возьмем любое $\sigma > 0$. Имеем тождество

$$I(\sigma) = \int_0^1\int_0^1 \frac{x^{r+\sigma}y^{s+\sigma}}{1-xy}\,dxdy = \int_0^1\int_0^1 x^{r+\sigma}y^{s+\sigma}\sum_{k=0}^{\infty}(xy)^k\,dxdy =$$

$$= \sum_{k=0}^{\infty}\frac{1}{k+r+\sigma+1}\frac{1}{k+s+\sigma+1} = \frac{1}{r-s}\left(\frac{1}{s+\sigma+1}+\cdots+\frac{1}{r+\sigma}\right) = \frac{P}{Q},\ (P,Q) = 1.$$

а) При $\sigma = 0$ получим

$$\int_0^1\int_0^1 \frac{x^r y^s}{1-xy}\,dxdy = \frac{1}{r-s}\left(\frac{1}{s+1}+\cdots+\frac{1}{r}\right) = \frac{P}{Q}.$$

Отсюда имеем

$$Q \mid [r-s, s+1, s+2, \ldots, r] \mid [2, \ldots, r]^2$$

б) Имеем

$$I'(\sigma) = \int_0^1\int_0^1 \frac{\ln xy}{1-xy}x^{r+\sigma}y^{s+\sigma}\,dxdy = \frac{1}{r-s}\left(-\frac{1}{(s+\sigma+1)^2}-\cdots-\frac{1}{(r+\sigma)^2}\right) = \frac{P}{Q}.$$

Кроме того, справедливы соотношения

$$Q \mid [r-s, (s+1)^2, (s+2)^2, \ldots, r^2] \mid [2, \ldots, r]^3.$$

в) При $r = s$ для величины $I(\sigma)$ имеем

$$\int_0^1\int_0^1 \frac{x^{r+\sigma}y^{r+\sigma}}{1-xy}\,dxdy = \sum_{k=0}^{\infty}\frac{1}{(k+r+\sigma+1)^2}.$$

Отсюда при $\sigma = 0$ получим

$$\int_0^1\int_0^1 \frac{x^r y^r}{1-xy}\,dxdy = \zeta(2) - 1 - \frac{1}{2^2} - \cdots - \frac{1}{r^2};$$

г) Дифференцируя по σ выражение п. в), получим

$$-\int_0^1\int_0^1 \frac{\ln xy}{1-xy}x^{r+\sigma}y^{r+\sigma}\,dxdy = \sum_{k=0}^{\infty}\frac{2}{(k+r+\sigma+1)^3}.$$

Следовательно,

$$-\int_0^1\int_0^1 \frac{x^r y^r}{1-xy}\ln(xy)\,dxdy = 2\left(\zeta(3) - 1 - \frac{1}{2^3} - \cdots - \frac{1}{r^3}\right).$$

11.67. Наименьшее общее кратное $L = L(r)$ чисел $2,\ldots,r$ можно представить в виде $\prod_{p\le r} p^{k_p}$, где $k_p = [\ln r/\ln p]$. Следовательно,

$$L = \prod_{p\le r} p^{[\ln r/\ln p]} \le \prod_{p\le r} e^{\ln r} = e^{\pi(r)\ln r},$$

где $\pi(r)$ — количество простых чисел, не превосходящих r. Для величины $\pi(r)$ при $r\to\infty$ справедлива асимптотика $\pi(r)\sim\frac{r}{\ln r}$.[1)] Используя это, получим, что существует r_0 такое, что для всех $r > r_0$ выполняется неравенство $L < 3^r$.

11.68. а) Рассмотрим многочлен Лежандра

$$P_n(x) = \frac{1}{n!}\frac{d^n}{dx^n}\left(x^n(1-x)^n\right).$$

Используя результаты пп. а) и в) задачи 11.66, имеем

$$J_n = \int_0^1\int_0^1 \frac{(1-y)^n P_n(x)}{1-xy}\,dxdy = \frac{A_n + B_n\zeta(2)}{d_n^2}.$$

Оценим сверху $|J_n|$. Интегрируя по частям, получим

$$|J_n| = \left|\int_0^1\int_0^1 \frac{y^n(1-y)^n x^n(1-x)^n}{(1-xy)^{n+1}}\,dxdy\right| \le$$

$$\le \max_{x,y\in[0,1]}\left(\frac{xy(1-x)(1-y)}{1-xy}\right)^n \int_0^1\int_0^1 \frac{dxdy}{1-xy} = \left(\frac{\sqrt{5}-1}{2}\right)^{5n}\frac{\pi^2}{6}.$$

Следовательно,

$$\left|\zeta(2) + \frac{A_n}{B_n}\right| \le \frac{1}{B_n}d_n^2\left(\frac{\sqrt{5}-1}{2}\right)^{5n}\frac{\pi^2}{6} \le \frac{1}{B_n}\left(3\left(\frac{\sqrt{5}-1}{2}\right)^5\right)^n\frac{\pi^2}{6} < \frac{1}{B_n}\frac{\pi^2}{6}\left(\frac{5}{6}\right)^n.$$

Это означает, что последовательность $\left\{\frac{-A_n}{B_n}\right\}$ является последовательностью хороших приближений числа $\zeta(2)$. Отсюда согласно задаче 11.65 число $\zeta(2)$ — иррациональное.

б) Согласно задаче 11.66 б), г) имеем

$$G_n = -\int_0^1\int_0^1 \frac{\ln xy}{1-xy}P_n(x)P_n(y)dxdy = \frac{A_n + B_n\zeta(3)}{d_n^3}.$$

[1)] см., например, И. М. Виноградов. Элементы высшей математики. (Аналитическая геометрия. Дифференциальное исчисление. Основы теории чисел). Учеб. для вузов. М.: Высш. шк., 1999, с. 362, вопрос 9.

Воспользуемся тем, что

$$-\frac{\ln xy}{1-xy} = \int_0^1 \frac{dz}{1-(1-xy)z}.$$

Получим

$$G_n = \int_0^1\int_0^1\int_0^1 \frac{(1-x)^n(1-y)^n(1-z)^n x^n y^n z^n}{(1-(1-xy)z)^{n+1}}\,dxdydz \le (\sqrt{2}-1)^{4n} I,$$

где

$$I = \int_0^1\int_0^1\int_0^1 \frac{dxdydz}{1-(1-xy)z}.$$

Отсюда находим

$$\left|\zeta(3) + \frac{A_n}{B_n}\right| \le \frac{1}{B_n} d_n^3 (\sqrt{2}-1)^{4n} I < \frac{1}{B_n}\left(\frac{4}{5}\right)^n.$$

Следовательно, согласно задаче 11.65 число $\zeta(3)$ — иррациональное.

§ 12. ГЕОМЕТРИЯ ЧИСЕЛ

Точка плоскости называется **целой**, если обе ее координаты — целые числа. Множество целых точек называется **целочисленной решеткой.** Целая точка называется **примитивной**, если ее координаты взаимно просты. Только такие точки "видны" из начала координат.

Параллелограмм с вершинами в целых точках называется **фундаментальным**, если он не содержит больше никаких других целых точек. Точки $(x;y)$ и $(u;v)$ называются **соседними**, если они вместе с началом координат и точкой $(x+u;y+v)$ определяют фундаментальный параллелограмм.

Площади фигур на клетчатой бумаге

12.1. Проверьте, что площадь фундаментального параллелограмма, определенного соседними точками, равна

$$|xv - yu| = 1.$$

12.2*. Докажите, что площадь любого фундаментального параллелограмма равна 1.

12.3. Докажите, что пустой треугольник с вершинами в целых точках, т. е. не содержащий других целых точек, является половиной фундаментального параллелограмма, значит его площадь равна $1/2$.

12.4. *(Г.Полиа)* Сопоставьте каждой дроби из последовательности Фарея F_n примитивную точку из треугольника с вершинами в точках

$(0;0)$, $(n;0)$, $(n;n)$. Проверьте, что это соответствие будет взаимно однозначным и внутри любого угла, образованного направлениями на две примитивные точки, соответствующие соседним дробям из F_n, не содержится в пределах рассматриваемого треугольника ни одной целой точки. Докажите, что соседним дробям из F_n соответствуют соседние примитивные точки и модуль разности этих дробей обратен произведению их знаменателей (это другое доказательство теоремы Фарея – Коши, см. § 3).

12.5. Докажите, что все примитивные точки из треугольника с вершинами в точках $(0;0)$, $(n;0)$, $(n;n)$ могут быть получены из точек $(1;0)$ и $(1;1)$ с помощью вставки между соседними из ранее построенных точек их суммы, т. е. точки, соответствующей сумме векторов, соединяющих начало координат с этими точками (операция образования суммы точек соответствует построению медианы дробей).

12.6. Выведите из теорем 12.5 и 12.4 утверждение 3.1.

12.7*. *(Формула Пика)* Все вершины несамопересекающегося многоугольника являются целыми точками. Докажите, что его площадь равна $a/2+b-1$, где a — число целых точек, лежащих на его границе, а b — внутри.

12.8*. *(Блихфельдт)* На плоскости расположена фигура площади S, не равной целому числу. Докажите, что ее можно передвинуть параллельно самой себе так, что на ней окажется:

а) не более $[S]$;

б) не менее $]S[$ целых точек.

12.9. *(Москва, .85)* На плоскости расположен квадрат площади четыре. Какое наименьшее число целых точек он содержит?

12.10. *(Москва, 85)* На плоскости расположен квадрат площади четыре, содержащий не менее семи целых точек. Доказать, что он содержит ровно девять целых точек.

12.11*. *(Ньюмен)* Квадрат размера $n \times n$ накрывает не более $(n+1)^2$ целых точек.

12.12*. *(Минковский)* На плоскости расположен выпуклый центрально - симметричный многоугольник площади не меньше 4, центр симметрии которого является целой точкой. Докажите, что этот многоугольник накрывает еще две целые точки.

12.13. Пусть в условии задачи 12.12 число 4 заменено на число $\pi = 3,14\ldots$. Докажите, что этот многоугольник можно повернуть вокруг своего центра симметрии так, чтобы он накрыл еще две целые точки.

12.14. Докажите с помощью 12.12 теорему Дирихле: *для любого α и сколь угодно больших натуральных q справедливо неравенство* $\|q\alpha\| \leq 1/q$.

12.15*. *(Г.Полиа)* Вокруг каждой целой точки из круга с центром в начале координат и радиусом R описан кружок радиуса r. Докажите,

что при $r \leq 1/\sqrt{R^2+1}$ они не заслоняют вида из начала координат, а при $r \geq 1/R$ — заслоняют.

12.16*. *(Москва, 86)* Вокруг каждой целой точки описан круг радиуса r. Докажите, что при $R > (3 + r^{-2})/2$ любая окружность с радиусом R пересекает хотя бы один из этих кругов.

Теоремы Минковского и диофантовы приближения

12.17. *(Минковский)* Пусть $|ad - bc| = \Delta \neq 0$, $mn \geq \Delta$. Докажите, что найдутся целые x и y, такие, что $|ax + by| \leq m$ и $|cx + dy| \leq n$.

12.18*. *(Минковский)* Пусть $|ad - bc| \leq \Delta/2$, $|bd| \leq \Delta, b > 0$. Докажите, что для некоторого целого u справедливы неравенства

$$|a + bu||c + du| \leq \Delta/4, \quad |a + bu| \leq b.$$

12.19*. *(Минковский)* Пусть $|ad - bc| = \Delta \neq 0$, m, n — произвольные числа, тогда для некоторых целых x, y

$$|ax + by + m||cx + dy + n| \leq \Delta/4.$$

Если a/b иррационально, то для любого $\varepsilon > 0$ найдется целочисленное решение предыдущего неравенства, для которого $|ax + by + m| < \varepsilon$.

12.20. Покажите, что в 12.12 и 12.19 константы 4 и 1/4 нельзя, вообще говоря, улучшить.

12.21*. *(Минковский)* Если α иррационально и β не представимо в виде $m\alpha + n$, где m, n— целые, то для бесконечно многих целых q

$$||q\alpha + \beta|| < 1/(4q).$$

12.22. Укажите еще одно доказательство утверждения 11.35.

Целые точки в круге

12.23*. *(Гаусс)* Докажите, что число целых точек в круге радиуса $R \geq 2$ заключено между $\pi(R - \sqrt{2})^2$ и $\pi(R + \sqrt{2})^2$.

12.24. *(BMO, 68)* На плоскости расположена окружность радиуса 100, не проходящая через целые точки и не касающаяся прямых целочисленной решетки. Сколько квадратов этой решетки она пересекает?

12.25*. *(Эйлер)* Целая точка может лежать на окружности радиуса R с центром в начале координат, лишь когда $R = \sqrt{N}$, где N — натуральное число. Докажите, что если N делится на простое число p вида $4k + 3$, то на этой окружности не может быть примитивных целых точек.

12.26. *(Эйлер)* Докажите, что если в разложение N на простые множители некоторое простое число p вида $4k + 3$ входит в нечетной степени, то на соответствующей окружности нет целых точек.

12.27. *(Эйлер)* Докажите, что для всех остальных чисел N на соответствующей окружности имеются целые точки.

12.28. *(Эйлер)* Пусть n — делитель числа N и n делится только на простые числа вида $4k+1$, а частное N/n — только на простые числа вида $4k+3$, причем они входят в его разложение на простые множители только в четных степенях (т. е. число N удовлетворяет условиям 12.27). Докажите, что на окружностях с центром в $(0;0)$ и с радиусами $\sqrt{N}$ и $\sqrt{n}$ лежит поровну целых точек, причем на первой из них нет примитивных целых точек.

12.29. *(Эйлер)* Докажите, что на окружностях с общим центром в $(0;0)$ и радиусами $\sqrt{n}$ и $\sqrt{2n}$, где n — натуральное число, лежит поровну целых точек, а если число n нечетно — то поровну и примитивных целых точек.

12.30. Докажите, что все целочисленные пифагоровы треугольники имеют длины сторон $2pq$, p^2-q^2, p^2+q^2, где p, q — натуральные числа.

12.31. Докажите, что при нечетном n примитивных целых точек на окружности радиусом n столько же, как и на окружности с радиусом $\sqrt{n}$ и тем же центром $(0;0)$.

12.32. Докажите, что при четном n на окружности радиуса n с центром $(0;0)$, а при n, кратном 4, и на окружности радиуса $\sqrt{n}$ нет примитивных целых точек.

12.33. Назовем произведением целых точек $(x;y)$ и $(X;Y)$ целую точку $(xX-yY;xY+yX)$. Проверьте, что вектор $(xX-yY;xY+yX)$ получается из вектора $(x;y)$ растяжением в $\sqrt{X^2+Y^2}$ раз и поворотом на угол, зависящий только от X, Y.

12.34. Докажите тождество Фибоначчи:

$$(xX-yY)^2+(xY+yX)^2=(x^2+y^2)(X^2+Y^2)$$

и проверьте, что произведение может быть примитивно, лишь когда сомножители примитивны.

12.35*. *(Гаусс)* Пусть $N=p_1^{\alpha_1}\dots p_m^{\alpha_m}$, где p_i — простые вида $4k+1$. Докажите, что число целых точек на окружности с центром $(0;0)$ и радиусом $\sqrt{N}$ равно $4d(N)$, где $d(N)=(\alpha_1+1)\dots(\alpha_m+1)$ — число всех натуральных делителей N, а число примитивных целых точек равно 2^{m+2}.

Для любого натурального N определим $\sigma(N)$ как $d(n)$, где n делит N и n делится только на простые числа вида $4k+1$, а N/n — произведение четных степеней простых вида $4k+3$; если в разложение N какое-то простое вида $4k+3$ входит в нечетной степени, то положим $\sigma(N)=0$. Если N делится на простое вида $4k+3$ или на 4, то положим $\eta(N)=0$, в противном случае определим $\eta(N)$ как 2^m, где m — число различных простых делителей вида $4k+1$ у числа N.

12.36. Докажите, что число целых точек на окружности с центром $(0;0)$ и радиусом $\sqrt{N}$ равно $4\sigma(N)$, а число примитивных целых точек

равно $4\eta(N)$. Проверьте, что функции $\sigma(N)$ и $\eta(N)$ обладают свойством мультипликативности: если $(p,q)=1$, то

$$\sigma(pq)=\sigma(p)\sigma(q), \quad \eta(pq)=\eta(p)\eta(q).$$

12.37. Докажите, что если на окружности с центром $(0;0)$ есть целые точки, то их не менее восьми, причем ровно восемь их может быть только тогда, квадрат ее радиуса есть простое число вида $4k+1$.

12.38. Докажите, что если на окружности с центром $(0;0)$ лежат только примитивные целые точки, то квадрат радиуса не будет делится ни на один квадрат натурального числа, и обратно.

12.39. Докажите, что для любого $\varepsilon>0$ и некоторой константы $C(\epsilon)$ число целых точек на окружности с центром $(0;0)$ и радиусом N меньше, чем $C(\varepsilon)N^{\epsilon}$.

Геометрическое доказательство теорем Дирихле и Маркова - Бореля - Гурвица

Предположим далее, что на плоскости введена система координат с началом в точке O и через нее проведена прямая $y=\alpha x$, где $\alpha>0$ — произвольное иррациональное число. Для произвольной точки A с координатами $(q;p)$, $q,p>0$, обозначим A' "проекцию" точки A на прямую $y=\alpha x$, т. е. пересечение этой прямой с прямой $x=q$ — перпендикуляром, опущенным из точки A на ось абсцисс. Координаты точки A' есть $(q;\alpha q)$.

12.40. Докажите, что площадь треугольника OAA' равна

$$|\alpha-p/q|q^2/2.$$

Параллелограмм единичной площади с целочисленными координатами вершин назовем **фундаментальным** (согласно задаче 12.2 это определение равносильно данному в начале главы.)

12.41. Докажите, что существует последовательность пересекающихся прямой $y=\alpha x$ и лежащих в положительном квадранте плоскости фундаментальных параллелограммов $OA_nB_nC_n$ с возрастающими координатами вершин.

С помощью этих задач легко доказать *теорему Дирихле.*

Доказательство теоремы. Пусть $OA_nB_nC_n$ — один из параллелограммов задачи 12.41 и прямая $y=\alpha x$ пересекает, например, отрезок A_nB_n (через точку B_n она проходить не может, ибо α — иррациональное число). Тогда треугольник OA_nA_n' содержится в треугольнике OAB, значит площадь треугольника OA_nA_n' меньше $1/2$. Обозначим через $(q_n;p_n)$ координаты точки A. Тогда согласно задаче 12.40

$$|a-p_n/q_n|<\frac{1}{q_n^2},$$

а согласно задаче 12.41 имеем $q_n \to \infty$. Теорема доказана.

Иногда полезно использовать теорему Дирихле в другой, несколько более сильной, форме: *для любого действительного числа α и любого $N > 0$ найдутся такие целое p и натуральное $q < N$, что*

$$|\alpha - p/q| < \frac{1}{qN}.$$

Для доказательства рассмотрим множество всех фундаментальных параллелограммов $OA_nB_nC_n$, пересекающихся прямой $y = \alpha x$, у которых абсциссы вершин A_n и C_n неотрицательны и меньше N (это множество содержит, например, единичный квадрат), и выберем в нем параллелограмм с наибольшей возможной абсциссой вершины B_n (он существует, так как эта абсцисса натуральна и ограничена сверху числом $2N$.) Если абсцисса вершины A_n положительна, то абсцисса вершины B_n больше N, так как в противном случае, предполагая, например, что треугольник OA_nB_n пересекается прямой $y = \alpha x$, и достраивая его до параллелограмма $OA_nD_nB_n$, очевидно, принадлежащего рассматриваемому множеству, замечаем, что у него абсцисса вершины D_n больше, чем у B_n, вопреки предположению. Если же вершина A_n лежит на оси ординат, то полученный параллелограмм имеет абсциссу точки D_n, такую же, как и у B_n, но при этом точка D_n имеет большую, чем у B_n, ординату, но не превосходящую $\alpha + 1$ (рассматриваемая ситуация возможна лишь при единичной ординате точки A_n, единичной абсциссе точек B_n и D_n — в противном случае площадь параллелограмма $OA_nD_nB_n$ была бы больше 1), и выбирая среди таких параллелограммов тот, у кого будет наибольшей ордината точки D_n, замечаем, что прямая $y = \alpha x$ должна пересекать отрезок D_nB_n (иначе в нашем множестве можно указать параллелограмм с еще большей ординатой точки D_n), и достраивая треугольник OD_nB_n до параллелограмма $OD_nC_nB_n$, опять получаем в нашем множестве параллелограмм с большей абсциссой "диагональной" вершины, чем параллелограмм $OA_nB_nC_n$, вопреки предположению.

Итак, можно считать, что параллелограмм $OA_nB_nC_n$ фундаментальный, пересекается с прямой $y = \alpha x$ и имеет абсциссы точек A_n и C_n меньше N, а абсциссу точки B_n — больше N. Пусть прямая $y = \alpha x$ пересекает, например, отрезок B_nC_n. Выберем на нем точку K с абсциссой N, а на прямой $y = \alpha x$ — точку C' с той же абсциссой q, что и у точки C_n. Тогда четырехугольник $OC'KC_n$ содержится в треугольнике $OB_nC'_n$ и поэтому имеет площадь, не большую $1/2$. Применяя для вычисления площади треугольника $OC'C_n$ задачу 12.40 и аналогичным образом вычисляя площадь треугольника $C'KC_n$, получаем, что площадь четырехугольника $OC'KC_n$ равна

$$|q\alpha - p|q/2 + |q\alpha - p|(N - q)/2 = |q\alpha - p|N/2,$$

где p — ордината точки C_n. Так как эта площадь не больше $1/2$, то $|q\alpha - p|N/2 \le 1/2$, значит, $|\alpha - p/q| \le 1/qN$.

Это рассуждение несколько длиннее предыдущего, но зато оно не ссылается на 12.41 и доказывает более сильное утверждение.

С помощью более тонких рассуждений можно доказать несколько более сильную, чем теорема Дирихле, **теорему Валена:** *для любого иррационального числа α существует бесконечно много рациональных дробей p_n/q_n таких, что*

$$|\alpha - p_n/q_n| < 1/2q^2.$$

Подобно теореме Дирихле она вытекает из следующей геометрической леммы.

Лемма. *Пусть $OA_nB_nC_n$ — один из параллелограммов задачи* 12.41. *Тогда площадь одного из треугольников OXX', где $X = A_n$ или C_n, меньше* $1/4$.

Доказательство. Прямая $y = \alpha x$ пересекает отрезок A_nC_n в точке D, отличной от его середины (иначе эта прямая проходит через точку с рациональными координатами, что невозможно). Без ограничения общности считаем, что треугольник $OA_nA'_n$ содержится в треугольнике OA_nD, тогда треугольник $OC_nC'_n$ содержит треугольник OC_nD. Если отрезок A_nD короче половины отрезка A_nC_n, то площадь треугольника $OA_nA'_n$ меньше $1/4$, так как с треугольником OA_nC_n площади $1/2$ у него общая высота и более чем в два раза меньшее основание. Если отрезок A_nD длиннее половины отрезка A_nC_n, то площадь треугольника $A_nA'_nD$ больше площади треугольника $C_nC'_nD$ ввиду их подобия в силу равенства углов (и того, что последний из них меньше первого), значит, площадь невыпуклого пятиугольника $OA_nA'_nC'_nC_n$, составленного из этих треугольников меньше площади треугольника OA_nC_n, равной $1/2$. Отсюда следует утверждение леммы, так как в противном случае площадь пятиугольника $OA_nA'_nC'_nC_n$ была бы не меньше $1/2$. Случай, когда этот пятиугольник вырождается в треугольник OA_nC_n, очевиден.

Докажем теперь *теорему Маркова.* Она немедленно вытекает подобно теореме Дирихле из следующей геометрической леммы.

Лемма. *Пусть $OA_nB_nC_n$ — один из параллелограммов задачи* 12.41. *Тогда площадь одного из треугольников OXX', где $X = A_n$, B_n или C_n, меньше* $1/(2\sqrt{5})$.

Далее мы предлагаем доказательство этой леммы, использующее некоторые тригонометрические вычисления, разбитое на ряд несложных задач. Заметим, что лемма легко бы доказывалась, если бы параллелограмм был квадратом, а прямые OA'_n и $A_nA'_n$ были бы перпендикулярны. Свести лемму к этому частному случаю не удается,

можно свести к случаю, когда параллелограмм будет прямоугольником. Это делается с помощью следующих двух задач.

Назовем *"перекосом"* преобразование плоскости, переводящее точку с координатами $(x;y)$ в точку с координатами $(x+ky;y)$, где k — *коэффициент "перекоса"*.

12.42. Докажите, что с помощью подходящего "перекоса" можно преобразовать чертеж леммы так, что площади параллелограмма и треугольников не изменятся, а прямые XX', где $X = A_n, B_n$ или C_n, будут перпендикулярны к прямой OX'.

Назовем *"сжатием"* преобразование плоскости, которое переводит точку с координатами $(x;y)$ в точку с координатами $(x;ky)$, где k — *коэффициент "сжатия"*.

12.43. Предполагая выполненным утверждение задачи 12.42, докажите, что с помощью подходящего "сжатия" можно преобразовать чертеж леммы так, что отношения площадей параллелограммов и треугольников не изменятся, а параллелограмм станет прямоугольником. Выполнив потом гомотетию, можно считать, что его площадь равна единице.

12.44. Докажите, что при "перекосе" и "сжатии" прямые переходят в прямые и отношение, в котором делит отрезок внутренняя точка, не меняется.

После применения задач 12.42 – 12.44 можно считать, что $OABC$ — прямоугольник, A', B', C' — перпендикулярные проекции A, B, C на ось ординат (или абсцисс — это все равно) и отрезки OA', OB', OC' соизмеримы, так как они были соизмеримы до применения перекоса и сжатия в силу целочисленности координат точек A, B, C. Надо доказать, что площадь одного из треугольников OXX', где $X = A, B$ или C, меньше $1/(2\sqrt{5})$. Без ограничения общности считаем, что $|OA| = a \geq 1$, и обозначим угол $\angle COC'$ через φ. Допустим, что площади треугольников OXX', где $X = A$ или C, не меньше $1/(2\sqrt{5})$. Тогда надо доказать, что площадь OBB' меньше $1/(2\sqrt{5})$.

12.45. Докажите, что удвоенные площади треугольников OXX', где $X = A, C, B$, равны соответственно

$$\frac{1}{2}a^2\sin 2\varphi, \quad \frac{1}{2}a^{-2}\sin 2\varphi, \quad \left|a\cos\varphi - a^{-1}\sin\varphi\right|\left(a\sin\varphi + a^{-1}\cos\varphi\right) =$$

$$= \left|-\frac{1}{2}(a^2 - a^{-2})\sin 2\varphi + \cos 2\varphi\right| = \frac{1}{2}(a^2 + a^{-2})\left|\sin(2\varphi + 2\beta)\right|,$$

где $\beta = \angle AOB$.

Из сделанных предположений следует, что

$$a^2\sin 2\varphi \geq 2/\sqrt{5}, a\sin^{-2} 2\varphi \geq 2/\sqrt{5},$$

значит,

$$1 \le a^2 \le \sqrt{5}/2, \quad \sin 2\varphi \ge 2a^2/\sqrt{5} \ge 2/\sqrt{5} > \sqrt{3}/2,$$

поэтому $2\pi/3 > 2\varphi > \pi/3$.

12.46. Докажите, что площадь треугольника OBB' не превосходит $\left|a^4/\sqrt{5} - 1/\sqrt{5} + \sqrt{1-4a^4/5}\right|$ и равенство возможно лишь при условии $\sin 2\varphi = 2a^2/\sqrt{5}$.

12.47. Докажите неравенство $0 \le a^4/\sqrt{5} + \sqrt{1-4a^4/5} \le 2/\sqrt{5}$ при $1 \le a^2 \le \sqrt{5}/2$. Равенство возможно лишь при $a = 1$.

Теорема Маркова – Бореля – Гурвица вытекает теперь из следующей задачи.

12.48. Площадь треугольника OBB' меньше $1/(2\sqrt{5})$.

Геометрическая интерпретация Клейна цепной дроби

Предположим, как и в предыдущем цикле задач, что на плоскости введена система координат с началом в точке O и через эту точку проведена прямая $y = \alpha x$, где $\alpha > 0$ — произвольное иррациональное число. Для произвольной точки A с координатами $(q;p)$, $q,p > 0$ обозначим A' "проекцию" A на прямую $y = \alpha x$, т. е. пересечение этой прямой с прямой $x = q$ — перпендикуляром, опущенным из точки A на ось абсцисс. Координаты точки A' есть $(q;\alpha q)$. Длину отрезка AA', равную $|q\alpha - p|$, назовем **расстоянием** до прямой $y = \alpha x$.

Предположим, что во всех целых точках первого квадранта плоскости поставлены колышки. Привяжем к колышку $(1;0)$ веревку и натянем ее вдоль прямой, не пересекая ее, так, чтобы между веревкой (которая примет форму бесконечной ломаной с вершинами в некоторых колышках) и прямой не было колышков. Аналогично, отправляясь от $(0;1)$, натянем выше прямой вторую веревку. Веревки вместе с осями координат ограничат бесконечные многоугольники, называемые полигонами Клейна. Обозначим вершины верхнего полигона через $A_1, A_3, A_5, \ldots$, а нижнего — через $A_2, A_4, A_6, \ldots$. Координаты точки A_n обозначим $(p_n;q_n)$. Для любого i определим вектор $A_nA_{n,i}$ равным вектору OA_{n+1}, умноженному на i.

Обозначим через a_n элементы бесконечной цепной дроби, равной числу α.

12.49. Докажите, что точка $A_{n,a_{n+1}}$ совпадает с точкой A_{n+1}, а точка $A_{n,a_{n+1}+1}$ — с точкой $A_{n+1,1}$, треугольники

$$OA_nA_{n,1}, OA_{n,1}A_{n,2}, \ldots, OA_{n,a_{n+1}-2}A_{n,a_{n+1}-1}, OA_{n,a_{n+1}-1}A_{n+2}$$

не содержат целых точек и

$$|q_n\alpha - p_n| = a_{n+1}|q_{n+1}\alpha - p_{n+1}| + |q_{n+2}\alpha - p_{n+2}|,$$

$$|q_{n+2}\alpha - p_{n+2}| < |q_{n+1}\alpha - p_{n+1}|.$$

12.50. Докажите, что координаты точки A_n совпадают с числителем и знаменателем n-й подходящей дроби к числу α, а также равенство $||q_n\alpha|| = |q_n\alpha - p_n|$.

12.51. Выведите из предыдущих задач утверждения задач 7.9–7.10 и 11.21.

12.52. Докажите, что если $q < q_{n+1}$, то $||q\alpha|| > ||q_n\alpha||$ и выведите отсюда утверждение 11.14.

12.53. Докажите, что если $p/q < \alpha$ и $q < q_{2n+1}$, то

$$p/q < p_{2n+1}/q_{2n+1},$$

а если $p/q > \alpha$ и $q < q_{2n}$, то $p/q > p_{2n}/q_{2n}$, т. е. наилучшими односторонними приближениями являются подходящие дроби.

12.54. Докажите, что полигоны Клейна выпуклы, т. е. вместе с любыми двумя точками содержат соединяющий их отрезок.

12.55. Докажите утверждение 11.12.

Цепные дроби и "прыжки" по окружности

12.56. *(Материалы жюри IMO)* На окружности с центром O радиуса 1 от точки A_0 отложим точки $A_1, \ldots, A_{1000}$ так, что угол A_0OA_k равен в радианной мере k. Окружность в точках A_i разрезается. Сколько различных по длине дуг при этом получится?

Пусть $0 < \varepsilon < 1$. Расположим в порядке возрастания числа ε, $2\varepsilon, \ldots, N\varepsilon$ (дробные части от $\varepsilon, 2\varepsilon, \ldots, N\varepsilon$.) Обозначим через α наименьшее, а $1-\beta$ — наибольшее из них, $\alpha = a\varepsilon$, $1-\beta = b\varepsilon$.

12.57*. Докажите, что для всех $s \le N-a$ имеем $(s+a)\varepsilon - s\varepsilon = \alpha$ и для всех $u \le N-b$ справедливо равенство $u\varepsilon - (u+b)\varepsilon = \beta$, и, значит, $N \le a+b-1$. Докажите, что при $N = a+b-1$ после разрезания отрезка $[0,1]$ точками $\varepsilon, 2\varepsilon, \ldots, N\varepsilon$ получается ровно a отрезков длины β и b отрезков длины α, откуда следует, что

$$ba + ab = 1,\ aB - bA = 1,\ A/a < \varepsilon < B/b,$$

где $A = [a\varepsilon]$, $B = 1 + [b\varepsilon]$.

Пусть $0 < \varepsilon < 1/2$. Определим монотонные последовательности натуральных чисел q_n и p_n, $q_1 = 1$, $p_1 = 0$, так, что

$$||q_n\varepsilon|| = |q_n\varepsilon - p_n|, ||q_{n+1}\varepsilon|| < ||q_n\varepsilon||$$

и при $0 < q < q_{n+1}$

$$||q\varepsilon|| \ge ||q_n\varepsilon||.$$

12.58. Докажите, что $q_{n+1}p_n - q_np_{n+1} = (-1)^n$,

$$q_n||q_{n+1}\varepsilon|| + q_{n+1}||q_n\varepsilon|| = 1, (q_n\varepsilon - p_n)(q_{n+1}\varepsilon - p_{n+1}) \le 0.$$

12.59. Докажите, что при $n \geq 2$ для некоторого натурального a_n

$$q_{n+1} = q_n a_{n+1} + q_{n-1}, p_{n+1} = p_n a_{n+1} + p_{n-1},$$

$$|q_{n-1}\varepsilon - p_{n-1}| = a_{n+1}|q_n\varepsilon - p_n| + |q_{n+1}\varepsilon - p_{n+1}|.$$

12.60*. Докажите, что при $N = (m+1)q_{n+1} + q_n + k$, где цел $0 \leq k < q_{n+1}, m \geq 0$, справедливы равенства

$$\alpha = \|q_{n+1}\varepsilon\|, \beta = \|q_n\varepsilon\| - (m+1)\|q_{n+1}\varepsilon\|$$

и отрезок $[0,1]$ разбивается точками $\varepsilon, 2\varepsilon, \ldots, N\varepsilon$ на $N - q_{n+1}$ отрезк длины α, $q_{n+1} - k - 1$ отрезков длины $\alpha + \beta$ и $k+1$ отрезков длины

12.61. Выведите из 12.60 утверждения 12.56 и 12.59.

Круги Форда

Обозначим через $\overline{|h/k}$ круг радиуса $1/2k^2$, касающийся сверху ос Ox в точке с абсциссой h/k, где h/k — несократимая дробь, $k > 0$

12.62. Докажите, что разные круги Форда $\overline{|h/k}$ и $\overline{|H/K}$ пересек ются и могут касаться лишь когда $h/k - H/K = \pm 1/Kk$.

12.63. Докажите, что круг Форда $\overline{|(h+H)/(k+K)}$ касается круго $\overline{|h/k}$ и $\overline{|H/K}$ и оси Ox.

12.64. Докажите, что между любыми двумя касающимися кругами Форда $\overline{|h/k}$ и $\overline{|H/K}$ расположена бесконечная в обе стороны последовательность кругов Форда, каждый из которых касается своих соседей справа и слева и одного из кругов $\overline{|h/k}$ и $\overline{|H/K}$, и проекции кругов этой последовательности заполняют весь интервал $(h/k, H/K)$.

12.65. Докажите **теорему Валена:** *для любого иррационального α найдется бесконечно много рациональных дробей p/q таких, что*

$$|\alpha - p/q| < \frac{1}{2q^2}.$$

Пусть a, b, c — проекции на ось Ox вершин криволинейного тр угольника ABC, ограниченного попарно касающимися друг дру кругами $\overline{|(h+H)/(k+K)}$, $\overline{|h/k}$ и $\overline{|H/K}$.

12.66. Докажите, что

$$a = \frac{hk + HK}{(k^2 + K^2}, \quad b = \frac{hk + h_1k_1}{k^2 + k_1^2}, \quad c = \frac{h_1k_1 + HK}{k_1^2 + K^2},$$

где

$$k_1 = k + K, \quad h_1 = h + H, \quad b - a = \frac{K^2(s^2 - s - 1)}{(k^2 + K^2)(k^2 + k_1^2)},$$

где $s = K/k$, а также, что неравенство $b > a$ равносильно неравенств вида $s > (1 + \sqrt{5})/2$, а неравенство $b < a$ равносильно неравенств вида $s < (1 + \sqrt{5})/2$.

Пусть прямая $x = \alpha$ пересекает криволинейный треугольник ABC. Без ограничения общности считаем, что $K \leq k$.

12.67. Докажите, что если $a < b$, то

$$|\alpha - H/K| = H/K - \alpha < H/K - a = \theta(s)/K^2 < 1/(\sqrt{5}K^{-2}),$$

где $\theta(s) = s/(s^2+1)$, а если $a > b$, то

$$\left|\alpha - \frac{h_1}{k_1}\right| = \frac{h_1}{k_1} - \alpha < \frac{h_1}{k_1} - b = \frac{\zeta(s)}{k_1^2} < \frac{1}{\sqrt{5}k_1^2},$$

где

$$\zeta(s) = \frac{s(s+1)}{s^2 + (s+1)^2}.$$

12.68. Докажите еще раз **теорему Маркова – Бореля – Гурвица:** *для любого иррационального α найдется бесконечно много рациональных дробей p/q таких, что*

$$|\alpha - p/q| < \frac{1}{\sqrt{5}q^2}.$$

Последний в этом параграфе цикл задач посвящен обобщению теоремы Маркова – Бореля – Гурвица на односторонние приближения, указанному Б.Сегре. Другое доказательство было предложено И.Нивеном. Далее приводится еще одно доказательство, в основе которого лежит следующая геометрическая лемма.

12.69.** Пусть $OABC$ — параллелограмм единичной площади, прямая $y = \alpha x$, проходящая через начало координат O, пересекает отрезок BC, и точки X, Y, Z выбраны на этой прямой так, что AX, BY, CZ параллельны оси Oy. Тогда если площади треугольников OAX и OBY не меньше $\tau/(2\sqrt{1+4\tau})$, то площадь треугольника OCZ не больше $1/(2\sqrt{1+4\tau})$, причем равенство возможно лишь когда площади треугольников OAX и OBY равны $\tau/(2\sqrt{1+4\tau})$.

12.70. *(Б.Сегре)* Для любых иррационального α и положительного τ существует бесконечно много рациональных дробей p/q таких, что

$$-\frac{1}{\sqrt{1+4\tau}q^2} < \alpha - p/q < \frac{\tau}{\sqrt{1+4\tau}q^2}.$$

УКАЗАНИЯ

12.2. Разрежьте параллелограмм на части квадратами решетки и проверьте, что, параллельно переместив эти части, можно из них составить единичный квадрат.

12.3. Если во второй половине параллелограмма есть целая точка, отличная от его вершин, то симметричная ей относительно центра параллелограмма точка тоже целая, лежит в нашем треугольнике и отлична от его вершин.

12.4. Воспользуйтесь 12.3 и 12.1.

12.5. С помощью 12.3 проверьте, что сумма двух точек будет соседней с ними обеими.

12.7. Проверьте справедливость формулы Пика для пустых треугольников и для любого многоугольника, составленного из многоугольников, для которых верна формула Пика, и разрежьте любой многоугольник с вершинами в целых точках на пустые треугольники с вершинами в целых точках.

Можно также непосредственно проверить формулу Пика для прямоугольников со сторонами, параллельными линиям решетки целых точек, потом для прямоугольных треугольников с катетами, параллельными линиям решетки целых точек, и, наконец, для произвольных треугольников, причем для простоты можно ввиду сказанного выше ограничится случаем пустых треугольников.

12.8. Разрежьте фигуру на части квадратами решетки и перенесите их параллельно самим себе так, чтобы они собрались в одном квадрате решетки, и заметьте, что некоторые его точки будут покрыты частями фигуры не более $[S]$, а некоторые другие, — не менее $]S[$ раз.

12.9. Уже вписанный в квадрат круг накрывает не менее двух узлов. Квадрат с центром в точке с одной целой, а с другой полуцелой координатами и сторонами, наклоненными под углом 45° к осям координат, содержит ровно две целые точки.

12.10. Если квадрат содержит две целые точки на расстоянии $2\sqrt{2}$, то он содержит девять целых точек. Остается случай, когда он содержит семь целых точек, выпуклая оболочка которых образует симметричный шестиугольник. Докажите, что проекция этого шестиугольника на одно из двух взаимно перпендикулярных направлений не меньше двух.

12.11. Рассмотрите выпуклую оболочку всех целых точек, накрытых квадратом, заметьте, что ее площадь не больше n^2, периметр не больше $4n$ и не меньше числа целых точек, лежащих на нем. Далее примените 12.7.

12.12. Делая, если надо, преобразование подобия с коэффициентом $1+\varepsilon$, можно считать, что площадь больше 4. Применяя 12.8, заметьте, что в многоугольнике найдутся две точки, соединяющиеся вектором с четными координатами (для этого примените подобие с коэффициентом $1/2$). Потом отразите одну из них относительно центра симметрии и соедините отрезком со второй — середина полученного отрезка является целой точкой, принадлежащей многоугольнику, так же как и симметричная ей точка.

12.13. Многоугольник имеет диаметр длины большей 2, проходящий через центр симметрии. Вращая его, можно накрыть еще две целые точки.

12.14. Примените 12.9 к параллелограмму, ограниченному прямыми $y = \alpha x \pm 1/X, x = \pm X, X > 1$. Тогда для некоторых натуральных чисел p, q точка $(p;q)$ принадлежит ему, откуда $|q\alpha - p| \leq 1/X \leq 1/q$.

12.15. Для доказательства второго утверждения примените 12.8 к каждому прямоугольнику с длиной $2R$ и шириной $2/R$ и центром в начале координат или вместо 12.8 примените рассуждение, подобное решению 12.4, рассмотрев в порядке возрастания углов все примитивные точки в круге радиуса R и обратив внимание на их соседство в смысле задачи 12.1, заметьте, что сумма соседних точек лежит вне круга, и расстояние от них до прямой, направленной на сумму, меньше $1/R$.

Для доказательства первого утверждения рассмотрите точки $(1;0)$ и $([R-1];1)$ и прямую, направленную на их сумму.

12.16. Рассмотрите самую крайнюю прямую целочисленной решетки, пересекающую окружность, и на ней выберите два соседних кружка, лежащие один внутри, а другой вне ее; отдельно рассмотрите случай, когда такие кружки найти нельзя.

12.17. Проверьте, что площадь параллелограмма, ограниченного указанными неравенствами, равна $4mn/\Delta$, и примените 12.8.

12.18. Можно считать, что $-b \le a < 0$ и $c \ge 0$, взяв в случае необходимости вместо a и c соответственно $a+by$ и $c+dy$ при подходящем целом y и $-c$, $-d$ вместо c и d; тогда $u=0$ или 1 обеспечивает справедливость теоремы (рассмотрите отдельно случаи $c+d \le 0$ или $c+d>0$ и примените неравенство $\sqrt{xy} \le (x+y)/2$ и условия теоремы).

12.19. Согласно 12.17 найдутся целые x_0, y_0, такие, что $|ax_0+by_0| \le \varepsilon$ и $|cx_0+dy_0| \le \Delta/\varepsilon$ и можно при этом считать, что $ax_0+by_0>0$. Выберем x_1 и y_1 так, чтобы $x_0y_1-x_1y_0=1$, и сделаем замену переменных $x=x'x_0+y'x_1$, $=x'y_0+y'y_1$, тогда $ax+by=a'x'+b'y'$ и $cx+dy=c'x'+d'y'$, где $ad-bc=a'd'-b'c'$ и $< a' \le \varepsilon, |b| \le \Delta/\varepsilon$. Остается выбрать целое y' так, чтобы $|mc'-na'-\Delta y'| \le \Delta/2$, применить предыдущую задачу при $a=b'y'+m$, $c=d'y'+n$, $b=a'$, $d=c'$. Для доказательства первого утверждения в качестве ε надо взять $|\Delta|m^{1/2}$.

12.20. Заметьте, что $|x+1/2||y+1/2| \ge 1/4$.

12.21. Из 12.19 следует, что для любого $\varepsilon>0$ найдутся целые p и q, такие, что $|q||q\alpha+\beta+p| \le 1/4$ и $|q\alpha+\beta+p| \le \varepsilon$. Устремите ε к нулю и заметьте, что $1/4$ достигается самое большее один раз, так как иначе α было бы рациональным.

12.22. Воспользуйтесь 12.21.

12.23. Сопоставьте каждой целой точке квадрат решетки, у которого эта точка является левой нижней и заметьте, что полученный квадрильяж содержит круг радиуса $R-\sqrt{2}$ и содержится в круге радиуса $R+\sqrt{2}$.

12.24. *Ответ:* 800 или 799.

12.25. Пусть $x^2+y^2=N, (x,y)=1, p \mid N$, тогда $(p,x)=(p,y)=1$, значит при некотором целом m число p делит $mx-y$, откуда следует, что $p \mid x^2+(mx)^2$, поэтому $p \mid x^2+1$ и $p \mid x^{p-1}+1$ вопреки малой теореме Ферма.

12.26. Пусть $x^2+y^2=N, (x,y)=d$, тогда $(x/d)^2+(y/d)^2=N/d^2$ и $p|N/d^2, (x/d, y/d)=1$ вопреки 12.25.

12.27. Примените аналог задачи 10.21 и задачу 11.40.

12.28. Пусть $x^2+y^2=N$, $(x,y)=d$, p — любой простой делитель числа N вида $4k+3$, тогда $(x/d)^2+(y/d)^2=N/d^2$ и $(p, N/d^2)=1$ согласно 12.25, значит, N/d^2 — делитель n, причем $d^2n/N=m^2$, поэтому $(mx/d)^2+(my/d)^2=n$, где $mx/d, my/d$, $d/m=\sqrt{N}/n$ — целые числа.

12.29. Пусть $(x;y)$ — целая точка первой окружности, тогда $(x+y;x-y)$ — целая точка второй окружности и обратно, если $(x;y)$ — целая точка второй окружности, тогда $((x+y)/2;(x-y)/2)$ — целая точка первой окружности.

12.30. Пусть числа x, y, z попарно взаимно просты и $x^2+y^2=z^2$, тогда z нечетно и, например, y тоже нечетно, откуда

$$(x/2)^2=uv, u=(z-y)/2, v=(z+y)/2, (u,v)=1,$$

значит, $u=p^2, v=q^2$, p, q — натуральные, и $(p,q)=1$.

12.31. Воспользуйтесь 12.30 и заметьте, что восьмая часть всех примитивных целых точек на окружности с радиусом $\sqrt{n}$ имеет вид $(p;q)$, $p>q$, а восьмая часть всех примитивных целых точек на окружности с радиусом n имеет вид $(2pq;(p^2-q^2))$, $p>q$.

12.35. Пусть

$$x^2+y^2=N, \ (x,y)=d,$$

p — любой простой делитель N/d^2, тогда при

$$x_1 = x/d,\ \ y_1 = y/d,\ \ N_1 = N/d^2$$

справедливы равенства

$$x_1^2 + y_1^2 = N_1,\ \ (x_1, y_1) = (x_1, p) = (x_1, p) = 1,\ \ p|x_1 - \sigma h y_1,$$

где $\sigma = \pm 1$, β — наибольшая степень, на которую делится N_1, а h — такое единственное число, что $p^\beta | 1 + h^2$, $1 < h < p^\beta/2$. Единственность h следует из того, что если $p^\beta | h^2 - h_1^2$, то или $p^\beta | h - h_1$, или $p^\beta | h + h_1$. Существование числа h при $\beta = 1$ следует из того что для $a = ((p-1)/2)!$ число $a^2 + 1$ делится на p, так как $p \mid a^2 - (p-1)!$, $p \mid (p-1)! + 1$, а при $\beta > 1$ существование такого числа a доказывается индукцией по β путем прибавления, если надо, к предыдущему значению a подходящего кратного $p^{\beta-1}$ и выбором h в виде $\pm a + p^\beta s$. Пусть числа x_2, y_2 таковы, что $x_2^2 + y_2^2 = p^\beta$, $p^\beta | x_2 - \sigma h y_2$ (существование их следует из 12.5, 12.34 и предыдущих рассуждений), тогда точка $(x; y)$ является произведением примитивных целых точек $(x_2; y_2)$ и $((x_1 x_2 + y_1 y_2)/p^\beta; (-x_1 y_2 + x_2 y_1)/p^\beta)$ и далее по индукции она разлагается в произведение n примитивных целых точек, где n равно числу различных простых делителей N_1, причем таких разложений, как и различных примитивных точек на окружности $\sqrt{N_1}$, будет ровно 2^n.

12.36. Воспользуйтесь 12.35, 12.32, 12.29, 12.28, 12.26.

12.37, 12.38. Воспользуйтесь 12.36.

12.41. Выберите $A_1 = (0; 1)$, $B_1 = (1; 1)$, $C_1 = (1; 0)$ и далее в качестве $OA_nB_nC_n$ выбирайте параллелограмм, изображающий сложение либо векторов $O\bar{A}_n$ и $O\bar{B}_n$, либо векторов $O\bar{B}_n$ и $O\bar{C}_n$.

12.42. Примените "перекос", взяв за ось абсцисс прямую O_nA', и воспользуйтесь тем, что площадь треугольника не меняется, если не меняются его основание и высота.

12.43. Докажите, что при "сжатии" площадь параллелограмма умножается на k. Воспользуйтесь тем, что площадь треугольника с гипотенузой b и углом β равна $\frac{1}{4}b^2 \sin 2\beta$.

12.45. Заметьте, что $1 \geq \operatorname{tg}\beta \geq 2/\sqrt{3} > 1/\sqrt{3}$, значит, $\pi/4 > \beta > \pi/6$, и поэтому $\pi/2 < 2(\varphi + \beta) < 4\pi/3$, следовательно, площадь треугольника OBB', равная

$$\left|\frac{1}{2}(a^2 - a^{-2}) \sin 2\varphi + \frac{1}{2}\cos 2\varphi\right| = (a^2 + a^{-2})\,|\sin(2\varphi + 2\beta)|,$$

не превосходит

$$\left|\frac{1}{2}(a^2 - a^{-2}) 2a^2/\sqrt{5} - \sqrt{1 - 4a^4/5}\right|.$$

12.46. Неравенство

$$a^4/\sqrt{5} - \sqrt{1 - 4a^4/5} \geq 0$$

верно, так как $a \geq 1$ и

$$a^4/\sqrt{5} \geq 1/\sqrt{5} \geq \sqrt{1 - 4a^4/5}.$$

Для доказательства неравенства

$$a^4/\sqrt{5} + \sqrt{1 - 4a^4/5} \leq 2/\sqrt{5}$$

положите $x = \sqrt{1-4a^4/5}$ и проверьте, что на отрезке $0 \le x \le 1/\sqrt{5}$ функция $x + \sqrt{5}(1-x^2)/4$ возрастает, так как ветви параболы направлены вниз, ее ось симметрии есть прямая $x = 2/\sqrt{5}$, и наш отрезок лежит левее ее. Значение функции в точке $x = 1/\sqrt{5}$ равно $2/\sqrt{5}$.

12.47. Из 12.45 и 12.46 следует, что площадь треугольника OBB' не больше $1/2\sqrt{5}$, причем равенство было бы возможно, лишь когда $a = 1$ и $\sin 2\varphi = 2a^2/\sqrt{5} = 2/\sqrt{5}$. Но тогда $OC'/OA' = \operatorname{tg}\varphi$, а так как

$$\sin 2\varphi = (2\operatorname{tg}\varphi)/(\operatorname{tg}^2\varphi + 1),$$

то $\operatorname{tg}\varphi$ иррационален, что противоречит соизмеримости отрезков OA', OB', OC', вытекающей из сохранения преобразованиями "перекоса" и "сжатия" отношения, в котором точка делит отрезок.

12.49. Примените индукцию.

12.50. Воспользуйтесь 12.49 и тем, что подходящая и промежуточная дроби p_{n+3}/q_{n+3} и $(p_{n+2}+p_{n+1})/(q_{n+2}+q_{n+1})$ лежат по одну сторону от α, а подходящая дробь p_{n+2}/q_{n+2} — по другую.

12.51. Разбейте треугольник $OA_{n+1}A_n$ на треугольники OA_nA_n', $A_n'A_nA_{n+1}$, $OA_n'A_{n+1}$, где A_n' — точка с координатами $(q_n; \alpha q_n)$, и воспользовавшись 12.1, 12.3, 12.40, заметьте, что их площади равны

$$1/2,\ q_n\|q_n\alpha\|/2,\ (q_{n+1}-q_n)\|q_n\alpha\|/2,\ q_n\|q_{n+1}\alpha\|/2,$$

откуда

$$q_n\|q_{n+1}\alpha\| + q_{n+1}\|q_n\alpha\| = 1.$$

12.52-12.54. Примените 12.49 – 12.50.

12.55. Рассмотрите треугольники OA_nA_{n+1}, OA_nA_n', $OA_{n+1}A_{n+1}'$, $A_nA_n'C$, $A_{n+1}A_{n+1}'C$, где C — точка пересечения прямой $y = \alpha x$ и отрезка A_nA_{n+1}, вычислите их площади с помощью 12.40 и 12.3 (как в указании к 12.51) и заметьте, что последние два из них подобны, а потом, применяя 12.49 – 12.50, докажите, что площадь первого из них больше. Выведите отсюда, что

$$q_{n+1}\|q_{n+1}\alpha\| + q_n\|q_n\alpha\| < 1.$$

12.57. Если бы первое утверждение было неверно, то $(s+a)\varepsilon < \alpha$. Второе утверждение доказывается аналогично. Для проверки третьего утверждения заметьте, что $(b+a)\varepsilon < \alpha$.

12.58. Воспользуйтесь 12.57 при $N_n = q_{n+1} + q - 1$, тогда

$$a = q_n, b = q_{n+1}.$$

12.59. Воспользуйтесь 12.58 и заметьте, что $(p_n, q_n) = 1$ и $p_n(q_{n+1}-q_n) = q_n(p_{n+1}-p_n)$.

12.60. Проведите индукцию по N.

12.62. Квадрат расстояния между центрами кругов минус квадрат суммы их радиусов равен

$$\frac{(Hk-Kh)^2-1}{(kK)^2}.$$

12.63. Воспользуйтесь 12.62 и заметьте, что

$$\left|\frac{h+H}{k+K} - \frac{h}{k}\right| = \frac{1}{k(k+K)}, \left|\frac{h+H}{k+K} - \frac{H}{K}\right| = \frac{1}{K(k+K)}.$$

12.64. Воспользуйтесь 12.63.

12.65. Примените 12.64 и заметьте, что прямая $x = \alpha$ пересекает бесконечно много кругов Форда.

12.67. В первом случае $s > (1+\sqrt{5})/2$ и $\theta(s)$ монотонно убывает, а во втором $s < (1+\sqrt{5})/2$ и $\zeta(s)$ монотонно возрастает.

12.68. Прямая $x = \alpha$ пересекает бесконечно много криволинейных треугольников, ограниченных кругами Форда.

12.69. Положим для краткости $\lambda = 1/\sqrt{1+4\tau}$, $\mu = \lambda\tau$, тогда $\mu = (1-\lambda^2)/4\lambda$, $1 - 4\lambda\mu = \lambda^2$. Выполнив афинное преобразование, можно считать, что $OABC$ — прямоугольник, его стороны $OA = a$, $OC = 1/a$, а роль прямой $y = \alpha x$ играет ось ординат (при афинных преобразованиях отношение площадей не меняется). Обозначим угол между вектором OC и осью абсцисс через $\pi/2 - \psi$, а угол $\angle AOB$ — через δ. Тогда $\psi + \delta < \pi/2$ и площади треугольников OAX, OCZ и OBY равны соответственно

$$\frac{a^2 \sin 2\psi}{4}, \quad \frac{a^{-2} \sin 2\psi}{4},$$

$$\frac{(a^2 + a^{-2}) \sin 2(\psi+\delta)}{4} = \frac{(a^2 - a^{-2}) \sin 2\psi + 2\cos 2\psi}{4}.$$

Поэтому для доказательства леммы достаточно предположить, что $a^2 \sin 2\psi \geq 2\mu$, $a^{-2} \sin 2\psi \geq 2\lambda$ и вывести отсюда неравенство

$$\frac{(a^2 - a^{-2}) \sin 2\psi}{2} + \cos 2\psi \leq \mu.$$

Обозначим $\max\{2\mu/a^2, 2\lambda a^2\}$ через γ. Очевидно, что если выполнено неравенство $\gamma \geq \cos 2\delta$, то $2\psi \geq \pi/2 - 2\delta$, значит, функция $\sin 2(\psi+\delta)$ убывает с ростом ψ, поэтому нужное неравенство следует из неравенства

$$(a^2 - a^{-2})\gamma/2 + \sqrt{1-a^2}\gamma \leq \mu. \qquad (*)$$

Докажем его вместе с неравенством $\gamma \geq \cos 2\delta$. Очевидно, что $\gamma \leq 1$.

Рассмотрим два случая. Пусть $2\mu/a^2 \leq 2\lambda a^2$, тогда имеем $\tau \geq a^4$, $\gamma = 2\mu/a^2$, а так как $\gamma \leq 1$, то

$$1 \geq 2\lambda a^2, \quad \gamma = 2\frac{\mu}{a^2} \geq 4\mu\lambda = \frac{4\tau}{1+4\tau},$$

и неравенство $\gamma \geq \cos 2\delta$ вытекает из неравенства

$$\frac{4\tau}{1+4\tau} \geq \frac{\operatorname{tg}^2\delta - 1}{\operatorname{tg}^2\delta + 1} = \frac{a^4 - 1}{a^4 + 1},$$

а оно очевидно в силу неравенств

$$a^4 < 4\tau, \quad \frac{a^4-1}{a^4+1} \leq \frac{4\tau - 1}{4\tau + 1} < \frac{4\tau}{4\tau+1}.$$

Неравенство $(*)$ в рассматриваемом случае принимает вид

$$\mu - \mu a^{-4} + \sqrt{1 - (2\mu/a^2)^2} \leq \mu.$$

Полагая $x = \mu/a^4$, получаем из него неравенство $\sqrt{1-4\mu x} \le x$, которое при $x \ge \mu/\tau = \lambda$ очевидно, так как его правая часть возрастает, а левая — убывает, и при $x = \lambda$ оно обращается в равенство.

Предположим теперь, что $2\mu/a^2 < 2\lambda a^2$. Тогда

$$\tau < a^4, \quad \gamma = 2\lambda a^2 \ge \cos 2\delta = \frac{a^4-1}{a^4+1},$$

потому, что при $a \le 4\tau$

$$\gamma \ge \frac{2\mu}{a^2} \ge 4\mu\lambda = \frac{4\tau}{4\tau+1} > \frac{a^4-1}{a^4+1},$$

а при $a^4 > 4\tau$ производная по a левой части, равная $4\lambda a$, больше производной по a левой части, равной $8a^3(a^4+1)^{-2}$, так как

$$\lambda = \frac{1}{\sqrt{1+4\tau}} > \frac{1}{4\tau+1} > \frac{1}{a^4+1} \ge 2a^2(a^4+1)^{-2}.$$

Неравенство (*) в рассматриваемом случае принимает вид

$$\lambda a^4 - \lambda + \sqrt{1-4\lambda^2 a^4} \le \mu.$$

Полагая $x = \lambda a^4$, получаем из него неравенство

$$x + \sqrt{1-4\lambda x} \le \mu + \lambda,$$

которое при $x > \lambda\tau = \mu$ выполняется, потому что при $x = \mu$ обращается в равенство, а его левая часть убывает, так как ее производная по x равна $1 - 2\lambda/\sqrt{1-4\lambda x}$ и при $x > \mu$ она меньше -1. Из доказанного следует, что неравенство (*) обращается в равенство лишь при $a^4 = \tau$ и $\sin 2\psi = \gamma = 2\mu/a^2 = 2\lambda a^2$, т.е. когда площади треугольников OAX и OCZ равны $\mu/2$ и $\lambda/2$.

12.70. Построим на координатной плоскости последовательность параллелограммов $OA_nB_nC_n$ с единичными площадями и целочисленными координатами вершин такую, что прямая $y = \alpha x$ пересекает отрезки B_nC_n. Построение проводится по индукции. Полагаем $A' = B_n, C' = C_n$, и в качестве вектора $\overline{OB'}$ берем $\overline{OB_n} + \overline{OC_n}$. Прямая $y = \alpha x$ пересекает либо $B'C'$, либо $A'B'$. Если имеет место первый случай, то полагаем $OA_{n+1}B_{n+1}C_{n+1} = OA'B'C'$. Во втором случае строим по рекуррентным формулам

$$A'_{k+1} = A'_k, C'_{k+1} = B'_k, OB'_{k+1} = OB'_k + OA'_k$$

последовательность параллелограммов $OA'_kB'_kC'_k$, начиная с параллелограмма $OA'_1B'_1C'_1 = OA'B'C'$ до тех пор, пока не получим параллелограмм $OA'_mB'_mC'_m$, в котором сторона $B'_mC'_m$ пересекает прямую $y = \alpha x$, и полагаем $OA_{n+1}B_{n+1}C_{n+1} = OA'_mB'_mC'_m$.

Координаты последовательностей A_n и B_n возрастают, а последовательность C_n не может стабилизироваться с некоторого номера m. Поэтому можно выбрать подпоследовательность параллелограммов $OA_nB_nC_n$ со стремящимися к бесконечности координатами.

Применяя лемму к параллелограмму $OA_nB_nC_n$, получаем, что либо площадь одного из треугольников OA_nX и OB_nY меньше $\tau/(2\sqrt{1+4\tau})$, либо площадь треугольника OC_nZ меньше, чем $1/(2\sqrt{1+4\tau})$, либо все три площади равны указанным значениям. Вычисляя площади этих треугольников через координаты

вершин A_n, B_n, C_n по формуле половина произведения основания на высоту (высоту проводим из вершины O), выводим, что для некоторой последовательности рациональных дробей p_n/q_n справедливы неравенства

$$-\frac{1}{\sqrt{1+4\tau q_n^2}} \le \alpha - \frac{p_n}{q_n} \le \frac{\tau}{\sqrt{1+4\tau q_n^2}}.$$

На самом деле при иррациональном α эти неравенства строгие, так как иначе, в силу равенства площадей треугольников OA_nX и OB_nY и рационального отношения их высот q и q', отношение их оснований $p-\alpha q$ и $p'-\alpha q'$ тоже рационально, а так как $p/q \ne p'/q'$ (из-за неколлинеарности векторов OA_n и OB_n), то и α рационально, что противоречит предположению

§ 13. ПОКРЫТИЕ ПРЯМОУГОЛЬНИКА КВАДРАТАМИ, ЭЛЕКТРИЧЕСКИЕ ЦЕПИ И РЕАЛИЗАЦИЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ ФОРМУЛАМИ

Работу алгоритма Евклида[1)] можно представить следующим образом: в прямоугольник размерами $l_1 \times l_2$ укладываем a_1 квадратов размера $l_2 \times l_2$, в оставшийся прямоугольник размерами $l_2 \times l_3$ укладываем a_2 квадратов размера $l_3 \times l_3$ и т. д., пока не покроем прямоугольник размера $l_1 \times l_2$ квадратами k разных размеров в общем количестве $a_1 + \ldots + a_k$ штук (см. § 8).

Если считать целью алгоритма Евклида покрытие прямоугольника квадратами, то он действует как "жадный алгоритм": на каждом шаге помещает в прямоугольник на свободное место квадрат максимальных размеров. На первый взгляд кажется, что он всегда строит минимальное (по числу используемых квадратов) покрытие. Далее мы увидим, что это не так.

Обозначим через $L(m,n)$ наименьшее число квадратов в покрытии прямоугольника размером $m \times n$. Обозначим через $l(r)$ сумму элементов цепной дроби, представляющей рациональное число r. Число квадратов в покрытии прямоугольника размером $m \times n$, которое строит алгоритм Евклида, равно $l(m/n)$.

13.1. Докажите, что $L(5,6) = 5$, $l(5/6) = 6$.

Далее будет показано, что $L(m,n)$ может быть гораздо меньше, чем $l(m/n)$.

Рассмотрим следующий класс покрытий (разбиений) прямоугольника. Разрежем прямоугольник на два прямоугольника, потом какой-нибудь из них разрежем на два прямоугольника и т. д. до тех пор, пока не получим разбиение исходного прямоугольника на квадраты.

[1)] Евклид свой метод алгоритмом, конечно, не называл, термин этот стал популярен в нашем веке и происходит от искажения имени Аль Хорезми — выдающегося среднеазиатского математика, название одной из книг которого дало имя целому разделу математики — алгебре.

Такие разбиения назовем **последовательно-параллельными** (сокращенно П) разбиениями (покрытиями) и обозначим минимальное число квадратов в П-разбиении прямоугольника $m \times n$ через $L_{\Pi}(m, n)$.

13.2. Докажите, что введенная функция симметрична и зависит только от отношения m/n и то же верно для функции $L(m, n)$.

Далее будет показано, что иногда $L(m, n) < L_{\Pi}(m, n)$.

Определим теперь понятие последовательно-параллельной электрической цепи из единичных резисторов. Один-единственный резистор считаем П-цепью с сопротивлением единица. Если R_1 и R_2 — П-цепи с сопротивлениями r_1 и r_2 соответственно, то цепь, которая получается из цепей R_i параллельным соединением, имеет сопротивление $(r_1^{-1} + r_2^{-1})^{-1}$, а цепь, получающаяся из тех же цепей R_i последовательным соединением имеет сопротивление $r_1 + r_2$. Наименьшее число единичных сопротивлений, из которых можно построить П-цепь с сопротивлением r, обозначим через $L_{\Pi}(r)$.

13.3. Установите взаимно-однозначное соответствие между П-разбиениями прямоугольника $m \times n$ и П-цепями с сопротивлением m/n и выведите отсюда, что

$$L_{\Pi}(n, m) = L_{\Pi}(m, n) = L_{\Pi}(m/n) = L_{\Pi}(n/m).$$

Далее под словом цепь будем понимать П-цепь, если не оговорено противное. Повторим построение произвольной цепи Ξ, заменив на каждом его шаге параллельное соединение подцепей на последовательное, а последовательное соединение подцепей на параллельное. В результате получаем новую цепь Ξ^*, которую назовем **двойственной цепью** для цепи Ξ.

Очевидно, что двойственная цепь для цепи Ξ^* совпадает с первоначальной цепью Ξ.

13.4. Докажите, что двойственные друг другу цепи имеют взаимно обратные сопротивления, и выведите отсюда последнее равенство задачи 13.3.

Далее рассмотрим некоторые классы формул, реализующих рациональные числа. В качестве базисов будем рассматривать следующие множества операций:

$$B = \{x + y, x - y, xy, x^{-1}, 1\}, : B_1 = \{x + y, xy, x^{-1}, 1\},$$

$$B_2 = \{x + y, x^{-1}, 1\}, B_3 = \{x + y, (x^{-1} + y^{-1})^{-1}, 1\}.$$

Понятие формулы над базисом B (или B_i) и реализуемой ею функции определим индуктивно. Константу 1 объявляем формулой. Если Φ_1 и Φ_2 — формулы в базисе B и r_1, r_2 — реализуемые ими числа, а $\omega \in B$ — базисная операция, то выражение $\Phi = \omega(\Phi_1, \Phi_2)$ по определению является формулой, реализующей число $\omega(r_1, r_2)$.

Если операция $\omega(x)$ есть операция обращения x^{-1}, то выражение $\omega(\Phi_1) = \Phi_1^{-1}$ является формулой, реализующей число $\omega(f_1) = f_1^{-1}$.

Сложностью формулы назовем число символов констант 1 в формуле. **Сложностью числа** r назовем минимальную сложность реализующей его формулы и обозначим ее через $L_B(r)$. Обозначим через $L(r)$ знаменатель обычной несократимой дроби, равной r.

Определим по индукции понятие **ветвящейся цепной дроби.** Обычные цепные дроби считаем частным случаем ветвящихся цепных дробей. Если R_i, $i = 1, \ldots, n$, — ветвящиеся цепные дроби, a — натуральное число, то дробь

$$\frac{1}{a + R_1 + \ldots + R_n}$$

тоже назовем **ветвящейся,** а все элементы дробей R_i и число a — ее **элементами.** Сумму ветвящихся цепных дробей и произвольного целого a тоже считаем ветвящейся цепной дробью, а ее элементами — все элементы слагаемых и число a.

Докажите утверждения 13.5 — 13.9.

13.5. Для любой дроби r число $L_{B_2}(r)$ равно наименьшей сумме элементов в ветвящихся цепных дробях, представляющих r.

13.6. Для любой дроби r справедливо равенство $L_{B_3}(r) = L_{\Pi}(r)$.

13.7. Для любой дроби $L_{B_3}(r) = L_{B_2}(r)$.

13.8. Для любой дроби $L_{B_2}(r) = L_{B_2}(1/r)$.

13.9*. Для любой дроби r

$$L_{B_2}(r) \le l(r) \le \max L(r), L(1/r),$$

причем равенство достигается лишь для аликвотных дробей и для дробей вида $1 - 1/q = 1/(1 + 1/(q-1))$.

Простейшую нижнюю оценку для $L_{B_2}(p/q)$ и $L_{B_3}(p/q)$ дает следующая задача.

13.10*. Справедливы соотношения

$$L_{B_2}(p/q) = L_{B_3}(p/q) = L_{B_2}(q/p) = L_{B_3}(q/p) \ge \max(q,p)/\min(p,q).$$

Равенство достигается только на аликвотных дробях.

Как показывает следующая задача, базис B_1 сильно отличается от B_2 и B_3.

13.11*. Справедливо неравенство

$$L_{B_1}(p/q) \ge 3\log_3(\max(q,p)/\min(p,q)),$$

которое достигается только при $p/q = 3^n$, n — целое.

Вернемся к произвольным разбиениям прямоугольника на квадраты. Им можно сопоставить плоские электрические цепи, состоящие из единичных сопротивлений. Для этого выделим в прямоугольнике все горизонтальные отрезки, состоящие из сторон квадратов разбиения и не удлиняемые с сохранением этого свойства (в их число входят и обе горизонтальные стороны прямоугольника). В середине каждого из выделенных отрезков возьмем точку. Две точки соединяем отрезком, если некоторый квадрат разбиения касается обоих отрезков, на которых выбирались эти точки.

Если от первоначального чертежа оставить только выбранные точки и соединяющие их отрезки, то получится плоское изображение графа. **Графом** называется объект, состоящий из некоторого множества **вершин** и некоторого множества **ребер,** соединяющих эти вершины попарно. Если вершинам графа сопоставить точки на плоскости, а ребрам — отрезки, соединяющие соответствующие вершины, то получается **изображение графа.** Изображение называется **плоским,** если отрезки в нем пересекаются только в вершинах. Граф, имеющий плоское изображение, называется также **плоским.**

Если ориентировать каждое ребро рассматриваемого графа в направлении от одной горизонтальной стороны прямоугольника к другой и написать на каждом ребре длину стороны квадрата, изображаемого этим ребром, то получим **ориентированный граф** с нагруженными ребрами, называемый также **двухполюсной сетью** (полюсами являются вершины, изображающие горизонтальные стороны прямоугольника).

Заметим, что сумма чисел, приписанных всем ребрам, выходящим из одного полюса, равна сумме чисел, приписанных всем ребрам, входящим в другой полюс, и обе они равны длине горизонтальной стороны прямоугольника. Если заменить каждое ребро графа единичным резистором, то получим электрическую схему, соответствующую нашему разбиению. Если считать, что сила тока в каждом резисторе равна числу, приписанному соответствующему ребру, то для каждой вершины сумма втекающих в нее токов будет равна сумме вытекающих. Действительно, обе эти суммы равны длине горизонтального отрезка, в центре которого выбиралась рассматриваемая вершина.

Назовем **гранью** любую часть плоскости, ограниченную двумя непересекающимися ориентированными цепями ребер графа с общими началом и концом. Количество вершин графа обозначим b, а количество граней — r.

Для каждой грани суммы чисел, приписанных ребрам обеих цепей, равны друг другу. Действительно, каждой грани можно сопоставить вертикальный отрезок внутри прямоугольника, состоящий из сторон квадратов разбиения и ограниченный сверху и снизу подобными же горизонтальными отрезками, тогда обе рассматриваемые суммы равны

длине этого отрезка. Каждую из этих сумм можно интерпретировать как сумму падений напряжения на каждой из рассматриваемых цепей. В результате получаются $b+r$ **уравнений Кирхгофа** для рассматриваемой схемы. Падение напряжения между полюсами схемы равно длине вертикальной стороны прямоугольника, а ее сопротивление — отношению вертикальной и горизонтальной сторон.

Электрическую схему можно сопоставить нашему разбиению и другим способом, а именно, повернув прямоугольник на 90°. Эту схему назовем **двойственной** первоначальной схеме.

13.12. Проверьте, что для П-цепей введенное понятие двойственности совпадает со старым.

В теории графов **двойственным графом** данного плоского графа называется граф, у которого вершинами являются грани исходного графа, а ребра, соединяющие вершины, соответствуют ребрам, принадлежащим одновременно обоим циклам, ограничивающим грани, соответствующие этим вершинам. Число вершин в двойственном графе равно числу граней в исходном и наоборот, а число ребер в обоих графах одинаково. Обозначим его через p.

13.13. Установите связь между понятием двойственности для плоских электрических цепей и двойственностью для плоских графов.

13.14*. *(Эйлер)* Для любого плоского графа докажите формулу $b-p+r=1$.

13.15. Перечислите все графы не более чем с девятью ребрами, соответствующие не П-разбиениям.

13.16. *(Москва,40)* Докажите, что прямоугольник нельзя разбить не более чем на шесть разных квадратов.

13.17*. Докажите, что имеются только два разных разбиения прямоугольника не более чем на девять разных квадратов.

Далее понадобятся некоторые факты о числах Фибоначчи, частично известные читателю по § 7.

13.18. Докажите, что:

$$F_nF_{k-1}+F_{n+1}F_k=F_{n+k};$$
$$F_nF_{k+1}-F_{n+1}F_k=(-1)^kF_{n-k};$$
$$F_{n-1}/F_n+F_{n+k-2}/F_{n+k}=(F_nF_{n+k}+(-1)^nF_k)/F_nF_{n+k};$$
$$F_{n-1}/F_n+F_{n-1}/F_{n+1}=(F_nF_{n+1}+(-1)^n)/F_nF_{n+1};$$
$$F_{n-1}/F_n+F_n/F_{n+2}=(F_nF_{n+2}+(-1)^n)/F_nF_{n+2};$$
$$F_{n-2}/F_n+F_{n+k-1}/F_{n+k}=(F_nF_{n+k}+(-1)^{n+1}F_k)/F_nF_{n+k};$$
$$F_{n-2}/F_n+F_n/F_{n+1}=(F_nF_{n+1}+(-1)^{n+1})/F_nF_{n+1};$$
$$F_{n-2}/F_n+F_{n+1}/F_{n+2}=(F_nF_{n+2}+(-1)^{n+1})/F_nF_{n+2};$$

$$F_{n-1}/F_n - F_{n+k-1}/F_{n+k} = (-1)^n F_k/F_nF_{n+k}; \quad (9)$$

$$F_{n-1}/F_n - F_n/F_{n+1} = (-1)^n/F_nF_{n+1}; \quad (10)$$

$$F_{n-1}/F_n - F_{n+1}/F_{n+2} = (-1)^n/F_nF_{n+2}; \quad (11)$$

$$(F_n, F_k) = F_{(n,k)}; \quad (12)$$

$$F_{n+k} \le F_{n+1}F_{k+1} \le F_{n+k+1}; \quad (13)$$

причем левое неравенство в (13) обращается в равенство при $k = 1$ или $n = 1$, а правое — при $k = 0$ или $n = 0$;

$$F_{n+k+m-1} \le F_{n+1}F_{k+1}F_{m+1} - F_{n-1}F_{k-1}F_{m-1}, \quad (14)$$

причем равенства возможны лишь при $n, k, m \le 2$;

$$F_k \le n \Leftrightarrow k \le \left[\log_\varphi((n + 1/2)\sqrt{5})\right]. \quad (15)$$

Следующий цикл задач посвящен сложности реализации рациональных чисел формулами. Сначала докажите три неравенства задач 13.19 – 13.21.

13.19*. Если $0 \le y_i, p_i, q_i \le x_i$ и $p_i + q_i \le x_i + y_i$, $i = 1, 2$, то $p_1p_2 + q_1q_2 \le x_1x_2 + y_1y_2$, причем при $0 < y_i < x_i$, $i = 1, 2$, равенство возможно, лишь когда $p_i = x_i$, $q_i = y_i$ или когда $p_i = y_i$, $q_i = x_i$, $i = 1, 2$.

13.20. Если $0 \le y_i, p_i, q_i \le x_i$ $p_i + q_i \le x_i + y_i$, $i = 1, \ldots, n$, то $p_1 \ldots p_n + q_1 \ldots q_n \le x_1 \ldots x_n + y_1 \ldots y_n$.

13.21*. В условиях задачи 13.19 справедливо неравенство $p_1q_2 + p_2q_1 + q_1q_2 \le x_1y_2 + x_2y_1 + x_1x_2$. При $0 < y_i < x_i$, $i = 1, 2$, равенство возможно, лишь когда $p_i = y_i$, $q_i = x_i$, $i = 1, 2$.

Далее даются оценки сложности рациональных чисел.

13.22**. *(О. М. Касим-заде)* Пусть p/q — несократимая дробь, p, q — целые, $L_B(p/q) = L$. Тогда $|p|, |q| \le F_{L+1}$, $|p| + |q| \le F_{L+2}$.

13.23. Для любой несократимой дроби p/q, где p, q —натуральные,

$$L_{B_2}(p/q) \ge L_{B_1}(p/q) \ge L_B(p/q) \ge [\log_\varphi(\sqrt{5}(\max(q, p) - 1/2))],$$

$$L_{B_2}(p/q) \ge L_{B_1}(p/q) \ge L_B(p/q) \ge [\log_\varphi(\sqrt{5}(p + q - 1/2))] - 1.$$

13.24**. В случае $\max(q, p) = F_n$ первое из неравенств задачи 13.23 достигается только на дробях $p/q = F_kF_{n-k}/F_n$ или F_n/F_kF_{n-k}, где $(k, n) \le 2$. В случае $p + q = F_n$ это неравенство достигается только на дробях $p/q = F_n/(F_kF_{n-k}) - 1$ или $F_kF_{n-k}/(F_n - F_kF_{n-k})$, где $(n, k) \le 2$.

13.25**. Среди всех несократимых дробей со знаменателем F_n наименьшую сумму элементов в представляющих их обыкновенных

цепных дробях имеют дроби F_{n-1}/F_n и F_{n-2}/F_n. Минимальные формулы в базисах B, B_0, B_1, B_2 для этих чисел соответствуют цепным дробям

$$[0; \underbrace{1 \ldots, 1}_{n-1}] \text{ и } [0; \underbrace{1 \ldots, 1}_{n-3} 2],$$

где $2 = 1 + 1$, и цепным дробям

$$[0; 2 \underbrace{1 \ldots, 1}_{n-3}] \text{ и } [0; 2 \underbrace{1 \ldots, 1}_{n-4} 2],$$

где $2 = 1+1$ или $1+1^{-1}$. Сложность каждой из них равна $n-1$. Среди всех несократимых дробей со знаменателем F_n наименьшую сумму элементов в представляющих их ветвящихся цепных дробях имеют дроби $F_k F_{n-k}/F_n$, где $(k, n) \leq 2$.

Минимальные формулы в упомянутых базисах для этих чисел соответствуют ветвящимся цепным дробям вида

$$\frac{1}{\Phi_1 + \Phi_2},$$

где Φ_1– формула, соответствующая цепным дробям

$$[0; \underbrace{1 \ldots, 1}_{p-1}] \text{ или } [0; \underbrace{1 \ldots, 1}_{p-3} 2],$$

а Φ_2 — формула, соответствующая цепным дробям

$$[1; \underbrace{1 \ldots, 1}_{s-1}] \text{ или } [1; \underbrace{1 \ldots, 1}_{s-3} 2],$$

где $\{s, p\} = \{k, n-k\}$ (формулы, записи которых в приведенной формулировке не имеют смысла из-за отрицательности чисел $s-3$, $p-3$, $n-3$, $n-4$, естественно, следует исключить из этой формулировки). Сложность каждой из них равна $n-2$.

13.26. Докажите, что для любого положительного рационального числа r справедливы неравенства

$$L_B(-r) \leq 2 + L_B(r), \quad L_B(-r) \geq L_B(r),$$

$$L_B(-F_{n-1}/F_n) = n, \quad L_B(-F_{n-2}/F_n) = n.$$

В следующей задаче приводятся новые примеры чисел, для которых достигаются оценки 13.23.

13.27. Первое неравенство из неравенств задачи 13.23 достигается при $n, m \geq 2$ для дробей $F_n F_m/(F_{m+1} F_{n+1})$, у которых $(n+1, m) \leq 2$,

$(m+1,n) \le 2$, дробей $F_{n-1}F_m/(F_{n+1}F_{m+1})$, у которых $(n-1,m+1) \le 2$, $(n+1,m) \le 2$, и дробей $F_{n-1}F_{m-1}/(F_{n+1}F_{m+1})$, у которых $(n-1,m+1) \le 2, (n+1,m-1) \le 2$ (это утверждение теоремы верно и для базиса B_1), а также для дробей $F_n/F_{n+1} \circ F_m/F_{m+1}$, $F_{n-1}/F_{n+1} \circ F_m/F_{m+1}$, $F_{n-1}/F_{n+1} \circ F_{m-1}/F_{m+1}$, у которыхх $(n+1,m+1) \le 2$, $n,m \ge 2$, а символ $\circ$ означает $+$ или $-$ (если символ $\circ$ есть $+$, то утверждение теоремы верно и для базисов B_2 и B_3).

13.28**. Второе неравенство задачи 13.23 достигается для дробей

$$\frac{1}{(F_{k-\kappa}/F_{k+1}) + (F_{l-\lambda}/F_{l+1}) + (F_{m-\mu}/F_{m+1})},$$

у которых $\kappa,\lambda,\mu = 0,1$ и $(k+1,l+1) \le 2$, $(k+1,m+1) \le 2$, $(l+1,m+1) \le 2$, $k,m,l \ge 2$, причем для этих дробей первое неравенство не достигается (это утверждение теоремы верно и для базисов B_2 и B_3).

13.29*. Если $L_B(p/q) = L$, $i = 0,1,2,3$, и при некотором натуральном числе k

$$F_k p + F_{k+1} q \ge F_{L+k}, F_{k-1}p + F_k q \ge F_{L+k-1},$$

то при любом натуральном n

$$L_{B_i}([0;\underbrace{1\ldots1}_{n}p/q]) = L + n.$$

Следующая теорема дает серию дробей, для которых не только достигается первое из неравенств задачи 13.13, но и достигается первое неравенство задачи 13.9.

13.30**. Для следующих дробей r :

$$r = [0;1\ldots1],[0;1\ldots121\ldots1],[0;1\ldots1221\ldots1],[0;1\ldots12221\ldots1],$$

$$[0;1\ldots122221\ldots1],[0;1\ldots1222221\ldots1],[0;2222221\ldots1],$$

$$[0;1\ldots131\ldots1],[0;1\ldots1231\ldots1],[0;1\ldots12231\ldots1],$$

$$[0;1\ldots122231\ldots1],[0;1\ldots12321\ldots1],[0;1\ldots1321\ldots1],$$

$$[0;1\ldots13221\ldots1],[0;31\ldots1],[0;331\ldots1],[0;41\ldots1],[0;421\ldots1]$$

выполняется равенство

$$L_{B_i}(r) = l(r) = \left]\log_\varphi(\sqrt{5}(L(r)-1/2))\right[+ c, \quad c = 0 \text{ или } c = 1$$

Следующая теорема дает некоторые точные неравенства между мерами сложности l, L, L_{B_i}.

13.31*. Для любого положительного рационального r справедливы соотношения

$$l(r) \geq L_{B_3}(r) = L_{B_2}(r) \geq L_{B_1}(r) \geq L_B(r) \geq [\log_\varphi(\sqrt{5}(L(r) - 1/2))] \geq$$

$$\geq [\log_\varphi(\sqrt{5}(l(r) - 1/2))] \geq [\log(\sqrt{5}(L_{B_2}(r) - 1/2))].$$

Для $r = (q+1)/q, q/(q+1)$, где $q = F_nF_{n+1}$ или F_nF_{n+2}, $n \geq 2$,

$$L_{B_3}(r) = L_{B_2}(r) = L_{B_1}(r) = L_B(r) =$$

$$= [\log_\varphi(\sqrt{5}(l(r) - 1/2))] = [\log_\varphi(\sqrt{5}(L(r) - 1/2))],$$

а для $r = 1/q$ при тех же q

$$L_B(r) = [\log_\varphi(\sqrt{5}(L(r) - 1/2))] = [\log_\varphi(\sqrt{5}(L_{B_2}(|r|) - 1/2))].$$

Вернемся к покрытиям прямоугольника квадратами.

13.32. Докажите, что

$$l(m/n) \geq L_\Pi(n, m) \geq [\log_\varphi(\sqrt{5}(\max(m, n) - 1/2))] \geq$$

$$\geq [\log_\varphi(\sqrt{5}(l(m/n) - 1/2))],$$

а для $q = F_nF_{n+1}$ или F_nF_{n+2}, $n \geq 2$,

$$L_\Pi(q+1, q) = [\log_\varphi(\sqrt{5}(l((q+1)/q) - 1/2))] =$$

$$= [\log_\varphi(\sqrt{5}(\max(q+1, q) - 1/2))].$$

Задача 13.32 показывает, в частности, что $L_\Pi(n, m)$ может быть гораздо меньше $l(m/n)$, и устанавливает точное неравенство между ними.

Для базиса B и любого рационального $r \in (0, 1)$ сложности чисел r и $1 - r$, а также r и $1/(1+r)$ отличаются не более чем на 1. Для базисов B_i при $i > 1$ дело обстоит иначе, что видно из следующей задачи.

13.33. Для любого рационального числа $r \in (0, 1)$

$$L_{B_i}(1 + r) = L_{B_i}(1/(1 + r)) \geq [\log_\varphi(\sqrt{5}(L_{B_i}(r) - 1/2))],$$

$$L_{B_i}(1 - r) \geq [\log_\varphi(\sqrt{5}(L_{B_i}(r) - 1/2))],$$

причем для $r = 1/q$, где $q = F_nF_{n+1}$ или F_nF_{n+2}, $n \geq 4$,

$$L_{B_i}(1/(1 + r)) = L_{B_i}(1 - r) = [\log_\varphi(\sqrt{5}(L_{B_i}(r) - 1/2))].$$

13.34*. Докажите, что $L(m,n)$ может быть меньше $L_{\Pi}(n,m)$.

13.35***. Докажите, что для некоторых последовательностей m_k и n_k справедливо неравенство

$$L(m_k,n_k)/L_{\Pi}(m_k,n_k) < 0.89.$$

13.36***. *(М.Ден)* Докажите, что если прямоугольник разрезан произвольным образом на квадраты, то его стороны соизмеримы.

13.37***. Докажите оценку $L(m,n) > \log_2(m+n)$.

УКАЗАНИЯ

13.7. Так как функция $(x^{-1}+y^{-1})^{-1}$ выражается в базисе B_2 в виде бесповторной суперпозиции, то любую формулу в базисе B_3 можно без изменения сложности преобразовать в формулу в базисе B_2, откуда $L_{B_3}(r) \geq L_{B_2}(r)$. Любая подформула вида Φ^{-1} формулы в базисе B представима в виде $(\Phi_1^{-1}+\ldots+\Phi_n^{-1})^{-1}$, где Φ_i — подформулы меньшей сложности или константы 1. Тогда формула Φ эквивалентна формуле той же сложности

$$((\ldots((((\Phi_1^{-1}+\Phi_2^{-1})^{-1})^{-1}+\Phi_3^{-1})^{-1})^{-1}+\ldots+)^{-1}+\Phi_n^{-1})^{-1} =$$

$$= \gamma(\gamma(\ldots\gamma(\gamma(\Phi_1,\Phi_2),\Phi_3),\ldots),\Phi_n),$$

где $\gamma(x,y) = (x^{-1}+y^{-1})^{-1}$, построенной в базисе $B_2 \cup B_3$ и содержащей на один символ $^{-1}$ меньше. Повторяя это преобразование, получим для любой формулы в базисе B_2 эквивалентную ей формулу той же сложности в базисе B_3. Значит, $L_{B_3}(r) \leq L_{B_2}(r)$, откуда $L_{B_3}(r) = L_{B_2}(r)$.

13.9. Очевидно, что любую конечную цепную дробь с натуральными элементами можно преобразовать в формулу в базисе B_2 сложности, равной сумме элементов цепной дроби (заменяя каждый элемент a на формулу $1+\ldots+1$). Поэтому $L_{B_2}(r) \leq l(r)$.

Неравенство $l(r) \leq L(r)$ доказывается индукцией по высоте цепной дроби для r, которую можно считать правильной. База ($n=1$) очевидна.

Шаг индукции. Так как

$$r = \frac{1}{a_1 + \frac{1}{r_1}},$$

где $r_1 = [0; a_2 \ldots, a_n]$, то согласно предположению индукции имеем $l(r_1) \leq L(r_1)$, значит,

$$l(r) = l(r_1) + a_1 \leq l(r_1) + a_1 + (l(r_1)-1)(a_1-1) = l(r_1)a_1 + 1 \leq$$

$$\leq L(1/r_1)a_1 + 1 \leq L(r).$$

Равенство возможно, лишь когда $l(r_1) = 1$ или $a_1 = 1$ и одновременно r_1 — натуральное, т. е. либо когда $r = 1/(a_1+1)$, либо когда

$$r = 1/(1+1/a_2) = a_2/(1+a_2).$$

13.10. Докажем индукцией, что $1/L_{B_2}(r) \leq r$. Пусть Φ — формула сложности $L(r)$ в базисе B_2, реализующая r. Можно считать, что Φ не содержит подформул вида $((\Phi_1)^{-1})^{-1}$. Рассмотрим оба возможных случая. Пусть $\Phi = \Phi_1 + \Phi_2$, Φ_i

реализует r_i и имеет сложность $L_i = L(r_i)$, тогда $L_1 = L_2 + L_1$, $r_2 = r_2 + r_2$. Согласно предположению индукции $r_i \geq 1/L_i$, откуда

$$r = r_1 + r_2 \geq 1/L_1 + 1/L_2 > 1/L.$$

Если же $\Phi = (\Phi_1 + \Phi_2)^{-1}$, то в силу предположения индукции $1/r_i \geq 1/L_i$, откуда $1/r = r_1 + r_2 \leq L_1 + L_2 = L$, причем равенство возможно, лишь когда $r_i = L_i$, т. е. $r = 1/L$.

13.11. Докажем индукцией, что

$$3^{-L/3} \leq r \leq 3^{L/3},$$

где $L = L_{B_1}(r)$. Пусть Φ — формула сложности $L(r)$ в базисе B_2, реализующая r. Можно считать, что Φ не содержит подформул вида $((\Phi_1)^{-1})^{-1}$. Рассмотрим три возможных случая. Предположим, что формула $\Phi = \Phi_1 + \Phi_2$, Φ_i реализует r_i и имеет сложность $L_i = L(r_i)$, тогда $L = L_1 + L_2, r = r_1 + r_2$. Согласно предположению индукции

$$3^{L_i/3} \geq r \geq 3^{-L_i/3},$$

откуда

$$r = r_1 + r_2 \geq 3^{-L_1/3} + 3^{-L_2/3} > 3^{-L/3}.$$

В случае $L_1 + L_2 \geq 3$ очевидно, что

$$r = r_1 + r_2 \leq L_1 + L_2 = L \leq 3^{L/3}.$$

Если $L_1 = 1$ и $L_2 \geq 3$, то в силу неравенства

$$1 < 3(3^{1/3} - 1) \leq 3^{L_2/3}(3^{1/3} - 1)$$

имеем

$$r = r_1 + r_2 \leq 1 + 3^{L_2/3} < 3^{(L_2+1)/3} = 3^{L/3},$$

и аналогично рассматриваем случай $L_2 = 1$ и $L_1 \geq 3$.

Если же $L_1 \geq 2$ и $L_2 \geq 2$, то в силу неравенства

$$1 < (3^{2/3} - 1)(3^{2/3} - 1) \leq (3^{L_2/3} - 1)(3^{L_1/3} - 1)$$

верно, что

$$r = r_1 + r_2 \leq 3^{L_1/3} + 3^{L_2/3} <$$

$$< 3^{L_1/3} + 3^{L_2/3} - 1 + (3^{L_1/3} - 1)(3^{L_2/3} - 1) = 3^{(L_1+L_2)/3} = 3^{L/3}.$$

Во всех рассмотренных случаях равенство возможно, только если $r = 3$.

Случай $\Phi = (\Phi_1 + \Phi_2)^{-1}$, очевидно, сводится к уже рассмотренному. В случае $\Phi = \Phi_1 \cdot \Phi_2$, из предположения индукции следует, что

$$3^{-L_1/3} \cdot 3^{-L_2/3} \leq r_1 r_2 = r = r_1 r_2 \leq 3^{L_1/3} \cdot 3^{L_2/3} = 3^{L/3},$$

причем равенства возможны, только если $r_i = 3^{L_i/3}$ и соответственно $r_i = 3^{L_i/3}$, т. е. когда $r = 3^n, n \in \mathbb{Z}$.

Случай $\Phi = (\Phi_1 \cdot \Phi_2)^{-1}$ рассматривается аналогично.

13.18. Равенства (3) и (6) следуют из (2), а (4),(5),(7)—(11) следуют из (3) и (6), (13) следует из (1). Неравенство (14) доказывается по индукции.

13.19. Сначала заметим, что при условиях $p \le x, 0 \le b \le a$ и $p+q \le x+y$ справедливо неравенство $pa+qb \le xa+yb$. Действительно,

$$pa+qb-xa-yb=(x-p)(b-a)+b(p+q-x-y) \le 0.$$

В силу симметричности условия, можно считать, что $p_1 \ge q_1$. Тогда, применяя два раза сформулированное выше неравенство, получаем

$$p_1p_2+q_1q_2 \le p_1x_2+q_1y_2 \le x_1x_2+y_1y_2.$$

При $p_1 > q_1 > 0$ равенство возможно, так как $p_i = x_i$, $q_i = y_i$, $i = 1,2$. При $q_1 = 0$ равенство невозможно, поскольку $p_1+q_1 < x_1+y_1$. При $p_1 = q_1 > 0$ равенство опять невозможно, ибо тогда равенства $p_1+q_1 = x_1+y_1$, $p_1 = x_1$ несовместны.

13.20. Примените индукцию.

13.21. Сначала заметим, что при $p_1+q_1 \le x_1$

$$p_1q_2+p_2q_1+q_1q_2 \le (p_1+q_1)(p_2+q_2) \le x_1(x_2+y_2) <$$

$$< x_1y_2+x_2y_1+x_1x_2,$$

и, аналогично, такое же строгое неравенство справедливо при $p_2+q_2 \le x_2$. Считая далее, что $p_i+q_i > x_i$, имеем

$$p_1q_2+p_2q_1+q_1q_2=(p_1+q_1)(p_2+q_2)-p_1p_2=$$

$$=(p_1+q_1)(p_2+q_2)-(p_1+q_1-q_2)(p_2+q_2-q_2) \le$$

$$\le (p_1+q_1)(p_2+q_2)-(p_1+q_1-x_1)(p_2+q_2-x_2)=$$

$$=(p_1+q_1)x_2+x_1(p_2+q_2)-x_1x_2 \le (x_1+y_1)x_2+(x_2+y_2)x_1-x_1x_2=$$

$$=x_1y_2+x_2y_1+x_1x_2.$$

13.22. Оба неравенства докажем по индукции. База индукции ($L=1$) очевидна.

Выполним шаг индукции. Пусть Φ — формула сложности L в базисе B. Тогда или $\Phi = \Phi_1 \pm \Phi_2$, или $\Phi = \Phi_1 \cdot \Phi_2$, где Φ_i — формулы сложности L_i, $L_1+L=L$, или $\Phi = \Phi_1^{-1}$, где Φ_1 имеет сложность L. В последнем случае обоснование шага индукции очевидно. Рассмотрим первые два случая. Согласно предположению индукции формулы Φ_i реализуют дроби p_i/q_i, такие, что

$$|p_i|, |q_i| \le F_{L_i+1}, |p_i|+|q_i| \le F_{L_i+2}, p_i,\ q \in \mathbb{Z}.$$

Тогда формула Φ реализует дробь p/q, такую, что $q = q_1q_2$, и $p = p_1q_2 \pm q_1p_2$ в первом и $p = p_1p_2$ во втором случае.

В первом случае, применяя задачу 13.19 при $x_i = F_{L_i+1}$, $y_i = F_{L_i}$ и используя соотношение (1) 13.18, получаем неравенство

$$|p| \le |p_1||q_2|+|q_1||p_2| \le F_{L_1+1}F_{L_2+1}+F_{L_1}F_{L_2} = F_{L_1+L_2+1}.$$

Во втором случае такое же неравенство, очевидно, следует из одного только соотношения (13) из 13.18. Так же доказывается неравенство для $|q|$. Оценим теперь $|q|+|p|$. В первом случае, применяя 13.21 при $x_i = F_{L_i+1}$, $y_i = F_{L_i}$ и используя соотношение (1) из 13.18, получаем неравенство

$$|q|+|p| \le |p_1||q_2|+|q_1||p_2|+|q_1||q_2| \le$$

$$\leq F_{L_1+1}F_{L_2+1} + F_{L_1+1}F_{L_2} + F_{L_1}F_{L_2+1} = F_{L_1+1}F_{L_2+2} + F_{L_1}F_{L_2+1} =$$
$$= F_{L_1+L_2+2}.$$

Во втором случае, так же как и в неравенстве для $|p|$ первого случая,

$$|q| + |p| \leq |p_1||p_2| + |q_1||q_2| \leq F_{L_1+1}F_{L_2+1} + F_{L_1}F_{L_2} = F_{L_1+L_2+1}.$$

13.23. Начальные неравенства в обеих цепочках очевидны, так как базисы B_2 и B_1 содержатся в B_0 . Докажем неравенство

$$L_B(p/q) \geq [\log_\varphi(\sqrt{5}(\max(p,q) - 1/2))].$$

Обозначив $L_B(p/q)$ через L и применив 13.22,. получаем, что $\max(p,q) \leq F_{L+1}$. Отсюда и из соотношения (15) задачи 13.18 получаем, что

$$L + 1 \geq [log_\varphi(\sqrt{5}(\max(p,q) - 1/2))]$$

а, значит, и наше неравенство. Неравенство

$$L_{B_0}(p/q) \geq [\log_\varphi(\sqrt{5}(p + q - 1/2))] - 1$$

доказывается аналогично, только вместо первого неравенства задачи 13.2 используем неравенство $p + q \leq F_{L+2}$.

13.24. В случае $\max(p,q) = F_n$ неравенство

$$L_{B_0}(p/q) \geq \lfloor \log \varphi(\sqrt{5}(\max(p,q) - 1/2)) \rfloor$$

принимает вид $L \geq n-1$. В равенство оно обращается тогда и только тогда, ког $\max(p,q) = F_n = F_{L+1}$. Пусть Φ — формула сложности L, реализующая дро p/q. Тогда $\Phi = \Phi_1 \circ \Phi_2$ или $(\Phi_1 \circ \Phi_2)^{-1}$, где $\circ$ — одна из арифметических операц $<< + >>, << - >>, << \cdot >>$, а Φ_i — подформулы сложности $L_i, L_1 + L_2 =$ Обозначим дроби, реализуемые формулами Φ_i , через p_i/q_i. Можно счита что $q_i \in \mathbb{N}$. Согласно задаче 13.22

$$\max(|p_i|, q_i) \leq F_{L_i+1}, |p_i| + q_i \leq F_{L_i+2}.$$

Тогда в случае $\Phi = \Phi_1 \circ \Phi_2$ в силу 13.19, как и в доказательстве теоремы 13.2 имеем

$$p \leq |p_1||q_2| + |p_2||q_1| \leq F_{L_1+1}F_{L_2+1} + F_{L_1}F_{L_2} = F_{L_1+L_2+1} = F_{L+1},$$

$$|q_1||q_2| \leq F_{L_1+1}F_{L_2+1} < F_{L_1+L_2+1} = F_{L+1},$$

Но $\max(p,q) = F_{L+1}$, а согласно задаче 13.19 равенство здесь возможно, ли когда

$$|p_1|/q_1 = F_{L_1}/F_{L_1+1}, |p_2|/q_2 = F_{L_2+1}/F_{L_2}$$

или когда

$$|p_1|/q_1 = F_{L_1+1}/F_{L_1}, |p_2|/q_2 = F_{L_2}/F_{L_2+1},$$

и только при $\circ = +$ и положительных p_i, или при $\circ = +$, положительном p_1 отрицательном p_2 (ведь в случае $\circ = \cdot$ согласно задаче 13.18 было бы

$$p \leq |p_1||p_2| \leq F_{L_1+1}F_{L_2+1} < F_{L_1+L_2+1} = F_{L+1}.)$$

Во всех этих случаях p/q равно

$$F_{L+1}/(F_{L_1}F_{L_2+1})$$

или

$$F_{L+1}/(F_{L_2}F_{L_1+1}),$$

т. е. $p/q = F_n/(F_kF_{n-k})$. Последняя дробь, в силу следующих из 13.18 равенств

$$(F_n, F_k) = F_{(n,k)} = F_{(n,n-k)} = (F_n, F_{n-k}),$$

будет несократимой тогда и только тогда, когда $(n,k) \leq 2$.

Случай $(\Phi_1 \circ \Phi_2)^{-1}$, рассматривается аналогично. В этом случае равенство $\max(p,q) = F_{L+1}$ возможно тогда и только тогда, когда $q/p = F_n/(F_kF_{n-k}), (n,k) \leq 2$. Из доказанного следует, что минимальная формула Φ для числа $F_n/(F_kF_{n-k})$ при $(n,k) \leq 2$ имеет вид $\Phi_1 \pm \Phi_2$, где Φ_1 — минимальная формула для числа F_{s-1}/F_s (числа F_{s+1}/F_s), а Φ_2 — минимальная формула для числа F_{p+1}/F_p (числа F_{p-1}/F_p), где $\{s,p\} = \{k, n-k\}$, и минимальная формула для $(F_kF_{n-k})/F_n$ — вид $\Phi_1 \pm \Phi_2$.

Найдем условия равенства в случае $p+q = F_n$. В этом случае неравенство

$$L_{B_0}(p/q) \geq \lfloor \log\varphi(\sqrt{5}(p+q-1/2)) \rfloor$$

принимает вид $L \geq n-2$. В равенство оно обращается тогда и только тогда, когда $p+q = F_n = F_{L+2}$. Пусть, как и в предшествующих рассмотрениях, Φ — формула сложности L, реализующая дробь p/q, $\Phi = \Phi_1 \circ \Phi_2$ или $(\Phi_1 \circ \Phi_2)^{-1}$, , где $\circ$ — одна из операций $<<+>>, <<->>, <<\cdot>>$, а Φ_i — подформулы сложности L_i, реализующие числа p_i/q_i, такие, что

$$L_1 + L_2 = L, q_i \in \mathbb{N}, \max(|p_i|, q_i) \leq F_{L_i+1}, |p_i| + q_i \leq F_{L_i+2}.$$

Тогда в случае $\Phi = \Phi_1 \circ \Phi_2$ в силу 13.21 как и в доказательстве теоремы 13.22, имеем

$$p+q \leq |p_1||q_2| + |p_2||q_1| + q_1q_2 \leq$$

$$\leq F_{L_1+1}F_{L_2+1} + F_{L_1+1}F_{L_2} + F_{L_2+1}F_{L_1} = F_{L_1+L_2+2} = F_{L+2}.$$

Но $p+q = F_{L+2}$, а согласно 13.21 равенство здесь возможно, лишь когда

$$|p_1|/q_1 = F_{L_1}/F_{L_1+1}, |p_2|/q_2 = F_{L_2}/F_{L_2+1},$$

и только при $\circ = +$ и положительных p_i , или при $\circ = -$, положительном p_1 и отрицательном p_2 (ведь в случае $\circ = \cdot$ согласно 13.19 было бы

$$p+q \leq |p_1p_2| + q_1q_2 \leq F_{L_1+L_2+1} = F_{L+1}.)$$

Во всех случаях

$$\frac{p}{q} = \frac{F_n - F_kF_{n-k}}{F_kF_{n-k}} = \frac{F_n}{F_kF_{n-k}} - 1,$$

где $(n,k) \leq 2$ (последнее условие есть условие несократимости дроби).

Случай $(\Phi_1 \circ \Phi_2)^{-1}$, рассматривается аналогично. В этом случае равенство $p+q = F_{L+2}$ возможно тогда и только тогда, когда

$$\frac{q}{p} = \frac{F_n}{F_kF_{n-k}} - 1, (n,k) \leq 2.$$

Из доказанного следует, что минимальная формула Φ для числа

$$\frac{F_n}{F_k F_{n-k}} - 1$$

при $(n,k) \leq 2$ имеет вид $\Phi_1 \pm \Phi_2$, где Φ — минимальная формула числа F_{s-1}/F_s, а Φ_2 — минимальная формула для числа F_{p-1}/F_p, где $\{s,p\} = \{k, n-k\}$, и минимальная формула для числа

$$\frac{F_k F_{n-k}}{F_n - F_k F_{n-k}}$$

— вид $(\Phi_1 \pm \Phi_2)^{-1}$.

13.25. Утверждения о сумме элементов цепных и ветвящихся дробей следуют из 13.23 и 13.5, а также утверждения о дробях F_{n-1}/F_n, которое доказывается индукцией по n. База $(n = 2)$ очевидна.

Выпоним шаг индукции. Пусть Φ — минимальная формула в базисе B_i, $i \leq 2$, реализующая F_{n-1}/F_n. Согласно задаче 13.24 формула Φ имеет сложность $n-1$ и вид $(\Phi_1 \pm \Phi_2)^{-1}$, где Φ_1 — формула сложности $n-2$ для F_{n-2}/F_{n-1} и Φ_2 — формула сложности 1 для $\pm F_2/F_1 = \pm 1$. Так как число -1 имеет сложность больше 1, то формула Φ может иметь только вид $(\Phi_1 + 1)^{-1}$, где Φ_1 — минимальная формула для F_{n-2}/F_{n-1}. По предположению индукции Φ_1 соответствует одной из цепных дробей $\underbrace{1\ldots,1}_{n-2}$ и $\underbrace{1\ldots,1,2}_{n-4}$. Значит, Φ соответствует одной из цепных дробей $\underbrace{1\ldots,1}_{n-1}$ и $\underbrace{1\ldots,1,2}_{n-3}$, что и завершает индукцию.

Пусть теперь Φ — минимальная формула, реализующая F_{n-2}/F_n. Согласно задаче 13.24, формула Φ имеет сложность $n-1$ и вид $(\Phi_1 \pm \Phi_2)^{-1}$, где Φ_1 — формула сложности $n-3$ для F_{n-3}/F_{n-2} и Φ_2 — формула сложности 1 для $\pm F_3/F_2 = \pm 2$. Так как число -2 имеет сложность больше 2, то формула Φ может иметь только вид $(\Phi_1 + 2)^{-1}$, где Φ — минимальная формула для F_{n-3}/F_{n-2} . Используя доказанную выше часть утверждения 13.25, получаем, что формула Φ соотвествует цепным дробям $\underbrace{1\ldots,1}_{n-3}$ и $\underbrace{1\ldots,1}_{n-4}$, что и требовалось.

Пусть теперь Φ — минимальная формула, реализующая $F_k F_{n-k}/F_n$, где $(k,n) \leq 2$. Согласно задаче 13.24, формула Φ имеет сложность $n-1$ и вид $(\Phi_1 \pm \Phi_2)^{-1}$, где Φ_1 — формула сложности s для F_{s+1}/F_s и Φ_2 —формула сложности $p-1$ для $\pm F_{p-1}/F_p$, где $left\{s, pright\} = left\{k, n-kright\}$. Легко доказать по индукции, что сложность числа $-F_{n-1}/F_n$ не меньше n. Действительно, база индукции $(n = 2)$ очевидна, а если Φ — формула сложности $n-1$, реализующая F_{n-1}/F_n, то она согласно задаче 13.24 имеет вид $(\Phi_1 \pm \Phi_2)^{-1}$, где Φ_1 — формула сложности $n-2$ для $-F_{n-2}/F_{n-1}$ и Φ_2 — формула сложности 1 для F_2/F_1, что невозможно по предположению индукции.

Из доказанного следует, что минимальная формула, реализующая $F_k F_{n-k}/F_n$, имеет вид $(\Phi_1 + \Phi_2)^{-1}$, где Φ_1 — формула сложности s для F_{s+1}/F_s и Φ_2 — формула сложности $p-1$ для F_{p-1}/F_p. Применяя доказанную выше часть утвержденииия 13.25, получаем последнее утверждение теоремы.

13.26. В доказательстве предыдущего утверждения было показано, что

$$\mathcal{L}_B(-F_{n-1}/F_n) \geq n.$$

Так как

$$-F_{n-1}/F_n = F_{n-2}/F_n - 1,$$

то на самом деле

$$L_B(-F_{n-1}/F_n) \geq n,$$

и, аналогично,

$$L_B(-F_{n-2}/F_n) \geq n.$$

13.27. Из утверждения 13.25 легко вытекает, что первые три числа, указанные в формулировке, имеют сложность $m+n$, а последнее — сложность $m+k+l$. Как известно, если дроби a/b и c/d несократимы, то дробь ac/bd несократима тогда и только тогда, когда

$$(a,d) = (b,c) = 1,$$

дробь

$$a/b + c/d = (ad+bc)/bd$$

несократима тогда и только тогда, когда $(b,d) = 1$, а дробь

$$a/b + c/d + f/g = (adg + cbg + fbd)/bdg$$

несократима тогда и только тогда, когда

$$(b,d) = (d,g) = (b,g) = 1.$$

Условия, наложенные на m и n, в силу соотношения (12) из 13.18 гарантируют несократимость упомянутых дробей. Тот факт, что сложность дробей

$$F_n/F_{n+1} \circ F_m/F_{m+1}, F_{n-1}/F_{n+1} \circ F_m/F_{m+1}, F_{n-1}/F_{n+1} \circ F_{m-1}/F_{m+1}$$

не меньше $m+n$, вытекает теперь из первого неравенства задачи 13.23 и соотношения (13) из 13.18.

13.28. Тот факт, что сложность дробей

$$\frac{1}{\frac{F_{k-\kappa}}{F_{k+1}} + \frac{F_{l-\lambda}}{F_{l+1}} + \frac{F_{m-\mu}}{F_{m+1}}}$$

не меньше $m+l+k$, вытекает из второго неравенства 13.23 и неравенства

$$F_{k-1}F_{l+1}F_{m+1} + F_{k+1}F_{l-1}F_{m+1} + F_{k+1}F_{l+1}F_{m-1} + F_{k+1}F_{l+1}F_{m+1} >$$

$$> F_{k+l+m+1}.$$

Правильность упомянутых дробей обосновывается очевидным неравенством

$$F_{k-1}/F_{k+1} + F_{l-1}/F_{l+1} + F_{m-1}/F_{m+1} > 1/3 + 1/3 + 1/3 = 1,$$

ведь

$$F_{n+1} = F_n + F_{n-1} = 2F_{n-1} + F_{n-2} < 3F_{n-1}.$$

Докажем предыдущее неравенство двойной индукцией по k и l. Проверим базу индукции. При $k=2, l=2$ неравенство принимает вид

$$2F_{m+1} + 2F_{m+1} + 4F_{m-1} + 4F_{m+1} > F_{m+5},$$

и, очевидно, выполняется, так как

$$F_{m+5} = F_{m+4} + F_{m+3} = 2F_{m+3} + F_{m+2} = 3F_{m+2} + 2F_{m+1} =$$

$$= 5F_{m+1} + 3F_m,$$

$$3F_{m+1} + 4F_{m-1} > 3F_{m-1} + 3F_{m-2} = 3F_m.$$

При $k = 2, l = 3$ или $k = 3, l = 2$ неравенство принимает вид

$$3F_{m+1} + 2F_{m+1} + 6F_{m-1} + 6F_{m+1} > F_{m+6},$$

и, очевидно, выполняется, так как

$$F_{m+6} = F_{m+4} + F_{m+5} = 3F_{m+1} + 2F_m + 5F_{m+1} + 3F_m = 8F_{m+1} + 5F_m,$$

$$3F_{m+1} + 6F_{m-1} = 3F_m + 9F_{m-1} = 12F_{m-1} + 3F_{m-2} >$$

$$> 5F_{m-1} + 5F_{m-2} = 5F_m.$$

При $k = 3, l = 3$ неравенство принимает вид

$$3F_{m+1} + 3F_{m+1} + 9F_{m-1} + 9F_{m+1} > F_{k+7},$$

и, очевидно, выполняется, так как

$$F_{m+7} = F_{m+5} + F_{m+6} = 5F_{m+1} + 3F_m + 8F_{m+1} + 5F_m$$

$$= 13F_{m+1} + 8F_m,$$

$$2F_{m+1} + 9F_{m-1} = 2F_m + 11F_{m-1} > 8F_m,$$

ведь

$$11F_{m-1} = 6F_{m-1} + 5F_{m-1} = 6F_{m-1} + 5F_{m-2} + 5F_{m-3} >$$

$$> 6F_{m-1} + 5F_{m-2} + F_{m-3} + F_{m-4} = 6F_{m-1} + 6F_{m-2} = 6F_m.$$

Сделаем шаг индукции от $(k-1, l, m)$ и (k, l, m) к $(k+1, l, m)$. Согласно предположению индукции

$$F_{k-2}F_{l+1}F_{m+1} + F_kF_{l-1}F_{m+1} + F_kF_{l+1}F_{m-1} + F_kF_{l+1}F_{m+1} >$$

$$> F_{k+l+m},$$

$$F_{k-1}F_{l+1}F_{m+1} + F_{k+1}F_{l-1}F_{m+1} + F_{k+1}F_{l+1}F_{m-1} + F_{k+1}F_{l+1}F_{m+1} >$$

$$> F_{k+l+m+1}.$$

Складывая эти неравенства, и учитывая, что

$$F_{k-2} + F_{k-1} = F_{k+1},\ F_{k+1} + F_k = F_{k+2},$$

$$F_{k+l+m} + F_{k+l+m+1} = F_{k+l+m+2},$$

получаем неравенство

$$F_kF_{l+1}F_{m+1} + F_{k+2}F_{l-1}F_{m+1} + F_{k+2}F_{l+1}F_{m-1} + F_{k+2}F_{l+1}F_{m+1} >$$

$$> F_{k+l+m+2},$$

которое и означает справедливость доказываемого неравенства для троек индексов $(k+1, l, m)$.

Шаг индукции от $(k, l-1, m)$ и (k, l, m) к $(k, l+1, m)$ обосновывается (в силу симметрии доказываемого неравенства относительно любых перестановок индексов) аналогично.

Применяя индукцию по k, получаем справедливость неравенства для всех троек индексов $k, 2, m$ и $k, 3, m$, а применяя индукцию по l, получаем наше неравенство для любых $k, l, m \geq 2$. Воспользоваться первым неравенством 13.23 нельзя, так как при $k, l, m \to \infty$

$$F_{k-1}F_{l+1}F_{m+1} + F_{k+1}F_{l-1}F_{m+1} + F_{k+1}F_{l+1}F_{m-1} < F_{k+l+m},$$

что легко проверяется с помощью формул

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}, \varphi = \frac{\sqrt{5}+1}{2},$$

и неравенства $3\varphi < 5$.

13.31. Первое неравенство уже доказано в 13.9. Второе неравенство доказано в 13.23. Последнее неравенство вытекает из предыдущего и второго неравенства задачи 13.9.

Докажем остальные утверждения. Пусть $q = F_nF_{n+1}$. Применяя в зависимости от четности n одно из равенств

$$F_{n-1}/F_n + F_{n-1}/F_{n+1} = (F_nF_{n+1} + (-1)^n)/F_nF_{n+1},$$

$$F_{n-2}/F_n + F_n/F_{n+1} = (F_nF_{n+1} + (-1)^{n+1})/F_nF_{n+1},$$

и пользуясь равенствами

$$l(F_{n-1}/F_n) = l(F_{n-2}/F_n) = n-1,$$

получаем, что

$$L_{B_i}(1+1/q) \leq L_{B_i}(F_{n-1}/F_n) + L_{B_i}(F_{n-1}/F_{n+1}) \leq n-1+n = 2n-1,$$

или

$$L_{B_i}(1+1/q) \leq L_{B_i}(F_{n-2}/F_n) + L_{B_i}(F_n/F_{n+1}) \leq n-1+n = 2n-1.$$

Применяя неравенство из задачи 13.18

$$F_{n+k} < F_{n+1}F_{k+1} < F_{n+k+1}, n, k \geq 2,$$

замечаем, что при $n \leq 2$

$$F_{2n-1} < q = F_nF_{n+1} < F_{2n},$$

значит, $q+1 \leq F_{2n}$, откуда согласно задаче 13.18

$$\lfloor \log_\varphi(\sqrt{5}(q+1/2)) \rfloor = 2n-1,$$

а согласно 13.9,

$$L_{B_i}(1+1/q) \geq \lfloor \log_\varphi(\sqrt{5}(q+1/2)) \rfloor = 2n-1,$$

значит,

$$L_{B_i}(1+1/q) = 2n-1 = \lfloor \log_\varphi(\sqrt{5}(q+1/2)) \rfloor.$$

Пусть теперь $q = F_nF_{n+2}$. Применяя, в зависимости от четности n, одно из равенств

$$F_{n-1}/F_n + F_n/F_{n+2} = (F_nF_{n+2} + (-1)^n)/F_nF_{n+2},$$

$$F_{n-2}/F_n + F_{n+1}/F_{n+2} = (F_nF_{n+2} + (-1)^{n+1})/F_nF_{n+2},$$

получаем аналогично предыдущему

$$L_{B_1}(1 + 1/q) \leq 2n.$$

Опять применяя неравенство задачи 13.18, замечаем, что при $n \leq 2$

$$F_{2n} < q = F_nF_{n+2} < F_{2n+1},$$

откуда опять согласно задаче 13.18

$$\lfloor \log_\varphi(\sqrt{5}(q + 1/2)) \rfloor = 2n,$$

и согласно утверждению 13.9

$$L_{B_1}(1 + 1/q) = 2n = \lfloor \log_\varphi(\sqrt{5}(q + 1/2)) \rfloor.$$

13.32. Примените 13.31.

13.33. Примените 13.29 и 13.3.

13.34. Используя 13.17, покажите, что $L(61,69) = 9$. Из 13.22 выведите, что $L_\Pi(61,69) \geq 10$.

13.35. Рассмотрите электрическую цепь с вершинами $1,2,\ldots,8$ и единичными резисторами, соединяющими пары вершин (1,2), (1,3), (2,3), (2,6), (3,4), (3,5), (4,5), (4,7), (5,6), (5,7), (6,8), (7,8). Проверьте, что при напряжении между полюсами 1 и 8, равном 377, по резисторам пойдет ток (в направлении от меньших номеров к большим) силы 123, 138, 10, 113, 68, 75, 7, 61, 28, 54, 141, 115 соответственно. Постройте по этой цепи разбиение прямоугольника 256×377 на 12 квадратов со сторонами 123, 138, 10, 113, 68, 75, 7, 61, 28, 54, 141, 115. Рассмотрите последовательность прямоугольников с размерами $p_n \times q_n$, определяемую рекуррентными формулами

$$p_{n+1} = p_n^2 + q_n^2, \quad q_{n+1} = p_nq_n, \quad p_0 = 377, \quad q_0 = 256,$$

и докажите по индукции, что $\text{НОД}(p_n, q_n) = 1$ и $L(p_n, q_n) \leq 2^n \cdot 12$ (в доказательстве неравенства шаг индукции обосновывается тем, что прямоугольник $p_n \times q_n$ разбивается на два прямоугольника, подобных прямоугольнику $p_{n-1} \times q_{n-1}$). Отсюда следует, что

$$L(p_n, q_n)/\log_\varphi p_n < 12/\log_\varphi 377 < 0,89.$$

Далее примените 13.23.

13.36. Напишите систему линейных уравнений для сторон $x_1,\ldots,x_n$ квадратов разбиения прямоугольника $X \times Y$ и решите ее методом исключения переменных. Если все неизвестные выразятся через одну, то все ясно. Допустим, что неизвестные $x_1,\ldots,x_k$ выразились через свободные переменные $x_{k+1},\ldots,x_n,X,Y$ и покажем, что это невозможно. Если изменить Y на достаточно малую величину ε, то получим бесконечно много разбиений прямоугольников $X \times Y(\varepsilon)$ на квадраты со сторонами

$$x_1(\varepsilon),\ldots,x_k(\varepsilon),x_{k+1},\ldots,x_{n-1},x_n + \varepsilon,$$

соответствующих одной и той же электрической цепи. Из геометрических соображений интуитивно ясно, что некоторые из функций $x_1(\varepsilon), \ldots, x_k(\varepsilon)$ должны меняться с изменением ε, поэтому в формулах

$$x_i(\varepsilon) = x_i + A_i\varepsilon$$

не все A_i равны нулю. Записав вытекающие из сравнения площадей равенства

$$XY = x_1^2 + \ldots + x_n^2, X(Y+\varepsilon) = x_1^2(\varepsilon) + \ldots + x_k^2(\varepsilon) + x_{k+1}^2 + \ldots + x_n^2,$$

рассмотрев их разность и разложив по степеням ε, получаем

$$x = 2(A_1x_1 + \ldots + A_kx_k) + \varepsilon(A_1^2 + \ldots + A_k^2),$$

а это противоречит произвольности ε.

13.37. Докажем, что если прямоугольник $m \times n$ разрезан на L квадратов и $(m,n) = 1$, то $m+n < 2^L$. Достаточно это доказать в предположении, что сторона ни одного из этих квадратов не совпадает со стороной прямоугольника. Действительно, тогда утверждение в общем случае легко доказывается индукцией по L.

Рассмотрим электрическую схему, соответствующую рассматриваемому разбиению. Обозначим через a общее число резисторов, выходящих из обоих полюсов схемы, и через b — длину цикла из резисторов, ограничивающего эту схему. Из сделанного предположения следует, что $a \geq 4$ и $b \geq 4$, причем ровно четыре резистора одновременно входят в оба рассматриваемых множества. Напишем систему уравнений Кирхгофа, состоящую из v уравнений для вершин схемы и g уравнений для граней плоского графа, изображающего схему. Матрица коэффициентов этой линейной системы имеет размеры $(L-1) \times L$ и состоит из 0 и ± 1, причем в четырех столбцах (соответствующих упомянутым четырем резисторам) будет по две ± 1, в $a+b-4$ столбцах (соответствующих остальным резисторам из упомянутых двух множеств) будет по три ± 1 и в остальных $L-a-b$ столбцах — по четыре ± 1 (потому, что каждый такой резистор принадлежит ровно двум граням и входит ровно в две вершины). Перенеся переменную x_i из каждого уравнения (в котором она есть) в правую часть, получим систему из $L-1$ уравнения с $L-1$ неизвестными $x_j, j \neq i$. Так как исходная система имела согласно задаче 13.36 для каждого значения x_i ровно одно решение, то рассматриваемая система тоже имеет для каждого значения x_i ровно одно решение, находя которое по правилу Крамера, получаем

$$x_j = p_{ji}x_i/q_i,$$

где p_{ji} и q_i — целые (так как определители с целыми коэффициентами — целые). Так как все векторы $(x_1, \ldots, x_L)$, удовлетворяющие указанному соотношению, коллинеарны, то целочисленное решение системы $y_i, 1 \leq i \leq L$, состоящее из взаимно простых в совокупности чисел, определяется однозначно с точностью до смены знака, поэтому квадраты в рассматриваемом разбиении прямоугольника имеют стороны $y_i \leq q_i$. Если обозначить номера переменных, соответствующих четырем выделенным ранее резисторам, через $i_1, \ldots, i_4$, а номера резисторов, содержащихся в цикле, ограничивающем схему, или входящих в полюса схемы, обозначить $j_1, \ldots, j_{a+b-4}$, то будет справедливо соотношение

$$2(m+n) = 2\left(y_{i_1} + \ldots + y_{i_4} + y_{j_1} + \ldots + y_{j_{a+b-4}}\right) \leq$$

$$\leq 2\left(q_{i_1}+\ldots+q_{i_4}+q_{j_1}+\ldots q_{j_{a+b-4}}\right)\cdot$$

Так как согласно неравенству Адамара определитель $n\times n$ матрицы $A=(a_{ij})$ не превосходит

$$\left(\prod_{i=1}^{n}\sum_{j=1}^{n}a_{ij}^2\right)^{1/2},$$

то

$$q_{i_k}^2\leq 2^3\cdot 3^{a+b-4}\cdot 4^{L-a-b},\quad q_{j_k}^2\leq 2^4\cdot 3^{a+b-5}\cdot 4^{L-a-b}.$$

Поэтому

$$2(m+n)\leq 4\cdot\left(2^3\cdot 3^{a+b-4}\cdot 4^{L-a-b}\right)^{1/2}+(a+b)\left(2^4\cdot 3^{a+b-5}\cdot 4^{L-a-b}\right)^{1/2}\leq$$

$$\leq 2^{L-5/2}+(1/9)2^{L+3/2}\cdot(a+b)\cdot(3/4)^{(a+b)/2}<2^{L+1},$$

так как $a+b\geq 8$ и

$$(a+b)\cdot(3/4)^{(a+b)/2}\leq 8\cdot 81/256=81/32.$$

§ 14. О СЛОЖНОСТИ ПРИБЛИЖЕННОГО ВЫЧИСЛЕНИЯ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

Будут рассматриваться следующие меры сложности приближения действительных чисел рациональными:

$$L(\alpha,\varepsilon)=\min\{L(r):|\alpha-r|<\varepsilon\},$$

где $L(r)$ — знаменатель несократимой дроби, представляющей число r, а также

$$L_{B_i}(\alpha,\varepsilon)=\min\{L_{B_i}(r):|\alpha-r|<\varepsilon\},\ i=1,2,$$

где базисы B_i были определены в предыдущем параграфе.

14.1. Докажите, что

$$L(\alpha,\varepsilon)\leq\left[\frac{1}{2\varepsilon}\right]$$

и при α рациональном

$$L(\alpha,\varepsilon)\leq C_\alpha,$$

где C_α — зависящая от α константа, а также

$$L_B(\alpha,\varepsilon)\leq L_{B_1}(\alpha,\varepsilon)\leq L_{B_2}(\alpha,\varepsilon).$$

Рассмотрим приближения только дробями со знаменателями 10 и соответственно изменим определение функции $L(\alpha,\varepsilon)$.

14.2*. Найдите точную верхнюю грань для произведения $L(\alpha,\varepsilon)\varepsilon$.

Числа α и β называются **эквивалентными**, если $\alpha = \frac{a\beta+b}{c\beta+d}$, где a,b,c,d целые, $|ad-cb|=1$. Как было доказано в § 11, $\alpha=[a_0;a_1,\ldots]$ и $\beta=[b_0;b_1,\ldots]$ эквивалентны тогда и только тогда, когда при некотором n и любом $m \geq m_0$ справедливо равенство $a_m = b_{m+n}$. Число $[0;111\ldots]$, обратное числу $\varphi=[1;111\ldots]$, называется *золотым сечением*. Как известно из § 8,

$$\varphi = \frac{\sqrt{5}+1}{2}, \quad F_n = \frac{\varphi^n - (-\varphi)^n}{\sqrt{5}}.$$

Имеет место следующее известное экстремальное свойство золотого сечения.

14.3. Для любого иррационального числа α и некоторой последовательности ε_n, стремящейся к нулю, докажите, что

$$L(\alpha,\varepsilon_n) < \frac{1}{\sqrt{\sqrt{5}\varepsilon_n}},$$

и для всех α, эквивалентных φ, при некотором $\delta(\varepsilon)$, стремящемся к нулю, когда ε стремится к нулю, докажите, что

$$L(\alpha,\varepsilon) > \frac{1-\delta(\varepsilon)}{\sqrt{\sqrt{5}\varepsilon}}.$$

14.4. Для α, не эквивалентного φ, и некоторой последовательности $\varepsilon_n \to 0$ докажите, что

$$L(\alpha,\varepsilon_n) < \frac{1}{\sqrt{\sqrt{8}\varepsilon_n}}.$$

Далее понадобятся некоторые факты о цепных дробях, известные нам по предыдущим разделам, которые для удобства собраны в следующих задачах.

14.5. Последовательность $\varepsilon_n = |\alpha - p_n/q_n| = 1/(q_n(\alpha_{n+1}q_n + q_{n-1}))$ монотонно стремится к нулю при возрастании n. Четные подходящие дроби, возрастая, стремятся к α. Нечетные подходящие дроби, убывая, стремятся к α. Если дробь p/q лежит между дробями p_n/q_n и p_{n-1}/q_{n-1}, то $q \geq q_{n-1}$, а если к тому же $p/q \neq p_{n-1}/q_{n-1}$, то $q \geq q_n$. Последовательность q_n удовлетворяет равенствам $q_{n+1} = a_{n+1} + q_n + q^{n-1}$ и поэтому возрастает. Последовательность остатков дроби α удовлетворяет равенствам $\alpha_n = a_n + 1/\alpha_{n+1}$.

Определим промежуточные дроби $p_{n,r}/q_{n,r}$ при $1 \geq r < a_{n+2}$ равенством

$$\frac{p_{n,r}}{q_{n,r}} = \frac{rp_{n+1}+p_n}{rq_{n+1}+q_n}.$$

14.6. Последовательность

$$\varepsilon_{n,r} = \left|\alpha - \frac{p_{n,r}}{q_{n,r}}\right| = \frac{\alpha_{n+2} - r}{q_{n,r}\left(\alpha_{n+2}q_{n+1} + q_n\right)}$$

монотонно убывает при возрастании r от 0 до a_{n+2}, а последовательность $\{q_{n,r}\}$ — возрастает. Последовательность $p_{n,r}/q_{n,r}$ при $0 \geq r \geq a_{n+2}$ монотонно изменяется от p_n/q_n до p_{n+2}/q_{n+2}. Если дробь p/q лежит между промежуточными дробями $p_{n,r}/q_{n,r}$ и $p_{n,r-1}/q_{n,r-1}$, $1 \geq r \geq a_{n+2}$, то $q \geq q_{n,r-1}$, а если к тому же $p/q \neq p_{n,r-1}/q_{n,r-1}$, то $q \geq q_{n,r}$.

В следующей задаче точно вычисляются функции $L_{B_i}(\varphi, \varepsilon)$ и $L(\varphi, \varepsilon)$.

14.7.** Для любого $i = 1, 2$ докажите, что

$$\frac{1}{2}\log_\varphi\left(\sqrt{5}/\varepsilon + 1\right) - 1 \leq L_{B_i}(\varphi, \varepsilon) =$$

$$= \max\left\{-2\left[\frac{2 - \log_\varphi\left(\sqrt{5}/\varepsilon - 1\right)}{4}\right], -2\left[\frac{-\log_\varphi\left(\sqrt{5}/\varepsilon + 1\right)}{4}\right] - 1\right\} <$$

$$< \frac{1}{2}\log_\varphi\left(\sqrt{5}/\varepsilon + 1\right) + 1,$$

$$L(\varphi, \varepsilon) = F_{L_{B_i}(\varphi,\varepsilon)} = \frac{1}{\sqrt{5}}\left(\varphi^{L_{B_i}(\varphi,\varepsilon)} - (-\varphi)^{L_{B_i}(\varphi,\varepsilon)}\right).$$

Назовем **верхним пределом** $\limsup\limits_{\varepsilon\to 0} f(\varepsilon)$ наибольший из всех пределов $\lim\limits_{n\to\infty} f(\varepsilon_n)$, взятых для стремящихся к нулю последовательностей $\{\varepsilon_n\}$. Аналогично (с заменой наибольшего предела на наименьший) определяется **нижний предел**. Будем писать $f(\varepsilon) \underset{\sim}{\leq} g(\varepsilon)$, если $\liminf\limits_{\varepsilon\to 0} \frac{g(\varepsilon)}{f(\varepsilon)} \geq 1$.

14.8*. Докажите, что

$$\frac{1}{\sqrt{\sqrt{5}\varepsilon}} \underset{\sim}{\leq} L\varphi, \varepsilon) \underset{\sim}{\leq} \sqrt{\frac{\frac{1}{2} + \frac{3}{2\sqrt{5}}}{\varepsilon}},$$

$$\limsup_{\varepsilon\to 0} L(\varphi, \varepsilon)\sqrt{\varepsilon} = \sqrt{\frac{\frac{1}{2} + \frac{3}{2\sqrt{5}}}{\varepsilon}}, \quad \liminf_{\varepsilon\to 0} L(\varphi, \varepsilon)\sqrt{\varepsilon} = \frac{1}{\sqrt[4]{5}}.$$

Целью дальнейшего изложения будет доказательство четырех теорем о мере сложности приближения иррациональных чисел $L(\alpha, \varepsilon)$. Первая теорема дает одно экстремальное свойство золотого сечения.

Теорема 1. *Для всех иррациональных чисел* α

$$\liminf_{\varepsilon\to 0} L(\varphi,\varepsilon)\sqrt{\varepsilon} \le \frac{1}{\sqrt[4]{5}}, \quad \limsup_{\varepsilon\to 0} L(\varphi,\varepsilon)\sqrt{\varepsilon} \ge \sqrt{\frac{\frac{1}{2}+\frac{3}{2\sqrt{5}}}{\varepsilon}},$$

$$\frac{\limsup\limits_{\varepsilon\to 0} L(\varphi,\varepsilon)\sqrt{\varepsilon}}{\liminf\limits_{\varepsilon\to 0} L(\varphi,\varepsilon)\sqrt{\varepsilon}} \ge \varphi,$$

причем каждое неравенство обращается в равенство лишь при α, *эквивалентных* φ.

Во второй теореме устанавливаются неравенства для меры сложности $L(\alpha,\varepsilon)$ в терминах скорости роста элементов цепной дроби для α. С ее помощью строятся примеры чисел, у которых функция $L(\alpha,\varepsilon)$ для некоторой последовательности $\{\delta_n\}$ растет очень медленно, а для некоторой последовательности $\{\varepsilon_n\}$ — почти максимально быстро.

Теорема 2. *Пусть* $f(x)$ — *функция, равная в нуле нулю и монотонно стремящаяся к* $+\infty$ *при* $x\to+\infty$, *и положительное число* α *разлагается в цепную дробь с элементами* $a_n\in N$, *которые бесконечно часто удовлетворяют асимптотическому неравенству* $a_{n+1}\gtrsim f(q_n)$, *где* p_n/q_n — n-*я подходящая дробь. Обозначим* $g(x)$ *обратную функцию к функции* $f(x)x$. *Тогда для некоторых последовательностей* $\{\varepsilon_n\}$ *и* $\{\delta_n\}$, *стремящихся к нулю, справедливы асимптотические неравенства*

$$L(\alpha,\varepsilon_n)\gtrsim \frac{1}{2\varepsilon_n g(1/\varepsilon_n)}, L(\alpha,\delta_n)\lesssim g(1/\delta_n).$$

Если же всегда $a_{n+1}\le f(q_n)$, *то*

$$L(\alpha,\varepsilon)\gtrsim \frac{1}{2\varepsilon g(1/\varepsilon)}, L(\alpha,\delta)\lesssim g(1/\delta).$$

Для того чтобы сформулировать третью теорему, введем следующие обозначения.

Пусть $\alpha=[a_0;a_1\dots,a_n\dots]$ — бесконечная цепная дробь, p_n/q_n — последовательность подходящих дробей к ней, $\psi_{n+1}=q_n/q_{n+1}$, а $\alpha_n=[a_n;a_{n+1}\dots]$ — последовательность остатков.

Если a_{n+2} нечетно, то положим $r_n=(a_{n+2}+1)/2$.

Если a_n четно, то положим $r_{n+2}=a_{n+2}/2$ в случае $\psi_{n+1}\alpha_{n+2}>1$ и $r=(a_{n+2}+2)/2$ в противном случае. Положим

$$F_r(\psi,\alpha,a)=\frac{(r+1+\psi)^2((a-r)\alpha+1)}{(r+\psi)(1+\alpha(a+\psi)}, G_r(\psi,\alpha,a)=\frac{(r+\psi)^2\alpha}{1+\alpha(a+\psi)},$$

$$\gamma(\alpha)=\limsup_{n\to\infty}\gamma_n(\alpha),$$

где

$$\gamma_n(\alpha)=\max\left\{G_{r_n}\left(\psi_{n+1},\alpha_{n+3},a_{n+2}\right), F_{r_n}\left(\psi_{n+1},\alpha_{n+3},a_{n+2}\right)\right\}.$$

Теорема 3. *Справедливо равенство*

$$\limsup_{\varepsilon\to 0} \varepsilon L^2(\alpha,\varepsilon) = \gamma(\alpha).$$

Обозначим через K_a множество всех положительных чисел α, у которых разложения в цепные дроби не содержат элементов, превосходящих $a, a > 1$. В четвертой теореме указываются экстремальные свойства некоторых цепных дробей в классах K_a.

Теорема 4. *При любом четном a и нечетном $a \geq 7$ для всех $\alpha \in K$ справедливо неравенство $\gamma(\alpha) < \gamma([1; a1a1\ldots])$, причем равенство возможно лишь для чисел, в разложениях которых в цепную дробь содержатся сколь угодно длинные последовательности следующих друг за другом элементов, совпадающие с последовательностями $a1a1\ldots$. При $a = 5$ среди чисел $\alpha \in K_5$ наибольшую величину $\gamma(\alpha)$ имеют числа вида*

$$\alpha = [\ldots \underbrace{1515\ldots51}_{k_1} 4 \underbrace{1515\ldots151}_{k_2} \ldots \underbrace{1515\ldots151}_{k_{2n-1}} 4 \underbrace{1515\ldots151}_{k_{2n}} \ldots],$$

где последовательность $\{\min(k_{2n-1}, k_{2n})\}$ имеет верхним пределом бесконечность, а в промежутках между соседними блоками

$$\underbrace{1515\ldots151}_{k_{2n-1}} 4 \underbrace{1515\ldots151}_{k_{2n}},$$

могут стоять любые элементы, и только такие числа.

При $a = 3$ среди чисел $\alpha \in K$ наибольшую величину $\gamma(\alpha)$ имеют подобным же образом определяемые числа

$$[\ldots \underbrace{1313\ldots31}_{k_1} 2 \underbrace{1313\ldots131}_{k_2} \ldots \underbrace{1313\ldots131}_{k_{2n-1}} 2 \underbrace{1313\ldots131}_{k_{2n}} \ldots],$$

и только они.

Для доказательства этих теорем понадобится ряд лемм. Предложим их в виде задач.

14.9**. *(Модернизация теоремы Гюйгенса – Смита)* Докажите, что

$$\limsup_{\varepsilon\to 0} \varepsilon L^2(\alpha,\varepsilon) = \limsup_{n\to\infty} \max\left(q_{n,r_n}^2 \varepsilon_{n+1}, q_{n,r_n+1}^2 \varepsilon_{n,r_n}\right).$$

Теперь можно доказать теорему 3.

14.10*. Докажите, что $\limsup_{\varepsilon\to 0} \varepsilon L_2(\alpha,\varepsilon) = \gamma(\alpha)$.

Для доказательства теорем 1 и 2 понадобится еще несколько лемм.

14.11. Докажите, что если $\psi_{n+1}\alpha_{n+3} > 1$ и a_{n+2} четно, то

$$\gamma_n(\alpha) = F_{r_n}(\psi_{n+1}, \alpha_{n+3}, a_{n+2}) = q^2_{n,r_n+1}\varepsilon_{n,r_n}.$$

Далее для краткости будем опускать индексы у $r_n, \psi_{n+1}, \alpha_{n+3}$ и a_{n+2} (если это не вызывает недоразумений). Также для краткости введем следующие обозначения:

$$g_r(\psi) = (r+\psi)^3 - (r-1)(r+\psi+1)^2, \quad f_r(\psi) = (r+\psi+1)^2/g_r(\psi),$$

$$h_r(\psi) = \frac{(r+\psi+2)^2}{g_{r+1}(\psi) + (r+\psi+2)^2}.$$

14.12*. Если $a = 2r-1$, то $F_r(\psi,\alpha,a) > G_r(\psi,\alpha,a)$ тогда и только тогда, когда или $g_r(\psi) \le 0$, или $g_r(\psi) > 0$ и $\alpha < f_r(\psi)$. Условие $g_r(\psi) \le 0$ равносильно

$$r \ge \frac{2\psi^2 + 1 + \sqrt{4\psi+5}}{2(1-\psi)}.$$

Функция

$$\frac{2\psi^2 + 1 + \sqrt{4\psi+5}}{2(1-\psi)}$$

растет на интервале $(0,1)$, поэтому неравенство $g_r(\psi) \ge 0$, равносильно $\psi > \psi_r$, где $g_r(\psi) = 0$. Функция $f_r(\psi)$ убывает на интервале $(\psi_r, 1)$.

14.13*. Если $a = 2r-2$ и $\psi\alpha \le 1$, то $F_r(\psi,\alpha,a) > G_r(\psi,\alpha,a)$ тогда и только тогда, когда $\alpha < h_{r-1}(\psi)$. При любом $\psi > 0$ справедливо неравенство $h_{r-1}(\psi) < 1/\psi$. Функция $h_{r-1}(\psi)$ убывает на интервале $(0,1)$.

14.14*. Функция $G_r(\psi,\alpha,a)$ монотонно растет при возрастании α или ψ (и фиксированных a и r) и удовлетворяет неравенствам

$$\frac{(r+1)^2}{2r-1} \ge \frac{(r+1)^2}{a+1} > G_r(\psi,\alpha,a) > \frac{r^2}{a+1} \ge \frac{r^2}{2r+1}.$$

14.15*. Функция $F_r(\psi,\alpha,a)$ убывает с ростом α. При $a \le 4$ и соответствующих r она убывает также с ростом ψ. При $a = 5$ и соответствующем $r = 3$ она убывает при $\psi < 2\alpha - 2$, имеет минимум при $\psi = 2\alpha - 2$ и возрастает при $\psi > 2\alpha - 2$, если, конечно, $\alpha < 3/2$, в противном случае она убывает при $0 < \psi < 1$. При $a = 6$ и $r = 4$ эту функцию имеет смысл рассматривать только при $\psi \le 1/\alpha$ (согласно определению r_n) и тогда она убывает при $0 < \psi < 2\alpha - 3$, имеет минимум при $\psi = 2\alpha - 3$ и возрастает при $\psi > 2\alpha - 3$, если, конечно, $2\alpha - 3 < 1/\alpha$, т. е. при $\alpha < (3+\sqrt{17})/4$, в противном случае

она убывает при $0 < \psi < 1/\alpha$. Во всех остальных случаях функция $F_r(\psi, \alpha, a)$ возрастает с ростом ψ.

14.16. Докажите, что

$$\frac{r^2}{2r+1} \le \frac{r^2}{1+a} \le \max(F_r(\psi,\alpha,a), G_r(\psi,\alpha,a)) < \frac{(r+2)^2}{r+1}.$$

Положим $m(a) = [0; a1a1\ldots]$ и $M(a) = [a; 1a1a\ldots]$. Очевидно, что $m(a) \in K$ и $M(a) \in K$.

14.17. Докажите, что

$$m(a) = \frac{1}{a + \frac{1}{1+m(a)}} = \frac{1+m(a)}{a+1+am(a)} = \frac{\sqrt{a^2+4a}-a}{2a} = \frac{\sqrt{1+4/a}-1}{2},$$

$$a \cdot m^2(a) + a \cdot m(a) = 1, M(a) = 1/m(a) = \frac{\sqrt{a^2+4a}+a}{2}.$$

14.18. Во множестве K_a элемент $m(a)$ — минимальный, а $M(a)$ — максимальный. Все его рациональные точки изолированы друг от друга.

Положим при $k = 2r-1$

$$B(a,k) = \max\{\max(F_r(\psi,\alpha,k), G_r(\psi,\alpha,k)) :$$

$$m(a) \le \psi \le \frac{1}{1+m(a)}, 1+m(a) \le \alpha \le M(a)\},$$

$$b(a,k) = \min\{\max(F_r(\psi,\alpha,k), G_r(\psi,\alpha,k)) :$$

$$m(a) \le \psi \le \frac{1}{1+m(a)}, 1+m(a) \le \alpha \le M(a)\},$$

а при $k = 2r$

$$B(a,k) = \max\{\max(F_{r_0}(\psi,\alpha,k), G_{r_0}(\psi,\alpha,k)) :$$

$$m(a) \le \psi \le \frac{1}{1+m(a)}, 1+m(a) \le \alpha \le M(a)\},$$

$$b(a,k) = \min\{\max(F_{r_0}(\psi,\alpha,k), G_{r_0}(\psi,\alpha,k)) :$$

$$m(a) \le \psi \le \frac{1}{1+m(a)}, 1+m(a) \le \alpha \le M(a)\},$$

где $r_0(r,\psi,\alpha) = r$, если $\alpha\psi > 1$, и $r_0(r,\psi,\alpha) = r+1$, если $\alpha\psi \le 1$.

14.19.** Докажите, что при $r \ge 4$

$$b(a, 2r-1) = F_r(m(a), M(a), 2r-1), b(a,5) = F_3(\psi_1(a), M(a), 5),$$

$$b(a,3) = F_2(\psi_0(a), M(a), 3),$$

где $f_3(\psi_1(a)) = M(a), f_2(\psi_0(a)) = M(a)$.

14.20. Докажите, что при $r \geq 3$

$$B(a, 2r-1) = F_r\left(\frac{1}{m(a)+1}, m(a)+1, 2r-1\right),$$

$$B(a,3) = F_2(m(a), m(a)+1, 3).$$

14.21.** Докажите, что при любом натуральном r

$$B(a,2r) = G_{r+1}\left(\frac{1}{m(a)+1}, m(a)+1, 2r\right) =$$

$$= F_r\left(\frac{1}{m(a)+1}, m(a)+1; 2r\right).$$

14.22*.** Докажите, что при любом $r \geq 1$

$$b(a,2r) = G_{r+1}\left(m(a), \max\left(h_r\left(m(a)\right), m(a)+1\right), 2r\right),$$

при $r \geq 3$

$$b(2r,2r) = G_{r+1}\left(m(2r), h_r\left(m(2r)\right), 2r\right),$$

при $r \geq 2$

$$b(2r,2r) = G_{r+1}\left(m(2r), m(2r)+1, 2r\right).$$

Заметим, что при доказательствах 14.19 – 14.22 нигде не использовались формулы для $m(a)$ и $M(a)$, и, значит, эти леммы были доказаны для любых m и M, таких, что $mM = 1$, $0 < m < 1/2$. Заменив в определениях функций $b(a,k)$ и $B(a,k)$ числа $m(a)$ и $M(a)$ на произвольные m и M, удовлетворяющие соотношениям $mM = 1$, $0 < m < 1/2$, получим определения последовательностей $\{b(m,k)\}$ и $\{B(m,k)\}$. Тогда справедлива следующая лемма.

14.23*.** Докажите следующие утверждения. Последовательности

$$\{b(m,2r-1)\}, \{b(2r-1,2r-1)\}, \{b(m,2r)\}, \{b(2r,2r)\},$$

$$\{B(m,2r)\}, \{B(m,2r-1)\}$$

монотонно возрастают. Последовательность $\{b(m,k)\}$ монотонно возрастает, начиная с $k=3$. Последовательность $\{B(m,k)\}$ монотонно возрастает, начиная с $k=5$. При $r \geq 3$ и $k = 2r-1$ справедливы неравенства

$$B(m,k) \leq k/4 + 3/2 - 1/(4k+12),$$

а при $k = 2r$ — неравенства

$$B(m,k) \le k/4 + 3/2 + 1/(k+2), B(k,k) \le k/4 + 3/2 + 1/(2k+2).$$

При $r \ge 3$ и $k = 2r-1$ справедливы неравенства

$$b(m,k) > k/4 + 1 - O(1/k), b(k,k) > k/4 + 1 - m(k)/5,$$

а при $k = 2r$ — неравенства

$$b(m,k) \ge k/4 + (1+m)/2 - 1/(2k+4m).$$

14.24**. Докажите, что для эквивалентных чисел α и α' величины $\gamma(\alpha)$ и $\gamma(\alpha')$ совпадают.

14.25***. Докажите теорему 1.

14.26***. Докажите теорему 4.

Для доказательства теоремы 2 нам понадобится следующая лемма. Через R_+ обозначается множество всех действительных положительных чисел.

14.27*. Пусть непрерывная функция $f : R_+ \to R_+$ такова, что отношение $f(x)/x$ монотонно стремится к бесконечности и $g = f^{-1}$ — обратная к ней функция. Тогда при любом $y \ge f(x)$ справедливо неравенство

$$2g(y) \le x + \frac{yx}{f(x)}.$$

В частности, при $y_0 > y$ имеем

$$g(y) \le g(y_0) \le g(y)\left(1 + \frac{y_0 - y}{2y}\right).$$

14.28***. Докажите теорему 2.

УКАЗАНИЯ

14.3. Утверждение этой задачи легко вытекает из известной нам по предыдущим разделам теоремы Маркова – Гурвица: для любого иррационального числа α существует бесконечно много рациональных дробей p/q таких, что

$$|\alpha - p/q| < 1/\left(\sqrt{5}q^2\right)$$

и для чисел α, эквивалентных φ, и любого положительного $\kappa < 1/\sqrt{5}$ неравенство

$$|\alpha - p/q| > \kappa/q^2$$

имеет лишь конечное число решений.

14.4. Воспользуйтесь задачей 11.29.

14.5, 14.6. Воспользуйтесь задачами из § 7.

14.7. Положим $\varepsilon_n = |\varphi - \varphi_n|$, где $\varphi_n = p_n/q_n = F_{n+2}/F_{n+1}$ —n-я подходящая дробь для φ. Согласно задаче 14.6 для произвольного числа $\varepsilon \in [\varepsilon_{n+1}, \varepsilon_n)$ имеем

$$\varepsilon_{n+1} = \varepsilon_{n-1,1} \leq \varepsilon < \varepsilon_n < \varepsilon_{n-1,0} = \varepsilon_{n-1},$$

а так как

$$|\varphi - p_{n-1,1}/q_{n-1,1}| = \varepsilon_{n-1,1} \leq \varepsilon,$$

то, согласно определению,

$$L(\varphi, \varepsilon) \leq q_{n-1,1} = q_{n+1} = F_{n+2}.$$

Докажем, что при $\varepsilon \in [\varepsilon_{n+1}, \varepsilon_n)$ справедливо неравенство

$$L(\varphi, \varepsilon) \geq q_{n+1}$$

и, значит,

$$L(\varphi, \varepsilon) = q_{n+1} = F_{n+2}.$$

Пусть $|\varphi - p/q| \leq \varepsilon$. Если дробь p/q лежит по ту же сторону от числа φ, что и p_n/q_n , то p/q лежит между дробями p_{n+1}/q_{n+1} и p_n/q_n, причем $p/q \neq p_n/q_n$ в силу неравенств

$$|\varphi - p/q| \leq \varepsilon < \varepsilon_n = |\varphi - p_n/q_n|.$$

Поэтому, согласно 14.5, имеем $q \geq q_{n+1}$. Если же дроби p/q и p_n/q_n лежат по разные стороны от числа φ, то в силу неравенства

$$|\varphi - p/q| \leq \varepsilon < \varepsilon_{n-1}$$

дробь p/q лежит между дробями p_{m+2}/q_{m+2} и p_m/q_m , где индекс $m = n + 2k - 1 \geq n - 1$. Значит, согласно 14.6, эта дробь лежит между $p_{m,1}/q_{m,1}$ и $p_{m,0}/q_{m,0}$, причем при $m = n - 1$ дробь $p/q \neq p_{m,0}/q_{m,0}$ ввиду неравенства

$$|\varphi - p/q| \leq \varepsilon < \varepsilon_{n-1}.$$

Применяя еще раз 14.6, получаем, что при $m \neq n - 1$

$$q \geq q_{m,0} = q_m \geq q_{n+1},$$

а при $m = n - 1$ в силу неравенства $p/q \neq p_{m,0}/q_{m,0}$ получаем, что

$$q \geq q_{m,1} = q_{m+2} = q_{n+1}.$$

Значит, во всех случаях равенство $L(\varphi, \varepsilon) = F_{n+2}$ доказано.

Применяя 14.22, выводим отсюда для произвольного $\varepsilon \in [\varepsilon_{n+1}, \varepsilon_n)$ неравенство

$$L_{B_1}(\varphi, \varepsilon) \geq n + 1,$$

а применяя 14.24, из неравенства

$$|\varphi - F_{n+1}/F_{n+2}| \leq \varepsilon$$

выводим неравенство $L_{B_1}(\varphi, \varepsilon) \leq n + 1$, и, значит, в результате равенство $L_{B_1}(\varphi, \varepsilon) = n + 1$. Так как согласно 14.5

$$\varepsilon_n = 1/\left(F_{n+1}^2 \varphi + F_{n+1} F_n\right),$$

то при $\varepsilon \in [\varepsilon_{n+1}, \varepsilon_n)$ число n является максимальным натуральным числом, удовлетворяющим неравенству

$$F_{n+1}^2 \varphi + F_{n+1} F_n \le \frac{1}{\varepsilon}.$$

В силу равенства

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}$$

предыдущее неравенство равносильно каждому из следующей цепочки неравенств

$$\frac{5}{\varepsilon} > \left(\varphi^{n+1} - (-\varphi)^{-n-1}\right)^2 \varphi + \left(-\varphi^{n+1} - (-\varphi)^{-n-1}\right)\left(\varphi^n - (-\varphi)^{-n}\right) \Leftrightarrow$$

$$\Leftrightarrow \frac{5}{\varepsilon} > \varphi^{2n+3} + 2(-1)^n \varphi + \varphi^{-2n-1} + \varphi^{2n+1} - \varphi^{-2n-1} - (-1)^n \varphi + (-1)^n / \varphi \Leftrightarrow$$

$$\Leftrightarrow \frac{5}{\varepsilon} > \varphi^{2n}\left(\varphi^3 + \varphi\right) + (-1)^n (\varphi + 1/\varphi) \Leftrightarrow \frac{5}{\varepsilon(\varphi + 1/\varphi)} > \varphi^{2n+2} + (-1)^n \Leftrightarrow$$

$$\Leftrightarrow \frac{\sqrt{5}}{\varepsilon} - (-1)^n > \varphi^{2n+2} \Leftrightarrow \log_\varphi \left(\frac{\sqrt{5}}{\varepsilon} - (-1)^n\right) > 2n + 2.$$

При четном n это неравенство равносильно неравенству

$$-\left[-\frac{log_\varphi\left(\sqrt{5}/\varepsilon - 1\right)}{4} + \frac{1}{2}\right] - 1 \ge n/2,$$

а при n нечетном — неравенству

$$-\left[-\frac{log_\varphi\left(\sqrt{5}/\varepsilon + 1\right)}{4}\right] - 1 \ge (n+1)/2.$$

Из полученных неравенств следует, что при $\varepsilon \in [\varepsilon_{n+1}, \varepsilon_n)$ максимальное значение n равно

$$\max\left\{-2\left[-\frac{log_\varphi\left(\sqrt{5}/\varepsilon - 1\right)}{4} + \frac{1}{2}\right] - 2, -2\left[-\frac{log_\varphi\left(\sqrt{5}/\varepsilon + 1\right)}{4}\right] - 3\right\}.$$

Отсюда следуют все равенства 14.7.

14.8. Так как при $\varepsilon \in [\varepsilon_{n+1}, \varepsilon_n)$

$$L(\varphi, \varepsilon) = F_{n+2}, F_{n+1}^2 \varphi + F_{n+1} F_n < 1/\varepsilon,$$

то

$$L(\varphi, \varepsilon) = F_{n+2} \sim \varphi F_{n+1}^2,$$

$$F_2^{n+1}(\varphi + 1/\varphi) < (1 + o(1)) F_2^{n+1} \varphi + F_{n+1} F_n < 1/\varepsilon,$$

откуда

$$L(\varphi, \varepsilon) \sim \varphi F_{n+1} < \frac{\varphi(1 + o(1))}{\sqrt{(\varphi + 1/\varphi)\varepsilon}} \sim \sqrt{\frac{\frac{1}{2} + \frac{3}{2\sqrt{5}}}{\varepsilon}},$$

а при $\varepsilon - \varepsilon_n \to 0$

$$L(\varphi, \varepsilon) \sim \sqrt{\frac{\frac{1}{2} + \frac{3}{2\sqrt{5}}}{\varepsilon}},$$

значит,

$$\limsup_{\varepsilon \to 0} L(\varphi, \varepsilon)\sqrt{\varepsilon} = \sqrt{\frac{1}{2} + \frac{3}{2\sqrt{5}}}.$$

Аналогично, при $\varepsilon \in [\varepsilon_{n+1}, \varepsilon_n)$

$$F_{n+2}^2(\varphi + 1/\varphi) \sim F_{n+2}^2\varphi + F_{n+2}F_{n+1} \geq 1/\varepsilon,$$

поэтому

$$L(\varphi, \varepsilon) = F_{n+2} > \frac{1 + o(1)}{\sqrt{\varepsilon(\varphi + 1/\varphi)}} \sim \frac{1}{\sqrt[4]{5}\sqrt{\varepsilon}},$$

а при $\varepsilon = \varepsilon_{n+1}$

$$L(\varphi, \varepsilon) \sim \frac{1}{\sqrt[4]{5}\sqrt{\varepsilon}},$$

откуда

$$\liminf_{\varepsilon \to 0} L(\varphi, \varepsilon)\sqrt{\varepsilon} = \sqrt[4]{\frac{1}{5}}.$$

14.9. Используя 14.5, проверяем, что при $r \geq r_n$

$$\frac{q_{n,r}}{q_{n+1}} = r + \psi_{n+1} \leq a_{n+2} + \frac{1}{\alpha_{n+3}} - r = \alpha_{n+2} - r,$$

откуда

$$\frac{\alpha_{n+2} - r}{q_{n,r}} \leq \frac{1}{q_{n+1}},$$

а так как, согласно 14.5 и 14.6,

$$\varepsilon_{n+1} = |\alpha - p_{n+1}/q_{n+1}| = \frac{1}{q_{n+1}(\alpha_{n+2}q_{n+1} + q_n)}$$

и

$$\varepsilon_{n,r} = |\alpha - p_{n,r}/q_{n,r}| = \frac{\alpha_{n+2} - r}{q_{n+1}(\alpha_{n+2}q_{n+1} + q_n)},$$

то при $r \geq r_n$ справедливо неравенство $\varepsilon_{n+1} \leq \varepsilon_{n,r}$. Поэтому для произвольного $\varepsilon \in [\varepsilon_{n+2}, \varepsilon_{n+1})$ либо найдется такое $r \geq r_n$, что

$$\varepsilon_{n,r+1} \leq \varepsilon < \varepsilon_{n,r},$$

либо

$$\varepsilon_{n,r_n} \leq \varepsilon < \varepsilon_{n+1} \leq \varepsilon_{n,r_n - 1}.$$

Рассмотрим первый случай. Тогда, так как

$$|\alpha - p_{n,r+1}/q_{n,r+1}| = \varepsilon_{n,r+1} \leq \varepsilon,$$

то согласно определению $L(\alpha, \varepsilon) \leq q_{n,r+1}$. Докажем, что

$$L(\alpha, \varepsilon) \geq q_{n,r+1}$$

и, значит, $L(\alpha, \varepsilon) = q_{n,r+1}$ при $\varepsilon_{n,r+1} < \varepsilon \leq \varepsilon_{n,r}$.

Пусть $|\alpha - p/q| \le \varepsilon$. Если дробь p/q лежит по ту же сторону от числа α, что и p/q, то p/q лежит между дробями p_{n+2}/q_{n+2} и p_{n+2}/q_{n+2}, причем $p/q \ne p_{n+1}/q_{n+1}$ в силу неравенств

$$|\alpha - p/q| \le \varepsilon < \varepsilon_{n+1} = |\alpha - p_{n+1}/q_{n+1}|.$$

Поэтому, согласно 14.5,

$$q \ge q_{n+2} = a_{n+2}q_{n+1} + q_n \ge (r+1)\,q_{n+1} + q_n = q_{n,r+1}.$$

Если же дроби p/q и p_{n+1}/q_{n+1} лежат по разные стороны от числа α, то в силу неравенства

$$|\alpha - p/q| \le \varepsilon \le \varepsilon_{n,r} \le \varepsilon_n$$

дробь p/q лежит между подходящими дробями p_{m+2}/q_{m+2} и p_m/q_m, где $m = n+2k, k \ge 0$. Значит, согласно 14.6, эта дробь лежит между промежуточными дробями $p_{m,s+1}/q_{m,s+1}$ и $p_{m,s+1}/q_{m,s+1}$, причем при $m = n$ непременно $s \ge r$, а в случае $s = r$ дробь p/q не равна дроби $p_{n,r}/q_{n,r}$ в силу неравенства

$$|\alpha - p/q| \le \varepsilon \le \varepsilon_{n,r}.$$

Применяя еще раз 14.6, получаем, что при $m \ne n$

$$q \ge q_{m,s} \ge q_m \ge q_{n+2} \ge q_{n,r+1},$$

а при $m = n$, $s \ge r$ имеем $q \ge q_{n,s} \ge q_{n,r+1}$, и в случае $m = n$, $s = r$

$$q \ge q_{n,r+1}$$

в силу неравенства $p/q \ne p_{n,r}/q_{n,r}$. Значит, во всех случаях при $\varepsilon_{n,r+1} \le \varepsilon < \varepsilon_{n,r}$ равенство $L(\alpha,\varepsilon) = q_{n,r+1}$ доказано.

Пусть теперь

$$\varepsilon_{n,r_n} \le \varepsilon < \varepsilon_{n+1} \le \varepsilon_{n,r_n-1}.$$

Так как при $r = r_n - 1$ справедливо неравенство

$$|\alpha - p_{n,r}/q_{n,r}| = \varepsilon_{n,r} \le \varepsilon,$$

то согласно определению $L(\alpha,\varepsilon) \le q_{n,r_n}$. Применяя при $r = r_n - 1$ только что доказанное при условии $\varepsilon_{n,r+1} \le \varepsilon < \varepsilon_{n,r}$ неравенство

$$L(\alpha,\varepsilon) \ge q_{n,r+1},$$

имеем

$$L(\alpha,\varepsilon) \ge q_{n,r_n},$$

а, значит, верно равенство $L(\alpha,\varepsilon) = q_{n,r_n}$ при условии

$$\varepsilon_{n,r_n} \le \varepsilon < \varepsilon_{n+1}.$$

Из доказанных равенств следует, что при $r \ge r_n$

$$\sup\{\varepsilon L^2(\alpha,\varepsilon) : \varepsilon_{n,r+1} \le \varepsilon < \varepsilon_{n,r}\} = \varepsilon_{n,r}q_{n,r+1}^2,$$

а также

$$\sup\{\varepsilon L^2(\alpha,\varepsilon) : \varepsilon_{n,r_n} \le \varepsilon < \varepsilon_n\} = \varepsilon_{n+1}q_{n,r_n}^2,$$

откуда имеем

$$\sup\{\varepsilon L^2(\alpha,\varepsilon):\varepsilon_{n+2}\le\varepsilon<\varepsilon_{n+1}\}=\max\left(q_{n,r_n}^2\varepsilon_{n+1},\max_{r\ge r_n}\left(q_{n,r+1}^2\varepsilon_{n,r}\right)\right).$$

Докажем теперь равенство

$$\max_{r\ge r_n}\left(q_{n,r+1}^2\varepsilon_{n,r}\right)=q_{n,r_n+1}^2\varepsilon_{n,r_n}.$$

Для этого заметим, что согласно задаче 14.6

$$\varepsilon_{n,r}q_{n,r+1}^2=\frac{q_{n,r+1}^2\left(\alpha_{n+2}-r\right)}{q_{n+1}\left(\alpha_{n+2}q_{n+1}+q_n\right)},$$

а последовательность $\{q_{n,r+1}/q_{n,r}\}=\{1+q_{n+1}/q_{n,r}\}$ убывает с ростом r и последовательность $\{q_{n,r+1}(\alpha_{n+2}-r)\}$ тоже убывает с ростом r при $r\ge r_n$, так как выражение

$$q_{n,r+1}\left(\alpha_{n+2}-r\right)=\left(\left(r+1\right)q_{n+1}+q_n\right)\left(\alpha_{n+2}-r\right)\}=$$

$$=q_{n+1}\left(r+1+\psi_n\right)\left(\alpha_{n+2}-r\right)$$

относительно r является квадратным трехчленом с полусуммой корней, а значит, и максимумом, в точке

$$\left(\alpha_{n+2}-1-\psi_n\right)/2=\left(a_{n+2}+1/\alpha_{n+3}-1-\psi_n\right)/2<a_{n+2}/2\le r_n.$$

Положим для краткости

$$s=\max\left(q_{n,r_n+1}^2\varepsilon_{n,r_n},\varepsilon_{n+1}q_{n,r_n}^2\right).$$

Из доказанных равенств

$$\max_{r\ge r_n}\left(q_{n,r+1}^2\varepsilon_{n,r}\right)=q_{n,r_n+1}^2\varepsilon_{n,r_n},$$

$$\sup\{\varepsilon L^2(\alpha,\varepsilon):\varepsilon_{n+2}\le\varepsilon<\varepsilon_{n+1}\}=\max\left(q_{n,r_n}^2\varepsilon_{n+1},\max_{r\ge r_n}\left(q_{n,r+1}^2\varepsilon_{n,r}\right)\right)$$

следует равенство

$$\sup\{\varepsilon L^2(\alpha,\varepsilon):\varepsilon_{n+2}\le\varepsilon<\varepsilon_{n+1}\}=s_n.$$

Пусть $\{\delta_n\}$ — такая последовательность, что $\delta_n\to 0$ и

$$\lim_{n\to\infty}\delta_nL^2(\alpha,\delta_n)=\limsup_{\varepsilon\to 0}\varepsilon L^2(\alpha,\varepsilon).$$

Определим последовательность $\{k_n\}$ так, чтобы

$$\delta_n\in[\varepsilon_{k_n+2},\varepsilon_{k_n+1}),$$

тогда

$$\lim_{n\to\infty}\delta_nL^2(\alpha,\delta_n)=\limsup_{\varepsilon\to 0}\varepsilon L^2(\alpha,\varepsilon)\le\limsup_{n\to\infty}s_{k_n}\le\limsup_{n\to\infty}s_n.$$

Выберем теперь последовательность $\{m_n\}$ так, чтобы

$$\lim_{n\to\infty}s_{m_n}=\limsup_{n\to\infty}s_n,$$

а последовательность $\{\delta'_n\}$, $\delta'_n \in [\varepsilon_{m_n+2}, \varepsilon_{m_n})$, так, чтобы

$$s_{m_n} - \delta'_n L^2(\alpha, \delta'_n) \to 0.$$

Тогда

$$\lim_{n\to\infty} \delta'_n L^2(\alpha, \delta'_n) \geq \limsup_{\varepsilon\to 0} \varepsilon L^2(\alpha, \varepsilon) = \limsup_{n\to\infty} s_{m_n} = \limsup_{n\to\infty} s_n.$$

Из полученных неравенств следует равенство

$$\lim_{n\to\infty} \delta'_n L^2(\alpha, \delta'_n) = \limsup_{n\to\infty} s_n.$$

14.10. Для доказательства заметим, что

$$q^2_{n,r_n+1}\varepsilon_{n,r_n} = \frac{((r_n+1)q_{n+1}+q_n)^2(\alpha_{n+2}-r_n)}{q_{n,r_n}(\alpha_{n+2}q_{n+1}+q_n)} =$$

$$= \frac{((r_n+1)q_{n+1}+q_n)^2(\alpha_{n+2}-r_n)}{(r_nq_{n+1}+q_n)(\alpha_{n+2}q_{n+1}+q_n)} =$$

$$= \frac{((r_n+1)q_{n+1}+q_n)^2(a_{n+2}+1/\alpha_{n+3}-r_n)}{(r_nq_{n+1}+q_n)((a_{n+2}+1/\alpha_{n+3})q_{n+1}+q_n)},$$

откуда, сокращая на q^2_{n+1}/α_{n+3} и заменяя q_n/q_{n+1} на ψ_{n+1}, получаем

$$q^2_{n,r_n+1}\varepsilon_{n,r_n} = F_{r_n}(\psi_{n+1}, \alpha_{n+3}, a_{n+2}) =$$

$$= \frac{(r_n+1+\psi_{n+1})^2((a_{n+2}-r_n)\alpha_{n+3}+1)}{(r_n+\psi_{n+1})((a_{n+2}+\psi_{n+1})\alpha_{n+3}+1)},$$

и, аналогично,

$$q^2_{n,r_n}\varepsilon_{n+1} = \frac{(r_nq_{n+1}+q_n)^2}{q_{n+1}(\alpha_{n+2}q_{n+1}+q_n)} =$$

$$= \frac{(r_n+\psi_{n+1})^2}{\alpha_{n+2}+\psi_{n+1}} = \frac{(r_n+\psi_{n+1})^2}{a_{n+2}+1/\alpha_{n+3}+\psi_{n+1}} =$$

$$= \frac{\alpha_{n+3}(r_n+\psi_{n+1})^2}{a_{n+2}\alpha_{n+3}+1+\psi_{n+1}\alpha_{n+3}} = G_{r_n}(\psi_{n+1}, \alpha_{n+3}, a_{n+2}).$$

Остается применить 14.9.

14.11. Для доказательства заметим, что при $\psi\alpha \geq 1$ и $a = 2r$ справедливо неравенство $G_r(\psi, \alpha, a) < F_r(\psi, \alpha, a)$. Действительно,

$$\frac{F_r(\psi, \alpha, a)}{G_r(\psi, \alpha, a)} = \frac{\frac{(r+1+\psi)^2((a-r)\alpha+1)}{(r+\psi)(1+\alpha(a+\psi))}}{\frac{(r+\psi)^2}{1+\alpha(a+\psi)}} =$$

$$= \frac{(r+1+\psi)^2(r\alpha+1)}{(r+\psi)^3\alpha} > \frac{(r+1+\psi)^2 r}{(r+\psi)^3} > 1,$$

так как

$$\frac{(r+1+\psi)^2}{(r+\psi)^2} > \frac{r+\psi}{r},$$

потому что

$$\frac{(r+1+\psi)^2}{(r+\psi)^2} > \frac{r+\psi}{r} > 1+\frac{2}{(r+\psi)} > 1+\frac{2}{r+1} \geq 1+\frac{1}{r} > 1+\frac{\psi}{r} = \frac{\psi+r}{r}.$$

14.12. Для доказательства заметим, что при $a = 2r-1$ неравенство

$$\frac{F_r(\psi,\alpha,a)}{G_r(\psi,\alpha,a)} = \frac{(r+1+\psi)^2((r-1)\alpha+1)}{(r+\psi)^3\alpha} > 1$$

равносильно неравенству

$$\frac{(r-1)\alpha+1}{\alpha} > \frac{(r+\psi)^3}{(r+\psi+1)^2},$$

а, значит, и неравенству

$$\frac{1}{\alpha} > \frac{(r+\psi)^3}{(r+\psi+1)^2} + 1 - r = \frac{1}{f_r(\psi)}.$$

Это неравенство выполнено при любом α, если $g_r(\psi) \leq 0$. Так как

$$(r+\psi)^3 - (r-1)(r+\psi+1)^2 =$$

$$= \psi(r+\psi)^2 + r\left((r+\psi)^2 - (r+\psi+1)^2\right) + (r+\psi+1)^2 =$$

$$= \psi(r+\psi)^2 - r(2r+2\psi+1) + (r+\psi+1)^2 =$$

$$= \psi(r+\psi)^2 - r(r+\psi) + (r+\psi+1)(\psi+1) =$$

$$= \psi(r+\psi)^2 - r(r+\psi) + r(\psi+1) + (\psi+1)^2 =$$

$$= (\psi-1)r^2 + (2\psi^2+1)r + \psi^3 + (\psi+1)^2$$

и у этого квадратного (относительно r) трехчлена дискриминант равен

$$(2\psi^2+1)^2 + 4(1-\psi)\left(\psi^3 + (\psi+1)^2\right) =$$

$$= (2\psi^2+1)^2 + 4(\psi^3 - \psi^4 + (\psi+1)(1-\psi^2)) =$$

$$= 4\psi^4 + 4\psi^2 + 1 + 4(\psi^3 - \psi^4 + \psi + 1 - \psi^2 - \psi^3) = 4\psi + 5,$$

а корни его имеют разные знаки (согласно теореме Виета), то при r неравенство $g_r(\psi) \leq 0$ равносильно неравенству

$$r \geq \frac{2\psi^2+1+\sqrt{4\psi+5}}{2(1-\psi)}.$$

Поэтому при

$$r < \frac{2\psi^2+1+\sqrt{4\psi+5}}{2(1-\psi)}$$

имеем $g_r(\psi) > 0$, значит, при этом условии неравенство

$$1/\alpha > 1/f_r(\psi)$$

равносильно неравенству $\alpha < f_r(\psi)$. Так как числитель дроби

$$\frac{2\psi^2 + 1 + \sqrt{4\psi + 5}}{2(1-\psi)}$$

возрастает, а знаменатель — убывает с ростом величины ψ, то сама дробь растет на интервале $(0,1)$.

Функция $f_r(\psi)$ убывает при $\psi > \psi_r$, ведь дробь

$$\frac{1}{f_r(\psi)} = \frac{(r+\psi)^3}{(r+\psi+1)^2} - (r-1)$$

возрастает, так как функция

$$\frac{(r+\psi+1)^2}{(r+\psi)^3} = \frac{1}{r+\psi} + \frac{2}{(r+\psi)^2} + \frac{1}{(r+\psi)^3}$$

убывает.

14.13. Для доказательства заметим, что при $a = 2r-2$ неравенство

$$\frac{F_r(\psi,\alpha,a)}{G_r(\psi,\alpha,a)} = \frac{(r+1+\psi)^2((r-2)\alpha+1)}{(r+\psi)^3\alpha} > 1$$

равносильно неравенству

$$\frac{(r-2)\alpha+1}{\alpha} > \frac{(r+\psi)^3}{(r+\psi+1)^2},$$

а, значит, и неравенству

$$\frac{1}{\alpha} > \frac{(r+\psi)^3}{(r+\psi+1)^2} - r + 2 = \frac{1}{h_{r-1}(\psi)}.$$

Так как

$$(r+\psi)^3 - (r-2)(r+\psi+1)^2 =$$

$$= (r+\psi)^3 - (r-1)(r+\psi+1)^2 + (r+\psi+1)^2 =$$

$$= (\psi-1)r^2 + (2\psi^2+1)r + \psi^3 + (\psi+1)^2 + (r+\psi+1)^2 =$$

$$= \psi\cdot r^2 + (2\psi^2+1)r + \psi^3 + (\psi+1)^2 + (\psi+1)(2r+\psi+1) > 0,$$

то предыдущее неравенство равносильно неравенству $\alpha < h_{r-1}(\psi)$.

Неравенство $h_{r-1}(\psi) < 1/\psi$ равносильно неравенству

$$(r+\psi)^3 > (r-2+\psi)(r+\psi+1)^2,$$

которое при $x = r+\psi$ принимает вид

$$x > (x-2)(x+1)^2 = x^3 - 3x - 2,$$

т.е. становится очевидным.

Убывание функции h_r доказывается так же, как и убывание f_r в предыдущей задаче.

14.14. Функция

$$\frac{1}{G_r(\psi,\alpha,a)}=\frac{1}{\frac{(r+\psi)^2\alpha}{1+\alpha(a+\psi)}}\frac{1+\alpha(a-r)}{\alpha(r+\psi)^2}+\frac{1}{r+\psi}$$

убывает с ростом ψ, так как убывает каждое слагаемое. Поэтому

$$\frac{1}{\frac{(r+1)^2\alpha}{1+\alpha(a+1)}}<\frac{1}{G_r(\psi,\alpha,a)}<\frac{1}{\frac{r^2\alpha}{1+\alpha a}},$$

значит,

$$\frac{(r+1)^2\alpha}{1+\alpha(a+1)}>G_r(\psi,\alpha,a)>\frac{r^2\alpha}{1+\alpha a}.$$

Так как функции

$$\frac{(r+1)^2\alpha}{1+\alpha(a+1)},G_r(\psi,\alpha,a),\frac{r^2\alpha}{1+\alpha a}$$

дробно-линейны относительно α, при $\alpha=0$ равны нулю, а при $\alpha>0$ положительны, то при росте α они возрастают, следовательно

$$\frac{(r+1)^2}{2r-1}\geq\frac{(r+1)^2}{a+1}>\frac{(r+1)^2\alpha}{1+\alpha(a+1)}>$$

$$>G_r(\psi,\alpha,a)>\frac{r^2\alpha}{1+\alpha a}>\frac{r^2}{1+a}\geq\frac{r^2}{2r+1}.$$

Из свойств монотонности вытекает также, что

$$G_r(\psi,\alpha,a)<\frac{(r+\psi)^2\alpha}{a+\psi}<\frac{(r+1)^2}{1+a}.$$

14.15. Первое утверждение следует из того, что функция $F_r(\psi,\alpha,a)$ с точностью до не зависящего от α множителя совпадает с дробно-линейной относительно α функцией

$$\frac{(a-r)\alpha+1}{1+\alpha(a+\psi)},$$

которая при $\alpha=0$ равна 1, а при $\alpha\to\infty$ стремится к числу

$$\frac{a-r}{a+\psi}<1,$$

и поэтому убывает с ростом α. Для доказательства остальных утверждений исследуем знак производной функции

$$\frac{u}{v}=\frac{(r+1+\psi)^2}{(r+\psi)(1+\alpha(a+\psi))}$$

по переменной ψ (эта функция совпадает с $F_r(\psi,\alpha,a)$ с точностью до положительного не зависящего от ψ множителя). Знак производной совпадает со знаком выражения $u'v-v'u$, который совпадает со знаком выражения

$$2(r+\psi)(1+\alpha(a+\psi))-(r+\psi+1)(1+\alpha(a+\psi)+\alpha(r+\psi))=$$

$$=(r+\psi)(1+\alpha(a+\psi))-(1+\alpha(a+\psi))-\alpha(r+\psi)-\alpha(r+\psi)^2=$$

$$= (r+\psi)(1+\alpha(a-r)) - (1+\alpha(a+\psi)) - \alpha(r+\psi) =$$
$$= \psi(1+\alpha(a-r-2)) - (1+\alpha(a+r)) + r(1+\alpha(a-r)) =$$
$$= \psi(1+\alpha(a-r-2)) - 1 + r + \alpha(r(a-r-1)-a).$$

Так как при $a \leq 4$ справедливо неравенство $a \geq r \geq a-2$, то

$$a-r-2 \leq 0, a-r(a-r-1) \geq r,$$

откуда

$$\psi(1+\alpha(a-r-2)) - 1 + r + \alpha(r(a-r-1)-a) \leq \psi - 1 + r(1-\alpha) < 0,$$

значит, функция $F_r(\psi,\alpha,a)$ убывает с ростом переменной ψ при указанных ограничениях на a и r. При $r = a-2$ (а это возможно лишь при $a = 5,6$) имеем

$$\psi(1+\alpha(a-r-2)) - 1 + r + \alpha(r(a-r-1)-a) = \psi - 3 + a - 2\alpha,$$

откуда следует, что функция $F_r(\psi,\alpha,a)$ убывает при $\psi < 2\alpha + 3 - a$, имеет минимум при $\psi = 2\alpha + 3 - a$ и возрастает при $\psi > 2\alpha + 3 - a$. Учитывая, что следует рассматривать нашу функцию лишь при $0 < \psi < 1$, а если $a = 6, r = 4$, то даже при $0 < \psi < 1/\alpha$, отсюда получаем соответствующее утверждение леммы.

В остальных случаях (т.е. при $a = 6, r = 3$ и при $a \geq 7, a = 2r, 2r-1$, и $2r-2$) имеем $a-r-2 > 0, r(a-r-1)-a > 0$, значит,

$$\psi(1+\alpha(a-r-2)) - 1 + r + \alpha(r(a-r-1)-a) > 0,$$

и функция $F_r(\psi,\alpha,a)$ возрастает при $0 < \psi < 1$.

14.16. Нижняя оценка следует из 14.13. Оттуда же следует, что

$$G_r(\psi,\alpha,a) < \frac{(r+1)^2}{2r-1} < \frac{(r+2)^2}{r+1}.$$

Из задачи 14.15 выводим, что

$$F_r(\psi,\alpha,a) < F_r(\psi,0,a) = \frac{(r+1+\psi)}{r+\psi} < \frac{(r+2)^2}{r+1},$$

так как функция $F_r(\psi,0,a)$ возрастает с ростом ψ, ибо согласно доказательству 14.15 производная этой функции по переменной ψ равна

$$\psi(1+\alpha(a-r-2)) - 1 + r + \alpha(r(a-r-1)-a) = \psi - 1 + r \geq 0.$$

14.18. Из 14.5 легко следует, что любая точка из $K_a \backslash Q$ является предельной точкой множества $K_a \cap Q$. Докажем индукцией по длине дроби $\alpha \in K_a \cap Q$, что при $\alpha > 1$ справедливо неравенство

$$1 + m(a) < \alpha < M(a),$$

а при $0 < \alpha < 1$ — неравенство

$$m(a) < \alpha < M(a) - a = \frac{1}{1+m(a)}.$$

База индукции ($\alpha = 0, 1, \ldots, a$) очевидна.

Выполним шаг индукции. Пусть

$$\alpha = a' + 1/\alpha', 0 \le a' \le a, \alpha' \in K_a \cap Q.$$

Из предположения индукции следует, что $m(a) < \alpha' < M(a)$. Отсюда при $a' = 0$ имеем $\alpha = 1/\alpha'$ и поэтому из неравенства $\alpha' \ge 1$ следует, что $\alpha \le 1$ и при $\alpha \ne 1$ справедливы неравенства

$$m(a) = \frac{1}{M(a)} < 1/\alpha' = \alpha = 1/\alpha' < \frac{1}{(1 + m(a))} = M(a) - a,$$

а при $a' > 0$ имеем $\alpha > 1$ и, значит, справедливы неравенства

$$1 + m(a) \le a' + m(a) < a' + \frac{1}{\alpha'} = \alpha = a' + \frac{1}{\alpha'} < a' + \frac{1}{1 + m(a)} \le M(a).$$

Шаг индукции сделан и неравенства доказаны. Из них предельным переходом получаем, что аналогичные, но нестрогие неравенства, справедливы и для любого числа $\alpha \in K_a$. Для доказательства изолированности в K_a рациональных точек достаточно проверить, что для любых неравных чисел α и p/q из K_a справедливо неравенство

$$|\alpha - p/q| > \frac{1}{(a+1)aq^2}.$$

Действительно, пусть цепные дроби для чисел α и p/q различаются впервые в n-м элементе. Тогда, согласно 14.5, имеем

$$\frac{p}{q} = [a_0, a_1, \ldots, a_{n-1}, r_n] = \frac{r_n p_{n-1} + p_{n-2}}{r_n p_{n-1} + p_{n-2}}, r_n \in K_a \cap Q,$$

$$\alpha = [a_0, a_1, \ldots, a_{n-1}, \alpha_n] = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n p_{n-1} + p_{n-2}}, \alpha_n \in K_a \cap Q,$$

и целые части дробей r_n и α_n не совпадают. Если разность между целыми частями равна 1, то согласно доказанным выше неравенствам

$$|r_n - \alpha_n| \ge m(a) + 1 - M(a) + a =$$

$$= \frac{\sqrt{1 + \frac{4}{a}} - 1}{2} + 1 + a - \frac{a + \sqrt{a^2 + 4a}}{2} =$$

$$= \frac{1 + \sqrt{1 + \frac{4}{a}}}{2} - \frac{\sqrt{a^2 + 4a} - a}{2} = \frac{1 + \sqrt{1 + \frac{4}{a}}}{2} - a \cdot \frac{\sqrt{1 + \frac{4}{a}} - 1}{2} =$$

$$= 1 - (a-1) \cdot \frac{\sqrt{1 + \frac{4}{a}} - 1}{2} > 1 - (a-1) \cdot \frac{1 + \frac{2}{a} - 1}{2} = \frac{1}{a},$$

а если разность между целыми частями больше 1, то последнее неравенство тем более верно. Из полученного неравенства и следует, что

$$|\alpha - p/q| = \frac{|\alpha_n - r_n|}{q(\alpha_n q_{n-1} + q_{n-2})} > \frac{1/a}{q((1+a)q_{n-1} + q_{n-2})} > \frac{1}{(a+1)aq^2}.$$

14.19. Согласно задаче 14.10

$$\max\{F_r(\psi, \alpha, 2r-1), G_r(\psi, \alpha, 2r-1)\} = F_r(\psi, \alpha, 2r-1)$$

тогда и только тогда, когда или $g_r(\psi) \le 0$ или $g_r(\psi) > 0$ и $\alpha \le f_r(\psi)$, причем при $\alpha = f_r(\psi)$ справедливо равенство

$$F_r(\psi, \alpha, 2r-1) = G_r(\psi, \alpha, 2r-1).$$

Если $r \ge 3$, то согласно 14.13 и 13.15 при α и ψ, удовлетворяющих неравенствам

$$m(a) \le \psi, \alpha \le M(a),$$

$$F_r(m(a), M(a), 2r-1) \le F_r(\psi, a, 2r-1),$$

поэтому

$$b(a, 2r-1) \ge F_r(m(a), M(a), 2r-1).$$

Из утверждения 14.10 следует, что последнее неравенство обращается в равенство, если при $\psi = m(a)$

$$r \ge \frac{2\psi + 1 + \sqrt{4\psi+5}}{2(1-\psi)},$$

причем указанная дробь возрасстает на интервале $(0,1)$. Но

$$m(a) \le m(2) = (\sqrt{3}-1)/2 \le 0,4,$$

$r \ge 4$, поэтому неравенство для r будет выполнено, ведь

$$4 \ge \frac{1,32 + \sqrt{6,6}}{1,2}.$$

Если $r = 2$ или 3, то согласно 14.15 при α и ψ, удовлетворяющих неравенствам $m(a) \le \psi, \alpha \le M(a)$, имеем, что

$$F_r(\psi, M(a), 2r-1) \le F_r(\psi, a, 2r-1),$$

а так как

$$M(a) = \frac{a + \sqrt{a^2+4a}}{2} \ge \frac{2+\sqrt{12}}{2} \ge 3/2,$$

то $F_r(\psi, M(a), 2r-1)$ убывает с ростом ψ. Согласно утверждению 14.10 неравенство $g_r(\psi) \ge 0$ равносильно неравенству $\psi_r \ge \psi$, и функция $f_r(\psi)$ убывает при $\psi_r \ge \psi$. Следовательно, при $m(a) \le \psi \le \psi_{r-2}(a)$, где $f_r(\psi_{r-2}(a)) = M(a)$, и $\alpha \le M(a)$, согласно 14.10, 14.15 справедливо неравенство

$$\max\{F_r(\psi, a, 2r-1), G_r(\psi, a, 2r-1)\} = F_r(\psi, a, 2r-1) \ge$$

$$\ge F_r(\psi, M(a), 2r-1) \ge F_r(\psi_{r-2}(a), M(a), 2r-1).$$

Если же $1 \ge \psi \ge \psi_{r-2}(a)$ и $1 \le \alpha \le M(a)$, то согласно задачам 14.10, 14.13, 14.15 при $\alpha \ge f_r(\psi)$ имеем

$$\max\{F_r(\psi, a, 2r-1), G_r(\psi, a, 2r-1)\} = G_r(\psi, a, 2r-1) \ge$$

$$\ge G_r(\psi, f_r(\psi), 2r-1) = F_r(\psi, f_r(\psi), 2r-1),$$

и в противном случае

$$\max\{F_r(\psi, a, 2r-1), G_r(\psi, a, 2r-1)\} = F_r(\psi, a, 2r-1) \ge F_r(\psi, f_r(\psi), 2r-1).$$

Заметим, что функция

$$F_r(\psi, f_r(\psi), 2r-1) = G_r(\psi, f_r(\psi), 2r-1) = \frac{(r+\psi)^2 f_r(\psi)}{1 + f_r(\psi)(2r-1+\psi)} =$$

$$= \frac{(r+\psi)^2(r+\psi+1)^2}{g_r(\psi) + (r+1+\psi)^2(2r-1+\psi)} = \frac{(r+\psi)(r+\psi+1)^2}{(r+\psi)^2 + (r+1+\psi)^2}$$

возрастает, потому что функция

$$\frac{1}{G_r(\psi, f_r(\psi), 2r-1)} = \frac{r+\psi}{(r+1+\psi)^2} + \frac{1}{r+\psi}$$

убывает, ведь функция

$$\frac{1}{x + 2 + 1/x}$$

при $x = r + \psi$ убывает на интервале $(0, 1)$. Поэтому при $1 \geq \psi \geq \psi_{r-2}(a)$ и $1 \leq \alpha \leq M(a)$

$$\max\{F_r(\psi, a, 2r-1), G_r(\psi, a, 2r-1)\} \geq = F_r(\psi, a, 2r-1) \geq$$

$$\geq F_r(\psi, f_r(\psi), 2r-1) \geq F_r(\psi_{r-2}(a), M(a), 2r-1).$$

В итоге во всех случаях

$$\max\{F_r(\psi, a, 2r-1), G_r(\psi, a, 2r-1)\} \geq F_r(\psi_{r-2}(a), M(a), 2r-1),$$

откуда при $r = 2$ или 3

$$b(a, 2r-1) = F_r(\psi_{r-2}(a), M(a), 2r-1).$$

14.20. Согласно задаче 14.10

$$\max\{F_r(\psi, \alpha, 2r-1), G_r(\psi, \alpha, 2r-1)\} = F_r(\psi, \alpha, 2r-1)$$

тогда и только тогда, когда или $g_r(\psi) \leq 0$ или $g_r(\psi) \geq 0$ и $\alpha \leq f_r(\psi)$, причем при $\alpha = f_r(\psi)$

$$F_r(\psi, \alpha, 2r-1) = G_r(\psi, \alpha, 2r-1).$$

Если $r \geq 3$, то согласно утверждениям 14.13 и 14.15 при α и ψ, удовлетворяющих неравенствам $m(a) \leq \psi \leq 1/(1+m(a))$, $1 + m(a) \leq \alpha \leq M(a)$, справедливы неравенства

$$F_r\left(\frac{1}{1+m(a)}, 1+m(a), 2r-1\right) \geq F_r(\psi, \alpha, 2r-1),$$

$$G_r\left(\frac{1}{1+m(a)}, M(a), 2r-1\right) \geq G_r(\psi, \alpha, 2r-1),$$

причем последнее неравенство верно при любом r, поэтому

$$B(a, 2r-1) = \max\left\{F_r\left(\frac{1}{1+m(a)}, 1+m(a), 2r-1\right), G_r\left(\frac{1}{1+m(a)}, M(a), 2r-1\right)\right\}.$$

Если $r = 3$, то согласно задаче 14.15 при тех же α и ψ имеем

$$\max\left\{F_r(m(a), 1+m(a), 2r-1), F_r\left(\frac{1}{1+m(a)}, m(a), 2r-1\right)\right\} \geq$$

$$\geq F_r(\psi, \alpha, 2r-1),$$

так как максимум функции $F_3(\psi, 1+m(a), 5)$ достигается на концах отрезка $[m(a), 1/(1+m(a))]$, а минимум - в точке $\psi = 2m(a) \leq 1/(m(a)+1)$, ведь

$$m(a) = \frac{-1+\sqrt{1+4/a}}{2} \leq \frac{-1+\sqrt{3}}{2},\ 2m(a) = \frac{1}{\sqrt{3}+1} \leq \frac{1}{1+m(a)},$$

поэтому

$$B(a,5) = \max\left\{F_3\left(\frac{1}{m(a)+1}, 1+m(a), 5\right),\right.$$

$$\left.F_3\left(m(a), 1+m(a), 5\right), G_3\left(\frac{1}{m(a)+1}, M(a), 5\right)\right\}.$$

Если $r=2$, то согласно задаче 14.15 при тех же α и ψ

$$F(m(a), 1+m(a), 2r-1) \geq F(\psi, \alpha, 2r-1),$$

так как функция $F_r(\psi, 1+m(a), 2r-1)$ убывает на отрезке $\left[m(a), \frac{1}{m+1}\right]$, поэтом

$$B(a,3) = \max\{F_2(m(a), 1+m(a), 3), G_2(1/(m(a)+1)), M(a), 3)\}.$$

Покажем, что при $r \geq 3$

$$F_r(1/(m(a)+1)), 1+m(a), 2r-1) \geq G_r(1/(m(a)+1)), M(a), 2r-1),$$

откуда немедленно следует (с учетом доказанного выше равенства) первое равенств леммы при $r > 3$. Сначала заметим, что

$$m + \frac{1}{m+1} = \frac{m^2+m+1}{m+1} > 1,$$

и поэтому (здесь и далее опускаем в $m(a)$ и $M(a)$ для краткости скобки)

$$G_r\left(\frac{1}{1+m}, M, 2r-1\right) = \frac{(r+\frac{1}{1+m})^2 M}{(r+\frac{1}{1+m})^2} < \frac{(r\frac{1}{1+m})^2}{m+2r-1+\frac{1}{1+m}} <$$

$$< \frac{(r+\frac{1}{m+1})^2}{2r}$$

при любых $r \geq 1$ и $a \geq 1$. Так как при $x \geq 4$

$$x^3 - 4x^2 + 2 > 0,$$

ведь при $x=4$ это неравенство верно, а производная положительна, то

$$2x^4 - x^3 < 2(x^2-1)^2 = 2(x+1)^2(x-1)^2 < 2(x+1)^2(x-\frac{1}{m+1})^2,$$

значит,

$$\frac{x^2}{2(x-\frac{1}{m+1})} < \frac{(x+1)^2(x-1)}{x(2x-1)},$$

откуда при $x = r + 1/(m+1), r > 3$, следует, что

$$G_r\left(\frac{1}{1+m}, M, 2r-1\right) < \frac{\left(r+\frac{1}{m+1}\right)^2}{2r} <$$

$$< \frac{\left(r+1+\frac{1}{m+1}\right)^2\left(r-1+\frac{1}{m+1}\right)}{\left(r+\frac{1}{m+1}\right)\left(2r-1+\frac{2}{m+1}\right)} =$$

$$= \frac{\left(r+1+\frac{1}{m+1}\right)^2((r-1)(m+1)+1)}{\left(r+\frac{1}{m+1}\right)\left(1+(m+1)\left(2r-1+\frac{1}{m+1}\right)\right)} =$$

$$= F_r\left(\frac{1}{m+1}, 1+m, 2r-1\right).$$

При $r = 3$ последнее неравенство тоже верно, потому что при $x = 3+1/(m+1)$

$$\frac{x^2}{2\left(x-\frac{1}{m+1}\right)} = \frac{x^2}{6} < \frac{(x+1)^2(x-1)}{x(2x-1)}.$$

Действительно, при $3 < x < 4$ имеем $2x^4 - 8x^3 < 0$, значит,

$$2x^4 - 7x^3 - 6x^2 + 6x + 6 < x^3 - 6x^2 + 6x + 6 < 0,$$

ведь при $x = 3$ или $x = 4$ это неравенство верно, а при $x = 0$ — нет, поэтому рассматриваемый кубический многочлен имеет корни на интервалах $(0,3)$ и $(4,+\infty)$, следовательно, этот многочлен отрицателен на всем отрезке $[3,4]$, иначе он имел бы еще два корня на этом отрезке.

Для того чтобы доказать первое неравенство леммы при $r = 3$, осталось установить неравенство

$$F_3(1/(m+1), 1+m, 5) > F_3(m, 1+m, 5).$$

Оно равносильно неравенству

$$\frac{\left(4+\frac{1}{m+1}\right)^2(2(m+1)+1)}{\left(3+\frac{1}{m+1}\right)\left(1+(m+1)\left(5+\frac{1}{m+1}\right)\right)} = \frac{(4m+5)^2(2m+3)}{(3m+4)(5m+7)} >$$

$$> \frac{(4+m)^2(2(1+m)+1)}{(3+m)(1+(m+1)(5+m))},$$

которое равносильно неравенству

$$16m^5 + 184m^4 + 769m^3 + 1473m^2 + 1320m + 450 >$$

$$> 15m^5 + 176m^4 + 757m^3 + 1476m^2 + 1328m + 448,$$

очевидно следующему из неравенства $2 > 3m^2 + 8m$. Последнее же очевидно, так как $m = m(5) > 1/5$.

Для того чтобы доказать второе неравенство леммы, достаточно установить неравенство

$$G_2(1/(m+1), M, 3) < F_2(m, 1+m, 3).$$

Так как согласно доказанному выше неравенству

$$G_2\left(\frac{1}{m+1}, M, 3\right) < \frac{\left(2+\frac{1}{m+1}\right)^2}{4} = \left(1+\frac{1}{2m+2}\right)^2,$$

а

$$\left(1+\frac{1}{2m+2}\right)^2 < \left(1+\frac{1}{m+2}\right)^2 = \frac{(m+3)^2}{(m+2)^2} = F_2(m, 1+m, 3),$$

то это неравенство, а вместе с ним и лемма доказаны.

14.21. Согласно определению $B(a, 2r)$, и задачам 14.10 – 14.12 справедливо соотношение $B(a, 2r) = \max\{B_1, B_2, B_3\}$, где

$$B_1 = \max\left\{F_r(\psi, \alpha, 2r) : \alpha\psi \geq 1, m \leq \psi \leq \frac{1}{m+1}, 1+m \leq \alpha \leq M\right\},$$

$$B_2 = \max\left\{F_{r+1}(\psi, \alpha, 2r) : \alpha \leq h_r(\psi), m \leq \psi \leq \frac{1}{m+1}, 1+m \leq \alpha \leq M\right\},$$

$$B_3 = \max\left\{G_{r+1}(\psi, \alpha, 2r) : h_r(\psi) \leq \alpha\frac{1}{\psi},\right.$$

$$\left. m \leq \psi \leq \frac{1}{m+1}, 1+m \leq \alpha \leq M\right\}.$$

Из утверждения 14.15 следует равенство (учитываем, что $Mm = 1$)

$$B_1 = \max\left\{F\left(\psi, \frac{1}{\psi}, 2r\right) : m \leq \psi \leq \frac{1}{m+1}\right\},$$

а при $r \geq 3$ — равенство

$$B_2 = F_{r+1}(\psi_{m,r}, m+1, 2r),$$

где $h_r(\psi_{m,r}) = m+1$. Для доказательства последнего из них пользуемся монотонным убыванием функции $h_r(\psi)$, монотонным убыванием по α и монотонным возрастанием по ψ функции $F_{r+1}(\psi, a, 2r)$ (согласно 14.12, 14.15, учитывая, что $2(1+m) - 3 \leq 0$), а существование $\psi_{m,r}$ следует из неравенства $h_r(1/(m+1)) \leq m+1$ и

$$h_r(0) = \frac{(r+2)^2}{(r+1)^3 - (r-1)(r+2)^2} = \frac{(r+2)^2}{3r+5} \geq 25/14 \geq 1+m.$$

Из задачи 14.13 при любом r следует равенство (учитываем, что $Mm = 1$)

$$B_3 = \max\left\{G_{r+1}(\psi, 1/\psi, 2r) : m \leq \psi \leq \frac{1}{m+1}\right\}.$$

Так как функция

$$G_{r+1}(\psi, 1/\psi, 2r) = F_r(\psi, 1/\psi, 2r) = \frac{(r+1+\psi)(r/\psi+1)^2}{(r+\psi)(2+2r/\psi))} =$$

$$= \frac{(r+1+\psi)^2}{2(r+\psi)} = \frac{1}{2}\left((r+\psi) + \frac{1}{(r+\psi)}\right) + 1$$

монотонно возрастает, то

$$B_1 = B_3 = G_{r+1}\left(\frac{1}{m+1}, m+1, 2r\right).$$

Из равенства

$$B_2 = F_{r+1}\left(\psi_{m,r}, m+1, 2r\right)$$

вытекает неравенство $B_2 \leq B_1$, если учесть, что

$$F_{r+1}\left(\psi_{m,r}, m+1, 2r\right) = F_{r+1}\left(\psi_{m,r}, h_r\left(\psi_{m,r}\right), 2r\right) =$$

$$= G_{r+1}\left(\psi_{m,r}, h_r\left(\psi_{m,r}\right), 2r\right) =$$

$$= G_{r+1}\left(\psi_{m,r}, \frac{1}{\psi_{m,r}}, 2r\right) \leq G_{r+1}\left(\frac{1}{m+1}, m+1, 2r\right).$$

Значит, при $r \geq 3$

$$B\left(a, 2r\right) = \max\left\{B_1, B_2, B_3\right\} = B_1 = G_{r+1}\left(\frac{1}{m+1}, m+1, 2r\right).$$

Пусть теперь $r \leq 2$. Тогда из монотонного убывания по α и ψ функции $F_{r+1}\left(\psi, a, 2r\right)$ (согласно 14.15) следует равенство

$$B_2 = F_{r+1}\left(m, m+1, 2r\right).$$

Для окончания доказательства осталось проверить, что при $r \leq 2$

$$F_{r+1}\left(m, m+1, 2r\right) \leq G_{r+1}\left(\frac{1}{m+1}, m+1, 2r\right).$$

Так как уже проверено, что

$$G_{r+1}\left(\frac{1}{m+1}, m+1, 2r\right) = \frac{\left(r+1+\frac{1}{m+1}\right)^2}{2\left(r+1+\frac{1}{m+1}\right)}$$

и

$$F_{r+1}\left(m, m+1, 2r\right) = \frac{\left(r+2+m\right)^2\left(\left(r-1\right)\left(m+1\right)+1\right)}{\left(r+1+m\right)\left(1+\left(m+1\right)\left(2r+m\right)\right)},$$

то достаточно установить неравенство

$$\frac{\left(r+2+m\right)^2\left(\left(r-1\right)\left(m+1\right)+1\right)}{\left(r+1+m\right)\left(m+1\right)\left(2r+m\right)} \leq \frac{\left(\left(m+1\right)\left(r+1\right)+1\right)^2}{2\left(r\left(m+1\right)+1\right)\left(m+1\right)},$$

которое при $r = 1$ равносильно неравенству

$$\frac{\left(2m+3\right)^2}{2} \geq \frac{\left(3+m\right)^2}{\left(m+2\right)},$$

очевидно, верному, так как

$$\frac{1}{\left(m+2\right)} \leq \frac{1}{2},$$

и, значит,

$$2m^2+6m+9/2 \geq m+9/2 \geq m+4+\frac{1}{(m+2)}=\frac{(3+m)^2}{(m+2)},$$

а при $r=2$ равносильно неравенству

$$\frac{(4+m)(m+2)}{(3+m)} \leq \frac{(3m+4)^2}{2(2m+3)},$$

которое верно, так как у многочлена

$$(3m+4)(m+3)$$

все коэффициенты не меньше соответствующих коэффициентов многочлена

$$(4+m)(m+2)(4m+6).$$

14.22. Согласно определению $b(a,2r)$ и 14.10, 14.12 справедливо соотношение $b(a,2r)=\min\{b_1,b_2,b_3\}$, где

$$b_1=\min\left\{F_r(\psi,a,2r): a\psi\geq 1, m\leq\psi\leq\frac{1}{m+1}, 1+m\leq\alpha\leq M\right\},$$

$$b_2=\min\left\{F_{r+1}(\psi,a,2r): \alpha\leq h_r(\psi), m\leq\psi\leq\frac{1}{m+1}, 1+m\leq\alpha\leq M\right\},$$

$$b_3=\min\left\{G_{r+1}(\psi,a,2r): h_r(\psi)\leq\alpha\leq\frac{1}{\psi},\right.$$

$$\left. m\leq\psi\leq\frac{1}{m+1}, 1+m\leq\alpha\leq M\right\}.$$

Из задачи 14.15 при $r\geq 3$ следует равенство $b_1=F_r(m,M,2r)$ (учитываем, что $Mm=1$), а при $r\leq 2$ — равенство

$$b_1=F_r\left(\frac{1}{m+1},M,2r\right),$$

и при любом r — равенство

$$b_2=\min\{F_{r+1}(\psi,h_r(\psi),2r): m\leq\psi\leq\psi_{m,r}\},$$

где $\psi_{m,r}$ такая же, как в предыдущей лемме (в случае $\psi_{m,r}\leq m$ формально положим $b_2=+\infty$). Из 14.13 следует равенство

$$b_3=\min\left\{G_{r+1}(\psi,\max(h_r(\psi),m+1),2r): m\leq\psi\leq\frac{1}{m+1}\right\}.$$

Так как

$$F_{r+1}(\psi,h_r(\psi),2r)=G_{r+1}(\psi,h_r(\psi),2r)=\frac{(r+1+\psi)^2 h_r(\psi)}{1+h_r(\psi)(2r+\psi)}=$$

$$=\frac{(r+1+\psi)^2(r+2+\psi)^2}{(r+1+\psi)^3+(r+2+\psi)^2(r+1+\psi)}=\frac{(r+1+\psi)^2(r+2+\psi)}{(r+1+\psi)^2+(r+2+\psi)^2}=$$

$$= G_{r+1}\left(\psi, f_{r+1}(\psi), 2r+1\right),$$

то, согласно доказанной в 14.19 монотонности $G_r(\psi, f_r(\psi), 2r-1)$, функция

$$F_{r+1}\left(\psi, h_r(\psi), 2r\right) = G_{r+1}\left(\psi, h_r(\psi), 2r\right)$$

тоже монотонно возрастающая, поэтому согласно 14.13 при $\psi_{m,r} \geq m$

$$b_2 = F_{r+1}\left(m, h_r(m), 2r\right) = G_{r+1}\left(m, h_r(m), 2r\right) = b_3,$$

так как

$$\min\left\{G_{r+1}\left(\psi, \max\left\{h_r(\psi), m+1\right\}, 2r\right) : m \leq \psi \leq \frac{1}{m+1}\right\} =$$

$$\min\left\{\min\left\{G_{r+1}\left(\psi, h_r(\psi), 2r\right) : m \leq \psi \leq \psi_{m,r}\right\},\right.$$

$$\left.\min\left\{G_{r+1}\left(\psi, m+1, 2r\right) : \psi \leq \psi_{m,r}\right\}\right\}$$

$$= \min\left\{G_{r+1}\left(m, h_r(m), 2r\right), G_{r+1}\left(\psi_{m,r}, m+1, 2r\right)\right\} =$$

$$= \min\left\{G_{r+1}\left(m, h_r(m), 2r\right), G_{r+1}\left(\psi_{m,r}, h_r\left(\psi_{m,r}\right), 2r\right)\right\} =$$

$$= G_{r+1}\left(m, h_r(m), 2r\right) = \max\left\{G_{r+1}\left(m, h_r(m), 2r\right), G_{r+1}\left(m, m+1, 2r\right)\right\},$$

а при $\psi_{m,r} \leq m$

$$b_3 = G_{r+1}\left(m, \max\left(h_r(m), m+1\right), 2r\right) = G_{r+1}\left(m, m+1, 2r\right) =$$

$$= \max\left\{G_{r+1}\left(m, h_r(m), 2r\right), G_{r+1}\left(m, m+1, 2r\right)\right\}.$$

Согласно 14.13, неравенству $h_r(m) \leq 1/m$ из задачи 14.12, равенству $1/m = M$ и установленному в доказательстве предыдущей задачи равенству

$$G_{r+1}\left(\psi, 1/\psi, 2r\right) = F_r\left(\psi, 1/psi, 2r\right)$$

имеем, что при $r \geq 3$

$$b_1 = F_r\left(m, M, 2r\right) = F_r\left(m, 1/m, 2r\right) = G_{r+1}\left(m, 1/m, 2r\right) =$$

$$= G_{r+1}\left(m, M, 2r\right) \geq G_{r+1}\left(m, \max\left(h_r(m), m+1\right), 2r\right) = b_3.$$

Из полученных соотношений следует, что при $r \geq 3$

$$b\left(a, 2r\right) = \min\left\{b_1, b_2, b_3\right\} = \min\left\{F_r\left(m, M, 2r\right), b_3\right\} = b_3,$$

а при $r \leq 2$

$$b\left(a, 2r\right) = \min\left\{b_1, b_2, b_3\right\} = \min\left\{F_r\left(\frac{1}{m+1}, M, 2r\right), b_3\right\}.$$

Тем самым при $r \geq 3$ первое равенство задачи доказано. Для его доказательства при $r \leq 2$ достаточно проверить, что

$$F_r\left(\frac{1}{m+1}, M, 2r\right) \geq b_3.$$

Проверим, что

$$F_r\left(\frac{1}{m+1}, M, 2r\right) \geq G_{r+1}\left(m, m+1, 2r\right).$$

Так как

$$F_r\left(\frac{1}{m+1}, M, 2r\right) = \frac{\left(r+1+\frac{1}{m+1}\right)^2 (rM+1)^2}{\left(r+\frac{1}{m+1}\right)\left(1+M\left(2r+\frac{1}{m+1}\right)\right)} =$$

$$= \frac{((r+1)(m+1)+1)(r+m)}{(r(m+1)+1)((m+1)(m+2r)+1)} =$$

$$= G_{r+1}(m, m+1, 2r) = \frac{(r+m+1)_2 (m+1)}{1+(m+1)(2r+m)},$$

то при $r=1$ достаточно проверить, что

$$(2+m)^3 \le (2m+3)^2,$$

а это верно, ведь $m \le m(2) \le 1/2$, значит,

$$2m^2 + m^3 \le 1,$$

откуда

$$(2+m)^3 \le (2m+3)^2.$$

Если же $r=2$, то достаточно проверить, что

$$(2+m)(3m+4)^2 \ge (2m+3)(m+1)(m+3)^2,$$

или, полагая $2+m=x$, убедиться в справедливости неравенства

$$x(3x-2)^2 \ge (2x-1)(x-1)(x+1)^2.$$

Это неравенство равносильно неравенству

$$9x^3 - 12x^2 + 4x \ge 2x^4 + x^3 - 3x^2 - x + 1,$$

а значит, и неравенству

$$0 \ge 2x^4 - 8x^3 + 9x^2 - 5x + 1,$$

которое справедливо при $2 \le x \le 2,5$, а значит, и при $x = 2+m$, потому что рассматриваемый многочлен имеет корни в интервалах $(0;1), (2,5;+\infty)$, так как $1 \ge 0 \ge -1$ и $4 \cdot 1,5 \cdot (3,5)^2 - (2,5) \cdot (5,5)^2 \le 150/2 - 605/8 \le 0$. Если бы последнее неравенство не выполнялось, то еще два корня лежали бы на интервале $(2;2,5)$, и тогда сумма корней была бы больше 6, что противоречило бы теореме Виета.

Проверим, что

$$F_r\left(\frac{1}{m+1}, M, 2r\right) \ge G_{r+1}(m, h_r(m), 2r).$$

Так как функция $h_r(\psi)$, как доказано в 14.12, монотонно убывает, то при $r=1$

$$h_r(m) \le h_r(0) = \frac{(r+2)^2}{3r+5} = 9/8$$

и при $r=2$

$$h_r(m) \le \frac{16}{11}.$$

Согласно задаче 14.13

$$G_{r+1}(m, h_r(m), 2r) \le G_{r+1}(m, h_r(0), 2r)$$

и поэтому достаточно доказать, что при $r \le 2$

$$\frac{((r+1)(m+1)+1)^2(m+r)}{(r(m+1)+1)((m+1)(m+2r)+1)} > \frac{(r+m+1)^2 h_r(0)}{1+h_r(0)(2r+m)}.$$

При $r=1$ это неравенство заменой $x = 2+m$ сводится к неравенству

$$\frac{(2x-1)^2(x-1)}{x((x-1)x+1)} \ge \frac{9x^2/8}{1+9x/8},$$

которое равносильно неравенству

$$9x^5 - 45x^4 + 49x^3 + 19x^2 - 31x + 8 \le 0,$$

справедливому при $2 \le x \le 3$, поскольку тогда

$$9x^5 - 45x^4 + 49x^3 \le -5x^3,$$

так как квадратный трехчлен

$$9x^2 - 45x + 49$$

на концах отрезка $[2,3]$ принимает равные значения -5, и поэтому на этом отрезке он не превосходит -5, а многочлен $-5x^3 + 19x^2 - 31x + 8$ отрицателен на отрезке $[2,3]$, ведь он имеет корень на интервале $(0,2)$, так как принимает на его концах значения разных знаков, и если он принимает неотрицательные значения внутри отрезка $[2,3]$, то имеет там два корня (или один двукратный корень), значит, сумма его корней больше 4, что противоречит теореме Виета.

При $r=2$ неравенство

$$\frac{((r+1)(m+1)+1)^2(m+r)}{(r(m+1)+1)((m+1)(m+2r)+1)} > \frac{(r+m+1)^2 h_r(0)}{1+h_r(0)(2r+m)}$$

принимает вид

$$\frac{(m+2)^2(3m+4)^2}{(2m+3)((m+1)(m+4)+1)} > \frac{(3+m)\frac{16}{11}}{1+(4+m)\frac{16}{11}}$$

и, значит, равносильно неравенству

$$32m^5 + 256m^4 + 589m^3 + 338m^2 - 272m - 240 < 0,$$

которое справедливо при $m < 1/2$, так как тогда

$$m^5 < \frac{m^4}{2} < \frac{m^3}{4} < \frac{m^2}{8} < \frac{m}{16},$$

и, следовательно,

$$32m^5 + 256m^4 + 589m^3 + 338m^2 - 272m - 240 <$$

$$< m\left(2+32+\frac{589}{4}+169-272\right)-240<240m-240<0.$$

Из доказанных при $r\leq 2$ неравенств

$$F_r\left(\frac{1}{m+1},M,2r\right)>G_{r+1}\left(m,h_r\left(m\right),2r\right)$$

и

$$F_r\left(\frac{1}{m+1},M,2r\right)>G_{r+1}\left(m,,m+1,2r\right)$$

вытекает неравенство

$$F_r\left(\frac{1}{m+1},M,2r\right)>b_3$$

и тем самым первое равенство задачи доказано и в случае $r\leq 2$.

Для доказательства второго равенства задачи достаточно проверить, что при $r\geq 3$

$$h_r\left(m\left(2r\right)\right)>1+m\left(2r\right).$$

Это неравенство равносильно неравенству

$$\left(r+1+m\right)^3\left(m+1\right)-\left(r+2+m\right)^2\left(r\left(1+m\right)-m\right)<0,$$

а, значит, и неравенству

$$r^2\left(m^2+m-1\right)+r\left(2m^3+6m^2+5m-1\right)+\left(1+m\right)^4+m\left(m+2\right)^2<0.$$

Так как $m=m\left(2r\right)\leq 1/2r\leq 1/6$, то последнее неравенство следует из неравенства

$$r^2\left(\frac{1}{4}r^{-2}+\frac{1}{2}r^{-1}-1\right)+r\left(\frac{1}{4}r^{-3}+\frac{3}{2}r^{-2}+\frac{5}{2}r^{-1}-1\right)+$$

$$+\left(1+\frac{1}{6}\right)^4+\left(2+\frac{1}{6}\right)^2<0,$$

которое, в свою очередь, следует из неравенства

$$-r^2-\frac{r}{2}+\frac{1}{4}+\frac{5}{2}+\frac{3}{2}r^{-1}+\frac{1}{4}r^{-2}+\frac{48}{36}\frac{54}{36}+\frac{169}{216}<0,$$

очевидно, верного, так как

$$-r^2-\frac{r}{2}+\frac{3}{2}r^{-1}+\frac{1}{4}r^{-2}<-9-\frac{3}{2}+\frac{1}{2}+\frac{1}{36}=-10+\frac{1}{36}$$

и

$$-10+\frac{1}{36}+\frac{1}{4}+\frac{5}{2}+2+\frac{169}{216}<0.$$

Для доказательства последнего равенства задачи достаточно проверить, что при $r\leq 2$

$$h_r\left(m\left(2r\right)\right)<1+m\left(2r\right).$$

Это неравенство равносильно неравенству

$$r^2\left(m^2+m-1\right)+r\left(2m^3+6m^2+5m-1\right)+\left(1+m\right)^4+m\left(m+2\right)^2>0,$$

которое при $r=1$ имеет вид

$$m^2+m-1+2m^3+6m^2+5m-1+\left(1+m\right)^4+m\left(m+2\right)^2>0,$$

или, что равносильно,

$$m^4 + 7m^3 + 17m^2 + 14m - 1 > 0, \qquad (*)$$

а при $r = 2$ — вид

$$(m^2 + m - 1) + 2(2m^3 + 6m^2 + 5m - 1) + (1 + m)^4 + m(m + 2)^2 > 0,$$

или, что равносильно,

$$m^4 + 9m^3 + 26m^2 + 22m - 5 > 0. \qquad (**)$$

Так как

$$m(1) = \frac{\sqrt{3} - 1}{2} > \frac{3}{10},$$

то неравенство (*) справедливо, а так как

$$m(2) = \frac{\sqrt{2} - 1}{2} > \frac{1}{5},$$

то неравенство (**) тоже справедливо.

14.23. Согласно задачам 14.19, 14.22 при $r \geq 4$

$$b(m, 2r - 1) = F_r(m, M, 2r - 1) = \frac{(r + 1 + m)^2 (r - 1 + m)}{(r + m)(2r - 1 + 2m)}$$

и при $r \geq 3$

$$b(m, 2r) = G_{r+1}(m, h_r(m), 2r) = \frac{(r + m + 1)(r + m + 2)^2}{(r + m + 1)^2 + (r + 2 + m)^2}.$$

Проверим, что $b(m, 2r - 2) < b(m, 2r - 1)$. Действительно,

$$b(m, 2r - 2) = \frac{(r + m)(r + m + 1)^2}{(r + m)^2 + (r + 1 + m)^2} <$$

$$< \frac{(r + 1 + m)^2 (r - 1 + m)}{(r + m)(2r - 1 + 2m)} = b(m, 2r - 1),$$

так как

$$\frac{(r + m)}{(r + m)^2 + (r + 1 + m)^2} < \frac{(r - 1 + m)}{(r + m)(2r - 1 + 2m)},$$

потому что при $r \geq 2$

$$\frac{(r + m)^2 + (r + 1 + m)^2}{(r + m)^2} = 2 + \frac{2}{r + m} + \frac{1}{(r + m)^2} > 2 + \frac{2}{r + m} >$$

$$> 2 + \frac{1}{r + m - 1} = \frac{2r - 1 + m}{r - 1 + m},$$

откуда

$$\frac{(r + m)^2}{(r + m)^2 + (r + 1 + m)^2} < \frac{r - 1 + m}{2r - 1 + 2m}.$$

Проверим, что $b(m, 2r-1) \leq b(m, 2r)$. Действительно, неравенство

$$\frac{(r+1+m)^2(r-1+m)}{(r+m)(2r-1+2m)} < \frac{(r+m+1)(r+m+2)^2}{(r+m+1)^2+(r+2+m)^2}$$

равносильно неравенству

$$\frac{(r+1+m)(r-1+m)}{(r+m)(2r-1+2m)} < \frac{(r+m+2)^2}{(r+m+1)^2+(r+2+m)^2},$$

а так как

$$(r+m)(2r-1+2m) = 2(r+m)^2 - 2 - (r+m-1) + 1,$$

$$(r+m+1)^2 + (r+m+2)^2 = 2(r+m+2)^2 - (2r+m+3),$$

то равносильно и неравенству

$$2 - \frac{1}{r+m+1} + \frac{1}{(r+m+1)(r+m-1)} > 2 - \frac{2r+2m+3}{(r+m+2)^2},$$

которое, очевидно, выполняется, потому что

$$\frac{1}{r+m+1} < \frac{2r+2m+3}{(r+m+2)^2},$$

ведь при $r \geq 2$

$$(r+m+2)^2 = (r+m+1)^2 + 2(r+m+1) + 1 <$$

$$< 2(r+m+1)^2 + r + m + 1 = (r+m+1)(2r+2m+3).$$

Из доказанных при $r \geq 4$ неравенств

$$b(m, 2r-2) \leq b(m, 2r-1) \leq b(m, 2r)$$

следует монотонность последовательности $\{b(m,k)\}$ при $k \geq 6$.

Функция

$$\frac{x(x+1)^2}{x^2+(x+1)^2}$$

монотонно возрастающая. Справедливы неравенства

$$r + m(2r) \leq r+1 \leq r+1+m(2r+2).$$

Далее согласно задаче 14.19 при $r=2$ или $r=3$ имеем

$$b(m, 2r-1) = F_r(\psi_{r-2}(m), M, 2r-1) = \frac{(r+\psi)(r+\psi+1)^2}{(r+\psi)^2+(r+1+\psi)^2},$$

где

$$f_r(\psi_{r-2}(m)) = M, \psi = \psi_{r-2}(m).$$

При $r \geq 3$, согласно утверждению 14.22, также имеем

$$b(m, 2r) = G_{r+1}(m, h_r(m), 2r) = \frac{(r+m+1)(r+m+2)^2}{(r+m+1)^2+(r+2+m)^2}.$$

Используя это, получим, что последовательности $\{b(m,2r)\}$ и $\{b(2r,2r)\}$ монотонны, начиная с $r=3$, а последовательности $\{b(m,2r-1)\}$ и $\{b(2r-1,2r-1)\}$ монотонны, начиная с $r=2$. Значения $b(m,2r-1)$ и $b(2r-1,2r-1)$ при $r=1$ нам не понадобятся, но рассуждая таким же образом, можно заметить, что упомянутые последовательности монотонны, начиная с $r=1$.

Проверим, что последовательности $\{b(m,2r)\}$ и $\{b(2r,2r)\}$ монотонны, начиная с $r=1$. Заметим, что при $x=r+\psi$

$$\frac{1}{h_r(\psi)}=\psi+\frac{2}{x+1}+\frac{1}{x+2+1/x},$$

значит, последовательность $h_r(\psi)$ возрастает, а функция

$$\frac{G_{r+1}(\alpha,\psi,2r)}{\alpha}=\frac{(x+1)^2}{1+\alpha(2x-\psi)}$$

монотонно возрастает при $x\geq 1+\psi$ (в чем можно убедиться дифференцированием). Поэтому последовательность $\{max(1+m,h_r(m))\}$ возрастает, а так как при $r\geq 3$

$$max(1+m,h_r(m))=h_r(m),$$

то с помощью задач 14.13, 14.22 получаем, что последовательность $\{b(m,2r)\}$ монотонна, начиная с $r=1$.

Согласно утверждению 14.22, учитывая равенство $m(2)(m(2)+1)=1/2$, имеем

$$b(2,2)=G_2(m(2),m(2)+1,2)=$$

$$=\frac{(2+m)^2(m+1)}{m^2+3m+3}=\frac{m^3+5m^2+8m+4}{m^2+3m+3}=$$

$$=\frac{6+4,5m}{3,5+2m}=\frac{21+15\sqrt{3}}{26}=1,8069523\ldots.$$

Аналогично

$$b(4,4)=G_3(m(4),m(4)+1,4)=$$

$$=\frac{(3+m)^2(m+1)}{m^2+5m+5}=\frac{m^3+7m^2+15m+9}{m^2+5m+5}=$$

$$=\frac{10,5+9,25m}{5,25+4m}=\frac{47+37\sqrt{2}}{26+16\sqrt{2}}=2,0425905\ldots,$$

а при $r\geq 3$ после некоторых вычислений получаем

$$b(2r,2r)=G_{r+1}(m(2r),h_r(m(2r)),2)=\frac{(r+m+1)(r+m+2)^2}{(r+m+1)^2+(r+2+m)^2}=$$

$$=\frac{\sqrt{1+2/r}\,(6r^3+14r^2+8r+1)+(4r^4+14r^3+18r^2+14r+7)}{\sqrt{1+2/r}\,(8r^2+8r)+(8r^3+16r^2+12r+4)},$$

$$b(2r,2r)\geq b(6,6)=\frac{313\sqrt{5/3}+913}{96\sqrt{5/3}+400}=2,5138234\ldots,$$

что и доказывает монотонность последовательности $\{b(2r,2r)\}$.

Очевидно, что при [illegible]

$$b(m,k)\frac{(r+m+1)(r+m+2)^2}{(r+m+1)^2+(r+2+m)^2}=\frac{x+1}{2}-\frac{1}{4x}+\frac{1/4}{2x^2+2x+1}>$$

$$>\frac{r+m+1}{2}-\frac{1}{4(r+m)}=\frac{k}{4}+\frac{m+1}{2}-\frac{1}{2k+4m},$$

а при $k=2r-1$

$$b(m,k)=\frac{(r+1+m)^2(r-1+m)}{(r+m)(2r-1+2m)}=\frac{x}{2}+\frac{3}{4}-\frac{1}{8x}-\frac{9}{8(2x^2-x)}=$$

$$=\frac{k}{4}+\frac{m}{2}+1-\frac{O(1)}{k}.$$

Так как $x=r+m$ и $m=[0;k1\ldots]>1/2r$, то при $r\geq 3$

$$\frac{1}{8x}+\frac{9}{8(2x^2-x)}<\frac{1}{8x}+\frac{9}{40x}<\frac{7}{20r}=\frac{7}{5}\frac{1}{4r}<\frac{7m}{10},$$

значит,

$$b(k,k)>k/4+1-m/5.$$

Согласно задачам 14.20 – 14.21

$$B(m,2r)=G_r\left(\frac{1}{1+m},M,2r-1\right)=$$

$$=F_r\left(\frac{1}{m+1},1+m,2r-1\right)\frac{\left(r+1+\frac{1}{m+1}\right)^2}{2\left(r+\frac{1}{m+1}\right)},$$

и при $r\geq 3$

$$B(m,2r-1)=F_r\left(\frac{1}{1+m},m+1,2r-1\right)=$$

$$=\frac{\left(r+1+\frac{1}{1+m}\right)^2((r-1)(m+1)+1)}{\left(r+\frac{1}{1+m}\right)\left(1+(m+1)\left(2r-1+\frac{1}{1+m}\right)\right)}.$$

Очевидно, что при $r\geq 3$

$$B(m,2r-1)<B(m,2r),$$

так как

$$\frac{(r-1)(m+1)+1}{1+(m+1)\left(2r-1+\frac{1}{1+m}\right)}<\frac{1}{2}.$$

Проверим, что при $r\geq 4$

$$B(m,2r-2)<B(m,2r-1).$$

Это равносильно неравенству

$$2((m+1)(r+1)+1)^2((m+1)(r-1)+1)^2>$$

$$> ((m+1)r+1)^3((m+1)(2r-1)+2),$$

которое после разложения обеих его частей по степеням $m+1$ и сокращения на $m+1$ принимает вид

$$(m+1)^3(r^3-4r^2+2)+(m+1)(3r^2-8r)+(m+1)(3r-4)+1>0.$$

Очевидно, что это неравенство справедливо при $r \geq 4$ и любом m, так как все коэффициенты при степенях $m+1$ положительны. При $r=3$ оно принимает вид

$$7m^3+18m^2+10m<2,$$

и не выполняется при $m>1/6$, а, значит, и при $m=m(5)$. Поэтому

$$B(m,2r-1) \leq B(m,2r) \leq B(m,2r+1)$$

при $r \geq 3$, значит, начиная с $k=5$, последовательность $\{B(m,k)\}$ монотонно возрастает, но при $m=m(5)$

$$B(m,4) > B(m,5).$$

Монотонность при всех r последовательности $\{B(m,2r)\}$,

$$B(m,2r)=\frac{(r+1+\frac{1}{m+1})^2}{2(r+\frac{1}{m+1})},$$

легко следует из монотонности при $x>1$ функции $(x+1)^2/x$. По той же причине монотонно возрастает последовательность

$$\left\{\frac{(r+1+\psi)^2}{r\psi}\right\}.$$

Так как функция

$$\frac{(r-1)\alpha+1}{1+\alpha(2r-1+\psi)}$$

дробно-линейна относительно r, равна нулю при $r=1+1/\alpha$ и положительна при $r>1+1/\alpha$, то последовательность $\{\delta_r\}$,

$$\delta_r=\frac{(r-1)\alpha+1}{1+\alpha(2r-1+\psi)},$$

монотонно возрастает, а, значит, монотонно возрастает последовательность $\{F_r(\psi,\alpha,2r-1)\}$,

$$F_r(\psi,\alpha,2r-1)=\delta_r\frac{(r+1+\psi)^2}{r\psi}.$$

Поэтому

$$B(m,1)=F_1(m,m+1,1)<F_2(m,m+1,3)=$$
$$=B(m,3)<F_3(m,m+1,5),$$

а так как при решении 14.19 установлено, что

$$F_3(m,m+1,5)<F_3\left(\frac{1}{m+1},m+1,5\right)=B(m,5),$$

то последовательность $\{B(m, 2r-1)\}$ монотонна.

Наконец, оценим сверху $B(m,k)$. Если $k=2r-1$ и $x=r+\frac{1}{m+1}$, то

$$B(m,k)=\frac{(x+1)^2(x-1)}{x(2x-1)}<\frac{x}{2}+\frac{3}{4}-\frac{1}{8x}<\frac{k}{4}+\frac{3}{2}-\frac{1}{4k+12}.$$

Если же $k=2r$, то

$$B(m,k)=\frac{\left(r+1+\frac{1}{m+1}\right)^2}{2\left(r+\frac{1}{m+1}\right)}=\frac{r+1+\frac{1}{m+1}}{2}+1+\frac{1/2}{r+1+\frac{1}{m+1}}<$$

$$<\frac{r+3}{2}+\frac{1/2}{r+1}=\frac{k}{4}+\frac{3}{2}+\frac{1}{k+2}.$$

Так как

$$\frac{1}{k+1}\le m(k),\ \frac{1}{2(m+1)}<\frac{1}{2}-\frac{m}{2},$$

имеем

$$B(2r,2r)==\frac{r+1+\frac{1}{m+1}}{2}+1+\frac{1/2}{r+1+\frac{1}{m+1}}\frac{k}{4}+\frac{3}{2}+\frac{1}{k+2}-\frac{m}{2}<$$

$$<\frac{k}{4}+\frac{3}{2}+\frac{1}{2k+4}.$$

14.28. Докажем неравенство

$$L(\alpha,\varepsilon)\le 1/(2\varepsilon g(1/\varepsilon)).$$

Рассмотрим последовательность подходящих дробей $\{p_n/q_n\}$ к дроби α и положим

$$\varepsilon_n=|\alpha-p_n/q_n|.$$

Согласно утверждению 14.10 и введенным в доказательстве утверждения 14.23 обозначениям справедливо равенство

$$\sup\{\varepsilon L^2(\alpha,\varepsilon):\varepsilon_{n+1}\le\varepsilon\le\varepsilon_n\}=\gamma_{n-1}(\alpha)=\Gamma(\psi_n,\alpha_{n+2},a_{n+1}).$$

Положим

$$M_n=f(q_{n+2})+1,\quad m_n=1/M_n.$$

Тогда в силу указанных в 14.5 соотношений

$$\alpha_n=a_n+1/\alpha_{n+1},\quad \psi_n=[0;a_n,\dots,a_1],$$

монотонности функций f и $1/x$ и неравенства $a_{n+1}\le f_n(q)$ справедливы неравенства

$$m_n\le\psi_n\le 1/(m_n+1),\quad 1+m_n\le\alpha_{n+2}\le M_n.$$

Поэтому в силу утверждения 14.22 и определения функций $B(m,k)$ и $b(m,k)$ имеем

$$\frac{a_{n+1}}{4}+\frac{1}{2}-\frac{O(1)}{a_{n+1}}\le\Gamma(\psi_n,\alpha_{n+2},a_{n+1})\le\frac{a_{n+1}}{4}+\frac{3}{2}+\frac{1}{a_{n+1}+2},$$

откуда

$$\sup\{\varepsilon L^2(\alpha,\varepsilon):\varepsilon_{n+1}\le\varepsilon<\varepsilon_n\}=\gamma_{n-1}(\alpha)\le\frac{a_{n+1}}{4}+\frac{3}{2}+\frac{1}{a_{n+1}+2},$$

$$sup\{\varepsilon L^2(\alpha,\varepsilon):\varepsilon_{n+1}\le\varepsilon<\varepsilon_n\}=\gamma_{n-1}(\alpha)>\frac{a_{n+1}}{4}+\frac{1}{2}-\frac{O(1)}{a_{n+1}}.$$

При $\varepsilon_{n+1}\le\varepsilon<\varepsilon_n$ в силу неравенства $a_{n+1}\le f_n(q)$ и 14.5 справедливо неравенство

$$1/\varepsilon>1/\varepsilon_n>q_nq_{n+1}>a_{n+1}q_n^2\ge a_{n+1}h^2(a_{n+1})=$$
$$=f(h(a_{n+1}))\,h^2(a_{n+1}),$$

где h — обратная функция к f (и, следовательно, тоже монотонная), откуда в силу монотонности функции g, обратной к функции $x^2f(x)$, имеем, что $g(1/\varepsilon)>h(a_{n+1})$, и, значит,

$$f(g(1/\varepsilon))>f(h(a_{n+1}))=a_{n+1}.$$

Отсюда и из доказанного выше неравенства с учетом монотонности функции $x/4+1/(x+2)$ при $x>0$ следует, что

$$L^2(\alpha,\varepsilon)\le\left(\frac{a_{n+1}}{4}+\frac{3}{2}+\frac{1}{a_{n+1}+2}\right)\frac{1}{\varepsilon}<$$

$$<\left(\frac{1}{4}f\left(g\left(\frac{1}{\varepsilon}\right)\right)+\frac{3}{2}+\frac{1}{f\left(g\left(\frac{1}{\varepsilon}\right)\right)+2}\right)\frac{1}{\varepsilon}.$$

Так как $f(g(1/\varepsilon))\,g^2(1/\varepsilon)=1/\varepsilon$, то из последнего неравенства вытекает, что

$$L^2(\alpha,\varepsilon)<\frac{1}{4}f^2\left(g\left(\frac{1}{\varepsilon}\right)\right)g^2\left(\frac{1}{\varepsilon}\right)+\frac{3}{2\varepsilon}+g^2\left(\frac{1}{\varepsilon}\right)<$$

$$<\left(\frac{1}{2}f\left(g\left(\frac{1}{\varepsilon}\right)\right)g\left(\frac{1}{\varepsilon}\right)+\frac{3}{2}g\left(\frac{1}{\varepsilon}\right)\right)^2,$$

откуда

$$L(\alpha,\varepsilon)<\frac{1}{2}f(g(1/\varepsilon))\,g(1/\varepsilon)+\frac{3}{2}g(1/\varepsilon)=\frac{1}{2\varepsilon g(1/\varepsilon)}+\frac{3}{2}g(1/\varepsilon)=$$

$$=\frac{1}{2\varepsilon g(1/\varepsilon)}\left(1+3\varepsilon g^2(1/\varepsilon)\right)=\frac{1}{2\varepsilon g(1/\varepsilon)}\left(1+\frac{3}{f(g(1/\varepsilon))}\right).$$

Для получения нижней оценки выберем последовательность $\{m_n\}$ так, чтобы $a_{m_n+1}>c(q_{m_n})f(q_{m_n})$, и на интервале $(\varepsilon_{m_n+1},\varepsilon_{m_n})$ возьмем такую точку ζ_n, чтобы

$$\lim\left(\zeta_nL^2(\alpha,\zeta_n)-\sup\{\varepsilon L^2(\alpha,\varepsilon):\varepsilon_{m_n+1}\le\varepsilon<\varepsilon_{m_n}\}\right)=0.$$

Как установлено в доказательстве утверждения 14.9, число ζ_n можно выбрать в интервале $\left(\varepsilon_{m_n-1,r_{m_n-1}}-\delta,\varepsilon_{m_n}\right)$ при любом $\delta>0$. Значит, опуская для краткости нижние этажи в индексах, а также индексы при r, с помощью задач 14.5 – 14.6 получаем, что при $m\to\infty$ справедливы неравенства

$$\frac{1}{\zeta_n}<\frac{q_{m-1,r}(\alpha_{m+1}q_m+q_{m-1})}{\alpha_{m+1}-r}+\delta<$$

$$< \frac{(rq_m + q_{m-1})(q_m(a_{m+1}+1)+q_{m-1})}{a_{m+1}-r} <$$

$$< q_m^2(a_{m+1}+2)\left(1+\frac{6}{a_{m+1}-2}\right) < q_m^2(a_{m+1}+9),$$

а поэтому и неравенства

$$\frac{1}{\zeta_n} > \frac{1}{\epsilon_m} > a_{m+1}q_m^2 > c(q_m)q_m^2 f(q_m),$$

откуда в силу монотонности функции g имеем

$$g\left(\frac{1}{c(q_m)\zeta_n}\right) \geq q_m.$$

Отсюда, учитывая полученные выше соотношения, выводим неравенство

$$L^2(\alpha,\zeta_n) > \frac{1}{\zeta_n}\left(\frac{a_{m+1}}{4}+\frac{1}{2}-\frac{O(1)}{a_{m+1}}\right) > \frac{a_{m+1}^2 q_m^2}{4},$$

из которого следует, что

$$L^2(\alpha,\zeta_n) > \frac{a_{m+1}q_m}{2},$$

а так как

$$\frac{1}{\zeta_n} < q_m^2(a_{m+1}+9),$$

то получаем неравенство

$$L^2(\alpha,\zeta_n) > \frac{a_{m+1}q_m}{2} > \frac{a_{m+1}}{2(a_{m+1}+9)q_m\zeta_n} > \frac{1-\frac{9}{a_{m+1}}}{2q_m\zeta_n}.$$

Из него, учитывая неравенства

$$g\left(\frac{1}{c(q_m)\zeta_n}\right) \geq q_m,$$

имеем

$$L(\alpha,\zeta_n) > \frac{1-\frac{9}{a_{m+1}}}{2\zeta_n g\left(\frac{1}{c(q_m)\zeta_n}\right)}.$$

Из 14.27, полагая

$$y_0 = \frac{1}{c(q_m)\zeta_n}, \quad y = \frac{1}{\zeta_n},$$

выводим неравенство

$$g\left(\frac{1}{c(q_m)\zeta_n}\right) < g\left(\frac{1}{\zeta_n}\right)\left(1+\frac{1-c(q_m)}{2c(q_m)}\right).$$

Если $c(q_m) > 1/3$, то из предыдущих неравенств, учитывая, что

$$a_{m+1} > \frac{1}{c(q_m)f(q_m)},$$

получаем следующую нижнюю оценку:

$$L(\alpha,\zeta_n) > \frac{\left(1-\frac{9}{c(q_m)f(q_m)}\right)(3c(q_m)-1)}{4c(q_m)\zeta_n g\left(\frac{1}{\zeta_n}\right)}.$$

При $c(q_m) \to 1$ полученная оценка принимает вид

$$L(\alpha, \zeta_n) > (1 - o(1)) \frac{1}{2\zeta_n g\left(\frac{1}{\zeta_n}\right)}.$$

Из доказанных неравенств

$$\frac{1}{\zeta_n} < q_m^2 (a_{m+1} + 9) < q_m^2 (f(q_m) + 9),$$

$$q_m \le g\left(\frac{1}{\zeta_n}\right)\left(1 + \frac{1 - c(q_m)}{2c(q_m)}\right)$$

при стремящейся к единице величине $c(q_m)$ следует равенство

$$q_m = (1 + o(1))\, g\left(\frac{1}{\zeta_n}\right).$$

Если в качестве $c(q)$ взять $1 - O(1/f(q))$, то полученная оценка принимает вид

$$L(\alpha, \zeta_n) > \frac{1 - \frac{O(1)}{f\left(\frac{1}{2} g\left(\frac{1}{\zeta_n}\right)\right)}}{2\zeta_n g\left(\frac{1}{\zeta_n}\right)}.$$

Докажем нижнюю оценку для $L(\alpha, \zeta_n)$. Пусть

$$\varepsilon_{n+2} \le \varepsilon < \varepsilon_{n+1}.$$

Согласно 14.9, если

$$\varepsilon_{n,r} \le \varepsilon < \min\{\varepsilon_{n,r-1}, \varepsilon_{n+1}\}, \quad r_n - 2 \le r \le a_{n+2},$$

где

$$\varepsilon_{n,r} = \frac{a_{n+2} - r}{q_{n,r}(\alpha_{n+2} q_{n+1} + q_n)}, \quad q_{n,r} = r q_{n+1} + q_n, \quad \alpha_n = a_n + \frac{1}{\alpha_{n+1}}, \quad r_n > \frac{a_{n+2}}{2},$$

то, так как $\min\{\varepsilon_{n,r-1}, \varepsilon_{n+1}\} = \varepsilon_{n+1}$ лишь при $r = r_n - 2$, имеем

$$L(\alpha, \zeta_n) = q_{n,r}.$$

Так как при $r \le a_{n+2} - 1$

$$(a_{n+2} + 1) q_{n+1} + q_n < \frac{a_{n+2} + 1}{r} (r q_{n+1} + q_n) = \frac{a_{n+2} + 1}{r} q_{n,r},$$

то

$$\frac{1}{\varepsilon} \le \frac{1}{\varepsilon_{n,r}} < \frac{(r q_{n+1} + q_n)((a_{n+2} + 1) q_{n+1} + q_n)}{a_{n+2} - r} < \frac{(a_{n+2} + 1) q_{n,r}^2}{(a_{n+2} - r) r}.$$

Квадратный трехчлен $(a_{n+2} - r) r$ имеет максимум в точке $(a_{n+2})/2$ и убывает при $r \ge (a_{n+2})/2$, поэтому при $r \ge a_{n+2} - 1$ справедливо неравенство

$$\frac{1}{\varepsilon} \le \frac{1}{\varepsilon_{n,r}} < \frac{(a_{n+2} + 1) q_{n,r}^2}{(a_{n+2} - r) r} < \frac{(a_{n+2} + 1) q_{n,r}^2}{a_{n+2} - 1} < 3 q_{n,r}^2 = 3 L^2(\alpha, \varepsilon).$$

Если же $r = a_{n+2} - 1$, то в силу соотношений $q_{n+2} = q_{n,r}$ и $a_{n+3} \le f(q_{n,r})$ справедливо неравенство

$$\frac{1}{\varepsilon} \le \frac{1}{\varepsilon_{n,a_{n+2}}} = \frac{1}{\varepsilon_{n+2}} < q_{n+2}(a_{n+3}+2)q_{n+2} < q_{n,r}^2(f(q_{n,r})+2),$$

значит,

$$\frac{1}{\varepsilon(1+2/f(q_{n,r}))} < q_{n,r}^2 f(q_{n,r}),$$

причем последнее неравенство верно и при $r < a_{n+2}$, откуда следует, что

$$g\left(\frac{1}{\varepsilon(1+2/f(q_{n,r}))}\right) < q_{n,r} = L(\alpha,\varepsilon).$$

Применяя 14.27 при

$$y = \frac{1}{\varepsilon(1+2/f(q_{n,r}))}, \quad y_0 = \frac{1}{\varepsilon},$$

получаем неравенство

$$g(1/\varepsilon) \le g\left(\frac{1}{\varepsilon(1+2/f(q_{n,r}))}\right)(1+1/f(q_{n,r})),$$

с помощью которого предыдущее неравенство можно переписать в виде

$$g(1/\varepsilon)(1-1/f(q_{n,r})) < g(1/\varepsilon)(1+1/f(q_{n,r})) < L(\alpha,\varepsilon).$$

Так как $q_{n,r}$ стремится к бесконечности, то

$$q_{n,r} > \frac{1}{2}g(1/\varepsilon),$$

значит,

$$f(q_{n,r}) > f\left(\frac{1}{2}g(1/\varepsilon)\right),$$

и

$$g(1/\varepsilon)\left(1 - \frac{1}{f\left(\frac{1}{2}g(1/\varepsilon)\right)}\right) < L(\alpha,\varepsilon).$$

Из полученного неравенства следует асимптотическое неравенство

$$g(1/\varepsilon) < (1+o(1))L(\alpha,\varepsilon).$$

Докажем последнее утверждение теоремы. Согласно проведенным выше рассуждениям $L(\alpha,\varepsilon_n) = q_n$. Выбирая последовательность m_n так же, как и выше, и полагая $\delta_n = \varepsilon_{m_n}$, получаем (как и выше) неравенство

$$g\left(\frac{1}{c(q_m)\delta_n}\right) \ge q$$

(здесь и далее для краткости опускаем нижние этажи в индексах). Используя полученное выше неравенство

$$g\left(\frac{1}{c(q_m)\delta_n}\right) < g\left(\frac{1}{\delta_n}\right)\left(1 + \frac{1-c(q_m)}{2c(q_m}\right),$$

выводим отсюда, что

$$L(\alpha, \delta_n) \leq g\left(\frac{1}{\delta_n}\right)\left(1 + \frac{1 - c(q_m)}{2c(q_m}\right).$$

При $c(q_m) \to 1$ полученная оценка принимает вид

$$L(\alpha, \delta_n) < (1 + o(1))g(1/\delta_n).$$

Так как при $r = a_m$

$$q_m = q_{m-2,r} > \frac{1}{2}g(1/\varepsilon_{m-2,r}) = \frac{1}{2}g(1/\delta_n),$$

то в случае $c(q) = 1 - O(1/f(q))$ полученная оценка принимает вид

$$L(\alpha, \delta_n) < \left(1 + \frac{O(1)}{f\left(\frac{1}{2g(1/\delta_n}\right)}\right) g(1/\delta_n).$$

Заметим, что фактически были доказаны неравенства

$$L(\alpha, \varepsilon) < \frac{1 + 3/f(g(1/\varepsilon)}{2\varepsilon g(1/\varepsilon)},$$

$$g(1/\varepsilon)\left(1 - \frac{1}{f\left(\frac{1}{2}g(1/\varepsilon)\right)}\right) < L(\alpha, \varepsilon),$$

а если для некоторой последовательности $\{m_n\}$

$$a_{m_n+1} \geq f(q_{m_n}) - O(1),$$

то доказано, что для некоторых последовательностей $\{\delta_n\}$ и $\{\xi_n\}$ справедливы неравенства

$$L(\alpha, \delta_n) < \left(1 + \frac{O(1)}{f\left(\frac{1}{2}g(1/\delta_n)\right)}\right) g(1/\delta_n),\ L(\alpha, \xi_n) > \frac{1 - \frac{O(1)}{f(\frac{1}{2}g(1/\xi_n))}}{2\xi_n g(1/\xi_n)}.$$

§ 15. ДЕЛЕНИЕ ОТРЕЗКА НА РАВНЫЕ ЧАСТИ ЦИРКУЛЕМ И ЛИНЕЙКОЙ

Допустим, что на плоскости дано некоторое множество точек, прямых и окружностей, которое обозначим M_0.

Назовем **построением циркулем и линейкой** при заданном M_0 любую последовательность множеств $M_0, M_1, \ldots, M_L$, начинающуюся с M_0, и такую, что каждое следующее множество M_{i+1} получается из предыдущего множества M_i добавлением либо некоторой прямой, проходящей через какие-то две точки из множества M_i, либо окружности с центром в какой-то из точек множества M_i и радиусом, равным длине некоторого отрезка с концами в точках из M_i, а также всех

точек пересечения добавленной линии со всеми линиями из множества M_i. Число L назовем **сложностью этого построения**. **Сложностью построения множества** M точек, отрезков и окружностей и прямых при заданном M_0 назовем минимальную сложность такого построения M_0, $M_1, \ldots, M_L$, для которого множество M_L содержит все прямые и окружности из M, все точки из M и концы всех отрезков из M.

Аналогично определяется **сложность построения одним циркулем**.

Первый цикл задач принадлежит итальянскому математику Маскерони[1].

15.1. Даны единичная окружность с диаметром и отрезок длины x, $x < 1$. Постройте на этом диаметре отрезок длины x^2 одним циркулем со сложностью 2.

15.2. Решите предыдущую задачу со сложностью 3, если диаметр задан только одним своим концом, а не начерчен целиком.

15.3. Даны единичная окружность и отрезок длины $x > 1$ с началом в ее центре. Постройте отрезок длины x^{-1} одним циркулем со сложностью 2. Постройте отрезок длины x^{-1} одним циркулем со сложностью 3, если отрезок длины x задан только своими концами, а не начерчен целиком.

15.4. Даны отрезки с длинами a, b, c, где b и $c < 2a$. Постройте одним циркулем со сложностью 3 отрезок длины x такой, что $a : b = c : x$.

15.5. Даны единичная окружность, отрезок длины $c < 2$ с началом в ее центре и еще отрезок длины $b < 1$. Постройте одним циркулем отрезок длины bc со сложностью 2.

15.6. Постройте одним циркулем одновременно отрезки длины 2 и 3, лежащие на одной прямой с данным единичным отрезком, со сложностью 3.

15.7. Поделите пополам отрезок одним циркулем:

а) со сложностью 4, если дана прямая, на которой лежит отрезок;

б) со сложностью 5, если дан только сам отрезок;

в) со сложностью 6, если даны только его концы.

В первом издании "Математического калейдоскопа" Штейнгауза последняя задача была решена со сложностью 8.

15.8*. Поделите на три равные части отрезок одним циркулем:

а) со сложностью 5, если дана прямая, на которой лежит отрезок;

б) со сложностью 8, если дан только сам отрезок;

в) со сложностью 11, если даны только его концы.

Разумеется, с помощью линейки сложность построений можно уменьшить.

---

[1] Свою книгу "Геометрия циркуля" он подарил Наполеону.

15.9. Разделите циркулем и линейкой отрезок пополам со сложностью 3 и на четыре равные части со сложностью 6.

15.10*. *(Москва, 66)* Разделите циркулем и линейкой отрезок на шесть равных частей со сложностью 8.

15.11. Проведите через точку вне прямой параллельную ей прямую со сложностью 3.

15.12. На сторонах угла отложены от его вершины отрезки длины a, b и 1 (два из них — на одной стороне, а один — на другой). Постройте со сложностью 3 отрезок длины ab на одной из сторон угла.

Следующий цикл задач принадлежит Мору[1)].

15.13. Постройте со сложностью 5 одним циркулем одновременно отрезки длины $\sqrt{a^2-b^2}$, $2\sqrt{a^2-b^2}$, $2b$, $3b$, $\sqrt{3}b$, если отрезки a и b, $a > b$, заданы.

15.14. Постройте со сложностью 5 одним циркулем одновременно отрезки длины $\sqrt{2}a$, $\sqrt{3}a$, $\sqrt{8}a$, $2a, 3a$, если отрезок длины a задан.

15.15. Постройте со сложностью 11 одним циркулем одновременно отрезки длины $\sqrt{a^2+b^2}$, $2\sqrt{a^2+b^2}$, $\sqrt{a^2-b^2}$, $2\sqrt{a^2-b^2}$, $\sqrt{2}a$, $\sqrt{3}a$, $\sqrt{8}a$, $2a$, $3a$, $2b$, $3b$, $\sqrt{3}b$, если отрезки a и b, $a > b$, заданы.

15.16. Постройте со сложностью 15 одним циркулем одновременно отрезки длины $a+b$, $a-b$, $ab/\sqrt{a^2+b^2}$, $\sqrt{a^2+b^2}$, $2\sqrt{a^2+b^2}$, $\sqrt{a^2-b^2}$, $2\sqrt{a^2-b^2}$,$\sqrt{2}a$, $\sqrt{3}a$, $\sqrt{8}a$, $2a$, $3a$, $2b$, $3b$, $\sqrt{3}b$, если отрезки a и b, $a > b$, заданы.

15.17.Если отрезки длины a и b заданы на одной прямой, то отрезок длины $a+b$ можно построить одним циркулем со сложностью 2.

15.18. Даны отрезки длины 1 и $a < 1$ с общим концом, вложенные один в другой. Постройте со сложностью 7 одним циркулем отрезок длины $\sqrt{a}$. В случае $a > 1$ подобное построение можно осуществить со сложностью 9.

15.19. Докажите теорему Мора – Маскерони о построениях одним циркулем.

Следующий цикл задач посвящен "быстрому" делению отрезка на равные части циркулем и линейкой.

15.20.** Задан единичный отрезок. Постройте циркулем отрезок длины 2^{-2^n}:

а) со сложностью $2n+4$, если дана прямая, на которой лежит отрезок;

б) со сложностью $2n+5$, если дан только сам отрезок;

[1)]В своей книге "Датский Евклид" он на столетие раньше Маскерони доказал возможность проведения всех геометрических построений одним лишь циркулем. Эту книгу случайно нашел в двадцатые годы нашего века известный датский геометр Хьельмслев в букинистическом магазине в Копенгагене.

в) со сложностью $3n+6$, если даны только его концы.

15.21*. Разделите отрезок циркулем на 2^m равных частей:

а) при $m=2^n$ со сложностью $6+n+2^{m-1}$;

б) при $m=2^n+1$ со сложностью $5+n+2^{m-1}$,

если дана прямая, на которой лежит отрезок.

15.22. Разделите отрезок циркулем на восемь равных частей со сложностью 9, а на 16 частей — со сложностью 14.

Назовем **аддитивной цепочкой** любую начинающуюся с 1 последовательность натуральных чисел, в которой каждое число является суммой каких-то двух предыдущих чисел (или удвоением какого-то предыдущего числа). Обозначим $l(n)$ *наименьшую длину* аддитивной цепочки, заканчивающейся числом n.

15.23. Наименьшее число операций умножения, требующихся для возведения числа x в степень n, равно $l(n)$.

15.24**. *(А.Брауэр)* Докажите, что при $k<\log_2\log_2 n$ справедливо неравенство

$$l(n)<(1+1/k)]\log_2 n[+2^{k-1}-k+2.$$

15.25*. *(А.Брауэр)* Докажите, что

$$\lim_{n\to\infty} l(n)/\log_2 n=1.$$

15.26*. Задан единичный отрезок. Постройте циркулем отрезок длины 2^{-n} со сложностью не более $(2+\epsilon_n)\log_2 n$, где ϵ_n стремится к нулю при n, стремящемся к бесконечности.

15.27*. Постройте со сложностью не более $2n$ циркулем и линейкой такое множество точек, что среди отрезков с концами в этом множестве найдутся отрезки с длинами $1,2,\ldots,n^2$. Выполните то же построение со сложностью не более $4n$ одним циркулем.

15.28**. Дан отрезок длины $x<1$. Постройте со сложностью не более $4n$ одним циркулем такое множество точек, что среди отрезков с концами в этом множестве найдутся отрезки длиной $x,x^2,\ldots,x^{n^2}$.

15.29**. Задан единичный отрезок. Постройте циркулем отрезок длины 2^{-n} со сложностью не более

$$2\log_2 n+\frac{\log_2 n}{\log_2\log_2 n}+\frac{(2\log_2 n)(\log_2\log_2\log_2 n+C)}{(\log_2\log_2 n)^2}.$$

15.30**. Разделите данный отрезок на 2^n равных частей со сложностью не более $2^{n-1}+9$ одним циркулем, и со сложностью не более $2^{n-1}+7$ циркулем и линейкой.

Назовем **схемой вычисления многочлена** $p(x)$ начинающуюся с 1 и x и заканчивающуюся $p(x)$ последовательность многочленов, в которой каждый многочлен равен сумме, разности или произведению

каких-то предыдущих. **Сложностью многочлена** назовем длину *наикратчайшей* схемы его вычисления. Такие схемы назовем **минимальными.** Сложность можно понимать как наименьшее число арифметических операций, нужных для вычисления многочлена.

15.31*.** *(Лупанов – Сэвидж)* Докажите, что сложность произвольного многочлена степени n с коэффициентами 0 и 1 не превосходит

$$\frac{n}{\log_2 n}\left(1+\frac{3\log_2\log_2 n + C}{\log_2 n}\right),$$

где C — некоторая константа.

Далее n означает натуральное число. Назовем **схемой вычисления числа** n начинающуюся с 1 и заканчивающуюся n последовательность чисел, в которой каждое число равно сумме, разности или произведению каких-то предыдущих. **Сложностью числа** n назовем длину наикратчайшей схемы для его вычисления.

15.32.** *(Лупанов – Штрассен)* Докажите, что сложность произвольного числа n не превосходит

$$\frac{\log_2 n}{\log_2\log_2 n}\left(1+\frac{3\log_2\log_2\log_2 n + C}{\log_2\log_2 n}\right).$$

15.33.** Задан единичный отрезок. Постройте циркулем и линейкой отрезки длины n и $1/n$ со сложностью не более

$$\frac{\log_2 n}{\log_2\log_2 n}\left(1+\frac{3\log_2\log_2\log_2 n + C}{\log_2\log_2 n}\right).$$

15.34.** Улучшите предыдущую оценку до оценки

$$\frac{\log_2 n}{2\log_2\log_2 n}\left(1+\frac{3\log_2\log_2\log_2 n + C}{\log_2\log_2 n}\right).$$

15.35.** Разделите отрезок циркулем и линейкой на n равных частей со сложностью не более

$$\frac{n}{2}+\frac{\log_2 n}{2\log_2\log_2 n}\left(1+\frac{3\log_2\log_2\log_2 n + C}{\log_2\log_2 n}\right).$$

15.36. Докажите, что сложность разделения отрезка циркулем и линейкой на n равных частей не меньше $](n-1)/2[$.

15.37.** Задан единичный отрезок. Постройте одним циркулем отрезки длины n и $1/n$ сложностью не более

$$3\log_3 n+\frac{\log_3 n}{\log_3\log_3 n}\left(1+\frac{2\log_3\log_3\log_3 n + C}{\log_3\log_3 n}\right).$$

15.38**. Докажите, что сложность построения отрезка длины n одним только циркулем не меньше $[\log_\varphi (n+1/2)]$, где $\varphi = \left(\sqrt{5}+1\right)/2$.

15.39**. Разделите отрезок на n равных частей одним циркулем со сложностью не более

$$n + 3\log_3 n + \frac{\log_3 n}{\log_3 \log_3 n}\left(1 + \frac{2\log_3 \log_3 \log_3 n + C}{\log_3 \log_3 n}\right).$$

15.40. Докажите, что сложность разделения отрезка одним циркулем на n равных частей не меньше $n-1$.

15.41**. Задан единичный отрезок. Постройте отрезки длины m^n и m^{-n} со сложностью не более

$$(2+\epsilon_n)\log_2 n + (3+\epsilon_m)\log_2 m$$

где $\epsilon_n \to 0$ при $n \to \infty$, с помощью одного циркуля. Разделите отрезок на m^n равных частей со сложностью не более $m^n + (3+\epsilon_m)\log_2 m$ одним циркулем и со сложностью не более $m^n/2 + (3+\epsilon_m)\log_2 m$ циркулем и линейкой.

Из задач 15.38 и 15.34 вытекает, что в некоторых случаях использование линейки в построениях может уменьшить их сложность. Задача 15.26 показывает, что оценка задачи 15.34 иногда бывает грубой. Но в общем случае она точна по порядку, что видно из следующей задачи.

15.42**. Докажите, что для некоторой бесконечной последовательности чисел n сложность построения отрезка длины n циркулем и линейкой больше $\frac{1}{6}\frac{\log_2 n}{\log_2 \log_2 n}$.

15.43. Докажите, что сложность некоторого многочлена степени n с коэффициентами 0 и 1 больше $\frac{n}{2\log_2 n}$.

15.44***. Докажите, что число минимальных схем сложности L для вычисления произвольных многочленов от переменной x не превосходит $(L(L+1))^{L-2}/(L-2)!$

15.45***. *(Шеннон – Лупанов)* Докажите, что сложность некоторого многочлена степени n с коэффициентами 0 и 1 больше $\frac{n}{\log_2 n}\left(1 + \frac{\log_2 \log_2 n - C}{\log_2 n}\right)$, где C — некоторая константа.

Задача деления на n равных частей заданной дуги окружности циркулем и линейкой сильно отличается от задачи деления отрезка. Во-первых, она разрешима циркулем и линейкой для произвольной дуги только при $n = 2^m$.[1)] Во-вторых, покажем, что сложность ее решения в указанном случае несколько отлична от аналогичной задачи для отрезка.

[1)] Это доказал в тридцатые годы прошлого века немецкий математик Ванцель, опираясь на результаты Гаусса. Гаусс в восемнадцатилетнем возрасте полностью решил вопрос о возможности построения правильных многоугольников циркулем и линейкой, который эквивалентен делению окружности на n равных частей.

15.46*. Дуга окружности задана хордой a и радиусом r. Постройте одним циркулем одновременно центр окружности, отрезок длины $\sqrt{a^2+r^2}$ и середину данной дуги со сложностью 7.

Следующие задачи усиливают утверждения задач 15.15 – 15.16.

15.47. По данным отрезкам a и b постройте со сложностью 5 одним циркулем отрезок длины $\sqrt{a^2+b^2}$.

15.48*. По данным отрезкам a и b постройте со сложностью 11 одним циркулем одновременно отрезки длины $a+b$ и $a-b$.

В следующих задачах дуга задана вместе с ее радиусом.

15.49. Постройте со сложностью $2n+1$ циркулем и линейкой дугу, в 2^n раз меньшую данной.

15.50. Разделите со сложностью $2^{n-1}+2n$ циркулем и линейкой данную дугу на 2^n равных частей.

15.51*. Постройте со сложностью не более $5n+1$ одним циркулем дугу, в 2^n раз меньшую данной.

15.52**. Разделите со сложностью не более $2^{n-1}+4n+5$ циркулем данную дугу на 2^n равных частей при $n>2$. Разделите дугу на четыре равные части со сложностью 12.

15.53. Докажите, что нельзя разделить циркулем и линейкой данную дугу на 2^n равных частей со сложностью, меньшей 2^{n-1}.

15.54**. Докажите, что нельзя построить циркулем и линейкой дугу, равную 2^n-й части единичной окружности, со сложностью, меньшей $n-1$.

Введенное выше определение схемы вычисления числа n с помощью операций сложения и умножения легко обобщить на случай вычисления рациональных чисел с помощью всех арифметических операций, а также некоторых иррациональных чисел (далее называемых пифагоровыми), если к арифметическим операциям добавить операцию извлечения квадратного корня. Назовем **сложностью рационального числа** наименьшую длину вычисляющей его схемы *с арифметическими операциями*, а **сложностью пифагорова числа** — наименьшую длину вычисляющей его схемы *с использованием квадратного корня*. Назовем **арифметической сложностью ε - приближения произвольного действительного числа** α наименьшую сложность *рационального* числа, уклоняющегося от α не более чем на ε . **Геометрической сложностью ε - приближения числа** α назовем наименьшую сложность *пифагорова* числа, уклоняющегося от α не более чем на ε .

Следующий (и последний в этой главе) цикл задач труднее предыдущих.

15.55. Докажите, что отрезок длины α можно построить циркулем и линейкой тогда и только тогда, когда α — пифагорово число.

Как известно,[1] числа $\sqrt[3]{2}$ и $\sqrt{\pi}$ *не являются пифагоровыми,* откуда следует *неразрешимость циркулем и линейкой задач удвоения куба и квадратуры круга.* Изобретаемые иногда и до сих пор решения этих задач являются на самом деле лишь приближенными. В связи с этим введем следующее определение. **Сложностью ε-приближения числа α циркулем и линейкой** назовем наименьшую сложность построения отрезка, длина которого отличается от величины α не более чем на ε .

15.56***. Докажите, что сложность ε-приближения $\sqrt[3]{2}$ (как арифметическая, так и геометрическая) не превосходит величины $4\log_2\log_2 1/\varepsilon+4$, а сложность ε -приближения $\sqrt[3]{2}$ циркулем и линейкой не превосходит:

а) $6\log_2\log_2 1/\varepsilon+8$;

б) $9\log_3\log_3 1/\varepsilon+5$.

15.57***. *(J.M. Borwein, P.B.Borwein)* Докажите, что сложность ε-приближения $\sqrt{\pi}$ циркулем и линейкой не превосходят $C\log_2\log_2 1/\varepsilon$, где C — некоторая константа.

15.58***. Докажите, что арифметическая сложность ε-приближения $\sqrt[3]{2}$ и $\sqrt{\pi}$ больше $\log_2\log_2 1/\varepsilon - C$, где C — некоторая константа.

УКАЗАНИЯ

15.1. Проведите окружность с центром в конце данного диаметра и радиусом x и окружность того же радиуса с центром в точке пересечения первой окружности с заданной в условии окружностью и рассмотрите точку пересечения второй построенной окружности с заданным диаметром заданной окружности. Воспользуйтесь подобием треугольников.

15.2. Воспользуйтесь указанием 15.1, но проведите две окружности радиуса x с центрами в обеих точках пересечения первой окружности с заданной и заметьте, что точка пересечения этих окружностей совпадает с точкой, построенной в указании 15.1.

15.3. Проведите окружность радиуса x с центром в конце данного отрезка длины x и с центром в точке пересечения этой окружности с заданной единичной окружностью и постройте еще одну единичную окружность. Рассмотрите точку пересечения этой окружности с данным отрезком.

15.4. Проведите окружности радиуса a с центрами в концах данного отрезка длины c и с центром в точке пересечения этих окружностей проведите окружность радиуса b. Две подходящие точки пересечения этой окружности с двумя предыдущими задают нужный отрезок. Для доказательства найдите на чертеже два равных равнобедренных треугольника, а потом два подобных равнобедренных треугольника.

15.5. Примените задачу 15.4.

---

[1] первое из этих утверждений, а также неразрешимость трисекции угла, доказал Ванцель. Второе утверждение является легким следствием трансцендентности числа π, доказанной в восьмидесятые годы прошлого века немецким математиком Линдеманом.

15.6. Проведите две единичные окружности с единичным расстоянием между центрами, а потом с центром в одной из точек их пересечения проведите окружность, проходящую через вторую точку пересечения. Рассмотрите центры единичных окружностей и точки пересечения их с третьей построенной окружностью.

15.7. Примените 15.6 и 15.3.

15.8. а) Пусть AB — единичный отрезок, лежащий на данной прямой. С помощью единичной окружности с центром A построим на этой прямой отрезок CB длины 2, а с помощью окружности с центром B и радиусом 2 построим на этой прямой отрезок AD длины 3. Проведем окружность с центром D и радиусом $AD = 3$ до пересечения в точке E с упомянутой единичной окружностью, а потом проведем единичную окружность с центром E до пересечения в точке F с отрезком AB. Согласно 15.3 отрезок AF имеет длину $1/3$. Остается провести окружность с центром F и радиусом AF.

б) Примените задачи 15.7 и 15.3.

в) Примените задачу 15.4.

15.9. Поделите пополам и примените 15.1.

15.10. Постройте окружности с центрами в концах отрезка радиусами, равными его длине, через точки их пересечения проведите прямую, которая разделит отрезок пополам, проведите радиусом, равным половине отрезка, окружность, концентрическую к одной из построенных, до пересечения с отрезком, соединяющим ее центр с одной из ранее построенных точек пересечения, и соедините со второй из упомянутых точек только что построенную точку. Полученный отрезок делит данный отрезок в отношении $1:2$. Осталось провести окружности радиусами в третью и в шестую часть данного отрезка с центрами в его середине.

15.11. Пусть A — данная точка, а BC — данная прямая. Проведите окружности с центрами A и C и радиусами BC и AB соответственно и прямую через точку их пересечения и точку A.

15.12. Примените 15.11 и теорему Фалеса об отрезках, высекаемых на сторонах угла параллельными прямыми.

15.13. С помощью 15.7 постройте отрезок длины $2a$ вместе с его серединой, проведите окружности с центрами в его концах и радиусом b, и точки их пересечения соедините прямой.

15.14. С помощью 15.7 постройте отрезок длины $\sqrt{3}a$ и примените задачу 15.13 при $b = \sqrt{3}a$.

15.15. Примените 15.14 и постройте $\sqrt{2}a$, потом 15.13 и постройте $\sqrt{a^2 - b^2}$, и еще раз 15.13 при $b = \sqrt{2}a$ и $c = \sqrt{a^2 - b^2}$.

15.16. Примените 15.15 и 15.14.

15.17. Пусть на прямой даны отрезки AB и CD длиной a и b соответственно. Проведите окружности с центром A и радиусом AD и BC.

15.18. Обозначим координаты концов данных отрезков 1 и $1 - a$ (за начало координат на прямой, содержащей эти отрезки, берем второй конец единичного отрезка). Строим с помощью 15.17 точку $2 - a$, затем с помощью 15.3 точку $1/(2 - a)$ и, наконец, с центром в ней и тем же радиусом $1/(2 - a)$ окружность до пересечения с ранее построенной единичной окружностью с центром в точке 0. Отрезки, соединяющие эту точку с точками 1 и $1 - a$, равны $\sqrt{a}$.

В случае $a > 1$ примените теорему о произведении секущей на ее внешнюю часть, свойство перпендикулярности касательной к радиусу, проведенному в точку касания, свойство вписанного угла, опирающегося на диаметр, и задачу 15.7.

15.19. Алгебраический метод решения задач на построение сводит любую из них к построению по данным отрезкам a и b отрезков $a \circ b$, где $\circ = \pm, \cdot, /$, и отрезка $\sqrt{a}$. Эти задачи решаются с помощью 15.16, 15.4 и 15.18. Необходимое перед применением последних задач масштабирование осуществляется многократным применением 15.6 и 15.7.

15.20. Примените 15.7, затем n раз 15.1 или 15.2.

15.21. Поделите отрезок пополам с помощью 15.6, а потом, используя в первом случае окружность единичного радиуса, а во втором — единичного диаметра, проходящие через середину отрезка, примените 15.20. Во втором случае для деления пополам половины отрезка примените 15.3, воспользовавшись уже построенными окружностями. Построив концентричный с данным отрезок, имеющий в $k/2$ раз меньшую длину (где $k = 2^m$) и проводя $k/2-2$ окружностей с центрами в середине этого отрезка, разделите его на k равных частей. Обратите внимание, что часть окружностей проводить не нужно, так как они были построены ранее при применении 15.20.

15.22. Для деления на восемь частей примените 15.21, но при делении отрезка пополам воспользуйтесь 15.9. После этого, воспользовавшись одной построенной окружностью, примените 15.3 для построения 1/16 отрезка. Можно сэкономить одну окружность, не доводя до конца построение 1/8 отрезка, так как после проведения окружностей с центром середине отрезка и радиусами в $1/16,\ 2/16, \ldots, 7/16$ его длины отрезок делится на 16 равных частей. Заметьте, что окружность радиусом $4/16 = 1/4$ уже проведена ранее и ее можно не считать.

15.23. При логарифмировании мультипликативная цепочка превращается в аддитивную.

15.24. Представьте n в двоичной записи:

$$n = \sum_{i=0}^{m} \alpha_i 2^i,$$

где $\alpha_i = 0$ или 1, $m = [\log_2 n]$. Разбейте набор $(\alpha_0, \ldots, \alpha_m)$ не более чем на $]\frac{m+1}{k}[$ блоков $A_0, \ldots, A_s$, $s <]\frac{m+1}{k}[$, каждый из которых, кроме последнего, начинается с 1, состоит из подряд идущих цифр и последняя единица в нем отстоит от первой не более чем на $k-1$ позицию, а последний блок состоит ровно из k цифр (несколько подряд идущих нулей, возможно стоящих в начале, не входят ни в один из рассматриваемых блоков). Числа, двоичными записями которых являются эти блоки, не превосходят $2^k - 1$ и, кроме, возможно, последнего, нечетны. Пусть эти числа суть $a_0, \ldots, a_s$. Тогда n можно представить в виде

$$n = 2^{l_0}\left(2^{l_1}\ldots\left(2^{l_{s-2}}\left(2^{l_{s-1}}\left(2^{l_s}a_s + a_{s-1}\right) + a_{s-2}\right) + \ldots + a_1\right) + a_0\right),$$

где $l_s + l_{s-1} + \ldots + l_0 = m + 1 - k$. Все числа $a_0, \ldots, a_{s-1}$ содержатся в аддитивной цепочке $1, 2, 3, 5, 7, \ldots, 2^k - 1$ длины $2^{k-1}+1$. Поэтому для вычисления n достаточно добавить к ней последовательность

$$a_s, 2a_s, 4a_s, \ldots, 2^{l_s}a_s, 2^{l_s}a_s + a_{s-1},$$

$$2\left(2^{l_s}a_s + a_{s-1}\right), 4\left(2^{l_s}a_s + a_{s-1}\right), \ldots,$$

$$2^{l_{s-1}}\left(2^{l_s}a_s + a_{s-1}\right), 2^{l_{s-1}}\left(2^{l_s}a_s + a_{s-1}\right) + a_{s-2}, \ldots,$$

$$2^{l_{s-2}}\left(2^{l_{s-1}}\left(2^{l_s}a_s + a_{s-1}\right) + a_{s-2}\right),$$

$$2^{l_1}\left(\ldots 2^{l_{s-2}}\left(2^{l_{s-1}}\left(2^{l_s}a_s+a_{s-1}\right)+a_{s-2}\right)+\ldots+a_1\right)+a_0,\ldots,$$

$$2^{l_0}\left(2^{l_1}\left(\ldots 2^{l_{s-2}}\left(2^{l_{s-1}}\left(2^{l_s}a_s+a_{s-1}\right)+a_{s-2}\right)+\ldots+a_1\right)+a_0\right),$$

длина которой равна

$$l_s+l_{s-1}+\ldots+l_0+s+1=m+2+s-k.$$

Поэтому

$$l(n)<2^{k-1}+1+m+2+s-k<m+2+\left]\frac{m+1}{k}\right[+2^{k-1}-k.$$

Можно считать, что $n\neq 2^m$, тогда $m+1=]\log_2 n[$ и

$$l(n)<]\log_2 n[(1+1/k)+2^{k-1}-k+2.$$

15.25. Воспользуйтесь 15.24 при $k=[\log_2\log_2 n-2\log_2\log_2\log_2 n]$.

15.26. Примените 15.25, 15.2, 15.5.

15.27. Постройте на прямой точки с координатами

$$1,2,\ldots,n-1,n,2n,\ldots,(n-1)n,n^2$$

со сложностью $2n-2$ циркулем и линейкой и со сложностью $4n-1$ одним циркулем с помощью 15.6 и 15.17. Расстояния между построенными точками реализуют все числа от 1 до n^2, так как расстояние $an+b$ реализуется между точками $(a+1)n$ и $n-b$.

15.28. Постройте единичные окружности с центрами в точках A и B — концах единичного отрезка, потом окружность радиуса x с центром в B до пересечения в точке C с единичной окружностью с центром A, потом единичную окружность с центром C. Пересекая две построенные единичные окружности, проходящие через A, окружностью с центром A и радиусом x, получите согласно 15.4 отрезок длины x^2. Повторяя это построение с помощью окружности радиуса x^2, получите отрезок длины x^3 и т.д., пока не построите отрезок длины x^n. Далее, повторяя проведенное построение с x^n вместо x, постройте отрезки длины $x^{2n},\ldots,x^{(n-1)n}$ и проведите такими радиусами окружности с центром B до пересечения с единичной окружностью с центром B в точках $C_2,\ldots,C_{n-1}$ соответственно. Потом проведите единичные окружности с центрами в $C_2,\ldots,C_{n-1}$ (окружность с центром в точке C_1, такой, что $|BC_1|=x^n$, уже построена ранее). Применяя 15.4, заметьте, что окружность с центром в A и радиусом x^a при пересечении с единичными окружностями с центрами B и C дает отрезок длины x^{a+nb}.

15.29. Примените метод построения мультипликативных цепочек 15.25, предварительно построив с помощью задачи 15.28 со сложностью $4\cdot 2^{k/2}$ все отрезки с длинами $1/2,1/4,\ldots,2^{2^{-k}}$, и выполняя возведение в квадрат и умножение со сложностью 2 с помощью 15.2 и 15.4. Потом положите $k=2[\log_2\log_2 n-2\log_2\log_2\log_2 n]$.

15.30. С помощью 15.7 постройте середину A данного отрезка, потом со сложностью 5 постройте циркулем точки B и C, такие, что AB и AC равны данному отрезку, а BC — вдвое меньше его, и окружности с центрами в B и C, проходящие через A. Окружность, построенная на данном отрезке, как на

диаметре, в пересечении с окружностями B и C согласно 15.4 дает отрезок вчетверо меньший данного. Проведя радиусом, равным построенному отрезку, окружность с центром A, аналогично построим отрезок в восемь раз меньший данного, и т.д. Построив таким образом n окружностей, получим отрезок в 2^n раз меньший данного. Для разделения данного отрезка на 2^n равных частей остается провести $2^{n-1}-n$ окружностей с центром в A (так как n окружностей уже проведены). Радиусы их определяются "бесплатно" с помощью уже проведенных окружностей.

15.31. Решение этой задачи основано на идеях О.Б.Лупанова. Представим полином $p(x)$ в виде

$$\sum_{i=0}^{s} p_i(x)\, x^{k^2},$$

где $s = \rfloor n/k^2 \lfloor - 1$, $p_i(x)$ — полиномы степени k^2-1,

$$p_i(x) = \sum_{j=0}^{k-1} p_{ij}(x)\, x^{kj},$$

$p_{ij}(x)$ — полиномы степени $k-1$. Так как среди полиномов $p_{ij}(x)$ не более 2^k различных, и каждый из них представим в виде суммы некоторых слагаемых из списка $1, x, \ldots, x^{k-1}$, то для вычисления всех этих полиномов достаточно 2^k-3 операций. Для вычисления всех полиномов $p_{ij}(x)\, x^{kj}$ нужно еще не более $(2^k-1)(k-1)+1$ умножений. После этого для вычисления всех полиномов $p_i(x)$ достаточно $\rfloor n/k^2 \lfloor (k-1)$ сложений. Остается вычислить $p(x)$ по схеме Горнера

$$p(x) = \Big(\ldots\Big(p_s(x)\, x^{k^2} + p_{s-1}(x)\Big)\, x^{k^2} + \ldots + p_1(x)\Big)\, x^{k^2} + p_0(x),$$

затратив на это $2s+1$ операцию и положить $k = [\log_2 n - 3\log_2 \log_2 n]$. Заметим, что основная сложность приходится на операции сложения — их приблизительно n/k, а операций умножения не более $2^k k + n/k^2$.

15.32. Представьте n в двоичной записи:

$$n = \sum_{i=0}^{m} \alpha_i 2^i,$$

где $\alpha_i = 0$ или 1, $m = [\log_2 n]$, заметьте, что $n = p(2)$, где

$$p(x) = \sum_{i=0}^{m} \alpha_i x^i,$$

и примените 15.31.

15.33. Примените 15.3, 15.32 и замечание в конце указания к 15.31.

15.34. Примените 15.31 и 15.32 при четном k. Для построения системы отрезков $p_{ij}(2)\, 2^{kj}$ постройте с помощью 15.27 $a = 2\cdot 2^{k/2} - 2$ точек на прямой, расположенных на отрезке от 1 до 2^k, попарные расстояния между которыми реализуют все числа от 1 до 2^k-1, потом еще a точек, попарные расстояния между которыми реализуют числа $2^k, 2\cdot 2^k, \ldots, (2^k-1)\cdot 2^k$ (растянув с помощью подобия с коэффициентом 2^k ранее построенную систему), и т. д., и, наконец, систему из a точек, реализующую расстояния $2^{(k-1)k}, 2\cdot 2^{(k-1)k}, \ldots, (2^k-1)\, 2^{(k-1)k}$. Сложность построения всех систем вместе не превосходит $2k\cdot(2^{k/2}-1)$

После этого со сложностью $]n/k^2[(k-1)$ строятся все отрезки с длинами $p_i(2)$. И, наконец, с помощью 15.12 и схемы Горнера, приведенной в указании к 15.31, строится отрезок длины n со сложностью, не превосходящей $4n/k^2+3$. Полная оценка сложности этого построения имеет вид $n/k+3n/k^2+2k\cdot 2^{k/2}$. Остается выбрать $k=2[\log_2 n-3\log_2\log_2 n]$.

15.35. В случае четного n разделите отрезок пополам, применяя 15.34, постройте отрезок в n раз меньшей длины, и последовательно проводя окружности с центром в середине данного отрезка, разделите его на n равных частей. В случае нечетного n действуйте аналогично, только вначале стройте отрезок в $2n$ раз меньшей длины.

15.36. Через каждую из $n-1$ точек деления проходит хотя бы одна из линий построения, поэтому этих линий не меньше $n-1$. Но на самом деле при этом подсчете некоторые окружности могут учитываться два раза, так как пересекают отрезок в двух точках. Поэтому правильная нижняя оценка имеет вид $](n-1)/2[$.

15.37. Согласно 15.3, достаточно построить отрезок длины n. Представьте n в троичной записи:

$$n=\sum_{i=0}^{m}\alpha_i 3^i,$$

где $\alpha_i=0,1$ или 2, $m=[\log_3 n]$. Разбейте набор $(\alpha_0,\ldots,\alpha_m)$ не более чем на $]\frac{m+1}{k}[$ блоков $A_0,\ldots,A_s$, $s<]\frac{m+1}{k}[$, длины не более k каждый. Числа, троичными записями которых являются эти блоки, не превосходят 3^k-1. Пусть эти числа суть $a_0,\ldots,a_s$. Тогда n можно представить в виде

$$n=3^{l_0}+\left(3^{l_1}\ldots\left(3^{l_{s-2}}\left(3^{l_{s-1}}\left(3^{l_s}a_s+a_{s-1}\right)+a_{s-2}\right)+\ldots+a_1\right)+a_0\right),$$

где $l_s+l_{s-1}+\ldots+l_0=m+1-k$. С помощью 15.27 со сложностью не более $4\cdot 3^{k/2}-1$ одним циркулем постройте все отрезки с длинами $a_0,\ldots,a_s$ (k считаем четным). Потом, применяя 15.7 и 15.17, постройте отрезок длины n со сложностью не более

$$3(l_s+l_{s-1}+\ldots+l_0)+2s<3m+6-3k+2m/k.$$

Поэтому полная сложность построения отрезка n не превосходит

$$3m+5-3k+2m/k+4\cdot 3^{k/2}.$$

Остается выбрать $k=2[\log_3 m-2\log_3\log_3 m]$.

15.38. Докажите по индукции следующую лемму. Пусть множество M_n, состоящее из окружностей и точек их пересечения, получается из множества M_{n-1} добавлением некоторой окружности с центром в одной из точек M_{n-1} и радиусом, равным некоторому отрезку с концами из M_{n-1} , и точек пересечения ее с окружностями из M_{n-1} , а множество M_0 состоит из двух точек на расстоянии 1. Обозначим D_n максимальное расстояние между точками из M_n. Тогда

$$D_n<D_{n-2}+\ldots+2D_0,\ D_0=1,\ D_1=1,\ D_2=\sqrt{3}.$$

База индукции ($n=0,1,2$) проверяется непосредственно. Для доказательства индукционного перехода обозначаем $x_0,x_1,\ldots,x_{n-1}$ центры окружностей, которые

использовались в построении точек $M_1, \ldots, M_n$. Для произвольной точки y из M_n рассмотрим последовательность точек $x_{n_1}, \ldots, x_{n_1}$, где

$$n-2 > n_1 > n_1 - 1 > n_2 > \ldots > n_{k-1} - 1 > n_k,$$

и точку $x = x_0$ или x_1, такую, что точка x лежит на окружности с центром x_{n_1}, точка x_{n_1} — на окружности с центром $x_{n_2}, \ldots$, точка $x_{n_{k-1}}$ — на окружности с центром x_{n_k} (ведь точка x_{n_i} при $i < k$ лежит на пересечении двух окружностей с центрами в точках x_m, где $m < n_i$). Для другой точки y' из M_n аналогичным образом построим последовательность точек $x_{m_1}, \ldots, x_{m_s}$. Пусть p — минимальный номер, такой, что x_{n_p} лежит на окружности с центром x_{m_r}, $r > p$, а r — тоже минимальное число с этим свойством. Так как расстояние между точками x_{n_i} и $x_{n_{i+1}}$ не больше $D_{n_{i+1}}$, то, согласно неравенству треугольника, расстояние между точками y и y' не больше

$$D_{n_1} + D_{n_2} + \ldots + D_{n_p} + D_{m_1} + D_{m_2} + \ldots + D_{m_r},$$

а поэтому, согласно выбору числа p и в силу монотонности D_n, это расстояние при $m_r = n_p = k$ не больше

$$D_{n-2} + \ldots + D_{k+2} + 2D_k,$$

и при $k = m_r > n_p$ не больше

$$D_{n-2} + \ldots + D_k.$$

Если же такого p не существует, то аналогичным образом получается оценка

$$D_{n-2} + \ldots + 2D_0.$$

Применяя предположение индукции, получите, что во всех случаях

$$D_n < D_{n-2} + \ldots + 2D_0.$$

Из доказанного неравенства индукцией выведите, что $D_n < F_{n+1}$ при $n >$ Воспользуйтесь для этого равенством

$$F_{n-1} + \ldots + 2F_1 = F_{n+1},$$

которое доказывается индукцией с помощью равенства $F_{n+1} = F_n + F_{n-1}$. Из полученного неравенства с помощью задачи из §7 выведите, что если какие-то две точки множества M_k определяют отрезок длины n, то $k > [\log_\varphi (n + 1/2)]$, где $\varphi = \left(\sqrt{5}+1\right)/2$.

15.39. Разделите отрезок пополам, с помощью 15.37 постройте отрезок длины $1/n$ и проводя окружности с центром в середине отрезка и с центром в точке, удаленной от середины на $1/n$, в случае четного n разделите его на n частей точками пересечения этих окружностей. В случае нечетного n, постройте отрезки длины $1/2n$ и $1/n$ и действуйте аналогично.

15.40. Каждая из $n-1$ точек, делящих отрезок, получается в результате пересечения хотя бы двух окружностей. Каждая из окружностей пересекает отрезок не более чем в двух точках. Если в построении использовалось m окружностей, то $2m$ не меньше числа пар "окружность и точка деления отрезка, лежащая на ней", а число таких пар не меньше $2(n-1)$, значит $m \geq n-1$.

15.41. Примените задачу 15.37 и воспользуйтесь идеями построений задач 15.30 и 15.39. Отдельно рассмотрите случай нечетного n подобно задаче 15.39.

15.42. Рассмотрите последовательности множеств M_L, определенные в начале главы и начинающиеся с множества M_0 , состоящего из концов единичного отрезка. Оцените сверху число различных множеств M_L. Если его обозначить N_L, то имеет место неравенство

$$N_L \leq N_{L-1}(L^2 - 3L + 4)((L^2 - 3L + 4)^2 - 1)/2,$$

так как количество точек в N_L по сравнению с N_{L-1} увеличилось не более чем на $2L-2$ (добавленная линия пересекается с каждой из $L-1$ ранее проведенных не более чем в двух точках), откуда по индукции получается, что точек в N_L не более L^2-L+2, а если число точек в N_{L-1} обозначить a, то число способов провести L-ю линию не больше

$$\binom{a}{2} + a\binom{a}{2} = (a^2 - 1)a/2.$$

По индукции получите с помощью этого неравенства, что

$$N_L \leq 14((L-1)!/2)^6 2^{2-L} < ((L-1)!)^6 2^{-L} < L^{6L-6}2^{-L}.$$

Выведите отсюда, что количество различных отрезков с концами в одном из N_k , $k \leq L$, не превосходит

$$L^{6L-1}2^{-L}.$$

Значит, при $n \geq 4$ и

$$L = \frac{\log_2 n}{6 \log_2 \log_2 n}$$

число отрезков, которые можно построить со сложностью не больше L, не превосходит $2^{-L}n/L < n$, т. е. найдется такое натуральное m, что отрезок длины $m \leq n$ нельзя построить со сложностью, меньшей либо равной

$$L = \frac{\log_2 n}{6 \log_2 \log_2 n}.$$

15.43. Оцените сверху число различных схем сложности L. Если его обозначить N_L, то имеет место неравенство

$$N_L \leq N_{L-1}L(L-1).$$

Далее действуйте подобно указанию 15.42.

15.44. Занумеруем произвольным образом все элементы схемы от 3 до L (номера 1 и 2 присваиваем константе 1 и переменной x). Каждому элементу i сопоставим символ $(a(i), b(i), c(i))$, где $a(i) \leq b(i)$— номера элементов схемы, над которыми выполняет операцию элемент i, а $c(i) = 1$, если эта операция сложение, или 2, если она умножение. Сопоставим каждой минимальной схеме последовательность символов $(a(i), b(i), c(i))$. Оцените число всех таких последовательностей числом $(L(L+1))^{L-2}$. Переставьте любым из $(L-2)!$ способов номера элементов схемы и заметьте, что все полученные для этих перестановок последовательности будут различны (так как в силу минимальности схемы разным ее элементам сопоставляются разные символы, то будет получено противоречие, если найти такой элемент, что при перестановке номеров он

сменил номер, а элементы, над которыми он выполняет операцию, нет). Отсюда следует оценка

$$(L(L+1))^{L-2}/(L-2)!$$

для числа различных минимальных схем сложности L.

15.45. Примените предыдущую задачу и оцените различных минимальных схем сложности не выше L как $(3L)^L$ (при этом воспользуйтесь неравенствами $n! \geq (n/3)^n$ и $(1+1/n)^n < 3$). Тогда при

$$L = \frac{n}{\log_2 n}\left(1 + \frac{\log_2 \log_2 n - C}{\log_2}\right)$$

где C - некоторая константа, числа схем "не хватает" для реализации всех 2^{n+1} многочленов степени n с коэффициентами 0 или 1.

15.46. Пусть AB - заданная хорда длины a окружности радиуса r. Тогда центр O окружности строится как пересечение окружностей радиусов r с центрами A и B. Проведите окружность с центром O и радиусом a до пересечения с упомянутыми окружностями в точках C и D. Тогда согласно теореме о сумме квадратов диагоналей параллелограмма $CB = AD = \sqrt{2a^2 + r^2}$. Постройте точку K как пересечение окружностей радиуса $\sqrt{2a^2 + r^2}$. с центрами C и D. Из теоремы Пифагора следует, что $KO = \sqrt{a^2 + r^2}$. Постройте точку L как пересечение окружностей радиуса $\sqrt{a^2 + r^2}$. с центрами C и D. Из теоремы Пифагора следует, что $LO = r$, значит L - середина дуги AB окружности радиуса r с центром O, так как $AL = BL$ в силу того, что L лежит на срединном перпендикуляре к отрезкам AB и CD.

15.47. См. указание к предыдущей задаче.

15.48. Примените 15.46 при $r = b \geq a$, потом, проведя окружность радиуса a с центром D до пересечения с такой же окружностью с центром O, получите отрезок длины $\sqrt{3}a$ как их общую хорду, далее, проведя радиусом $\sqrt{3}a$ окружности с центрами C и D, постройте их общую точку M и радиусом OM, равным $\sqrt{2}a$ по теореме Пифагора, проведите окружность с центром D до пересечения с ранее построенной окружностью с диаметром CD в точках P и R. Из теоремы Пифагора следует, что PR — диаметр последней окружности, перпендикулярный диаметру CD, значит (см. указание к предыдущей задаче), $LP = b - a, LR = b + a$.

15.49. Примените n раз школьный метод деления дуги пополам, используя одну из окружностей во всех n построениях.

15.50. Примените 15.49 и, подобно решению задачи 15.35, разделите дугу на 2^n частей, проведя $2^{n-1} - 1$ окружностей с центрами в ее середине, последовательно определяя их радиусы.

15.51. Приемом, которым решалась задача 15.46, можно поделить данную дугу пополам со сложностью 6, так как точку L можно получить пересечением этой дуги и окружности радиуса $\sqrt{a^2 + r^2}$ с центром C (или D). Далее тем же приемом поделите пополам полученную половину дуги, и т.д., причем, как и в решении 15.49, можно использовать одну из окружностей во всех n повторениях этого построения.

15.52. Вначале со сложностью 6 методом 15.46 постройте середину L заданной дуги AB окружности радиуса r с центром O, а потом параллельно перенесите весь чертеж на вектор OL, получив дугу $A'B'$ с серединой L'. При этом точка A' получается пересечением ранее построенной окружности радиуса r с центром A и окружности радиуса r с центром L, аналогично (и уже без проведения новых окружностей) строится точка B', а точка L' получается пересечением только что построенной окружности с окружностью радиуса AL с центром A'

(или B'), таким образом, общая сложность построения равна 8. Далее, дуга A'B'делится так же как в предыдущей задаче (со сложностью $5(n-1)+1$) $n-1$ раз подряд пополам, вплоть до построения дуги в 2^n раз более короткой, чем дуга AB. При этом будут построены $n-1$ концентрических окружностей с центром L и радиусами, равными хордам дуг, равных половине, четверти, ..., 2^{n-1} части дуги AB. Далее делите дугу AB на 2^n равных дуг так, как указано в решении 15.50, но учитывая, что из требуемых $2^{n-1}-1$ окружностей с центрами в L уже построены $n-2$. Чтобы поделить дугу на четыре равные части, вначале, как и в 15.51, поделите два раза пополам со сложностью 11, а потом еще одной засечкой циркуля постройте третью точку деления.

15.53. Каждую из 2^n-1 точек деления можно получить лишь в результате пересечения данной дуги с какой-то окружностью. Но так как любая окружность пересекается с нашей дугой не более чем двух точках, то для построения нужных нам точек требуется не менее 2^{n-1}, окружностей.

15.54. Докажем, что число проведенных в этом построении линий не меньше $n-1$. Для этого рассмотрим определенную в начале параграфа последовательность множеств M_n и обозначим F_n минимальное комплексное числовое поле, содержащее все точки из M_n . Если M_{n+1} получается из M_n присоединением линии и точек ее пересечения с ранее проведенными линиями, то или F_{n+1} получается из F_n присоединением квадратного корня из какого-то элемента из F_n , не являющегося квадратом в поле F_n , или $F_{n+1}=F_n$. В справедливости этого утверждения легко убедиться, вычисляя координаты точек пересечения прямых и окружностей с помощью формул аналитической геометрии. Очевидно, F_1 - поле рациональных чисел. *Степенью поля F над подполем K, содержащимся в F,* называется максимальное число элементов $a_1,\dots,a_m$ поля F таких, что для любого набора $\alpha_1,\dots,\alpha_m$ элементов поля K, в котором есть ненулевые числа, сумма $\alpha_1a_1+\dots+\alpha_ma_m$ не равна нулю. По индукции докажите, что степень поля F_k над полем рациональных чисел равна 2^l , где l не превосходит числа окружностей в последовательности $M_1,\dots,M_k$. Минимальное поле F, содержащее число $e^{\pi i2^{1-n}}$, имеет степень над полем рациональных чисел 2^{n-1}. Поэтому $l\geq n-1$, если множество M_k содержит точку

$$e^{\pi i2^{1-n}}=i\sin\pi2^{1-n}+\cos\pi2^{1-n}.$$

15.55. Примените 15.4, 15.18, 15.48 и рассуждения из указания к предыдущей задаче.

15.56. Рассмотрите последовательность

$$x_0=3/2, x_{n+1}=2(x_n+x_n^{-2})/3.$$

Положим

$$\delta_n=(x_n^3-2)/3x_n^2,$$

тогда

$$\delta_n<x_n>0, x_n-\delta_n=x_{n+1},$$

и, рассуждая по индукции, получим, что

$$x_n^3-2=3x_n^2\delta_n, \varepsilon_{n+1}=x_{n+1}^3-2=(x_n-\delta_n)^3-2=3x_n\delta_n^2-\delta_n^3=$$

$$=\varepsilon_n^2(3x_n-\delta_n)/9x_n^4>0, \delta_{n+1}\geq 0, \varepsilon_{n+1}<\varepsilon_n^2/3x_n^3<\varepsilon_n^2/6.$$

Непосредственно проверяется, что

$$\varepsilon_2<0,005,$$

откуда следует, что

$$\varepsilon_{n+2} < 6 \cdot (5/6000)^{2^n} < 2^{-2^{n+3}}, 0 < x_{n+2} - 2^{1/3} < \varepsilon_{n+2} 3^{-1} 4^{-1/3} < 2^{-2^{n+3}}.$$

Так же непосредственно проверяется, что неравенство

$$0 < x_n - 2^{1/3} < 2^{-2^{n+1}}$$

верно при любом $n \geq 0$.

Подготовив число $2/3$ заранее, $(n+1)$-й член последовательности можно вычислить по n-у члену со сложностью 4, а циркулем и линейкой построить со сложностью 6. Для этого используйте 15.1, 15.3, 15.5, заранее построив точки с координатами $0, 2/3, 1$ на оси абсцисс, и проведя единичные окружности с этими центрами. Имея точку с абсциссой x_n, постройте точку x_n^{-1}, потом x_n^{-2}, и проведя окружность радиусом x_n^{-2}, с центром 0 постройте точку $-x_n^{-2}$, которая вместе с точкой x_n ограничивает отрезок длины $x_n^{-2} + x_n$. С центром в точке пересечения единичных окружностей с центрами 0 и $2/3$ проведите окружность радиусом $x_n^{-2} + x_n$. Согласно 15.5 она пересекает эти окружности в четырех точках, две из которых ограничивают отрезок длины $x_{n+1} = 2(x_n^{-2} + x_n)/3$. Проведя окружность этим радиусом с центром 0, получите точки $\pm x^{n+1}$ на оси абсцисс. Рассуждая по индукции, можно считать, что и в начале у нас были обе точки $\pm x^n$, так что точку $-x_n^{-2}$ можно не строить. Для обоснования базы индукции постройте со сложностью 9 упомянутые выше единичные окружности и точки с координатами $3/2$ и $-3/2$. Для этого проведите ось абсцисс, единичные окружности с центрами $0, 1, 2$, общую хорду последних двух, окружности радиусом $3/2$ с центрами в точках 0 и $3/2$, применяя 15.3 постройте точку $2/3$ и единичную окружность с ней в центре. Сложность построения отрезка длины x_n в результате будет равна $6n + 8$ (последнюю окружность радиуса x_n можно не проводить). Выбрав n так, чтобы

$$2^{-2^{n+1}} < \varepsilon \leq 2^{-2^n},$$

получаем, что при $\varepsilon \leq 1/4$ и $n = [\log_2 \log_2 1/\varepsilon]$ справедлива оценка

$$0 < x_n - 2^{1/3} < 2^{-2^{n+1}} < \varepsilon,$$

значит, ε-приближение к числу $2^{1/3}$ можно построить со сложностью не выше

$$8 + 6\lfloor \log_2 \log_2 1/\varepsilon \rfloor.$$

Для доказательства неравенства б) рассмотрим последовательность

$$x_0 = 3/2, x_{n+1} = x_n/2 + 3/(2(x_n^{-1} + x_n^2)).$$

Положим

$$\delta_n = (x_n^3 - 2)/(2x_n^2 + 2x_n^{-1}),$$

тогда, замечая, что

$$x_n - \delta_n = x_{n+1}, \delta_n < x_n \geq 0$$

и, рассуждая по индукции, получаем

$$x_n^3 - 2 = 2x_n^2\delta_n + 2\delta_n/x_n, \varepsilon_{n+1} = x_{n+1}^3 - 2 = (x_n - \delta_n)^3 - 2 =$$

$$= -x_n^2\delta_n + 2\delta_n/x_n + 3x_n\delta_n^2 - \delta_n^3 = \delta_n(2x_n^{-1} - x_n^2) + 3x_n\delta_n^2 - \delta_n^3 =$$

$$= \delta_n(-2x_n\delta_n - 2\delta_n/x_n^2) + 3x_n\delta_n^2 - \delta_n^3 = \delta_n^2(x_n - 2/x_n^2) - \delta_n^3 =$$

$$= \delta_n^2(2\delta_n + 2\delta_n x_n^{-3}) - \delta_n^3 = \delta_n^3(1 + 2x_n^{-3}) =$$

$$= \varepsilon_n^3(1 + 2x_n^{-3})\left(2x_n^2 + 2x_n^{-1}\right)^{-3} \geq 0, \delta_{n+1} \geq 0, \varepsilon_{n+1} < \varepsilon_{n+1}^3/54.$$

Непосредственно проверяется, что $\varepsilon_1 < 0,021$, откуда имеем

$$0 < x_{n+1} - 2^{1/3} < 3^{-1}4^{-1/3}\varepsilon_{n+1} < 3^{-1}4^{-1/3}\sqrt{54}(\varepsilon_1/\sqrt{54})^{3^n} < 3^{-5\cdot 3^n}.$$

Выбрав n так, чтобы $3^{-5\cdot 3^n}\varepsilon \leq 3^{-5\cdot 3^{n-1}}$, получаем, что при $\varepsilon \leq 1/27$ и $n = [\log_3 \log_3 1/\varepsilon]$ справедлива оценка

$$0 < x_n - 2^{1/3} < 3^{-5\cdot 3^n}\varepsilon.$$

Сначала, используя 15.1, 15.3, 15.5, построим точки с координатами $0, -1, 3/2$ на оси абсцисс и проведем единичные окружности с центрами 0 и -1. Имея точку с абсциссой x_n, построим точку x_n^{-1}, проведя вначале окружность с центром x_n и радиусом x^n. Потом, проведя окружность с центром 0 и радиусом x_n, и прямую через ее точки пересечения с предыдущей окружностью, построим точку $x_n/2$. Проведем окружность радиусом x_n и центром в точке пересечения единичной окружности с центром -1 и окружности с центром 0 и радиусом x_n. Построенная окружность пересекается с осью абсцисс в точке $-x_n^2$. С помощью отрезков длины $y_n = x_n^2 + x_n^{-1}$ и $3/2$ построим методом 15.4 со сложностью 3 отрезок длины $z_n = 3/2y_n$. Проведя окружность радиусом z_n с центром в $x_n/2$, построим, наконец, точку $x_{n+1} = x_n/2 + z_n$. Общая сложность построения x_{n+1} по данному x_n равна 9, откуда, применяя индукцию, выводим, что точку x_n можно построить со сложностью $5 + 9n$.

15.57. Воспользуйтесь алгоритмом J.M. Borwein, P.B.Borwein: пусть

$$x_0 = 6 - 4\sqrt{2}, y_0 = \sqrt{2} - 1, y_{n+1} = \left(1 - (1 - y_n^4)^{1/4}\right) / \left(1 + (1 - y_n^4)^{1/4}\right),$$

$$x_{n+1} = (1 + y_{n+1})^4 x_n - 2^{2n+3} y_{n+1}(1 + y_{n+1} + y_{n+1}^2),$$

тогда

$$0 < x_n - 1/\pi < 16 \cdot 4^n \cdot e^{-2\pi \cdot 4^n}.$$

Следовательно, последовательность точек $(x_0, y_0), \ldots, (x_n, y_n)$ можно построить со сложностью $O(n)$.

15.58. Определим по индукции понятие *арифметической формулы глубины* D. Формулой глубины 0 назовем константу 1. Если Φ_i уже определенные формулы глубины D_i, то $\Phi = (\Phi_1 \circ \Phi_2)$ при любой арифметической операции называется формулой глубины $max\{D_1, D_2\}$. *Сложностью формулы* назовем число единиц в ней, причем "верхние" единицы в "подформулах" вида $1/\Phi$ не будем учитывать. Проверьте, что арифметическая сложность любого числа не меньше наименьшей глубины вычисляющей его формулы. Докажите по индукции, что сложность формулы не превосходит 2^D, где D — ее глубина. Пусть p/q — несократимая рациональная дробь, вычисляемая этой формулой. Тогда из задачи 13.22 следует, что

$$q \leq F_{2^D+1},$$

где F_n — последовательность Фибоначчи. Поэтому при $q \geq 4$

$$D \geq \log_2 \log_2 q.$$

Пусть

$$|p/q - 2^{1/3}| \le \varepsilon \le 1/4096,$$

тогда

$$\varepsilon \ge |p/q - 2^{1/3}| = \frac{|p^3 - 2q^3|}{q^3((p/q)^2 + 2^{1/3}p/q + 4^{1/3})} \ge 1/8q^3,$$

$$D \ge \log_2 \log_2 q \ge \log_2 \log_2 (2^{-1}\varepsilon^{-1/3}) \ge \log^2 \log^2 1/\varepsilon - 2.$$

Утверждение о числе $\sqrt{\pi}$ доказывается точно так же, если воспользоваться известной теоремой Миньотта о том, что

$$|\pi - p/q| \ge q^{-20,6}, q > 1.$$

§ 16. РАСПРЕДЕЛЕНИЕ ЗНАЧЕНИЙ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Рассмотрим некоторую последовательность действительных чисел $x_1, \ldots, x_n, \ldots$ и построим соответствующую ей последовательность дробных частей

$$\{x_1\}, \ldots, \{x_n\}, \ldots .$$

Обозначим через $F(N, \alpha, \beta)$ — количество членов этой последовательности таких, что $\alpha \le \{x_n\} < \beta$ и $n \le N$, где $0 \le \alpha < \beta \le 1$.

Положим

$$D(N) = \sup_{0 \le \alpha < \beta \le 1} |F(N, \alpha, \beta)/N - (\beta - \alpha)|.$$

Величина $D(N)$ называется **отклонением** первых N членов последовательности $\{x_n\}$.

Будем говорить, что последовательность $\{x_n\}$ **равномерно распределена по модулю, равному единице** (сокращенно р.р. (mod 1) или просто р.р.), если $\lim\limits_{N \to \infty} D(N) = 0$. В решении задач этого параграфа часто будет использоваться следующая теорема, которая называется *критерием Г.Вейля* равномерной распределенности последовательности по модулю, равному единице.

Теорема. *Следующие утверждения эквивалентны:*

(i) последовательность $\{x_n\}$ *р.р.* (mod 1);

(ii) при любых фиксированных α *и* β, $0 \le \alpha < \beta \le 1$, *имеет место соотношение* $\lim\limits_{N \to \infty} F(N, \alpha, \beta)/N = \beta - \alpha$.

(iii) для любой интегрируемой по Риману функции $f(x)$, *определенной на отрезке* $[0, 1]$, *справедливо соотношение*

$$\lim_{N \to \infty} N^{-1} \sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)\, dx.$$

(iv) для любой непрерывной на отрезке $[0,1]$ *функции* $f(x)$ *справедливо равенство*

$$\lim_{N\to\infty} N^{-1}\sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)\,dx.$$

(v) при любом целом $m \neq 0$ *имеет место равенство*

$$\lim_{N\to\infty} N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n} = 0,$$

где величина e^{ix}, *по определению, равна* $\cos x + i\sin x$, *а* i — *мнимая единица.*

Приведем новый вариант доказательства этой классической теоремы. Докажем, что выполняется цепочка следствий

$$(i) \to (ii) \to (iii) \to (iv) \to (v) \to (i).$$

Следствия $(i) \to (ii)$ и $(iii) \to (iv) \to (v)$ очевидны. Докажем, что $(ii) \to (iii)$. Определим функцию $g(x)$, периодическую с периодом 1, равенством

$$g(x) = \begin{cases} 1, & \text{если} \quad \alpha \le x < \beta, \\ 0 & \text{— в противном случае.} \end{cases}$$

Тогда утверждение (ii) можно представить в виде

$$\lim_{N\to\infty} N^{-1}\sum_{n=1}^{N} g(x_n) = \int_0^1 g(x)\,dx.$$

Заметим, что если последнее равенство выполняется для нескольких функций $g_1(x), \ldots, g_k(x)$, то оно выполняется для любой их линейной комбинации $c_1 g_1(x) + \ldots + c_k g_k(x)$. Поэтому это равенство имеет место для любой кусочно-постоянной функции.

Возьмем теперь любую интегрируемую по Риману функцию $f(x)$, определенную на отрезке $[0,1]$. Тогда для всякого $\varepsilon > 0$ существует такое разбиение $T: 0 = x_0 < \ldots < x_r = 1$ отрезка $[0,1]$, что выполняются неравенства

$$s(T) \le \int_0^1 f(x)\,dx \le S(T), \quad S(T) - s(T) < \epsilon/3,$$

где

$$s(T)=\sum_{t=1}^{r} m_t \Delta x_t, \quad S(T)=\sum_{t=1}^{r} M_t \Delta x_t, \quad m_t=\inf_{x\in[x_{t-1},x_t)} f(x),$$

$$M_t=\sup_{x\in[x_{t-1},x_t)} f(x), \quad \Delta x_t = x_t - x_{t-1}.$$

Суммы Дарбу $s(T)$ и $S(T)$ можно также представить в виде

$$s(T)=\int_0^1 h(x)dx, \quad S(T)=\int_0^1 H(x)dx,$$

где $h(x)=m_t$ и $H(x)=M_t$, если $x\in[x_{t-1},x_t), t=1,...,r$. Так как $h(x)$ и $H(x)$ кусочно-постоянные функции, то существует такое число N_0, что для всех $N>N_0$ выполняются неравенства

$$\left| N^{-1}\sum_{n=1}^{N} h(x_n) - \int_0^1 h(x)\,dx \right| < \epsilon/3,$$

$$\left| N^{-1}\sum_{n=1}^{N} H(x_n) - \int_0^1 H(x)\,dx \right| < \epsilon/3.$$

Следовательно, имеем

$$s(T)-\epsilon/3 < N^{-1}\sum_{n=1}^{N} h(x_n) \le N^{-1}\sum_{n=1}^{N} H(x_n) < S(T)+\epsilon/3.$$

Поскольку для всех $x\in[0,1]$ выполняются следующие неравенства $h(x)\le f(x)\le H(x)$, будем иметь

$$N^{-1}\sum_{n=1}^{N} h(x_n) \le N^{-1}\sum_{n=1}^{N} f(x_n) \le N^{-1}\sum_{n=1}^{N} H(x_n).$$

Поэтому из предыдущего неравенства следует, что

$$s(T)-\epsilon/3 < N^{-1}\sum_{n=1}^{N} f(x_n) < S(T)+\epsilon/3.$$

Учитывая также неравенства между суммами Дарбу и интегралом от $f(x)$, выводим отсюда неравенство

$$\left| N^{-1}\sum_{n=1}^{N} f(x_n) - \int_0^1 f(x)dx \right| < S(T)-s(T)+2\epsilon/3 < \epsilon.$$

Это и означает, что утверждение (*iii*) доказано.

Труднее доказывается, что $(v) \to (i)$. Сначала заметим, что

$$F(N, \alpha, \beta) = \sum_{n=1}^{N} g(x_n),$$

где $g(x)$ была определена ранее. Положим $\rho(x) = 1/2 - \{x\}$ и заметим, что $g(x) = \rho(\beta - x) - \rho(\alpha - x) + \beta - \alpha$.

Для функции $\rho(x)$ при $N_0 \geq 1$ имеет место следующее соотношение (см. задачу 16.1):

$$\left| \rho(x) - \sum_{n=1}^{N_0} \frac{\sin 2\pi n x}{\pi n} \right| \leq \psi_M(x),$$

где $\psi_M(x) = \frac{1}{\sqrt{1+M^2 \sin^2 \pi x}}$, $M = \frac{\pi\sqrt{3}}{4}(2N_0 + 1) > N_0$.

Функция $\psi_M(x)$ представляется в виде ряда (относящегося к классу так называемых рядов Фурье)

$$\psi_M(x) = \sum_{m=-\infty}^{\infty} c_m e^{2\pi i m x} = \lim_{N\to\infty} \sum_{m=-N}^{N} c_m e^{2\pi i m x} =$$

$$= \lim_{N\to\infty} \sum_{m=0}^{N} a_m \cos 2\pi m x,$$

где коэффициенты a_m (называемые **коэффициентами Фурье**) оцениваются следующим образом (см. задачу 16.2):

$$0 \leq a_m \leq 2e^{m/M}(\ln M + 2)/M.$$

Таким образом,

$$g(x) = \beta - \alpha + \sum_{n=1}^{N_0} (\sin 2\pi n(\beta - x) - \sin 2\pi n(\alpha - x)) + R_{N_0}(x),$$

где

$$|R_{N_0}(x)| \leq \psi_M(\beta - x) + \psi_M(\alpha - x).$$

Положим $M_0 = [M \ln M] + 1$ и представим функцию $\psi_M(x)$ в виде

$$\psi_M(x) = \sum_{0<|m|\leq M_0} c_m e^{2\pi i m x} + \Psi(x),$$

где $|\Psi(x)| \le C(\ln M)/M$, C — некоторая константа (для оценки остаточного члена применяется формула суммирования геометрической прогрессии и неравенство $e^{-x} < 1 + x/2$, справедливое при малых положительных x).

Преобразуем теперь функцию $F(N, \alpha, \beta)$, исходя из соотношений на функцию $g(x)$. Учитывая неравенства $N_0 < M_0$ и

$$|(\sin 2\pi m(\beta - x_n) - \sin 2\pi m(\alpha - x_n))| < |T_m(\beta)| + |T_m(\alpha)|,$$

где $T_m(\beta) = \sum_{n=1}^{N} e^{2\pi i m(\beta - x_n)}$ и аналогично определяется $T_m(\alpha)$ (последнее неравенство вытекает из неравенства $b \le |a + bi|$), получаем следующую оценку:

$$|F(N, \alpha, \beta)/N - (\beta - \alpha)| = \left| N^{-1} \sum_{n=1}^{N} g(x_n) - (\beta - \alpha) \right| \le$$

$$\le N^{-1} \left(|c_m| + \frac{1}{\pi |m|} \right) (|T_m(\beta)| + |T_m(\alpha)|) + 2C(\ln M)/M.$$

Заметим, что для любого β справедливо равенство

$$|T_m(\beta)| = |e^{2\pi i m \beta}||T_m(0)| = |T_m(0)| = T_m.$$

Возьмем любое $\varepsilon, 0 < \varepsilon < 2C$ и выберем N_0 и соответственно M так, что $C(\ln M)/M < \varepsilon/4$.

По условию (v) существует такое число $N_1 = N_1(\varepsilon)$, что для всех $N > N_1$ и для всех $m \le M_0 = [M \ln M] + 1$ выполняется неравенство

$$N^{-1} T_m \le \varepsilon/(16(2 + \ln M_0)).$$

Учитывая, что

$$\sum_{0 < |m| \le M_0} \left(|c_m| + \frac{1}{\pi |m|} \right) \le$$

$$\le M^{-1}(2 + \ln M) \sum_{0 < m \le M_0} e^{-m/M} + \frac{2}{\pi} \sum_{0 < m \le M_0} \frac{1}{m} <$$

$$< (2 + \ln M) + 2(\ln M_0 + 1)/\pi < 4 \ln M_0 + 7,$$

выводим из полученных ранее оценок, что для всех $N > N_1$

$$D(N) = \sup_{0 \le \alpha < \beta \le 1} |F(N, \alpha, \beta)/N - (\beta - \alpha)| < \varepsilon.$$

Это и означает, что $\lim\limits_{N \to \infty} D(N) = 0$. Теорема доказана.

16.1**. Докажите, что для функции $\rho(x) = 1/2 - \{x\}$ при любом $N_0 \geq 1$ имеет место соотношение

$$\left|\rho(x) - \sum_{n=1}^{N_0} \frac{\sin 2\pi n x}{\pi n}\right| \leq \psi_M(x),$$

где $\psi_M(x) = \frac{1}{\sqrt{1+M^2 \sin^2 \pi x}}$, $M = \frac{\pi\sqrt{3}}{4}(2N_0 + 1) > N_0$.

16.2**. Докажите, что функция $\psi_M(x)$ представляется в виде ряда

$$\psi_M(x) = \sum_{m=-\infty}^{\infty} c_m e^{2\pi i m x} = \sum_{m=0}^{\infty} a_m \cos 2\pi m x,$$

где коэффициенты c_m и a_m оцениваются следующим образом:

$$|c_m| \leq M^{-1}(2 + \ln M)e^{-|m|/M}, \ |a_m| \leq 2M^{-1}(2 + \ln M)e^{-m/M}.$$

Следующие задачи, интересные и важные сами по себе, будут существенно использованы в решениях основного цикла задач.

16.3. Число e — основание натуральных логарифмов — обычно определяется как $\lim\limits_{n\to\infty}(1 + 1/n)^n$. Докажите, что при некотором $\theta = \theta(n), 0 < \theta < 1$, справедливо равенство

$$e = 1 + 1 + 1/2! + \ldots + 1/n! + \theta/n \cdot n!.$$

Докажите, что e — иррационально.

Далее будем использовать следующие обозначения: $f(x) = O(g(x))$, если $|f(x)| \leq C \cdot g(x)$, где $C > 0$ — некоторая константа; $f(x) = o(g(x))$ при $x \to x_0$, если $f(x)/g(x) \to 0$ при $x \to x_0$; вместо $f(x) = O(g(x))$ иногда будем писать $f(x) \ll g(x)$; $f(x) \sim g(x)$ будет заменять соотношение $f(x)/g(x) \to 1$.

16.4*. Докажите, что $1 + 1/2 + 1/3 + \ldots + 1/n = \ln n + \gamma + o(1)$, где γ — постоянная Эйлера, $\gamma = 0,577\ldots$.

16.5**. *(Харди)* Пусть $\gamma \geq 0$ и при x, стремящемся, монотонно возрастая, к единице, справедливо соотношение

$$\sum_{m=0}^{\infty} a_m x^m = \lim_{N\to\infty} \sum_{m=0}^{N} a_m x^m = o((1-x)^{-\gamma}),$$

и пусть также

$$\limsup_{n\to\infty} n a_n / n^\gamma = 0.$$

Докажите, что

$$\sum_{n\leq N} a_n = o(N^\gamma).$$

16.6*. *(Коши – Штольц)* а) Пусть $\lim\limits_{n\to\infty}|a_n|=0$. Докажите, что

$$\lim_{N\to\infty} N^{-1}\sum_{n=1}^{N}|a_n|=0.$$

б) Пусть последовательность $y_n>0$ такова, что $\sum\limits_{k=1}^{n} y_n$ неограниченно возрастает, и существует предел отношения x_n/y_n при $n\to\infty$. Тогда

$$\lim_{n\to\infty}\frac{\sum\limits_{k=1}^{n} x_n}{\sum\limits_{k=1}^{n} y_n}=\lim_{n\to\infty}\frac{x_n}{y_n}.$$

Напомним, что если $z=a+bi$ — комплексное число, то $z=a-bi$ — сопряженное к нему число, а $|z|=|\bar{z}|=\sqrt{z\bar{z}}=\sqrt{a^2+b^2}$. Складываются комплексные числа покомпонентно, а перемножаются по формуле

$$(a+bi)(c+di)=ac-bd+(ad+bc)i.$$

16.7***. *(Неравенство Вейля – ван дер Корпута)* Пусть заданы некоторые комплексные числа $u_1,\ldots,u_Q$; $\bar{u}_1,\ldots,\bar{u}_Q$ — сопряженные к ним, H — натуральное число, $1\le H<Q$. Докажите, что

$$\left|\sum_{0<q<Q} u_q\right|^2\le\frac{H+Q}{H}\sum_{0<q<Q}|u_q|^2+$$

$$+2\frac{H+Q}{H^2}\sum_{h=1}^{H}(H-h)\left|\sum_{0<q<Q-h}\bar{u}_q u_{q+h}\right|.$$

16.8***. *(ван дер Корпут)* Пусть $f(x)$ — дважды дифференцируемая при $a<x\le b$ функция и на всем промежутке $[a,b]$ выполняется неравенство $0<r<f''(x)$ (или $f''(x)<-r<0$). Докажите, что

$$\left|\sum_{a<n\le b} e^{2\pi i f(n)}\right|\le(|f'(a)-f'(b)|+2)(3+3r^{-1/2}).$$

Назовем **разностью функции** $f(x)$ в точке a с шагом h число $\Delta f(a)=f(a+h)-f(a)$, а **n-й разностью** функции $f(x)$ в точке a с шагом h — число $\Delta^n f(a)=\underbrace{\Delta(\Delta(\ldots\Delta f(a)\ldots))}_{n}$. Определим по индукции n-ю производную функции $f(x)$ равенством

$$f^{(n)}(x)=(f'(x))^{n-1}.$$

16.9*. *(Обобщенная теорема Лагранжа о конечных приращениях)* Докажите, что для некоторого ξ такого, что $a < \xi < a + nh$, выполняется равенство $\Delta^n f(a) = h^n f^{(n)}(\xi)$.

16.10*. *(Вон)* Пусть $f(n)$ – произвольная функция и $\Lambda(n)$ – функция Мангольдта,

$$\Lambda(n) = \begin{cases} \log p, & \text{если} \quad n = p^r, r \geq 1, p \quad - \text{простое}, \\ 0 & - \text{в противном случае.} \end{cases}$$

Докажите, что при $1 < u < N$ справедлива формула

$$\sum_{u<n<N} \Lambda(n) f(\eta) = \sum_{1\leq d\leq u} \mu(d) \sum_{l=1}^{[N/d]} f(ld) \log l -$$

$$- \sum_{1\leq d\leq u} \mu(d) \sum_{1\leq n\leq u} \Lambda(n) \sum_{r=1}^{[N/d]} f(rdu) -$$

$$- \sum_{u<m<N/u} \sum_{u<n<N/m} \Lambda(n) f(nm) \left(\sum_{d|m, d\leq u} \mu(d) \right).$$

16.11. Пусть последовательность $\{x_n\}$ р.р. (mod 1) и m – фиксированное целое число, не равное нулю. Докажите, что последовательность $\{mx_n\}$ р.р. (mod 1).

16.12. Докажите, что при добавлении или исключении конечного числа членов р.р. (mod 1) последовательности она остается р.р. (mod 1). Если две р.р. (mod 1) последовательности объединить в одну, чередуя члены этих последовательностей, то получится р.р. (mod 1) последовательность.

16.13. Докажите, что последовательность дробных долей р.р. (mod 1) всюду плотна на отрезке $[0, 1]$, т. е. на любом отрезке I, лежащем в $[0, 1]$, найдется бесконечно много чисел, равных дробным долям членов этой последовательности.

Множество натуральных чисел назовем **расширяемым** по основанию b, если для любой конечной последовательности b-ичных цифр найдется число из этого множества, b-ичная запись которого начинается с этой последовательности цифр.

16.14. Докажите, что множество $\{s_1, s_2, \ldots\}$ расширяемо по основанию b, если и только если последовательность дробных частей $\{\log_b s_n\}$ всюду плотна на отрезке $[0, 1]$.

В следующих далее задачах всюду n — натуральное число.

16.15. *(Кронекер)* Докажите, что последовательность $\{\alpha n + \beta\}$ всюду плотна на отрезке $[0, 1]$, если α — иррационально. Пользуясь этим, докажите, что функция $\sin x + \cos \sqrt{2} x$ непериодична.

16.16. Докажите, что последовательность a^n расширяема по основанию b, если и только если степень a с натуральным показателем не равна степени b с натуральным показателем. В частности, десятичная запись 2^n может начинаться с любой комбинации цифр.

16.17. Пусть последовательность $\{x_n\}$ всюду плотна на отрезке $[0,1]$, а последовательность $\{y_n\}$ имеет предел. Докажите, что последовательность $\{x_n + y_n\}$ всюду плотна на отрезке $[0,1]$.

16.18. Если упомянутый в предыдущей задаче предел целочисленный и отличный от нуля , а последовательность x_n ограничена, то последовательность $\{x_n y_n\}$ всюду плотна на отрезке $[0,1]$.

16.19*. В предыдущей задаче отбросить предположение о целочисленности предела, вообще говоря, нельзя. Точнее говоря, для любого нецелого a найдется такая ограниченная последовательность x_n, что $\{x_n\}$ всюду плотна на отрезке $[0,1]$, а последовательность $\{ax_n\}$ — нет.

16.20. В задаче 16.17 отбросить предположение об ограниченности последовательности x_n также, вообще говоря, нельзя. Точнее говоря, для любой стремящейся к бесконечности р.р. (mod 1) последовательности x_n найдется стремящаяся к нулю последовательность y_n такая, что последовательность $\{x_n y_n\}$ не всюду плотна на отрезке $[0,1]$.

16.21. Докажите, что если $\Delta x_n = x_{n+1} - x_n \to 0$ при $n \to \infty$ и x_n стремится к бесконечности, то последовательность $\{x_n\}$ всюду плотна на отрезке $[0,1]$.

В следующих задачах log означает логарифм по произвольному заданному основанию.

16.22. Докажите, что последовательность $\{\log n\}$ всюду плотна на отрезке $[0,1]$.

16.23*. Докажите, что последовательность $\{\log n!\}$ всюду плотна на отрезке $[0,1]$.

16.24. Докажите, что последовательность $n!$ расширяема по произвольному основанию.

16.25. *(Москва,66)* Докажите, что десятичная запись $n!$ может начинаться с цифр 1966.

16.26. Докажите, что последовательности n^k и C_n^k, где k — фиксированное натуральное число, расширяемы по произвольному основанию.

16.27. Докажите, что последовательности n^k и C_n^k, где k — фиксированное натуральное число, большее 1, не могут заканчиваться (в десятичных записях) на произвольную заданную комбинацию цифр.

16.28. *(Больцано – Вейерштрасс)* Докажите, что любая последовательность $\{x_n\}$ имеет на отрезке $[0,1]$ предельную точку (т. е. точку, к которой будет сходиться некоторая ее подпоследовательность). Если последовательность $\{x_n\}$ всюду плотна на отрезке $[0,1]$, то любая точка из $[0,1]$ является предельной.

16.29*. Докажите, что в любой последовательности (в том числе и р.р. (mod 1)) можно так переставить члены, что новая последовательность не будет р.р. (mod 1).

16.30***. *(ван дер Корпут)* Докажите, что в любой последовательности, дробные части которой всюду плотны на отрезке $[0,1]$, можно так переставить члены, что она станет р.р. (mod 1).

16.31. Пусть для множества $\{s_1, s_2, \ldots\}$ натуральных чисел последовательность дробных частей $\{\log_b s_n\}$ р.р. (mod 1), и $a < c$ — натуральные числа с одинаковыми длинами b-ичных записей. Докажите, что в этом множестве чаще встречаются числа, начало b-ичной записи которых совпадает с числом a, чем числа, начало которых совпадает с числом c. Другими словами, среди первых N чисел $s_1, s_2, \ldots, s_N$ доля "начинающихся с a" больше доли "начинающихся с числа c" (под словом "доля" мы понимаем здесь отношение количества чисел, удовлетворяющих заданному условию, к числу N).

Сравните следующую задачу с задачей 16.17.

16.32*. Пусть последовательность $\{x_n\}$ р.р. (mod 1), а последовательность $\{y_n\}$ имеет предел. Докажите, что последовательность $\{x_n + y_n\}$ р.р. (mod 1).

Сравните следующую задачу с задачами 16.11 и 16.18.

16.33. Пусть ограниченная последовательность $\{x_n\}$ равномерно распределена по модулю единица и последовательность $\{y_n\}$ имеет пределом целое число, не равное нулю. Докажите, что последовательность $\{x_n y_n\}$ р. р. (mod 1).

Следующая задача усиливает в частном случае задачу 16.32.

16.34*. Пусть последовательность $\{x_n\}$ р.р. (mod 1),

$$\lim_{N\to\infty} \sum_{n=1}^{N} |y_n| = 0.$$

Докажите, что последовательность $\{x_n + y_n\}$ р.р. (mod 1).

Следующая теорема усиливает теорему 16.15. Она появилась независимо в работах П.Боля, В.Серпинского и Г.Вейля.

16.35*. Докажите, что последовательность $\{\alpha n + \beta\}$ р.р. (mod 1), если α иррационально.

16.36. С какой цифры чаще начинается десятичная запись числа 2^n — с единицы или двойки ?

16.37*. *(Г.Полиа - Г.Сеге)* Пусть e — основание натуральных логарифмов. Докажите, что последовательность $\{ne\}$ р.р. (mod 1), но последовательность $\{n!e\}$ имеет число 0 в качестве единственной предельной точки.

16.38. Докажите, что $\lim\limits_{n\to\infty} \sin(2\pi e n!) = 0$.

16.39. Докажите, что последовательность $\{\sin n\}$ не имеет предела при $n \to \infty$.

Следующая задача усиливает предыдущую.

16.40*. Докажите, что последовательность $\{\sin n\}$ всюду плотна на отрезке $[0,1]$, но не р.р. (mod 1).

16.41*. Докажите, что последовательность $\{\sqrt{n}\}$ р.р. (mod 1).

Следующая задача дополняет 16.22.

16.42*. *(Френель)* а) Докажите, что последовательность $\{\log n\}$ не р.р. (mod 1).

б) *(Олимпиада мехмата МГУ)* Будет ли последовательность $\{1+1/2+1/3+\ldots+1/n\}$ р.р. (mod 1)?

16.43***. *(ван дер Корпут)* Пусть $\Delta f(n)$ монотонно стремится к нулю и $n|\Delta f(n)| \to \infty$ при $n \to \infty$, где $\Delta f(n) = f(n+1) - f(n)$. Докажите, что последовательность $\{f(n)\}$ р.р. (mod 1).

16.44*. *(Фейер)* Пусть функция $f(x)$ дифференцируема при $x \geq 1$, $f'(x) \to 0$ и $x|f'(x)| \to \infty$ при $x \to \infty$. Докажите, что последовательность $\{f(n)\}$ р.р. (mod 1).

Читатель "проникнется большой любовью" к критерию Г.Вейля, если попробует элементарно доказать про любую из большого количества приведенных далее последовательностей даже не р.р. (mod 1), а хотя бы всюду плотность на отрезке $[0,1]$.

16.45. Докажите, что последовательность $\{\alpha n^\sigma \ln^\tau n\}$ р.р. (mod 1), если выполнено одно из условий:

а) $\alpha \neq 0, 0 < \sigma < 1$ и τ — произвольное число;

б) $\alpha \neq 0, \sigma = 0$ и $\tau > 1$;

в) $\alpha \neq 0, \sigma = 1$ и $\tau < 0$.

16.46**. *(Кейперс - Кеннеди)* Пусть последовательность $\{f(n)\}$ р.р. (mod 1). Докажите, что $\limsup\limits_{n\to\infty} n|\Delta f(n)| = \infty$.

16.47**. *(ван дер Корпут)* Докажите, что последовательность $\{n \ln n\}$ р.р. (mod 1).

Следующая задача усиливает 16.23.

16.48**. Докажите, что последовательность $\{\log n!\}$ р.р. (mod 1).

16.49. С какой цифры чаще начинается десятичная запись числа $n!$ — с семерки или восьмерки ?

16.50**. Докажите, что последовательность $\{n \ln \ln n\}$ р.р. (mod 1).

Следующая задача обобщает задачи 16.50 и 16.47.

16.51**. Пусть функция $f(x)$ имеет непрерывную вторую производную и для любого сколь угодно малого $\varepsilon > 0$ найдется такое $x_0 = x_0(\varepsilon)$, что для всех $x > x_0$ при некоторых постоянных $A > 0$ и $B > 0$ выполняются неравенства $Ax^{-\sigma-\varepsilon} \leq f''(x) \leq Bx^{-\sigma-\varepsilon}$. Тогда при $0 < \sigma < 2$ последовательность $\{f(n)\}$ р.р. (mod 1).

16.52. Докажите, что последовательность $\{\alpha n^\sigma\}$ р.р. (mod 1) при $\alpha \neq 0$ и $1 < \sigma < 2$.

16.53*. Пусть функция $f(x)$ дважды дифференцируема при $x \geq 1$

и при $x \to \infty$ вторая производная $f''(x)$ монотонно стремится к нулю:

$$f'(x) \to \pm\infty, (f'(x))^2 x^{-2}/|f''(x)| \to 0.$$

Докажите, что последовательность $\{f(n)\}$ р.р. (mod 1).

16.54. Для фиксированного целого d и любого целого числа $a, 0 \le a < d$, последовательности $\{x_{dn+a}\}$ р.р. (mod 1). Докажите, что последовательность $\{x_n\}$ р.р. (mod 1).

16.55*.** *(Теорема ван дер Корпута о разностях)* Для любого натурального m последовательность $\{x_{n+m} - x_n\}$ р.р. (mod 1). Докажите, что последовательность $\{x_n\}$ р.р. (mod 1).

16.56. Покажите, что обращение предыдущей теоремы неверно.

16.57*. *(Г.Вейль)* Пусть у многочлена $F(n)$ старший коэффициент иррационален. Докажите, что последовательность $\{F(n)\}$ р.р. (mod 1).

16.58. Пусть у многочлена $F(n)$ все коэффициенты натуральные. С какой цифры чаще начинается десятичная запись числа $2^{F(n)}$ — с восьмерки или девятки?

16.59. Докажите, что число решений в целых числах системы неравенств

$$2x^4 + x^2 < y^2 < 2x^4 + 2x^2$$

бесконечно.

16.60.** *(Г.Вейль)* Пусть у многочлена $F(n)$ хотя бы один коэффициент, кроме свободного члена, иррационален. Докажите, что последовательность $\{F(n)\}$ р.р. (mod 1).

16.61. Если у многочлена $F(n)$ все коэффициенты, кроме свободного члена, рациональны, то последовательность $\{F(n)\}$ не всюду плотна на отрезке $[0, 1]$.

Из следующей теоремы легко следует утверждение задачи 16.35.

16.62.** *(ван дер Корпут)* Пусть $\Delta x_n = x_{n+1} - x_n \to \theta$ при $n \to \infty$, θ — иррационально. Докажите, что последовательность $\{x_n\}$ р.р. (mod 1).

16.63*. Пусть F_n — последовательность Фибоначчи. Докажите, что последовательность $\{\log_a F_n\}$ р.р. (mod 1) при любом натуральном a.

16.64. Докажите, что при любом натуральном a число Фибоначчи может начинаться с любой заданной комбинации a-ичных цифр.

16.65. Пусть u_n — рекуррентная последовательность, определяемая равенством $u_{n+2} = pu_{n+1} + qu_n$, где p и q — целые числа и уравнение $x^2 - px - q = 0$ имеет действительные иррациональные корни $x_1 > 1$ и $0 < x_2 < 1$. Докажите, что последовательность $\{\log_a u_n\}$ р.р. (mod 1) при любом натуральном a.

16.66. Докажите, что последовательность $\{x_1^n\}$, где x_1 взято из предыдущей задачи, не р.р. (mod 1).

16.67*. *(ван дер Корпут)* Пусть $f'(x) \to \theta$ при $x \to \infty, \theta$ — иррационально. Докажите, что последовательность $\{f(n)\}$ р.р. (mod 1).

16.68*. *(ван дер Корпут)* Пусть при некотором фиксированном k предел $\lim\limits_{n\to\infty} \Delta^k x_n$ иррационален. Докажите, что последовательность $\{x_n\}$ р.р. (mod 1).

16.69*. *(ван дер Корпут)* Пусть функция $f(x)$ является k раз дифференцируема при достаточно больших x и предел $\lim\limits_{x\to\infty} f^{(k)}(x)$ иррационален. Докажите, что последовательность $\{f(n)\}$ р.р. (mod 1).

16.70. Докажите, что последовательность $\{\alpha n^k + \varphi(n)\}$ р.р. (mod 1), если α иррационально и $\lim\limits_{x\to\infty} \varphi^{(k)}(x) = 0$.

16.71*. *(ван дер Корпут)* Пусть при некотором фиксированном k справедливо следующее:

а) $\Delta^k f(n)$ монотонно стремится к нулю при $n \to \infty$;

б) $n|\Delta^k f(n)| \to \infty$ при $n \to \infty$, где $\Delta^k f(n)$ — k-я разность последовательности $f(n)$. Докажите, что последовательность $\{f(n)\}$ р.р. (mod 1).

16.72*. *(Фейер – ван дер Корпут)* Пусть при некотором фиксированном k для некоторой k раз дифференцируемой функции $f(x)$ справедливо следующее:

а) k-я производная $f^{(k)}(x)$ монотонно стремится к нулю при $x \to \infty$;

б) $x|f^{(k)}(x)| \to \infty$ при $x \to \infty$.

Докажите, что последовательность $\{f(n)\}$ р.р. (mod 1).

16.73. *(Чиллаг)* При $\alpha \neq 0$ и нецелом σ последовательность $\{\alpha n^\sigma\}$ р.р. (mod 1).

Эта задача обобщает 16.41 и 16.52. Следующая задача обобщает задачи 16.73 и 16.45 а).

16.74*. При $\alpha \neq 0$, нецелом σ и произвольном действительном τ последовательность $\{\alpha n^\sigma \ln^\tau n\}$ р.р. (mod 1).

Далее следует задача, которая обобщает задачи 16.45 б), в) и дополняет задачу 16.74.

16.75*. Пусть k — натуральное число, $\alpha \neq 0, \tau < 0$ или $\tau > 1$. Докажите, что последовательность $\{\alpha n^k \ln^\tau n\}$ р.р. (mod 1).

16.76**. Пусть $\alpha \neq 0, 0 < \tau \leq 1$. Докажите, что последовательность $\{\alpha n^k \ln^\tau n\}$ р.р. (mod 1) при $k = 1$ и 2.

16.77**. *(Н.М.Коробов, А.Г.Постников)* Пусть $q \geq 1, q > r \geq 0$ — целые числа и при любом натуральном h последовательность $\{x_{n+h} - x_n\}$ р.р. (mod 1). Докажите, что последовательность $\{x_{qn+r}\}$ р.р. (mod 1).

16.78*. *(Фейер)* Пусть функция $g(x)$ такова, что:

а) $g(x)$ монотонно возрастает к бесконечности при $x \to \infty$;

б) ее производная $g'(x)$ непрерывна при $x \geq 1$ и монотонно стремится к нулю при $x \to \infty$ так, что $xg'(x) \to 0$. Докажите, что последовательность $\{g(n)\}$ — не р.р. (mod 1), но всюду плотна на отрезке $[0, 1]$.

16.79. Пусть $\alpha \neq 0, 0 < \tau \leq 1$. Докажите, что последовательность $\{\alpha(\ln n)^\tau\}$ — не р.р. (mod 1), но всюду плотна на отрезке $[0, 1]$.

16.80**.** *(А.А.Карацуба)* Пусть $\alpha > 0, 1 < \tau < 3/2$. Докажите, что последовательность $\{e^{\alpha \ln^\tau n}\}$ — р.р. (mod 1).

16.81**.** *(Эрдеш)* Пусть θ — иррациональное число, а $\omega(n)$ — количество различных простых делителей числа n. Докажите, что последовательность $\{\omega(n)\theta\}$ р.р. (mod 1).

16.82**.** *(И.М.Виноградов)* Пусть θ — иррациональное число и p принимает значения последовательных простых чисел. Докажите, что последовательность $\{p\theta\}$ р.р. (mod 1).

16.83**.** *(И.М.Виноградов)* Пусть у многочлена $F(n)$ хотя бы один коэффициент, кроме свободного члена, иррационален. Докажите, что последовательность $\{F(p)\}$ р.р. (mod 1).

16.84*.** Докажите, что последовательность $\{\log p\}$ не р.р. (mod 1), но всюду плотна на отрезке $[0, 1]$.

16.85. Докажите, что десятичные записи чисел вида p и $2^{F(p)}$, где $F(n)$ — произвольный многочлен с натуральными коэффициентами, а p — простое число, могут начинаться с любой заданной комбинации цифр.

16.86.** *(Полиа)* Пусть $1/n = \omega_1 < \ldots < \omega_{\varphi(n)} < 1$ — последовательность всех несократимых дробей со знаменателями n. Докажите, что для любого $\alpha, 1 \geq \alpha > 0$, количество $N(\alpha)$ этих дробей, не превосходящих α, удовлетворяет неравенству

$$|N(\alpha)/\varphi(n) - \alpha| \leq \frac{1}{\varphi(n)} \sum_{d|n} |\mu(d)|,$$

правая часть которого стремится к нулю при $n \to \infty$.

16.87.** *(Полиа)* Обозначим через S^n последовательность из задачи 16.86. Выписывая друг за другом последовательности $S_2, S_3, \ldots$, получаем перестановку всех рациональных чисел из интервала $(0, 1)$. Докажите, что полученная последовательность р.р. (mod 1).

16.88*. *(Полиа)* Пусть $1/n = \omega_1 < \cdots < \omega_N = 1$ — последовательность всех несократимых дробей со знаменателями, не большими n (ряд Фарея). Докажите, что для любой интегрируемой по Риману функции $f(x)$ имеет место равенство

$$\lim_{n\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\omega_n) = \int_0^1 f(x)\, dx.$$

16.89.** *(Френель - Ландау)* Пусть w_ν — ν-я дробь Фарея со знаменателем, не превосходящим n, $N_n = \varphi(1) + \cdots + \varphi(n)$ — их количество, а $\delta_\nu = w_\nu - \nu/N$. Докажите, что если для всякого $\epsilon > 0$ выполнено любое из неравенств:

а) $\limsup\limits_{n\to\infty} n^{1-\varepsilon}\sum_{\nu=1}^{N}\delta_\nu^2<\infty$;

б) $\limsup\limits_{n\to\infty} n^{1/2-\varepsilon}\sum_{\nu=1}^{N}|\delta_\nu|<\infty$, то

$$\left|\sum_{k=1}^{n}\mu(k)\right| = O(n^{1/2+\varepsilon})$$

(утверждение об оценке суммы значений функции Мёбиуса эквивалентно знаменитой гипотезе Римана о нулях дзета-функции, до сих пор не доказанной).

16.90*.** Пусть $\Delta_N \to 0$ при $N\to\infty$ и при $m \le \Delta_N^{-1}\ln\Delta_N^{-1}$ справедлива оценка

$$\mathrm{T}_N = \sum_{n\le N} e^{2\pi i x_n} \ll N\Delta_N.$$

Докажите, что для количества $\sigma(N;\alpha,\beta)$ членов последовательности $\{x_n\}$ с номерами, не превосходящими N, и таких, что $\alpha<\{x_n\}\le\beta$, при $N\to\infty$ выполняется асимптотическая формула

$$\sigma(N;\alpha,\beta) = (\beta-\alpha)N + O(N\Delta_N\ln\Delta_N^{-1}).$$

В следующих задачах дано обобщение понятия равномерного распределения по модулю единица.

16.91. *(М. Шю)* Пусть задана последовательность положительных вещественных чисел $\{\lambda_n\}$, удовлетворяющая условиям:

1^0 $\lambda_1\ge\lambda_2\ge\dots\ge\lambda_n\ge\dots$, 2^0 ряд $\sum\limits_{n=1}^{\infty}\lambda_n$ расходится.

Будем говорить, что последовательность $\{x_n\}$, $0\le x_n<1$, является **λ-равномерно распределенной по модулю единица,** если для любого интервала I, содержащегося в $[0,1]$ и имеющего индикаторную функцию $\varphi(x)$, которая равна 1 при $x\in I$ и нулю в противном случае, справедливо предельное соотношение:

$$\lim_{n\to\infty}\frac{\lambda_1\varphi(x_1)+\dots+\lambda_n\varphi(x_n)}{\lambda_1+\dots+\lambda_n} = |I|,$$

где $|I|$ — длина интервала I.

Докажите, что следующие утверждения эквивалентны:

(i) последовательность $\{x_n\}$ является λ-равномерно распределенной модулю единица;

(ii) для любой интегрируемой по Риману функции $f(x)$, определенной на отрезке $[0,1]$, справедливо соотношение

$$\lim_{n\to\infty}\frac{\lambda_1 f(x_1)+\dots+\lambda_n f(x_n)}{\lambda_1+\dots+\lambda_n} = \int_0^1 f(x)\,dx;$$

(iii) для любой непрерывной на отрезке $[0,1]$ функции $f(x)$ справедливо предельное соотношение предыдущего равенства;

(iv) при любом целом $m \neq 0$ имеет место равенство

$$\lim_{N\to\infty} \sum_{n=1}^{N} \lambda_n e^{2\pi i m x_n} = o\left(\sum_{n=1}^{N} \lambda_n\right),$$

где величина e^{ix}, по определению, равна $\cos x + i \sin x$, а i — мнимая единица.

16.92. *(М. Шю)* Пусть последовательность $\{x_n\}$ равномерно распределена по модулю единица, и пусть задана последовательность положительных вещественных чисел $\{\lambda_n\}$, удовлетворяющая условиям 1^0 и 2^0 предыдущей задачи. Тогда последовательность $\{x_n\}$ является λ-равномерно распределенной модулю единица.

16.93. *(И. Шёнберг)* Пусть на $E = [0,1]$ задана функция распределения $\varphi(\gamma)$:

$$\varphi(0) = 0,\ \varphi(1) = 1, \quad \text{неубывающая на } E,$$

и пусть для каждого интервала $(0,\gamma) \subset E$ отношение количества Q_N членов последовательности $\{x_n\}$, $1 \leq n \leq N$, попадающих в интервал $(0,\gamma)$, к числу N, стремится при $N \to \infty$ к величине $\varphi(\gamma)$, т. е. последовательность $\{x_n\}$ имеет функцию распределения $\varphi(\gamma)$. Докажите, что эта последовательность имеет функцию распределения $\varphi(\gamma)$ тогда и только тогда, когда для любого фиксированного числа $m \neq 0$ при $N \to \infty$ выполняется предельное соотношение:

$$\lim_{N\to\infty} \sum_{n=1}^{N} e^{2\pi i m x_n} = \int_0^1 e^{2\pi i \gamma}\, d\varphi(\gamma).$$

(Примеры последовательностей, имеющих функцию распределения, дают разложения иррациональных чисел в цепную дробь).

УКАЗАНИЯ

16.1. Положим $\rho(t) = 1/2 - \{t\}$ и докажем, что при $0 < t \leq 1/2$ справедлива формула

$$\rho(t) = \sum_{n=1}^{N} \frac{\sin 2\pi n t}{\pi n} + r_N(t),$$

где

$$r_N(t) = \int_t^{0,5} \frac{\sin \pi(2N+1)z}{\sin \pi z}\, dz.$$

Действительно, имеем

$$r_N(t) = \rho(t) - \sum_{n=1}^{N} \frac{\sin 2\pi nt}{\pi n} = 1/2 - t - \sum_{n=1}^{N} \frac{\sin 2\pi nt}{\pi n} =$$

$$= 1/2 - \int_0^t du - 2\sum_{n=1}^{N} \int_0^t \cos(2\pi nu)\, du = 1/2 - \int_0^t \frac{\sin \pi(2N+1)u}{\sin \pi u}\, du,$$

так как согласно формулам тригонометрии

$$\left(1 + 2\sum_{n=1}^{N} \cos(2nz)\right) \sin z =$$

$$= \sin z + \sum_{n=1}^{N} (\sin(2n+1)z - \sin(2n-1)z) = \sin(2N+1)z.$$

Поскольку при $t = 1/2$ выполняется равенство $r_N(1/2) = 0$, из предыдущего равенства получим, что

$$\int_0^{0,5} \frac{\sin \pi(2N+1)z}{\sin \pi z}\, dz = 0,5.$$

Следовательно, согласно свойству аддитивности интеграла, при $0 < t \leq 1/2$ имеем

$$r_N(t) = \int_t^{0,5} \frac{\sin \pi(2N+1)z}{\sin \pi z}\, dz.$$

Докажем теперь, что при $N \geq 1$ и $0 < t \leq 1/2$ имеет место неравенство

$$|r_N(t)| \leq \min(1/2, 2/(\pi(2N+1)\sin \pi t)).$$

Действительно, так как $1/\sin \pi u$ убывает и положительна на отрезке $[t, 1/2]$, то в силу второй теоремы интегрального исчисления о среднем значении найдется на этом отрезке такое число ξ, что

$$r_N(t) = \int_t^{0,5} \frac{\sin \pi(2N+1)z}{\sin \pi z}\, dz = \frac{1}{\sin \pi t} \int_t^{\xi} \sin \pi(2N+1)z\, dz.$$

Следовательно, интегрируя и используя то, что $|\cos x| \leq 1$, получаем неравенство

$$r_N(t)| \leq 2/(\pi(2N+1)\sin \pi t).$$

Покажем, что $|r_N(t)| \leq 1/2$. Сначала рассмотрим случай $1/(2N+1) < t \leq 1/2$. Поскольку $2N+1 \geq 3$, применяя предыдущее неравенство и учитывая убывание дроби $\sin x/x$ в силу выпуклости $\sin x$ на отрезке $[0, \pi/2]$, получим

$$|r_N(t)| \leq 2/(\pi(2N+1)\sin \pi t) < 2/(\pi(2N+1)\sin(\pi/(2N+1))) =$$

$$= \frac{2}{\pi^2}\frac{\pi/(2N+1)}{\sin \pi/3} \le \frac{2}{\pi^2}\frac{\pi/(2N+1)}{\sin \pi/3} = 4\sqrt{3}/9\pi < 1/2.$$

Рассмотрим теперь оставшийся случай $0 < t \le 1/(2N+1)$. Так как тогда, согласно известному неравенству $|\sin x| \le |x|$, при $1 \le n \le N$ имеем, что $0 < \sin 2\pi nt < 2\pi nt$, то для

$$r_N(t) = 1/2 - t - \sum_{n=1}^{N} \frac{\sin 2\pi nt}{\pi n}$$

получим оценки

$$-1/2 \le 1/2 - t(1+2N) < r_N(t) \le 1/2.$$

Следовательно, при $0 < t \le 1/2$ справедливо неравенство $|r_N(t)| \le 1/2$. Далее, так как при $|a| \le 1/2$

$$|a| = \left(\frac{1}{4a^2} + \frac{3}{4a^2}\right)^{-1/2} \le \left(1 + \frac{3}{4a^2}\right)^{-1/2},$$

а при $|a| > 1/2$ очевидно, что

$$1/2 < \left(1 + \frac{3}{4a^2}\right)^{-1/2},$$

то справедливо неравенство

$$\min(1/2, |a|) \le \left(1 + \frac{3}{4a^2}\right)^{-1/2},$$

учитывая которое, выводим из полученного ранее неравенства для $|r_N(t)|$ оценку $|r_N(t)| \le \psi_M(t)$, где

$$\psi_M(t) = \left(1 + M^2 \sin \pi t\right)^{-1/2},\ M = \pi(2N+1)\sqrt{3}/4.$$

Эта оценка имеет то преимущество, что функция $\psi_M(t)$ является аналитической. Заметим, что поскольку функции $|r_N(t)|$ и $\psi_M(t)$ четные периодические с периодом единица, последняя оценка имеет место для любого вещественного числа t.

16.2. Представим функцию $(1 + M^2 \sin^2 x)^{-1/2}$ в виде

$$\sum_{k=0}^{\infty} c_k \cos 2kx.$$

Для этого заметим, что

$$(1 + M^2 \sin^2 x)^{-1/2} = (1 + M^2)^{-1/2}(1 - q\cos^2 x)^{-1/2},$$

где $q = 1 - 1/(1 + M^2)$, и воспользуемся известными формулами

$$(1-t)^{-1/2} = \sum_{n=0}^{\infty} a_n t^n,\ a_n = \binom{n}{2n} 4^{-n}$$

(эта формула является частным случаем биномиального ряда Ньютона и легко доказывается с помощью формулы Тейлора) и

$$\cos^{2n} x = 2^{-2n+1}\left(\binom{n}{2n}/2 + \sum_{k=0}^{n} \cos 2kx\right)$$

(она легко доказывается индукцией с помощью формулы преобразования произведения косинусов в полусумму и тождества Паскаля для биномиальных коэффициентов). Получаем формулу

$$(1+M^2\sin^2 x)^{-1/2} = \sum_{k=0}^{\infty} c_k \cos 2kx,$$

где

$$c_k = \delta_k (1+M^2)^{-1/2} \sum_{n=k}^{\infty} \binom{n-k}{2n} 2^{-2n+1} a_n q^n,$$

$$\delta_k = \begin{cases} 1, & \text{если } k>0, \\ 1/2, & \text{если } k=0. \end{cases}$$

Так как

$$\binom{n-k}{2n} = \binom{n}{2n} b_{n,k},\ b_{n,k} = (n!)^2((n-k)!)^{-1}((n+k)!)^{-1},$$

и согласно 4.51 имеем $a_n^2 \le 1/(2n+1)$, то при $k>0$

$$c_k < 2M^{-1} \sum_{n=k}^{\infty} a_n^2 b_{n,k} q^n < M^{-1} \sum_{n=k}^{\infty} b_{n,k} q^n/n$$

и

$$c_0 < (2M)^{-1} \left(1 + \sum_{n=1}^{\infty} q^n/n\right).$$

Как известно, $1+x \le e^x$, так как касательная к графику функции e^x есть $1+x$ и расположена она ниже его. Поэтому производная разности $e^{-2x} - \frac{1-x}{1+x}$, равная $2(1+x)^{-2} - 2e^{-2x}$, неотрицательна, значит, при неотрицательном x справедливо неравенство

$$e^{-2x} \ge \frac{1-x}{1+x},$$

откуда при $n \ge 2k$

$$b_{n,k} = \frac{n}{n-k} \prod_{i=1}^{k} \frac{1-i/n}{1+i/n} < 2e^{-k^2/n},$$

а так как $b_{n,k} = b_{n-1,k}/(1-(k/n)^2)$, то $b_{n,k}$ растет с ростом n, и при $n \le 2k$ имеем, что $b_{n,k} < 2e^{-k/2}$, значит, при $k>0$

$$\sum_{n=k}^{2k} b_{n,k} q^n/n < 2(k+1)e^{-k/2}/k < 4e^{-k/2}.$$

Так как

$$b_{n,k} = \frac{n}{n+k} \prod_{i=1}^{k-1} \frac{1-i/n}{1+i/n} \le 1,$$

то, используя формулу суммирования геометрической прогрессии, и неравенство $1+x \le e^x$, получим, что при $m = [(k+1)(M^2+1)]+1$

$$\sum_{n=m}^{\infty} b_{n,k} q^n/n < (q^m/m)(1+q+q^2+\ldots) = q^m/(m(1-q)) \le$$

$$\leq (1+M^2)q^{(k+1)(M^2+1)}/(k+1)(M^2+1) \leq e^{-k-1}/(k+1).$$

В силу неравенства между средним геометрическим и средним арифметическим

$$k^2/n + n/(1+M^2) \geq 2k(1+M^2)^{-1/2} = \alpha,$$

поэтому при $n \geq 2k$

$$b_{n,k}q^n \leq 2e^{-k^2/n-n/(M^2+1)} \leq 2e^{\alpha},$$

значит,

$$\sum_{n=2k+1}^{m-1} b_{n,k}q^n/n < 2e^{\alpha} \sum_{n=2k+1}^{m-1} 1/n < 2e^{\alpha}(\ln((m-1)/(2k+1))+1) <$$

$$< 2e^{\alpha}(\ln(M^2+1)+1),$$

согласно неравенству

$$\sum_{k=n}^{m} 1/k \leq \ln(m/n)+1.$$

Поэтому при $M \geq M_0$ и любом $k \geq 0$ справедливо неравенство

$$c_k \leq M^{-1}(4e^{-k/2} + e^{-k} + 2e^{\alpha}(2\ln M + 2)) <$$

$$< 4e^{-2k(M^2+1)^{-1/2}}(\ln M + 2)/M < 2e^{-k/M}(\ln M + 2)/M.$$

Впрочем, при $k = 0$ можно получить лучшую оценку, если воспользоваться разложением в ряд Тейлора функции $\ln(1+x)$, а именно

$$c_0 < (2M)^{-1}\left(1 + \sum_{n=1}^{\infty} q^n/n\right) =$$

$$= (1 - \ln(1-q))/2M = (1+\ln(M^2+1))/2M.$$

16.3. Пусть

$$c_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}.$$

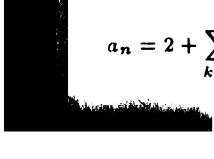
Имеем, что последовательность $\{c_n\}$ является монотонно возрастающей и ограниченной. Действительно,

$$c_n < 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-1}} = 3 - \frac{1}{2^{n-1}} < 3.$$

Следовательно, существует предел $\lim_{n\to\infty} c_n = e_1$. Далее, так как

$$a_n = \left(1 + \frac{1}{n}\right)^n = \sigma < c_n,$$

то $e \leq e_1$.



тда при фиксированном $s \leq n$ имеем

$$a_n = 2 + \sum_{k=2}^{n} \binom{n}{k}\frac{1}{n^k} \geq d_s(n) = 2 + \sum_{k=2}^{s} \frac{1}{k!}\left(1-\frac{1}{n}\right)\cdots\left(1-\frac{k-1}{n}\right).$$

Отсюда

$$e = \lim_{n\to\infty} a_n \geq \lim_{n\to\infty} d_s(n) = c_s,$$

т.е. e — верхняя грань для $\{c_s\}$. Но так как

$$\lim_{s\to\infty} c_s = \sup_s\{c_s\} = e_1,$$

то $e \geq e_1$. Следовательно, $e = e_1$. Заметим еще, что если $e = c_n + r_n$, то

$$0 < r_n = \sum_{k=n+1}^{\infty} \frac{1}{k!} \leq \frac{1}{(n+1)!}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)^2} + \dots\right) =$$

$$= \frac{1}{(n+1)!}\frac{1}{1-1/(n+2)} = \frac{n+2}{(n+1)(n+1)!} < \frac{1}{n\cdot n!}.$$

Покажем, что число e — иррациональное. Допустим противное. Тогда $e = p/q$, $(p,q) = 1$, и с учетом сделанного выше замечания имеем

$$0 < e - c_q < \frac{1}{q\cdot q!}.$$

Домножая обе части неравенства на $q!$, получим, что $A = q!(e - c_q)$ есть целое число и в то же время $0 < A < 1/q$, что невозможно.

16.4. Пусть

$$\gamma_n = 1 + \frac{1}{2} + \dots + \frac{1}{n} - \ln n.$$

Покажем, что существует предел $\gamma = \lim_{n\to\infty} \gamma_n$.

Последовательность $\{\gamma_n\}$ монотонно убывает. Действительно,

$$\gamma_{n+1} - \gamma_n = \frac{1}{n+1} - \ln(n+1) + \ln n = \frac{1}{n+1} - \ln\left(1 + \frac{1}{n}\right) < 0,$$

так как

$$1 < \ln\left(1 + \frac{1}{n}\right)^{n+1}, \quad \text{поскольку} \quad e < \left(1 + \frac{1}{n}\right)^{n+1} = b_n.$$

Далее покажем, что последовательность $\{\gamma_n\}$ ограничена снизу числом 0. Имеем

$$\ln\left(1 + \frac{1}{n}\right)^n < 1, \quad \text{т.е.} \quad \ln\frac{n+1}{n} < \frac{1}{n}.$$

Поэтому

$$\gamma_n = 1 + \frac{1}{2} + \dots + \frac{1}{n} - \ln n > \ln\frac{2}{1} + \ln\frac{3}{2} + \dots + \ln\frac{n+1}{n} - \ln n =$$

$$= \ln\frac{n+1}{n} > \frac{1}{n+1} > 0.$$

Следовательно, по теореме Вейерштрасса последовательность $\{\gamma_n\}$ имеет предел, что и требовалось доказать.

16.6. а) Пусть $\lim_{n\to\infty} a_n = a$. Покажем, что

$$\lim_{n\to\infty} \frac{a_1 + \dots + a_n}{n} = a.$$

Действительно, пусть $b_n = a_n - a$. Тогда $\lim\limits_{n\to\infty} b_n = 0$, и достаточно доказать, что

$$\lim_{n\to\infty} \frac{b_1 + \cdots + b_n}{n} = 0.$$

Так как $\{b_n\}$ — бесконечно малая последовательность , то существует $c > 0$ такое, что при всех n имеем

$$|b_n| < c \quad \text{при всех } n.$$

Кроме того, для любого $\varepsilon > 0$ существует $n_0 = n_0(\varepsilon)$ такое, что при всех $n > n_0$ справедливо неравенство $|b_n| < \varepsilon$. Следовательно,

$$\left|\frac{b_1 + \cdots + b_{n_0} + b_{n_0+1} + \cdots + b_n}{n}\right| \le \frac{cn_0}{n} + \frac{(n-n_0)\varepsilon}{n} < 2\varepsilon,$$

если только $cn_0/n < \varepsilon$, $n > cn_0/\varepsilon$, т.е. $n > \max\left(n_0, cn_0/\varepsilon\right)$. Отсюда уже легко следует требуемый результат.

16.7. Для удобства рассуждений определим числа u_n для всех целых значений n следующим образом: $u_n = 0$ при $n \le 0$ и при $n > Q$. Тогда имеет место равенство

$$H\sum_{n=1}^{Q} u_n = \sum_{n=1}^{Q+H-1}\sum_{m=0}^{H-1} u_{n-m}.$$

Возводя обе части этого равенства в квадрат, и, пользуясь неравенством Коши:

$$\left|\sum a_\nu b_\nu\right|^2 \le \sum |a_\nu|^2 \sum |b_\nu|^2,$$

получим

$$H^2\left|\sum_{n=1}^{Q} u_n\right|^2 \le (Q + H - 1)W,$$

где

$$W = \sum_{n=1}^{Q+H-1}\left|\sum_{m=0}^{H-1} u_{n-m}\right|^2.$$

Преобразуем сумму W. Для этого выделим сумму "диагональных" членов W_1 и сумму "недиагональных" членов W_2. Имеем

$$W = \sum_{m=0}^{H-1}\sum_{k=0}^{H-1}\sum_{n=1}^{Q+H-1} u_{n-m}\bar{u}_{n-k} = W_1 + W_2,$$

где

$$W_1 = \sum_{m=0}^{H-1}\left|\sum_{n=1}^{Q+H-1} u_{n-m}\right|^2,$$

$$W_2 = \sum\sum_{0\le m<k\le H-1}\sum_{n=1}^{Q+H-1} (u_{n-m}\bar{u}_{n-k} + \bar{u}_{n-m}u_{n-k}).$$

Очевидно, справедливо равенство

$$\sum_{n=1}^{Q+H-1} u_{n-m} = \sum_{n=1}^{Q} u_n,$$

поскольку $u_n = 0$ при $n \le 0$ и при $n > Q$. Поэтому

$$W_1 = H\left|\sum_{n=1}^{Q} u_n\right|^2.$$

Преобразуем сумму W_2. Для этого обозначим $n-m=l, n-k=l+h$. Получим

$$W_2 = \sum_{m=0}^{H-1}\sum_{h=1}^{H-m-1}\sum_{l=1}^{N-h}(u_l\bar{u}_{l+h} + \bar{u}_l u_{l+h}).$$

Меняя порядок суммирования по h и по m в сумме W_2 и переходя к неравенствам, имеем

$$|W_2| \le 2\sum_{h=1}^{H-1}\sum_{m=0}^{H-h-1}\left|\sum_{l=1}^{Q-h} u_l u_{l+h}\right| = 2\sum_{h=1}^{H-1}(H-h-1)\left|\sum_{n=1}^{Q-h} u_n u_{n+h}\right|.$$

16.11. Примените критерий Вейля.

16.14. Число a начинается с b-ичных цифр $a_1 \dots a_n$ тогда и только тогда, когда

$$\log_b(\overline{a_1, a_2 \dots a_n}) \le \log_b a < \log_b(\overline{a_1, a_2 \dots a_n} + b^{-n+1}).$$

16.15. Так как α — иррационально, то все числа вида $\{\alpha n + \beta\}$ различны. Для любого k среди первых $k+1$ этих чисел найдутся два, попадающие в один отрезок вида $[p/k, (p+1)/k], 0 \le p < k$. Беря их разность, получаем, что для некоторого $n \le k$ либо $\{\alpha n\} \le 1/k$, либо $1 - \{\alpha n\} \le 1/k$. Рассматривая подпоследовательность с номерами $n, 2n, \dots$, заметьте, что в любой из отрезков $[p/k, (p+1)/k]$ попадет ее член с номером, не большим $n(1/\min(1-\{\alpha n\}, \{\alpha n\})+1)$.

Для доказательства непериодичности функции $\sin x + \cos\sqrt{2}x$ следует заметить, что верхняя грань ее значений, равная 2, не достижима, но для любого $\varepsilon > 0$ функция принимает значение, большее $2-\varepsilon$, т. е. рассматриваемая функция не имеет максимума. Непрерывные же периодические функции имеют максимум.

16.16. Примените 16.14 и 16.15.

16.17. Рассмотрите отдельно случаи, $y_n = \text{const}$ и $y_n \to 0$.

16.18. Примените 16.11 и 16.17.

16.19. Если α — иррационально, то возьмите $x_n = n/\alpha$ и примените задачу 16.15. Если $\alpha = p/q$, p — целое, $q > 1$ — натуральное, $(p, q) = 1$, то выберите $m > 3\alpha$ и для каждого $k = 0, 1, \dots, m-1$ определите подпоследовательность x_{mn+k} так, чтобы ее дробные доли $\{x_{mn+k}\}$ были всюду плотны на отрезке $[k/m, (k+1)/m]$, а целые части $[x_{mn+k}]$ удовлетворяли равенству

$$\{\alpha[x_{mn+k}] + \alpha k/m\} = r/mq,\ 0 \le r < m.$$

Для этого в качестве числа r возьмите остаток от деления pk на m и выберите $[x_{mn+k}] = s$ так, чтобы $psm = r - pk + qmd$, d — целое число, с помощью леммы о том, что наибольший общий делитель a и b представим в виде $ax + by$, где x и y — целые (см. § 3); в случае $r - pk = 0$ выбирайте число s кратным q, а число d — кратным p так, чтобы $ps = qd$. Тогда последовательность $\{x_n\}$ всюду плотна на отрезке $[0, 1]$, а последовательность $\{\alpha x_n\}$ содержится на отрезке $[0, 1/q + \alpha/m]$, лежащем в отрезке $[0, 5/6]$.

16.20. Возьмите $y_n = 1/x_n$.

16.21. Для любого $\varepsilon > 0$ выберите такие N и M, что $|x_M - x_N| > 1$ и для всех $k, N < k \le M, |x_k - x_{k+1}| < \varepsilon$. Тогда на каждом отрезке длины ε, лежащем

в отрезке $[0,1]$, находится одно из чисел $\{x_k\}$, $N \le k \le M$. Для ограниченных последовательностей утверждение задачи неверно. Контрпримером служит любая последовательность, имеющая конечный предел.

16.22. Примените 16.21.

16.23. Пусть a — основание логарифма. Для любого $\varepsilon > 0$ выберите минимальное n так, что $a^n > 1 + \varepsilon/\ln a$, и заметьте, что при $k = N, \ldots, N + [4a/\varepsilon]$, $N = [a^{4n} + a^{3n}]$ и достаточно малом ε

$$\varepsilon/4a < \{\log(k+1)!\} - \{\log k!\} < \varepsilon,$$

поэтому на каждом отрезке длины ε, лежащем в отрезке $[0,1]$, находится одно из чисел $\{\log k!\}$, $k = N, \ldots, N + [4a/\varepsilon] + 1$.

16.24. Примените 16.23 и 16.14.

16.25. Следует из 16.24.

16.26. Примените 16.21 и 16.14.

16.27. Последовательность n^k не может оканчиваться на 10, так как если n^k кратно 5, то оно же кратно 5^k.

16.28. Постройте вложенную последовательность отрезков с длинами 2^{-1}, $2^{-2}, \ldots$, каждый из которых содержит бесконечно много членов последовательности. Докажите, что точка, общая всем этим отрезкам, является предельной.

16.29. Выберите какую-нибудь предельную точку и переставьте члены последовательности так, чтобы для любого 2^{-n} нашлось бы такое N_n, что среди первых N_n членов переставленной последовательности не более чем $\log_{N_n}$ членов были удалены от предельной точки более чем на 2^{-n}.

16.31. Число s_n начинается с b-ичных цифр $a_1 \ldots a_n$, изображающих число a. Тогда для этого n справедливо неравенство

$$\log_b(ab^{-n+1}) \le \{\log_b a\} < \log_b((a+1)b^{-n+1}).$$

Поэтому частота появления цифр числа a в начале записи членов последовательности s_n равна

$$\log_b((a+1)b^{-n+1}) - \log_b(ab^{-n+1}) = \log_b(1 + 1/a)$$

и поэтому монотонно убывает с ростом a.

16.32. Положите $y_n = l + \alpha_n$, воспользуйтесь критерием Г.Вейля и неравенством

$$\left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m(x_n+y_n)}\right| \le \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m(x_n+l)}\right| +$$

$$+\left|N^{-1}\sum_{n=1}^{N}\left(e^{2\pi i m(x_n+y_n)} - e^{2\pi i m(x_n+l)}\right)\right| \le$$

$$\le \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n}\right| + N^{-1}\sum_{n=1}^{N}\left|e^{2\pi i m\alpha_n} - 1\right| \le$$

$$\le \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n}\right| + N^{-1}\sum_{n=1}^{N} 2\left|\sin 2\pi m\alpha_n\right| \le$$

$$\le \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n}\right| + 2\pi m N^{-1}\sum_{n=1}^{N}|\alpha_n|$$

и теоремой Коши (см. задачу 16.4.).

16.33. Примените 16.11 и 16.31.

16.34. Примените критерий Г.Вейля и неравенство

$$\left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m(x_n+y_n)}\right| \le \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n}\right| +$$

$$+\left|N^{-1}\sum_{n=1}^{N}\left(e^{2\pi i m(x_n+y_n)} - e^{2\pi i m(x_n+l)}\right)\right| \le$$

$$\le \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n}\right| + N^{-1}\sum_{n=1}^{N}\left|e^{2\pi i m y_n} - 1\right| \le$$

$$\le \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n}\right| + N^{-1}\sum_{n=1}^{N} 2\left|\sin 2\pi m y_n\right| \le$$

$$\le \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n}\right| + 2\pi m N^{-1}\sum_{n=1}^{N}|y_n|.$$

16.35. Так как α — иррационально, то $\sin \pi m\alpha \neq 0$ при любом целом m и поэтому

$$\left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m(\alpha n+\beta)}\right| \le 1/(N|\sin \pi m\alpha|) \to 0$$

при $N \to \infty$. Далее примените критерий Г.Вейля.

16.36. Примените 16.35 и 16.31.

16.37. Воспользовавшись задачей 16.1 получите неравенство

$$0 < \{en!\} < 1/n,$$

выведите из него иррациональность e и примените 16.35.

16.38. Воспользовавшись неравенством из указания к 16.37 и периодичностью синуса, докажите, что

$$0 < \sin(2\pi men!) < \sin(2\pi/n) < 2\pi/n.$$

16.39. Пусть $\lim\limits_{n\to\infty} \sin n = a$. Тогда из формулы

$$\sin(n+1) = \sin n \cos 1 + \cos n \sin 1$$

следует, что $\lim\limits_{n\to\infty} \cos n = a(1-\cos 1)/\sin 1$. А из равенства

$$\sin(2n) = \sin(2n-2)\cos 2 + \cos(2n-2)\sin 2$$

следует, что тот же предел равен $a(1-\cos 2)/\sin 2$. Поэтому при $a \neq 0$ имеем $\cos 1 = 1$. В случае $a = 0$ получается, что $\lim\limits_{n\to\infty} \cos n = 0 = \lim\limits_{n\to\infty} \sin n$, а это противоречит равенству $\sin^2 n + \cos^2 n = 1$.

16.40. Возьмем любое $a, 0 \le a \le 1$, и выберем α так, что $a = \sin 2\pi\alpha$, $0 \le \alpha \le 1/4$. Зададимся произвольным $\varepsilon > 0$. Чтобы доказать первое утверждение задачи, достаточно найти такое n, что

$$\sin(2\pi(\alpha-\varepsilon)) < \{\sin n\} < \sin(2\pi(\alpha+\varepsilon)).$$

Для выполнения этого неравенства достаточно, чтобы

$$\alpha - \varepsilon < \{n/2\pi\} < \alpha + \varepsilon.$$

Но такое n существует в силу иррациональности π согласно задачи 16.15.

Покажем теперь, что последовательность $\{\sin n\}$ не р.р. (mod 1). Пусть $0 < \alpha < 1$, $\alpha = \sin(2\pi a)$, $1 - \alpha = \sin(2\pi b), 0 < a, b < 1/4$. Неравенству $\{\sin n\} \leq \alpha$ удовлетворяют такие числа n, что выполняется хотя бы одно из неравенств

$$\{n/2\pi\} \leq a, 1/2 - a \leq \{n/2\pi\} \leq 1/2, 1/2 + ble\{n/2\pi\} \leq 1 - b.$$

Так как $\cos(\pi/2 - 2\pi b) = \sin(2\pi b) = 1 - \alpha$, то сумма длин указанных отрезков равна $2a + \arccos(1-\alpha)/\pi$ и асимптотически равна $\sqrt{2\alpha/\pi}$ при $\alpha \to 0$. В силу р.р. (mod 1) последовательности $\{n/2\pi\}$ частота появления таких n, что $\{\sin n\} \leq \alpha$, асимптотически равна $\sqrt{2\alpha/\pi}$ при $\alpha \to 0$. Если бы последовательность $\{\sin n\}$ была бы р.р. (mod 1), то эта же частота равнялась бы α. Противоречие.

16.41. Из определения р.р. (mod 1) достаточно при любом фиксированном α, $0 < \alpha \leq 1$, показать, что число T решений системы неравенств

$$\{\sqrt{n}\} \leq \alpha,\ n \leq N,$$

асимптотически равно αN. Действительно, система равносильна тому, что при $m \leq \sqrt{N} < m + 1$ выполняется одно из неравенств

$$k \leq \sqrt{n} lek + \alpha,\ k = 1, ..., m-1,\ m \leq \sqrt{n} \leq \min\{\sqrt{N}, m + \alpha\}.$$

Следовательно, справедливо равенство

$$T = \sum_{k<m} ([2k\alpha + \alpha^2] + 1) + 2\theta_1\sqrt{N} + 1 = 2\alpha \sum_{k<m} k + 4\theta_2\sqrt{N} =$$

$$= \alpha m(m-1) + 4\theta_2\sqrt{N} = \alpha N + 4\theta\sqrt{N},$$

где $0 \leq \theta_1 < 1$, $|\theta| < 1$.

16.42. а) Аналогично предыдущей задаче число T решений системы неравенств

$$\{\log n\} \leq \alpha,\ n \leq N,$$

равно общему числу решений семейства неравенств

$$k \leq \log_a n \leq k + \alpha,\ k = 0, ..., m-1,\ [\log_a N] = m \leq$$

$$\leq \log_a n \leq \min(\log_a N, m + \alpha).$$

Следовательно, при $N_m = a^m$ справедливо равенство

$$T = T_m = \sum_{k<m} ([a^{k+\alpha} - a^k] + 1) + 1 = (a^\alpha - 1) \sum_{k<m} a^k + \theta m + 1 =$$

$$= (a^\alpha - 1)\frac{a^m - 1}{a - 1} + \theta m + 1 = N(a^\alpha - 1)/(a-1) + \theta m + 1,$$

где $0 \leq \theta \leq 1$.

Если бы последовательность $\{\log_a n\}$ была бы р.р. (mod 1), то частота появления $\{\log_a n\}$ в отрезке $[0, \alpha]$ была равна α. Тогда при всех α, $0 < \alpha \leq 1$, имеем

$$\alpha = \lim_{m\to\infty} T_m/N_m = (a^\alpha - 1)/(a-1).$$

Противоречие.

б) Примените пункт а) и задачи 16.4 и 16.32.

16.43. Примените критерий Г.Вейля. Для этого преобразуйте при $m \neq 0$ тригонометрическую сумму:

$$T_N = \sum_{n=1}^{N} e^{2\pi i m f(n)} = \sum_{n=1}^{N-1} e^{2\pi i m f(n)} + e^{2\pi i m f(N)} =$$

$$= \sum_{n=1}^{N-1} e^{2\pi i m f(n)} \frac{1 - e^{2\pi i m \Delta f(n)}}{1 - e^{2\pi i m \Delta f(n)}} + e^{2\pi i m f(N)} =$$

$$= \sum_{n=1}^{N-1} \frac{e^{2\pi i m f(n)} - e^{2\pi i m f(n+1)}}{1 - e^{2\pi i m \Delta f(n)}} + e^{2\pi i m f(N)} =$$

$$= \sum_{n=1}^{N-1} \frac{e^{2\pi i m f(n)}}{1 - e^{2\pi i m \Delta f(n)}} - \sum_{n=2}^{N} \frac{e^{2\pi i m f(n)}}{1 - e^{2\pi i m \Delta f(n-1)}} + e^{2\pi i m f(N)} =$$

$$= \frac{e^{2\pi i m f(1)}}{1 - e^{2\pi i m \Delta f(1)}} - \frac{e^{2\pi i m (f(N) + \Delta f(N-1))}}{1 - e^{2\pi i m \Delta f(N-1)}} +$$

$$+ \sum_{n=2}^{N-1} e^{2\pi i m f(n)} \left(\frac{1}{1 - e^{2\pi i m \Delta f(n)}} - \frac{1}{1 - e^{2\pi i m \Delta f(n-1)}} \right)$$

и перейдите в этом соотношении к неравенствам:

$$|T_N| \leq \frac{1}{2|\sin \pi m \Delta f(1)|} + \frac{1}{2|sin \pi m \Delta f(N-1)|} +$$

$$+ \frac{1}{2} \sum_{n=2}^{N-1} |\operatorname{ctg}(\pi m \Delta f(n)) - \operatorname{ctg} \pi m \Delta f(n-1)|$$

(для этого воспользуйтесь равенством

$$\left| \frac{1}{1 - e^{2i\alpha}} - \frac{1}{1 - e^{2i\beta}} \right| = \frac{1}{2} |\operatorname{ctg} \alpha - \operatorname{ctg} \beta|,$$

вытекающим из соотношений

$$\frac{1}{1 - e^{2i\alpha}} - \frac{1}{1 - e^{2i\beta}} = \frac{e^{2i\alpha} - e^{2i\beta}}{(1 - e^{2i\alpha})(1 - e^{2i\beta})}, \quad |1 - e^{2i\gamma}| = 2|\sin \gamma|,$$

$$|e^{2i\alpha} - e^{2i\beta}| = |e^{2i\alpha}||1 - e^{2i(\beta-\alpha)}| = |1 - e^{2i(\beta-\alpha)}|,$$

$$\frac{\sin(\beta - \alpha)}{\sin \alpha \sin \beta} = \operatorname{ctg} \alpha - ctg \beta).$$

Так как $\Delta f(n)$ монотонно стремится к нулю, то при любом фиксированном m для некоторого k при всех $N > k$ справедливо неравенство $|m\Delta f(N-1)| < 1/2$, значит (учитывая, что $|\sin x| \geq 2|x|/\pi$ при $|x| \leq \pi/2$),

$$N^{-1}|T_n| \leq \frac{1}{2N|\sin \pi m\Delta f(1)|} + \frac{1}{4|m|N\Delta f(N-1)} +$$

$$+\frac{1}{2N}\sum_{n=2}^{k} |\operatorname{ctg}(\pi m\Delta f(n)) - \operatorname{ctg}\pi m\Delta f(n-1)| +$$

$$+\frac{1}{2N}(\operatorname{ctg}(\pi m\Delta f(N-1))) - \operatorname{ctg}(\pi m\Delta f(k)).$$

Отсюда, используя предельное соотношение $\lim\limits_{N\to\infty} N\Delta f(N) = \infty$ и асимптотическое равенство $\operatorname{ctg}\alpha \sim 1/\alpha$ при $\alpha \to 0$, выведите, что

$$\lim_{N\to\infty} N^{-1}T_N = 0.$$

16.44. Примените 16.43 и теорему Лагранжа о конечных приращениях (см. задачу 16.9).

16.45. Положите $f(x) = \alpha x^{\sigma}\ln^{\tau} x$ и проверьте, что

$$f'(x) = \alpha x^{\sigma-1}(\sigma \ln^{\tau} x + \tau \ln^{\tau-1} x)$$

и в случаях а) — в) функция $f(x)$ удовлетворяет условиям предыдущей задачи.

16.46. Пусть последовательность $\{f(n)\}$ р.р. (mod 1) и

$$\limsup_{N\to\infty} N|\Delta f(N)| < +\infty.$$

Из критерия Вейля следует, что

$$\lim_{N\to\infty} N^{-1}\sum_{n=1}^{N} e^{2\pi i m f(n)} = 0.$$

Кроме того, справедливо неравенство (ввиду того, что хорда короче стягиваемой ею дуги)

$$|e^{2\pi i f(n+1)} - e^{2\pi i f(n)}| = |e^{2\pi i f(n)}||e^{2\pi i\Delta f(n)} - 1| =$$

$$= |e^{2\pi i\Delta f(n)} - 1| \leq 2\pi|\Delta f(n)| \leq C/n,$$

где $C > 0$ — некоторая постоянная (последнее неравенство имеет место в силу предположения об ограниченности верхнего предела). Из тауберовой теоремы Харди (см. задачу 16.5) тогда следует, что

$$\lim_{N\to\infty} e^{2\pi i m f(n)} = 0,$$

это противоречит равенству $|e^{2\pi i f(n)}| = 1$.

16.47. Пусть $f(x) = \alpha x\ln x$, $x \geq 1$, тогда $f'(x) = \alpha + \alpha\ln x$, $f''(x) = \alpha/x$. Имеем

$$T_N = \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m f(n)}\right| \leq N^{-1}\left|\sum_{k\leq r} S_k + S'_{r+1}\right|,$$

где

$$S_k = \sum_{2^{k-1}}^{2^k-1} e^{2\pi i m f(n)},\ S'_{r+1} = \sum_{n=2^r}^{N} e^{2\pi i m f(n)},\ 2^r \le 2^{r+1}.$$

Для оценки S_k и S'_{r+1} воспользуемся теоремой ван дер Корпута (см. задачу 16.8.). Получим

$$|S_k| \le 2^{k-1} m^{1/2} \lambda_2^{1/2} + 8m^{-1/2}\lambda^{-1/2},$$

где λ_2 — минимум $f''(x)$ на отрезке $[2^{k-1}, 2^k - 1]$, т.е. $\lambda_2 = \alpha 2^{1-k}$. Следовательно,

$$S_k| \le 2^{(k-1)/2+4} m^{1/2} \alpha^{1/2}.$$

Аналогично,

$$|S'_{r+1}| \le 2^{r/2+4} m^{1/2} \alpha^{1/2}.$$

Отсюда следуют неравенства

$$T_N = N^{-1}(\alpha m)^{1/2} \sum_{k=1}^{r+1} 2^{(k-1)/2+4} = N^{-1}(\alpha m)^{1/2} 16 \frac{(\sqrt{2})^{r+1} - 1}{\sqrt{2} - 1} <$$

$$< 32N^{-1}(\alpha m)^{1/2}(\sqrt{2N} - 1) < 64N^{-1/2}(\alpha m)^{1/2}.$$

Поэтому $T_N \to 0$ при $N \to \infty$. Значит, по критерию Вейля последовательность $\{\alpha n \ln n\}$ р.р. (mod 1).

16.48. Приведенное выше доказательство без существенных изменений проходит и для последовательности $\{(n + 1/2)\ln n - n\}$. Так как согласно формуле Стирлинга

$$\ln n! = (n + 1/2)\ln n - n + \ln\sqrt{2\pi} + \varepsilon_n,$$

где $\varepsilon_n \to 0$ при $n \to \infty$, то остается применить задачу 16.32.

16.49. Примените 16.48 и 16.31.

16.50. Рассуждайте так же, как и в задаче 16.47. Для оценки тригонометрической суммы

$$T(A) = \sum_{A \le n < 2A} e^{2\pi i m \alpha n \ln\ln n}$$

примените теорему ван дер Корпута и получите, что

$$|T(A)| \ll A(\alpha m)^{1/2} A^{-1/2} (\ln A)^{-1/2} + (\alpha m)^{-1/2} A^{1/2} (\ln A)^{1/2}.$$

Отсюда следует, что

$$T_N = \left| N^{-1} \sum_{n=1}^{N} e^{2\pi i m \alpha n \ln\ln n} \right| \ll (\alpha m)^{1/2} N^{-1/2} (\ln N)^{1/2}.$$

Поэтому $T_N \to 0$ при $N \to \infty$, и по критерию Вейля последовательность $\alpha n \ln\ln n$ р.р. (mod 1).

16.51. С помощью теоремы ван дер Корпута докажите, что

$$|T(A)| = \left| \sum_{A \le n < 2A} e^{2\pi i m n f(n)} \right| \ll m^{1/2} A^{1-\sigma/2-\varepsilon/2} + M^{-1/2} A^{\sigma/2+\varepsilon/2}.$$

Применяя критерий Вейля, как и в 16.47, выведите из этой оценки при $0 < \sigma < 2$, что последовательность $\{f(n)\}$ р.р. (mod 1).

16.52. Следует из 16.51.

16.53. Подобно 16.47 следует из критерия Вейля и оценки ван дер Корпута.

16.54. Примените последний пункт критерия Вейля или непосредственно определение.

16.55. Для любого натурального H и любого целого $m \neq 0$ согласно неравенству ван дер Корпута (см. задачу 16.6):

$$\left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n}\right|^2 \leq$$

$$\leq \frac{H+N-1}{HN} + \sum_{h=1}^{H-1} \frac{(H+N-1)(H-h)}{H^2 N}\left|N^{-1}\sum_{n=1}^{N-h} e^{2\pi i m(x_{n+h}-x_n)}\right|,$$

для любого фиксированного h последовательность $\{x_{n+h}-x_n\}$ является р.р. (mod 1), следовательно, согласно критерию Вейля при $N \to \infty$

$$N^{-1}\sum_{n=1}^{N-h} e^{2\pi i m(x_{n+h}-x_n)} \to 0.$$

Переходя к пределу в неравенстве ван дер Корпута, получим

$$\limsup_{N\to\infty}\left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n}\right|^2 \leq \frac{1}{H}.$$

Так как H можно взять сколь угодно большим, то

$$\lim_{N\to\infty} N^{-1}\sum_{n=1}^{N} e^{2\pi i m x_n} = 0,$$

а это согласно критерию Вейля и означает, что последовательность $\{x_n\}$ р.р. (mod 1).

16.56. Контрпримером служит последовательность задачи 16.15.

16.57. Индукция по степени многочлена. База индукции доказана в 16.35. Пусть для многочленов степени k теорема верна, а F — многочлен степени $k+1$. Тогда многочлен $\Phi(x) = F(x+h) - F(x)$ имеет степень k и при любом целом h его старший коэффициент —иррациональное число. Следовательно, по предположению индукции последовательность $\{\Phi(n)\}$ р.р. (mod 1). Но тогда согласно задаче 16.55 последовательность $\{F(n)\}$ р.р. (mod 1).

16.58. Примените 16.57 и 16.31.

16.59. Возьмите $y = \sqrt{2}x^2 + \delta$, где $2^{-3/2} < \delta < 1/2$ и x достаточно велико, тогда

$$2x^4 + x^2 < y^2 < 2x^4 + 2x^2.$$

Чтобы y можно при этом выбрать целым, подберите целое x так, чтобы

$$1/2 < \{\sqrt{2}x^2\} < 1 - 2^{-3/2}.$$

Для этого примените 16.57.

16.60. Сначала предположите, что все коэффициенты при нелинейных членах полинома F рациональны, т.е. $F = Px^2 + \alpha x + \beta$, где α — иррационально, а коэффициенты полинома $Q = Px^2$ — рациональны. Пусть наименьшее общее

кратное их знаменателей равно q, тогда последовательность $\{Q(n)\}$ периодична с периодом q, ибо $Q(n+q)-Q(n)$ — целое число (равное сумме слагаемых вида $(p/q)((n+q)-n)$, т.е. целых чисел). Поэтому у последовательности $x_n=\{F(n)\}$ каждая из q подпоследовательностей x_{nq+r}, $r=0,1,\ldots,q-1$, имеет вид

$$\{n(\alpha q)+(\alpha r+\beta+\{Q(r)\})\},$$

и, значит, равномерно распределена согласно задаче 16.35. Из 16.54 тогда следует равномерная распределенность последовательности x_n. Пусть теперь иррациональный коэффициент в многочлене F встречается у k-й степени, но ни у одного из членов высших степеней. Докажем теорему индукцией по k подобно задаче 16.57. База индукции ($k=1$) только что доказана. Индукционный переход выполняется так же, как и в 16.57. Нужно лишь заметить, что при любом целом h у многочлена

$$\Phi(x)=F(x+h)-F(x)$$

члены степени k и выше имеют рациональные коэффициенты, а член степени $k-1$ — иррациональный коэффициент.

16.61. Пусть наименьшее общее кратное знаменателей коэффициентов многочлена равно q, а свободный член равен β. Тогда последовательность $\{F(n)\}$ принимает лишь конечное число значений, а именно, значения вида $\{p/q+\beta\}$, $0\le p<q, p\in\mathbb{N}$.

16.62. Пусть

$$x_{n+1}-x_n=\theta+\alpha_n,\ \lim_{n\to\infty}\alpha_n=0,\ S_N=N^{-1}\sum_{n=1}^{N}e^{2\pi imx_n}.$$

Тогда

$$S_Ne^{2\pi im\theta}=N^{-1}\sum_{n=1}^{N}e^{2\pi imx_{n+1}-\alpha_n}=N^{-1}\sum_{n=1}^{N}e^{2\pi imx_{n+1}}+r_n,$$

где

$$r_N=N^{-1}\left(\sum_{n=1}^{N}e^{2\pi imx_{n+1}-\alpha_n}-e^{2\pi imx_{n+1}}\right).$$

Отсюда следует, что

$$S_N(1-e^{2\pi im\theta})=r_N+N^{-1}\left(e^{2\pi imx_{N+1}}-e^{2\pi imx_1}\right).$$

Правая часть этого равенства стремится к нулю при $N\to\infty$. Действительно,

$$|r_N|=N^{-1}\sum_{n=1}^{N}|e^{-2\pi im\alpha_n}-1|=2N^{-1}\sum_{n=1}^{N}|\sin\pi m\alpha_n|\le$$

$$\le 2\pi|m|N^{-1}\sum_{n=1}^{N}|\alpha_n|$$

в силу равенства $|e^{2ix}-1|=2|\sin x|$ и неравенства $|\sin x|\le|x|$, а так как $\lim\limits_{n\to\infty}\alpha_n=0$, то согласно теореме Коши (см. задачу 16.6)

$$\lim_{n\to\infty}N^{-1}\sum_{n=1}^{N}|\alpha_n|=0,$$

поэтому $\lim\limits_{n\to\infty} r_N = 0$. Так как в силу иррациональности θ имеем

$$1 - e^{2\pi i\theta} \neq 0,$$

то $\lim\limits_{N\to\infty} S_N = 0$, а это и означает, согласно критерию Вейля, что последовательность $\{x_n\}$ р.р. (mod 1).

16.63. Так как $F_{n+1}/F_n \to (\sqrt{5}+1)/2 = \varphi$ при $n \to \infty$ (см. § 7), то $\log_a F_{n+1} - \log_a F_n \to \log_a \varphi$ сходится к иррациональному числу (если бы $\log_a \varphi = p/q$, где p, q — натуральные, то $a^p = \varphi^q$, но a^p — целое, а

$$\varphi^q = \varphi^{q-2}(\varphi+1) = \varphi^{q-1} + \varphi^{q-2}\varphi^{q-3}(\varphi+1) + \varphi^{q-4}(\varphi+1) = \cdots = F_q\varphi + F_{q-1}$$

— иррациональное число, так как φ — иррациональное число), значит, согласно задаче 16.62 последовательность $\{\log_a F_n\}$ р.р. (mod 1) при любом натуральном числе a.

16.64. Примените 16.63 и 16.14.

16.65. Обобщение задачи 16.63.

16.66. При $n = 1, 2, \ldots$ последовательность $x_1^n + x_2^n$ принимает целые значения. Поэтому $\{x_1^n\} = \{1 - x_2^n\}$. Но $x_2^n \to 0$ при $n \to \infty$, значит, $\{x_1^n\} \to 0$.

16.67. Из теоремы Лагранжа о конечных приращениях следует, что $\lim\limits_{n\to\infty} \Delta f(n) = 0$. Отсюда на основании 16.62 последовательность $\{f(n)\}$ р.р. (mod 1).

16.68. Индукция по k. База ($k = 1$) доказана в 16.62. Шаг индукции. Пусть утверждение верно при $k = m$. Докажем, что оно верно при $k = m + 1$. По условию $\Delta^{m+1} x_n \to \theta$ при $n \to \infty$, θ — иррациональное число. Обозначим $x_{n+h} - x_n$ через $\Delta_h x_n$. Тогда

$$\Delta_h(\Delta^m x_n) = \Delta^m x_{n+h} - \Delta^m x_n =$$

$$= \Delta^{m+1} x_n + \Delta^{m+1} x_{n+1} + \cdots + \Delta^{m+1} x_{n+h+1}.$$

Поэтому при фиксированном $h \geq 1$ и $n \to \infty$

$$\Delta_h(\Delta^m x_n) \to h\theta.$$

Так как $\Delta_h(\Delta^m x_n) = \Delta^m(\Delta_h x_n)$, то в силу предположения индукции, примененного к последовательности $\Delta_h x_n$, она будет р.р. (mod 1) при любом фиксированном h. Тогда, согласно 16.55, последовательность $\{x_n\}$ р.р. (mod 1).

16.69. Примените обобщение теоремы Лагранжа (см. задачу 16.9) и задачу 16.68.

16.70. Следует из 16.69.

16.71. Индукция по k. При $k = 1$ утверждение доказано в 16.43. Пусть утверждение верно при $k = m$. Докажем, что оно верно при $k = m + 1$. Воспользуемся равенством

$$\Delta_h(\Delta^m f(n)) = \Delta^m(\Delta_h f(n)) =$$

$$= \Delta^{m+1} f(n) + \Delta^{m+1} f(n+1) + \cdots + \Delta^{m+1} f(n+h+1),$$

доказанным в решении 16.68. Из условия теоремы следует, что последовательность $h\Delta^m(\Delta_h f(n))$ монотонно стремится к нулю при $n \to \infty$ и $n|h\Delta^m(\Delta_h f(n))| \to \infty$ при $n \to \infty$. Следовательно, по предположению индукции последовательность

$\Delta_h f(n)$ р.р. (mod 1) при любом фиксированном h. Тогда, согласно 16.55, последовательность $\{f(n)\}$ р.р. (mod 1).

16.72. Примените предыдущую задачу и обобщенную теорему Лагранжа (см. задачу 16.9).

16.73. Примените предыдущую задачу при $k = [\sigma] + 1$.

16.74. Примените задачу 16.72 при $k = [\sigma] + 1$.

16.75. При $\tau > 1$ и $x \to \infty$ имеем, что

$$g(x) = (\alpha x_k \ln^\tau x)^{(k+1)} = (1 + o(1))(k+1)!\alpha\tau(\ln^\tau x)/x \to 0,$$

$$\lim_{x\to\infty} xg(x) = +\infty.$$

Следовательно, по утверждению задачи 16.72 при $\tau > 1$ последовательность $\{\alpha n^k \ln^\tau n\}$ р.р. (mod 1).

Если $\tau > 1$ и $x \to \infty$, то

$$h(x) = \left(\alpha x^k \ln^\tau x\right)^{(k)} = k!\alpha\tau \ln^\tau x(1 + o(1)) \to 0,$$

$$\lim_{x\to\infty} xh(x) \to +\infty.$$

Поэтому последовательность $\{\alpha n^k \ln^\tau n\}$ р.р. (mod 1).

16.76. Рассуждайте так же, как и в задаче 16.47. Для оценки тригонометрической суммы

$$T(A) = \sum_{A\le n<2A} e^{2\pi i m\alpha \ln^\tau n}$$

примените теорему ван дер Корпута. Так как на отрезке $[A, 2A]$ вторая производная функции $\alpha m x \ln^\tau x$ по порядку равна

$$(\alpha m \ln^{\tau-1} A)/A,$$

получите, что

$$|T(A)| \ll A(\alpha m)^{1/2}A^{-1/2}(\ln A)^{(\tau-1)/2} + (\alpha m)^{-1/2}A^{1/2}(\ln A)^{-(\tau-1)/2} \ll$$

$$\ll (\alpha m)^{-1/2}A^{1/2}(\ln A)^{(1-\tau)/2}.$$

Отсюда следует, что

$$T_N = \left|N^{-1}\sum_{n=1}^{N} e^{2\pi i m n\alpha \ln^\tau n}\right| \ll (\alpha m)^{-1/2}N^{-1/2}(\ln N)^{(1-\tau)/2}.$$

Поэтому $T_N \to 0$ при $N \to \infty$, и по критерию Вейля последовательность $\{\alpha n \ln^\tau n\}$ р.р. (mod 1).

Для доказательства р.р. (mod 1) последовательности

$$\{\alpha n^2 \ln^\tau n\},\ 0 < \tau \le 1,\ \alpha \ne 0,$$

согласно теореме ван дер Корпута достаточно доказать, что при любом фиксированном $h \in \mathbb{N}$ последовательность $\{\Delta_h \alpha n^2 \ln^\tau n\}$ р.р. (mod 1). Заметьте, что вторая производная функции $\Delta_h \alpha x^2 \ln^\tau x$ при $x \to \infty$ имеет такой же порядок, что и вторая производная функции $\alpha x \ln^\tau x$. Оценивая тригонометрическую сумму с функцией $m\alpha n^2 \ln^\tau n$ в экспоненте так же, как и в предыдущем случае, и применяя критерий Вейля, получите, что и $\{\alpha n^2 \ln^\tau n\}$ р.р. (mod 1).

16.77. При $q = 1$ утверждение совпадает с теоремой ван дер Корпута. Пусть $q > 1, m \neq 0$ и

$$S_N = N^{-1} \sum_{n=1}^{N} e^{2\pi i m x_{qn+r}}.$$

Так как при s, кратном q, сумма

$$q^{-1} \sum_{b=1}^{q} e^{2\pi i b s/q}$$

равна единице и при s, не кратном q, равна нулю (поскольку $e^{2\pi i s/q} \neq 1$) и согласно формуле суммирования геометрической прогрессии

$$\sum_{b=1}^{q} e^{2\pi i b s/q} = e^{2\pi i s/q} \frac{1 - e^{2\pi i b}}{1 - e^{2\pi i b/q}} = 0),$$

то

$$S_N = (Nq)^{-1} \sum_{b=1}^{q} \sum_{s=1}^{Nq} e^{2\pi i m (x_{s+r} + bs/mq)}.$$

Из условия теоремы и задачи 16.32 следует, что последовательность $y_s = \{x_{s+r+h} - x_{s+r} + bh/mq\}$ р.р. (mod 1). Значит, по теореме ван дер Корпута последовательность $z_s = \{x_{s+r} + bs/mq\}$ р.р. (mod 1), так как $y_s = z_{s+h} - z_s$. Поэтому, согласно критерию Вейля, при $N \to \infty$

$$(Nq)^{-1} \sum_{s=1}^{Nq} e^{2\pi i m (x_{s+r} + bs/mq)} \to 0.$$

Так как q — фиксированное число, то $S_N \to 0$ при $N \to \infty$. А это по критерию Вейля означает, что последовательность $\{x_{qn+r}\}$ р.р. (mod 1).

16.78. Так как $g(t)$ монотонно стремится к бесконечности и непрерывна (в силу дифференцируемости), то для любого α, $0 < \alpha < 1$, найдется такая, стремящаяся к бесконечности последовательность t_k, что $\{g(t_k)\} = \alpha$. Определим последовательность целых чисел m из условия $m_k \leq t_k < m_k + 1$. Из теоремы Лагранжа о среднем (см. задачу 16.9) следует, что при некотором ξ_k, $m_k < \xi_k < t_k$, и при некотором целом n_k справедливо неравенство

$$|g(m_k) - \alpha - n_k| = |g(m_k) - g(t_k)| \leq |g'(\xi_k)|,$$

а так как при $k \to \infty$ имеем $g'(\xi_k) \to 0$, то при достаточно большом k

$$\{g(m_k)\} - \alpha| = |g(m_k) - g(t_k)| \leq |g'(\xi_k)|,$$

и $\{g(m_k)\} \to \alpha$ при $k \to \infty$. Таким образом, из условий а), б) получаем, что последовательность $\{g(n)\}$ всюду плотна в $[0, 1]$.

Условие б) противоречит необходимому условию р.р. (mod 1), указанному в задаче 16.46.

16.79. Если $g(t) = a(lnt)^{\sigma}$, то $g'(t) = a\sigma(lnt)^{\sigma-1}/t$ монотонно стремится к нулю при $t \to \infty$ и $tg'(t) = a\sigma(lnt)^{\sigma-1}$ тоже. Согласно предыдущей задаче последовательность $\{g(n)\}$ всюду плотна в $[0, 1]$, но не является р.р. (mod 1).

16.80. Решение этой очень трудной задачи см. в книге А. А. Карацубы "Основы аналитической теории чисел" (М. Наука, 1983, с.103 и 210).

16.81. Решение этой трудной задачи см. в статьях: P.Erdos. On the uniform distribution of the functions. - Amer. J. Math., 1939. 61. P. 722 – 725; H.Delange. On some arithmetical functions. III. – Amer. J. Math. 1958. 2. P. 81 – 87.

16.82. Для решения этой исключительно трудной задачи понадобятся следующие леммы.

Лемма 1 (преобразование Абеля). *Пусть $f(x)$ непрерывно дифференцируема на отрезке $[a,b]$, c_n — произвольная последовательность,*

$$C(x)=\lim_{a<n\le x} c_n.$$

Тогда

$$\sum_{a<n\le b} c_n f(n)=C(b)f(b)-\int_a^b C(x)f'(x)dx.$$

Доказательство. Положим

$$g(n,x)=\begin{cases}1, & \text{если } n\le x\le b,\\ 0, & \text{если } x\le n.\end{cases}$$

Имеем

$$C(b)f(b)-\sum_{a<n\le b} c_n f(n)=\sum_{a<n\le b} c_n(f(b)-f(n))=\sum_{a<n\le b}\int_n^b c_n f'(x)\,dx=$$

$$=\sum_{a<n\le b}\int_a^b c_n g(n,x)f'(x)\,dx=\int_a^b\sum_{a<n\le b} c_n g(n,x)f'(x)\,dx=$$

$$=\int_a^b\sum_{a<n\le x} c_n f'(x)\,dx=\int_a^b C(x)f'(x)\,dx.$$

Лемма доказана.

Лемма 2. *При $P\ge 1$ и действительном α*

$$\left|\sum_{n=1}^{P} e^{2\pi i\alpha n}\right|\le \min(P,1/2\|\alpha\|).$$

Доказательство. Без ограничения общности считаем, что $0<\alpha<1$. Тогда в силу равенства $|e^{2\pi i\alpha}-1|=2|\sin\pi\alpha$ (вытекающего из того, что основание равнобедренного треугольника с единичными боковыми сторонами равно удвоенному синусу половины угла при вершине) и неравенства $\sin\pi\alpha>2\alpha$ при $0<\alpha\le 1/2$ (вытекающего из выпуклости синуса) имеем

$$\left|\sum_{n=1}^{P} e^{2\pi i\alpha n}\right|=\frac{|e^{2\pi i\alpha P}-1|}{|e^{2\pi i\alpha}-1|}\le\min(P,1/2\|\alpha\|).$$

Лемма доказана.

Лемма 3. *Для любых комплексных чисел a_k и b_k, $1\le k\le n$, справедливо неравенство Коши*

$$\left|\sum_{k=1}^{n} a_k b_k\right|^2\le\sum_{k=1}^{n}|a_k|^2\sum_{k=1}^{n}|b_k|^2.$$

Доказательство. Действительно, так как $|c|^2=c\bar c$, где $\bar c=x-iy$ при $c=x+iy$, то

$$\sum_{k=1}^{n}|a_k|^2\sum_{k=1}^{n}|b_k|^2-\left|\sum_{k=1}^{n}a_k b_k\right|^2=\sum_{k=1}^{n}|a_k|^2\sum_{k=1}^{n}|b_k|^2-\sum_{k=1}^{n}a_k b_k\sum_{k=1}^{n}\bar a_k\bar b_k=$$

$$=\sum_{i<j}(a_i\bar b_j-a_j\bar b_i)(\bar a_i b_j-\bar a_j b_i)=\sum_{i<j}|a_i\bar b_j-a_j\bar b_i|^2\ge 0.$$

Лемма доказана.

Лемма 4. *Если числа* a_n, b_n *действительны, то*

$$\left|\sum_{k=1}^{n} a_k e^{ib_k}\right|^2 = \sum_{k,j=1}^{n} a_k a_j e^{i(b_k - b_j)}.$$

Доказательство. Так как $\overline{ae^{ix}} = ae^{-ix}$ при действительных x и a, то

$$\left|\sum_{k=1}^{n} a_k e^{ib_k}\right|^2 = \sum_{k=1}^{n} a_k e^{ib_k} \overline{\sum_{k=1}^{n} a_k e^{ib_k}} =$$

$$= \sum_{k=1}^{n} a_k e^{ib_k} \sum_{k=1}^{n} a_k e^{-ib_k}.$$

Лемма доказана.

Лемма 5. *Пусть* $\alpha = a/q + \theta/q\tau$, $|\theta| \le 1$, $1 \le q \le \tau$, $(a,q) = 1$. *Тогда при любом* $\beta, U > 0, P \ge 1$ *имеем*

$$\sum_{n=1}^{P} \min(U,\ 1/\|\alpha n + \beta\|) \le 5(P/q + 1)(U + q\log q).$$

Доказательство. Достаточно доказать, что

$$S = \sum_{n=1}^{q} \min(U, 1/\|\alpha n + \beta\|) \le 5(U + q\log q).$$

Так как при $y = an + [q\beta]$ имеем

$$\alpha n + \beta = y/q + \theta'/q\tau,\ \theta' = \theta n + \{q\beta\}\tau,\ |\theta'| \le n + \tau \le 2\tau,$$

а функция $\|x\|$ — периодическая с периодом 1, то, делая замену $y = an + [q\beta] - qm$, где m — целое и $-q/2 \le y < q/2$, найдем

$$S = \sum_{-q/2 \le y < q/2} \min(U, 1/\|y/q + \theta'/q\tau\|).$$

Если $2 < |y| \le q/2$, то

$$\|y/q + \theta'/q\tau\| \ge (|y| - 2)/q,$$

и поэтому

$$S \le 5U + \sum_{2 < |y| \le q/2} q/(|y| - 2) < 5(U + q\log q),$$

так как

$$\sum_{k=3}^{n} 1/(k-2) \le 2\sum_{k=2}^{n} 1/k < 2\log n.$$

Лемма доказана.

Лемма 6. *Пусть* $\alpha = a/q + \theta/q\tau$, $|\theta| \le 1$, $1 \le q \le \tau$, $(a,q) = 1$. *Тогда*

$$\sum_{n=1}^{[q/2]} 1/\|\alpha n\| \le 4q \log q.$$

Доказательство. Для любого натурального числа n выберем $y = y(n)$ так, что $0 \le y = an - qm < q$, и положим

$$u(n) = \begin{cases} y, & \text{если } y \le q/2, \\ q - y, & \text{если } y > q/2. \end{cases}$$

Тогда

$$\|\alpha n\| = \|y/q + \theta/q\tau\| \ge \|u/q - 1/2q\|,$$

и, учитывая, что разным значениям n, $1 \le n \le q/2$, соответствуют разные значения $u(n)$, имеем

$$\sum_{n=1}^{[q/2]} 1/\|\alpha n\| \le q \sum_{n=1}^{[q/2]} 1/(n - 1/2) \le 4q \log q,$$

так как

$$\sum_{k=1}^{n} 1/k \le 2 \sum_{k=2}^{n} 1/k < 2 \log n.$$

Лемма доказана.

Лемма 7. *Пусть* $\alpha = a/q + \theta/q\tau$, $|\theta| \le 1$, $1 \le q \le \tau \le N$, $(a,q) = 1$.
Тогда при $U \le N$ *имеем:*

а) $\sum\limits_{d<U} \min(N/d, 1/\|\alpha d\|) \le 45(U + q + N/q) \log N$,

и при любом U *и* M

б) $\sum\limits_{d<U} \min(M, 1/\|\alpha d\|) \le 10(UM/q + U \log q + q \log q)$.

Доказательство. Сумму первых $[q/2]$ слагаемых оцениваем по лемме 6. Сумму остальных слагаемых разбиваем на непересекающиеся подсуммы вида $\sum\limits_{A \le d < A'}$, где $A' = \min(2A, U)$, и каждую из них оцениваем по неравенству а) леммы 5, учитывая, что

$$A/q + 1 \le 3A/q, \; N/d \le N/A.$$

Складывая полученные оценки

$$15(N/q + A \log q),$$

и применяя формулу суммирования геометрической прогрессии, получаем оценку

$$15((N/q) \log U + 3U \log q),$$

откуда и следует оценка а) леммы. Оценка б) доказывается аналогично, но проще, с помощью однократного применения леммы 5.

Лемма доказана.

Лемма 8. *Обозначим число делителей n через $\tau(n)$. Тогда при $x \geq 2$*

$$\sum_{n=1}^{x} \tau^2(n) = O(x \log x).$$

Доказательство. Переставляя порядок суммирования, имеем

$$\sum_{n \leq x} \tau^2(n) = \sum_{n \leq x} \tau(n) \sum_{m|n} 1 = \sum_{m \leq x} \sum_{n \leq x, m|n} \tau(n) =$$

$$= \sum_{m \leq x} (\tau(m) + \tau(2m) + \cdots + \tau(m[x/m])).$$

Используя очевидное неравенство $\tau(ab) \leq \tau(a)\tau(b)$, и оценку Дирихле из § 1, получаем, что

$$(\tau(m) + \tau(2m) + \cdots + \tau(m[x/m]) \leq \tau(m) \sum_{n \leq x/m} \tau(n) \ll \tau(m) x \log x/m$$

откуда

$$\sum_{n \leq x} \tau(n) \ll x \log x \sum_{n \leq x} \tau(n)/n.$$

Применяя лемму 1 и еще раз оценку Дирихле, находим, что

$$\sum_{n \leq x} \tau(n)/n \leq \sum_{n \leq x} \tau(n)/x + O(1) + \int_1^x (t \log t + O(t)) t^{-2}\, dt \leq$$

$$\leq \log x + O\left(\int_1^x t^{-1}\, dt\right) + \int_1^x t^{-1} \log t\, dt \leq \frac{1}{2} \log^2 x + O(\log x),$$

так как по формуле Ньютона – Лейбница

$$\int_1^x t^{-1}\, dt = \log x, \quad \int_1^x t^{-1} \log t\, dt = \frac{1}{2} \log^2 x.$$

Отсюда следует оценка леммы.

Лемма 9. *Для любого $\tau > 1$ и любого иррационального числа θ найдется такое натуральное число $q(\tau) \leq \tau$ и целое число $a(\tau)$, что*

$$\theta = a/q + \beta, \ |\beta| \leq 1/q\tau, \ (a, q) = 1,$$

причем $q(\tau) \to \infty$ при $\tau \to \infty$.

Доказательство. Все, кроме последнего утверждения, вытекают из теоремы Дирихле, многократно доказанной в этой книге. Предположим, что последнее утверждение неверно, тогда для некоторого c при любом $\tau > 1$ верно, что $q(\tau) < c$, значит, для любого N существуют τ_1, $\tau_2 > N$ такие, что

$$\theta = a_i/q_i + \beta_i, \ |\beta_i| \leq 1/q_i\tau_i, \ a_1/q_1 \neq a_2/q_2,$$

откуда имеем

$$c^{-2} \le 1/q_1q_2 \le |a_1/q_1 - a_2/q_2| = |\beta_1 - \beta_2| \le |\beta_1| + |\beta_2| \le$$

$$\le \tau_1 + \tau_2 < 2/N,$$

а это ведет к противоречию, так как $N \to \infty$.

Для доказательства теоремы И.М.Виноградова достаточно (согласно критерию Г.Вейля) проверить, что для любого фиксированного целого $k \neq 0$ справедливо соотношение

$$\lim_{N\to\infty} N^{-1} \sum_{p\le N} f(p) = 0,$$

где $f(n) = e^{2\pi i\theta kn}$, а переменная суммирования p пробегает последовательно все простые числа, не большие N. Используя лемму 7, положим $\tau = N/\log^h N$, где $h = 8$, представим θk в виде

$$\theta k = a/q + \beta,\ |\beta| \le 1/q\tau,$$

и рассмотрим два случая:

$$1) q \le \log^h N \quad \text{и} \quad 2) \log^h N < q \le N/log^h N.$$

Рассмотрим вначале второй случай. Используя обозначения, введенные в задаче 16.10, и применяя эту задачу и лемму 1, при некотором t_0, $U < t_0 \le N$, имеем

$$\sum_{p\le N} f(p) = \sum_{U<n\le N} f(n)\Lambda(n)/\log n + O(N^{1/2}\log N), U = N^{1/3},$$

(так как при $p^k < N$, $k > 1$, выполняются неравенства $p < N^{1/2}, k < \log N$),

$$\sum_{U<n\le N} f(n)\Lambda(n)/\log n = S(N)/\log N + \int_U^N S(t)\,dt/(t\log^2 t),$$

$$|f(n)\Lambda(n)/\log n| \le |S(N)|/\log N + |S(t_0)| \int_U^N dt/(t\log^2 t) =$$

$$= |S(N)|/\log N + |S(t_0)|(1/\log U - 1/\log N) \le$$

$$\le |S(t_0)|/\log U \le 3|S(t_0)|/\log N,$$

где

$$S(N) = \sum_{U<t\le N} f(n)\Lambda(n) = S_1 - S_2 - S_3,$$

$$S_1 = \sum_{d\le U} \mu(d) \sum_{j\le N/d} (\log j) f(jd),\ S_2 = \sum_{d\le U} \mu(d) \sum_{n\le U} \Lambda(n) \sum_{r\le N/dn} f(ndr),$$

$$S_3 = \sum_{U<m\le N/U} \sum_{d|m, d\le U} \mu(d) \sum_{U<n\le N/m} f(nm)\Lambda(n).$$

Для доказательства теоремы в рассматриваемом случае достаточно получить оценки $S_i = o(N/\log N)$.

Сначала оценим сумму S_1. Промежуток суммирования внутренней суммы $(1, N/d]$ разобьем на $O(\log N)$ промежутков вида $(M, M_1]$,

$$M \geq 1, M_1 = \min(2M, N/d).$$

Рассмотрим сумму

$$S_1(M) = \sum_{M < j \leq M_1} (\log j) f(jd).$$

Применяя леммы 1, 2, неравенство

$$\left| \int_M^{M_1} g(t)dt/t \right| \leq \int_M^{M_1} |g(t)|dt/t \leq \max_t |g(t)| \int_M^{M_1} dt/t = \max_t |g(t)| \log M/M$$

и лемму 7а), имеем

$$S_1(M) = \log M_1 \sum_{M < j \leq M_1} f(jd) - \int_M^{M_1} \left(\sum_{M < j \leq t} f(jd) \right) dt/t,$$

$$|S_1(M)| \leq (\log 4M) \min(M, 1/2\|\theta kd\|),$$

$$|S_1| \leq \sum_{d \leq U} \left| \sum_{j \leq N/d} (\log j) f(jd) \right| \leq \sum_{d \leq U} \sum_M |S_1(M)| =$$

$$= O(\log^2 N) \sum_{d \leq U} \min(N/d, 1/2\|\theta kd\|) = O(U + q + N/q) \log^3 N,$$

откуда ввиду неравенств $\log^h N < q \leq N/\log^h N$ следует, что

$$S_1 = o(N/\log N).$$

Сумма S_2 оценивается подобным же образом, но несколько проще. Перепишем ее в следующем виде:

$$S_2 = \sum_{m \leq U^2} a(m) \sum_{n \leq N/m} f(nm),$$

где

$$a(m) = \sum_{\substack{dr = m \\ d \leq U, r \leq U}} \mu(d) \Lambda(r).$$

Заметим, что $a(m) \leq \log m$. Действительно, если число m содержит в своем разложении хотя бы две нетривиальные степени простых, то для любых d и r таких, что $dr = m$, либо r не равно степени простого, либо d не свободно от квадратов, и поэтому, согласно определению функций μ и Λ, имеем $a(m) = 0$. Если же $m = p_1^\alpha p_2 \dots p_k$, то при $\alpha > 1$

$$|a(m)| \leq \max(|\Lambda(p_1^\alpha)\mu(p_2 \dots p_k)|, |\Lambda(p_1^{\alpha-1})\mu(p_1 p_2 \dots p_k)|) \leq \log p_1,$$

а при $\alpha = 1$

$$|a(m)| \leq \sum_{i=1}^{k} \Lambda(p_i) = \log m.$$

Поэтому

$$|S_2| \le \sum_{m \le U^2} |a(m)| \left| \sum_{n \le N/m} f(nm) \right| \le 2 \log U \sum_{m \le U^2} \left| \sum_{n \le N/m} f(nm) \right|.$$

Применяя леммы 2, 7а), имеем

$$|S_2| = O(\log N) \sum_{m \le U^2} \min(N/m, 1/2\|\theta km\|) = O(U^2 + q + N/q) \log^2 N,$$

откуда ввиду неравенств $\log^h N < q \le N/\log^h N$, следует, что

$$S_2 = O(N/\log N).$$

Рассмотрим сумму S_3. Разбивая в ней промежуток суммирования по m на промежутки вида $(M_1, M_2]$, где $M_1 \le M_2 \le 2M_1$, разложим ее на $O(\log N)$ сумм вида

$$S(M_1) = \sum_{M_1 < m \le M_1} b(m) \sum_{U < n \le N/m} \Lambda(n) f(nm),$$

где функции $\Lambda(m)$ и $b(n)$ удовлетворяют неравенствам

$$|b(m)| \le \tau(m), \ |\Lambda(m)| \le \log m.$$

Для оценки $S(M_1)$ применяем неравенство Коши. Имеем

$$|S(M_1)|^2 \le \sum_{M_1 < m \le M_1} |b(m)|^2 \sum_{M_1 < m \le M_1} \left| \sum_{U < n \le N/m} \Lambda(n) f(nm) \right|^2 =$$

$$= \sum_{M_1 < m \le M_1} |b(m)|^2 V,$$

где сумму V с помощью леммы 4 и перемены порядка суммирования можно представить в виде

$$V = \sum_{M_1 < m \le M_1} \sum_{U < n_1 \le N/m} \Lambda(n_1) \sum_{U < n_2 \le N/m} \Lambda(n_2) e^{2\pi i k \theta m (n_1 - n_2)}.$$

Перепишем последнюю сумму, переставляя порядок суммирования, в виде

$$V = \sum_{U < n_1 \le N/m} \Lambda(n_1) \sum_{U < n_2 \le N/m} \Lambda(n_2) \sum_{m = M_1}^{M} e^{2\pi i k \theta m (n_1 - n_2)},$$

где $M = \min(M_2, N/n_1, N/n_2)$.

Применяя лемму 2, имеем (слагаемые при $n_1 = n_2$ равны M_1)

$$V \le \log^2 N \sum_{n_1 \le N/M_1} \sum_{n_2 \le N/M_1} \min(M_1, 1/2\|\theta k(n_1 - n_2)\|).$$

Объединяя вместе слагаемые, для которых $|n_1 - n_2| = n$, получаем, что

$$V \le (2 \log^2 N) \left((N/M_1) \sum_{n \le N/M_1} \min(M_1, 1/2\|\theta kn\|) + N \right),$$

откуда с помощью леммы 7б) имеем оценку

$$V \le 20(\log^2 N)\,((N/M_1)(N/q + N\log N/M_1 + q\log N) + N) \le$$

$$\le 20(\log^2 N)\,((N/q + (N_1/M)\log N + qN\log N)/M_1 + N).$$

Применяя лемму 8, отсюда выводим, что

$$|S(M_1)|^2 \ll M_1 \log M_1 \log N((N^2/q + (N^2/M_1 + qN)\log N)/M_1 + N) \ll$$

$$\ll \log^5 N)(N^2/q + ((N^2/M) + qN)\log N + NM_1.$$

Воспользовавшись неравенством

$$(x+y+z+t)^{1/2} \le x^{1/2} + y^{1/2} + z^{1/2} + t^{1/2},$$

просуммировав получившиеся геометрические прогрессии и учитывая, что $U \le M_1 \le N/U$, имеем

$$|S_3| \le \sum |S(M)| \ll (Nq^{-1/2}\log N + (NU^{-1/2} + (qN)^{1/2})\log^{1/2} N +$$

$$+NU^{-1/2})\log^{5/2} N = (Nq^{-1/2} + NU^{-1/2} + (qN)^{1/2})\log^{7/2} N.$$

Отсюда при $\log^h N < q \le N/\log^h N$ следует, что

$$S_3 = o(N/\log N).$$

Рассмотрим первый случай, т.е. предположим, что

$$\theta k = a/q + \beta,\ |\beta| \le 1/q\tau,\ \tau = N/\log^h N, q \le \log^h N,\ (a,q) = 1.$$

Из полученного при рассмотрении второго случая равенства

$$\sum_{p\le N} f(p) = \sum_{U<n\le N} f(n)\Lambda(n)/\log n + O(N^{1/2}\log N),\ U = N^{1/3},$$

следует, что достаточно получить оценку для

$$S_0(N) = \sum_{n\le N} f(n)\Lambda(n)/\log n.$$

Справедлива следующая цепочка равенств:

$$S(N) = \sum_{n\le N} f(n)\Lambda(n) = \sum_{\substack{l=1\\(l,q)=1}}^{q} \sum_{\substack{n\le N\\ n\equiv l \pmod q}} \Lambda(n)e^{2\pi i(a/q+\beta)n} =$$

$$= \sum_{\substack{l=1\\(l,q)=1}}^{q} e^{2\pi i a/q} \sum_{\substack{n\le N\\ n\equiv l \pmod q}} \Lambda(n)e^{2\pi i\beta n}.$$

Обозначим через $\psi(x,q,l)$ сумму

$$\psi(x,q,l) = \sum_{\substack{n\le N\\ n\equiv l \pmod q}} \Lambda(n) = x/\varphi(q) + R(x,q,l).$$

В силу теоремы Зигеля – Вальфиша для любого фиксированного числа $h > 1$ и $1 \le q \le \log^h x$ существует постоянная $c = c(h) > 0$ такая, что

$$|R(x,q,l)| = O\left(xe^{-c\sqrt{\log x}}\right).$$

Применим преобразование Абеля (см. лемму 1) к внутренней сумме в выражении для $S_0(N)$. Получим

$$\sum_{\substack{n\le N\\ n\equiv l \pmod q}} \Lambda(n)e^{2\pi i\beta n} = \sum_{n\le N}(\psi(n,q,l)-\psi(n-1,q,l))e^{2\pi i\beta n} =$$

$$= e^{2\pi i\beta N}\psi(N,q,l) + \sum_{n\le N-1}\psi(n,q,l)(e^{2\pi i\beta n} - e^{2\pi i\beta(n+1)}) =$$

$$= \frac{N}{\varphi(q)}e^{2\pi i\beta N} + \sum_{n\le N-1}\frac{n}{\varphi(q)}(e^{2\pi i\beta n} - e^{2\pi i\beta(n+1)}) + R(N,q,l)e^{2\pi i\beta N} +$$

$$+ \sum_{n\le N-1} R(n,q,l)(e^{2\pi i\beta n} - e^{2\pi i\beta(n+1)}) = \frac{1}{\varphi(q)}\sum_{n\le N}e^{2\pi i\beta n} + R,$$

где

$$|R| \le |R(N,q,l)| + \sum_{n\le N-1}|R(n,q,l)||1-e^{2\pi i\beta}| \le$$

$$\le |R(N,q,l)| + 2\pi|\beta|\sum_{n\le N-1}|R(n,q,l)| =$$

$$= O\left(Ne^{-c\sqrt{\log N}} + 2\pi|\beta|Ne^{-b\sqrt{\log N}} + 2\pi|\beta|\sum_{\sqrt{N}<n<N} ne^{-c\sqrt{\log n}}\right) =$$

$$= O\left(Ne^{-b\sqrt{\log N}}\right),\ b = c/2,$$

в силу монотонности функции $xe^{-c\sqrt{\log x}}$ (очевидной после ее логарифмирования). Таким образом,

$$S_0(N) = \frac{1}{\varphi(q)}\sum_{\substack{l=1\\(l,q)=1}}^{q} e^{2\pi i a l/q}\sum_{n/leN} e^{2\pi i\beta n} + R_0 = s_0 + R_0,$$

где

$$|R_0| = \sum_{\substack{l=1\\(l,q)=1}}^{q}|R| = O\left(Nqe^{-b\sqrt{\log N}}\right) = O\left(Ne^{-d\sqrt{\log N}}\right),\ d = b/2.$$

Воспользуемся тем, что поскольку $(a,q) = 1$,

$$\sum_{\substack{l=1\\(l,q)=1}}^{q} e^{2\pi i a l/q} = \mu(q).$$

Поэтому

$$|s_0| \le \frac{1}{\varphi(q)}\left|\sum_{n\le N} e^{2\pi i\beta n}\right| \le \frac{N}{\varphi(q)}.$$

Учитывая, что $q \to \infty$ при $N \to \infty$, окончательно имеем

$$|S_0(N)|/N \le (|s_0| + |R_0|)/N \le O\left(e^{-d\sqrt{\log N}}\right) + \frac{1}{\varphi(q)} \to 0.$$

16.83. Решение этой трудной задачи можно получить, если воспользоваться критерием Вейля и формулой Вона (задача 16.7).

16.84. Рассмотрим следующие функции: $\varphi(m,\xi)$, которая равна $1/m$-й доле количества тех из первых m простых чисел, у которых дробная часть натурального логарифма не превосходит заданного ξ, где $0 < \xi < 1$; функции $\varphi_-(\xi)$ и $\varphi_+(\xi)$, которые равны соответственно нижнему и верхнему пределам $\varphi(m,\xi)$ при $m \to \infty$, и функцию $N(x)$, равную количеству простых p, не превосходящих e^x. Тогда

$$N(x)\varphi(N(x),\xi) = N(1+\xi) - N(1) + N(2+\xi) - N(2) + \cdots + N([x]-1+\xi) -$$

$$-N([x]-1) + N(min(x,[x]+\xi)) - N([x]).$$

Из асимптотического закона распределения простых чисел Адамара и Валле-Пуссена при $x \to \infty$ получим, что

$$N(x) \sim e^x/x$$

(знак $\sim$ здесь и далее обозначает асимптотическое равенство, т. е. $a(n) \sim b(n)$ означает, что $\lim\limits_{n=1} a(n)/b(n) = 1$). Отсюда и из теоремы Штольца – Коши (см. задачу 16.6) при $n \to \infty$ следуют равенства

$$N(n+\xi) \sim e^{n+\xi}/n, \ \sum_{k=1}^{n-1} N(k+\xi) \sim \sum_{k=1}^{n-1} e^{k+\xi}/k.$$

Проверим, что

$$(e-1)\sum_{k=1}^{n-1} e^k/k \sim e^n/n.$$

Для этого выберем число m так, что $2\sqrt{n} > n - m \ge \sqrt{n}$, и оценим сумму сверху и снизу следующим образом:

$$\sum_{k=1}^{n-1} e^k/k < \sum_{k=1}^{m-1} e^k + \frac{1}{m}\sum_{k=m}^{n-1} e^k < \frac{e^m}{e-1} + \frac{1}{m}\frac{e^n - e^m}{e-1} =$$

$$= \frac{1}{m}\frac{e^n}{e-1}(1+o(1)) = \frac{1}{n}\frac{e^n}{e-1}(1+o(1)),$$

$$\sum_{k=1}^{n-1} e^k/k > \frac{1}{n}\sum_{k=1}^{n-1} e^k = \frac{1}{n}\frac{e^n - e}{e-1} \ge \frac{1}{n}\frac{e^n}{e-1}.$$

Воспользовавшись тем, что

$$(e-1)\sum_{k=1}^{n-1} e^k/k \sim e^n/n,$$

получаем соотношение

$$\sum_{k=1}^{n-1} N(k+\xi) \sim e^{n+\xi}/(n(e-1)).$$

Последовательность $\{\ln p_n\}$ всюду плотна на $[0,1)$, так как отношение двух последовательных простых чисел стремится к единице при стремлении номера простого числа к бесконечности согласно асимптотическому закону распределения простых. Поэтому для любого $\alpha, 0 \le \alpha < 1$, существует такая последовательность натуральных чисел j_n, что $\{\ln p_{j_n}\} \to \alpha$ при $n \to \infty$. Заметим, что

$$N(\ln p_{j_n}) = j_n.$$

Проверьте, что если $a(n) \sim a'(n)$, $b(n) \sim b'(n)$, то

$$\min(a(n), b(n)) \sim \min(a'(n), b'(n)),$$

если $a(n)$, $b(n)$ и $a(n)+b(n)$ одного знака, то к тому же

$$a(n) + b(n) \sim a'(n) + b'(n),$$

а если при некоторых константах C_1 и $C_2 > 0$

$$C_1|a(n)| \le |a(n) - b(n)| \le C_2|a(n)|,$$

то $a(n) - b(n) \sim a'(n) - b'(n)$.

Тогда из предыдущих рассмотрений имеем

$$\lim_{n\to\infty} \varphi(N(\ln p_{j_n}, \xi)) = F(\xi, \alpha),$$

где

$$e^{\alpha} F(\xi,\alpha) = (e^{\xi} - 1)/(e-1) + \min(e^{\alpha}, e^{\xi}) - 1 =$$

$$= \begin{cases} (e^{\xi} - 1)/(e-1) + e^{\alpha} - 1, & \text{если} \quad 0 \le \alpha \le \xi, \\ e(e^{\xi} - 1)/(e-1), & \text{если} \quad \xi \le \alpha \le 1. \end{cases}$$

Функция $F(\xi, \alpha)$ на отрезках $[0,\xi]$ и $[\xi,1]$ принимает минимальные и максимальные значения в их концах 0, ξ, 1 и эти значения равны

$$(e^{\xi} - 1)/(e-1) \quad \text{и} \quad e(e^{\xi} - 1)/(e-1).$$

В силу выпуклости функции e^x справедливы при $0 < \xi < 1$ неравенства

$$\xi < e^{\xi} - 1 < (e-1)\xi.$$

Отсюда следует, что при $0 < \xi < 1$

$$0 \le \varphi_-(\xi) \le (e^{\xi} - 1)/(e-1) < \xi < e(e^{\xi} - 1)/(e-1) \le \varphi_+(\xi) \le 1.$$

В случае же равномерного распределения последовательности $\{\ln p\}$ согласно критерию Вейля

$$\varphi_-(\xi) = \xi = \varphi_+(\xi).$$

Приведенное решение принадлежит А.Уинтнеру (On the cyclical distribution of the prime numbers. //Quart.J.Math. 1935(1). 6. P.65 – 68).

16.85. Примените задачи 16.82, 16.83, 16.14.

16.86 – 16.88. Пусть $1/n = r_1/n < r_2/n < \cdots < r_{\varphi(n)}/n = (n-1)/n$ — все правильные несократимые дроби со знаменателем n. Согласно критерию Вейля для выполнения для любой интегрируемой функции $f(x)$ равенства

$$\lim_{n\to\infty} \frac{1}{\varphi(n)} \sum_{s=1}^{\varphi(n)} f(r_s/n) = \int_0^1 f(x)\,dx$$

необходимо и достаточно выполнения при любом целом k равенства

$$\lim_{n\to\infty}\frac{1}{\varphi(n)}\sum_{s=1}^{\varphi(n)}{}'\, g(kr_s/n)=0,$$

где $g(x)=e^{2\pi ix}$. Для доказательства последнего равенства воспользуемся тождеством для функции Мёбиуса

$$\sum_{d|n}\mu(d)=1,\quad \text{если}\quad n=1,\quad \text{и}\quad \sum_{d|n}\mu(d)=0,\quad \text{если}\quad n>1.$$

Меняя порядок суммирования, и заменяя далее индекс суммирования d на n/d, имеем

$$S_n=\sum_{s=1}^{\varphi(n)}g(kr_s/n)=\sum_{s=1}^{n}g(kr_s/n)\sum_{d|(r,n)}\mu(d)=$$

$$=\sum_{d|n}\mu(d)\sum_{r=1}^{[n/d]}g(kdr/n)=\sum_{d|n}\mu(n/d)\sum_{r=1}^{d}g(kr/d).$$

Отсюда с помощью формулы суммирования геометрической прогрессии выводим, что

$$S_N=\sum_{d|n}\mu(n/d)\sum_{r=1}^{d}g(kr/d)=\sum_{d/midn}\mu(n/d)d\delta(k,d),$$

где

$$\delta(k,d)=\begin{cases}1, & \text{если}\quad d\mid k,\\ .0 & -\ \text{в противном случае.}\end{cases}$$

Учитывая, что сумма имеет ненулевые слагаемые только при $d\mid k$ и $d\mid n$ (поэтому каждое из них и их количество не превосходят k) имеем оценку

$$|S_n|=\left|\sum_{d|n}\mu(n/d)d\delta(k,d)\right|=\left|\sum_{d|(n,k)}\mu(n/d)d\delta(k,d)\right|\le k^2,$$

из которой и следует, что

$$\lim_{n\to\infty}\frac{1}{\varphi(n)}\sum_{s=1}^{\varphi(n)}g(kr_s/n)=\lim_{n\to\infty}\frac{S_n}{\varphi(n)}=0,$$

так как $\varphi(n)\to\infty$ (как видно из формулы Эйлера). Тем самым доказано, что

$$\lim_{n\to\infty}t_n/\varphi(n)=\int_0^1 f(x)\,dx,$$

где

$$t_n=\sum_{s=1}^{\varphi(n)}f(r_s/n).$$

Применяя теорему Штольца, получаем

$$\lim_{n\to\infty}\left(\sum_{n=1}^{N} t_n\right)\Big/\left(\sum_{n=1}^{N}\varphi(n)\right)=\int_0^1 f(x)\,dx.$$

Приведенное решение принадлежит Дж.Пойя.

16.89. Условия а) и б) можно переписать в следующем виде:

1) $\sum\limits_{\nu=1}^{N}\delta_\nu^2=O(n^{\epsilon-1})$;

2) $\sum\limits_{\nu=1}^{N}|\delta_\nu|=O(n^{1/2+\epsilon})$.

Рассмотрим утверждение

3) $\left|\sum\limits_{k=1}^{n}\right|=O(n^{1/2+\epsilon})$.

Отметим, что оно эквивалентно не только гипотезе Римана о нулях дзета-функции, но также и следующему утверждению: для количества $\pi(x)$ всех простых чисел, не превосходящих x, справедлива формула

$$\pi(x)=\int_2^x\frac{dt}{\ln t}+O(x^{1/2+\epsilon}).$$

Доказывать это, однако, мы здесь не будем. Покажем, что справедлива цепочка следствий 1) $\to$ 2) $\to$ 3). На самом деле, также справедливо следствие 3) $\to$ 1), которое мы тоже здесь не будем доказывать. Утверждение 1) $\to$ 2) вытекает из частного случая неравенства Коши

$$\sum_{\nu=1}^{N}|\delta_\nu|\le N^{1/2}\left(\sum_{\nu=1}^{N}\delta_\nu^2\right)^{1/2}$$

и неравенства 1), которое вместе с предыдущим неравенством и теоремой Дирихле (см. § 3) дает, что

$$\sum_{\nu=1}^{N}|\delta_\nu|\le N^{1/2}n^{-1/2+\epsilon}\ll n^{1/2+\epsilon}.$$

Докажем утверждение 2) $\to$ 3). Применяя формулу

$$\sum_{d|n}\mu(d)=1,\quad\text{если}\quad n=1\quad\text{и}\quad\sum_{d|n}\mu(d)=0,\quad\text{если}\ n>1,$$

меняя порядок суммирования и используя формулу суммирования геометрической прогрессии, заметим, что

$$\sum_{\substack{m=1\\(m,k)=1}}^{k}e^{2\pi im/k}=\sum_{m=1}^{k}e^{2\pi im/k}\sum_{d|(m,k)}\mu(d)=$$

$$=\sum_{d|k}\mu(d)\sum_{s=1}^{k/d}e^{2\pi ids/k}=\mu(k).$$

Из этого равенства выводим цепочку равенств

$$\sum_{k=1}^{n}\mu(k)=\sum_{k=1}^{n}\sum_{\substack{m=1\\(m,k)=1}}^{k}e^{2\pi im/k}=\sum_{s=1}^{N}e^{2\pi iw_s}=\sum_{s=1}^{N}e^{2\pi i(\delta_s+s/N)}=$$

$$=\sum_{s=1}^{N}e^{2\pi is/N}+\sum_{s=1}^{N}e^{2\pi is/N}\left(e^{2\pi i\delta_s}-1\right)=S_1+S_2=S_2,$$

так как в силу формулы суммирования геометрической прогрессии

$$S_1=\sum_{s=1}^{N}e^{2\pi is/N}=0.$$

Далее имеем

$$|S_2|\le\sum_{s=1}^{N}\left|e^{2\pi i\delta_s}-1\right|=\sum_{s=1}^{N}|\sin\pi\delta_s|\le\sum_{s=1}^{N}|\pi\delta_s|.$$

Таким образом в силу 2) доказано неравенство

$$\left|\sum_{s=1}^{n}\mu(k)\right|\le\pi\sum_{s=1}^{N}|\delta_s|=O(n^{1/2+\epsilon}).$$

16.90. Для решения этой очень трудной задачи надо воспользоваться разложением в ряд вида $\sum a_k\sin 2\pi kx+b_k\cos 2\pi kx$ (ряд Фурье) функции $f(x)$ с периодом 1, определенной на интервале $[0,1)$ равенством

$$f(x)=\begin{cases}1, & \text{если } \alpha<x<\beta,\ 0\le\alpha<\beta<1,\\ 1/2, & \text{если } x=\alpha \text{ или } x=\beta,\\ 0 & \text{– в остальных случаях.}\end{cases}$$

(См. И.М.Виноградов. Метод тригонометрических сумм в теории чисел. М., Наука, 1980, с.22, лемма 2).

16.91 – 16.92. См. оригинальную работу M.Tsuji. On the uniform disribution of numbers mod.1.//Journal of the Mathematical Society of Japan. 1952. - V. 4, №3 – 4. P. 313 – 322.

16.93. См. I. Schoenberg. Ueber die asymptotische Verteilung reeller Zahlen mod.1.//Math. Z. 1928. – B. 28. S. 171 – 199.

§ 17. БЫСТРЫЕ ВЫЧИСЛЕНИЯ С ЦЕЛЫМИ ЧИСЛАМИ, МНОГОЧЛЕНАМИ И ДРОБЯМИ

Еще средневековые математики Ближнего Востока нашли простой подход к вычислениям с дробными числами — использование десятичных позиционных дробей. Позиционная десятичная система попала туда, видимо, из Индии, хотя позиционные дроби, правда не десятичные, а шестидесятеричные, были известны в Шумере, а десятичные дроби, кажется, впервые появились в Китае. Но заслуга введения

десятичных дробей и алгоритмов действия с ними в практику принадлежит нидерландскому ученому и инженеру Симону Стевину (1548 – 1620). Сейчас эти алгоритмы с успехом работают в любом микрокалькуляторе, что вполне может привести к тому, что школьники совсем разучатся их выполнять вручную.

Однако мало кто знает, что относительно недавно были открыты гораздо более быстрые алгоритмы умножения и деления многозначных чисел и многочленов (и, разумеется, позиционных дробей). Первый такой алгоритм придумал в 1962 г. А.А.Карацуба, отвечая на вопрос, поставленный А.Н.Колмогоровым.

Идею метода Карацубы можно пояснить на следующем примере. Пусть перемножаются восьмизначные числа $U = \overline{u_1 \dots u_8}$ и $V = \overline{v_1 \dots v_8}$. Представим их как двузначные числа в 10^4-значной системе счисления: $U = U_1U_2$, $V = V_1V_2$. Тогда их произведение можно представить в следующем виде:

$$UV = U_1V_1 10^8 + ((U_1 - U_2)(V_2 - V_1) + U_1V_1 + U_2V_2)10^4 + U_2V_2.$$

Эта формула сводит умножение восьмизначных чисел к трем операциям умножения и шести операциям сложения – вычитания четырехзначных чисел (с учетом переносов в следующие разряды). Обычный способ требует четырех умножений и трех сложений – вычитаний, но так как три раза сложить четырехзначные числа можно быстрее, чем один раз перемножить, то метод Карацубы уже восьмизначные числа умножает быстрее. В общем случае он требует для умножения n-значных чисел по порядку не больше

$$n^{\log_2 3} < n^{1,585}$$

операций над цифрами, для школьного же метода требуется по порядку n^2 операций.

Впоследствии А.Л.Тоомом (в 1963 г.) и Ф.Штрассеном совместно с А.Шенхаге (в 1969 г.) были построены более быстрые алгоритмы умножения n-значных чисел при больших значениях n (но эти алгоритмы существенно более сложные для понимания). Так, алгоритм Шенхаге–Штрассена, требующий для умножения n-значных чисел по порядку $n \log_2 n \log_2 \log_2 n$ операций, начинает превосходить по скорости работы метод Карацубы лишь при n порядка нескольких тысяч.

Далее читатель познакомится с некоторыми результатами о сложности вычислений более подробно.

В первом (очень простом) цикле задач речь идет о том, как по возможности быстрее следует производить арифметические операции с дробями, сводя их к операциям над целыми числами.

17.1. Пусть $(a,d)=g_1, (b,c)=g_2$. Докажите, что

$$((a/g_1)(c/g_2), (d/g_1)(b/g_2))=1.$$

17.2. Допустим, что дроби a/b и c/d несократимы и числа a,b,c,d меньше 10^n . Предложите способ умножения и деления этих дробей, в котором все промежуточные результаты будут меньше 10^n , если в окончательном ответе числитель и знаменатель меньше 10^n .

17.3. Пусть

$$(a,b)=(c,d)=1,\ \ (b,d)=g_1,\ \ t=ad/g_1+bc/g_1,\ \ (t,g_1)=g_2.$$

Докажите, что b делится на g_2 и

$$(t/g_2,\ \ (d/g_1)(b/g_2))=1.$$

17.4. Допустим, что дроби a/b и c/d несократимы и числа a,b,c,d меньше 10^n . Предложите способ сложения и вычитания этих дробей, в котором все промежуточные результаты будут меньше 10^n , кроме одного, который будет меньше 10^{2n} , если в окончательном ответе числитель и знаменатель меньше 10^n.

Легко видеть, что аналоги задач 17.1 – 17.4 имеют место и для алгебраических дробей.

Прорешав следующий цикл задач, читатель научится быстрее умножать многоразрядные числа и многочлены высоких степеней, чем его учили в школе.

17.5. Проверьте, что умножение двух многочленов степеней, меньших $2n$, можно свести к умножению трех пар многочленов степеней, меньших n, и сложению четырех пар многочленов степеней, меньших n, и вычитанию двух пар многочленов степеней меньших $2n$ с помощью тождества

$$(f_1x^n+f_0)(g_1x^n+g_0)=$$

$$=f_1g_1x^{2n}+((f_1+f_0)(g_1+g_0)-f_1g_1-f_0g_0)x^n+f_0g_0.$$

Обозначим через $M(n)$ наименьшее количество операций сложения, вычитания и умножения (выполняемых над коэффициентами многочленов и промежуточными числовыми результатами), требующихся для перемножения двух многочленов степеней, меньших n.

17.6. Докажите, что $M(n)\le 2M(]n/2[)+M([n/2])+4[n/2]+2n-4$.

17.7. Проверьте, что обычный способ умножения многочленов дает оценку $M(n)\le M_s(n)=n^2+(n-1)^2$.

17.8*. *(Карацуба)* Докажите, что при $2^k \mid n$ справедливо неравенство

$$M(n)\le 3^k\left(M\left(n/2^k\right)+8n/2^k-2\right)-8n+2,$$

а при любом n — неравенство

$$M(n) < (35/3)\, n^{\log_2 3}.$$

17.9*. Найдите наименьшее n, при котором $M(n) < M_s(n)$, и наименьшее n, начиная с которого $M(n) < M_s(n)$.

17.10*. Найдите возможно меньшую константу в оценке Карацубы при больших n

$$M(n) \leq C \cdot n^{\log_2 3}.$$

Обозначим через $M(m, n)$ наименьшее количество операций сложения, вычитания и умножения, требующихся для перемножения двух многочленов степеней меньших m и n соответственно.

17.11. Докажите, что при $m \geq n$ справедливо неравенство

$$M(m, n) \leq \rceil m/n \lfloor M(n) + m - m/n$$

и при $m/n \to \infty$ и предположении, что $M(n)/n \to \infty$ при $n \to \infty$, справедливо асимптотическое неравенство

$$M(m, n) \underset{\sim}{\leq} mM(n)/n.$$

Обозначим через $M(n)$ наименьшее количество операций сложения, вычитания и умножения, выполняемых над числами, меньшими a, требующихся для умножения двух n-значных чисел, записанных в позиционной системе счисления по основанию a.

17.12. Докажите, что сложение двух n-значных чисел можно выполнить за $2n - 1$ операцию, вычитание из большего меньшее – за $3n - 1$ операцию, вычитание с определением знака разности – за $4n - 1$ операцию, а сложение $(n + m)$-значного числа с n-значным можно выполнить за $2n + m - 1$ операцию.

17.13. Докажите, что обычный способ умножения чисел дает оценку

$$M(n) \leq M_s(n) = 5n^2 - 3n - 2.$$

17.14*. Докажите методом Карацубы, что

$$M(2n) \leq 3M(n) + 19n - 2, M(2n + 1) \leq 2M(n + 1) + M(n) + 17n + 10.$$

17.15*. Получите для $M(n)$ оценку Карацубы (по возможности с лучшей константой).

17.16*. Найдите наименьшее n, начиная с которого $M(n) < M_s(n)$.

Обозначим через $M(m, n)$ наименьшее количество операций сложения, вычитания и умножения, требующихся для умножения m-значного числа на n-значное.

17.17. Докажите, что при $m \geq n$ справедливо неравенство

$$M(m,n) \leq \lceil m/n \rceil M(n) + 2m - n + 1$$

и при $m/n \to \infty$ и предположении, что $M(n)/n \to \infty$ при $n \to \infty$, справедливо асимптотическое неравенство

$$M(m,n) \underset{\sim}{\leq} mM(n)/n.$$

17.18*. Предполагая, что $M(n)/n$ монотонно стремится к ∞ при $n \to \infty$, докажите, что для возведения записанного в двоичной системе числа x в N-ю степень достаточно $2M(\lfloor N \log_2 x \rfloor)(1 + o(1))$ операций. Если для любого C при достаточно большом m/n в сравнении с n справедливо неравенство $M(m)\,n/(M(n)\,m) > C$, то для любого ϵ при достаточно большом N в сравнении с x для вычисления x^N требуется не более $M(\lfloor N \log_2 x \rfloor)(1 + \epsilon)$ операций.

Получите аналогичный результат для возведения в степень многочленов.

Очередной цикл задач посвящен быстрому делению многочленов. В нем будет показано, что деление можно выполнять по порядку с той же сложностью, что и умножение.

Обозначим через $D_0(m,n)$ наименьшее количество арифметических операций над числами, требующихся для нахождения неполного частного при делении многочлена степени не выше m на многочлен степени n, а через $D(m,n)$ – сложность деления этих многочленов, в которую включается также сложность нахождения остатка от деления и произведения неполного частного на делитель. Очевидно, что при $m \leq n$ обе эти величины равны нулю. Далее для удобства изменим определение $M(n,m)$, заменив его на $M(n+1, m+1)$, т. е. обозначим через $M(m,n)$ сложность умножения двух многочленов степеней m и n соответственно.

Для любых двух многочленов $p(x)$ и $q(x)$ обозначим через $[p(x)/q(x)]$ целую часть рациональной функции $p(x)/q(x)$, т. е. неполное частное при делении $p(x)$ на $q(x)$. Дробную часть этой функции, т. е. разность $p(x)/q(x) - [p(x)/q(x)]$, обозначим через $\{p(x)/q(x)\}$. Тогда остаток от деления $p(x)$ на $q(x)$ равен числителю последней дроби, т. е. $q(x)\{p(x)/q(x)\}$.

17.19. Докажите, что если определить $D(m,n)$, не требуя вычисления произведения неполного частного на делитель, то сложность уменьшается не более чем на n.

17.20. Докажите, что при $m \geq n$ справедливо неравенство

$$D(m,n) < D_0(m,n) + M(m-n,n) + n.$$

17.21. Докажите, что при $m \geq n$ справедливо неравенство

$$D(m,n) \leq D(2n-1,n)\,[m/n] < mD(2n,n)/n.$$

Обозначим через $R(m,n)$ наименьшее количество арифметических операций над числами, требующихся для нахождения неполного частного при делении многочлена x^m на произвольный многочлен степени n. Очевидно, что $R(m,n) \leq D(m,n)$.

Правильной называется дробь, у которой степень числителя меньше степени знаменателя.

17.22. Докажите, что сумма правильных дробей – правильная дробь, сумма дробных частей нескольких рациональных функций равна дробной части их суммы, и то же самое верно для суммы их целых частей. Если разность между рациональными функциями равна правильной дроби, то их целые части равны.

17.23. Пусть у рациональной функции R_1 степень числителя не больше степени знаменателя. Тогда для любой рациональной функции R_2 справедливо равенство $[R_1\,[R_2]] = [R_1 R_2]$.

17.24. Докажите, что при $m \geq k$ сложность вычисления k старших коэффициентов в произведении многочленов степеней m и n не превосходит величины $M(k,n)$.

17.25. Докажите, что при $m \geq n$ справедливо неравенство

$$D_0(m,n) \leq R(m,n) + M(m,m-n).$$

17.26. Докажите, что функция $M(n,m)$ монотонна по обеим переменным, а $D(m,n)$ и $R(m,n)$ – только по первой.

17.27. Докажите неравенства

$$M(n,m) \geq n+m+1,\, D(n,m) \geq n+m+1.$$

17.28*. Пусть многочлен $P_k = \left[x^{k+n}/g\right]$, где g – заданный многочлен степени n со старшим коэффициентом a, а следующим – b. Докажите, что $P_1(x) = a^{-1}x - a^{-2}b$,

$$P_{2k+1} = 2\cdot x^{k+1}P_k - \left[P_k^2 g/x^{n-1}\right],\, P_{2k} = 2\cdot x^k P_k - \left[P_k^2 g/x^n\right].$$

17.29. Положим для краткости $R_k = R(n+k,n)$. Докажите, что при любом k справедлива оценка

$$R_k \leq R_{[k/2]} + M([k/2]) + M(k) + 2\,[k/2] + 2.$$

17.30. Положим

$$[k]_i = \left[[k]_{i-1}\right]_1,\, [k]_1 = [k/2],\, m = [\log_2 k],$$

и обозначим через $\nu(k)$ сумму всех цифр двоичной позиционной записи числа k.

Докажите, что

$$\sum_{i=1}^{m}[k]_i = \sum_{i=1}^{m}\left[k/2^i\right] = k - \nu(k).$$

17.31. Докажите, что справедливо неравенство

$$M(2n+1, n) \leq 2M(n) + n.$$

Пусть $\mathbb{M}(n)$ обозначает любую функцию такую, что

$$M(n) \leq \mathbb{M}(n) \leq \mathbb{M}(2n)/2.$$

17.32. Докажите, что $R_k \leq 3\mathbb{M}(k) + 2k + 2\left[\log_2 k\right] - 2\nu(k)$, в частности, при $k = 2^s - 1$, справедливо неравенство

$$R_k \leq 3\mathbb{M}(k) + 2k - 2.$$

17.33. Докажите, что

$$R(m, n) < 3\mathbb{M}(m-n) + 2(m-n) + 2\log_2(m-n).$$

17.34. Докажите, что $D(2n, n) < 6\mathbb{M}(n) + 4n + 2\log_2 n$.

17.35. Докажите, что при $m \geq 2n$ справедлива оценка

$$D(m, n) < \frac{6m\mathbb{M}(n)}{n} + 6m,$$

а при $n \to \infty$ и предположении, что $\mathbb{M}(n)/n \to \infty$ справедливо асимптотическое неравенство

$$D(m, n) \underset{\sim}{<} 6m\mathbb{M}(n)/n.$$

17.36. Докажите, что при $n \leq m < 2n$ справедлива оценка

$$D(m, n) \leq 2m\mathbb{M}(m-n)/(m-n) +$$

$$+4\mathbb{M}(m-n) + n + 2(m-n) + o(m-n),$$

а при условиях $m - n \to \infty$, $(m-n)/n \to 0$ и предположении, что $\mathbb{M}(n)/n \to \infty$ и $\mathbb{M}(n)/n^2 \to 0$ справедливо асимптотическое неравенство

$$D(m, n) \underset{\sim}{<} 2m\mathbb{M}(m-n)/(m-n).$$

17.37. Докажите, что при любых неотрицательных целых m, n, k, s справедливо неравенство $D(m+k+s, n+k) \geq D(m, n)$, и, в частности, последовательность $D(2n, n)$ монотонна.

17.38. Докажите, что при любых натуральных n, k, $k > 1$, имеет место неравенство $D(nk, n) \leq (k-1) D(2n, n)$.

17.39. Пусть для рациональных функций R_1 и R_2 удвоенная степень многочлена $[R_2]$ не меньше степени многочлена $[R_1]$. Докажите, что справедливо равенство $[R_1/[R_2]] = [R_1/R_2]$.

17.40. Докажите, что для любых многочленов f и g степени n справедливо тождество

$$fg = \left[\frac{x^{3n} f}{[x^{3n}/g]}\right].$$

Положим для краткости $D(n) = D(2n, n)$.

17.41. Докажите, что

$$M(n) \leq 2D(n) + D(2n).$$

17.42. Докажите, что $D(2n) > M(n)/2$.

Пусть $\Delta(n)$ обозначает любую функцию, удовлетворяющую соотношениям

$$D(n) \leq \Delta(n), \Delta(n)/\Delta(2n) \to 1/2.$$

17.43. Докажите, что $\Delta(n) \gtrsim M(n)/4$.

В следующем цикле задач речь идет о быстром делении чисел. Его результаты во многом аналогичны предыдущему циклу. Далее обозначаем через $\{\{x\}\}$ ближайшее целое к числу x, причем при целом n полагаем $\{\{n+1/2\}\} = n+1$, а вместо $[2^n x]\, 2^{-n}$ пишем x_n.

17.44*. Пусть $z_k = z_{k,-1} z_{k,0}, z_{k,1} \ldots z_{k,k}$ — двоичная k-разрядная дробь такая, что

$$|z_k - 1/q| \leq 2^{-k},$$

где $1/2 \leq q < 1$, и

$$z_{2k-1} = \left\{\left\{\left(2z_k - q_{2k+2} z_k^2\right) 2^{2k-1}\right\}\right\} 2^{1-2k}.$$

Докажите, что

$$|z_{2k-1} - 1/q| \leq 2^{-2k+1}, \quad 1 \leq z_{2k-1} \leq 2$$

и z_{2k-1} – двоичная $(2k-1)$-разрядная дробь.

Обозначим через R_k наименьшее количество операций над числами 0 и 1, требующихся для нахождения двоичной k-разрядной дроби z_k такой, что $|z_k - 1/q| \leq 2^{-k}$, где q – заданная двоичная дробь, $1/2 \leq q < 1$, а через $\mathbb{M}(n)$ – любую функцию, удовлетворяющую соотношениям $M(n) \leq \mathbb{M}(n) \leq \mathbb{M}(2n)/2$.

17.45. Докажите, что

$$R_k \leq R_{[k/2]+1} + M([k/2]+2) + M(2[k/2]+4) + O(k) \leq$$

$$\leq R_{[k/2]+1} + M([k/2]+1) + M(k) + O(k).$$

17.46. Докажите, что $R_k \leq 3\mathbb{M}(k) + O(k)$.

Обозначим через $R(m,n)$ наименьшее количество операций над числами 0 и 1, требующихся для нахождения $[2^{m-1}/Q]$, где Q – произвольное двоичное n-разрядное число, $Q = \sum_{i=0}^{n-1} 2^i \alpha_{n-i}$, где $\alpha_j = 0$ или $1, \alpha_{n-1} = 1$.

17.47. Докажите, что $R(k+n,n) \leq R_k + M(k,n) + 2k$.

17.48. Докажите, что

$$R(m,n) \leq 3\mathbb{M}(m-n) + M(m-n,n) + O(m-n).$$

Обозначим через $D(m,n)$ наименьшее количество операций над числами 0, 1 требующихся для нахождения неполного частного и остатка при делении не более чем m-разрядного двоичного числа на n-разрядное двоичное число, а также произведения неполного частного на делитель.

17.49. Докажите, что при $m > n$ справедливо неравенство

$$D(m,n) \leq 4\mathbb{M}(m-n) + M(n,m-n) + O(m).$$

17.50. Докажите, что функция $M(n,m)$ монотонна по обеим переменным, а $D(m,n)$ и $R(m,n)$ – только по первой. Докажите, что при любых неотрицательных целых m, n, k, s

$$D(m+k+s,n+k) \geq D(m,n),\ R(m+k+s,n+k) \geq R(m,n),$$

и, в частности, последовательность $\{D(n)\}$, равная по определению $\{D(2n,n)\}$, монотонна.

17.51. Докажите неравенства

$$M(n,m) \geq n+m-1,\ D(n,m) \geq n+m-1.$$

17.52. Докажите, что при $m \geq 2n$ справедливо неравенство

$$D(m,n) \leq D(n)(]m/n[-1) + O(m) < mD(n)/n + O(m).$$

17.53. Докажите, что $D(n) < 5\mathbb{M}(n) + O(n)$.

17.54. Докажите, что при $m \geq 2n$ справедливы оценки

$$D(m,n) < 5m\mathbb{M}(n)/n + O(m),$$

а при $n \to \infty$ и предположении, что $\mathbb{M}(n)/n \to \infty$, справедливо асимптотическое неравенство

$$D(m,n) \lesssim 5m\mathbb{M}(n)/n.$$

17.55. Докажите, что при $n < m < 2n$ справедлива оценка

$$D(m,n) \leq n\mathbb{M}(m-n)/(m-n) + 4\mathbb{M}(m-n) + O(n),$$

а при условиях $m-n \to \infty$, $(m-n)/n \to 0$ и предположении, что $\mathbb{M}(n)/n \to \infty$ и $\mathbb{M}(n)/n = o(n)$, справедливо асимптотическое неравенство

$$D(m,n) \lesssim n\mathbb{M}(m-n)/(m-n).$$

17.56. Пусть A и B – n-разрядные двоичные числа. Докажите, что

$$\left[\frac{2^{3n-1}A}{[2^{3n-1}/B]}\right] = AB.$$

17.57. Докажите, что $D(n+1) < D(n) + O(n)$.

17.58. Докажите, что

$$M(n) \leq 2D(n) + D(2n) + O(n).$$

17.59. Докажите, что $D(2n) \gtrsim M(n)/2$.

Пусть $\Delta(n)$ обозначает любую функцию, удовлетворяющую соотношениям $D(n) \leq \Delta(n)$, $\Delta(n)/\Delta(2n) \to 1/2, \Delta(n)/n \to \infty$.

17.60. Докажите, что $\Delta(n) \gtrsim M(n)/4$.

В последнем цикле задач речь о возведении чисел в квадрат и извлечении квадратных корней.

Обозначим через $K(n)$ сложность возведения n-разрядного числа в квадрат. Очевидно, что $K(n) \leq M(n)$.

17.61. Используя тождество

$$ab = \frac{(a+b)^2 - (a-b)^2}{4},$$

докажите неравенство $M(n) \leq 2K(n) + 11n + O(1)$.

17.62. Докажите, что для любого n-разрядного числа x число

$$\left[\frac{2^{4n-1}}{[2^{4n-1}/x] - [2^{4n-1}/(x+1)]}\right] - x$$

отличается от x^2 не более, чем на 3.

Обозначим для краткости $R(2n, n)$ через $R(n)$.

17.63. Докажите неравенство

$$K(n) < R(4n, 2n) + 2R(4n, n) + O(n) < 3R(3n) + O(n).$$

Из утверждений задач 17.53, 17.60, 17.61, 17.63 вытекает, что функции $K(n), M(n), D(n), R(n)$ имеют одинаковый порядок роста.

Определим теперь функцию $SQR(n)$ как сложность вычисления для любого n-разрядного числа x целой части его арифметического квадратного корня.

17.64. Докажите для любого целого x, $0 \leq x < 2^n$, равенство

$$\left[\sqrt{2^{12n+6} + x \cdot 2^{9n+6}}\right] = 2^{6n+3} + x \cdot 2^{3n+2} - x^2.$$

17.65. Докажите неравенство $K(n) < SQR(12n + 7) + 4n$.

17.66*. Докажите неравенство $SQR(n) < C \cdot M(n)$, где C – некоторая константа.

УКАЗАНИЯ

17.1. Воспользуйтесь тем, что $((a/g_1), (d/g_1)) = 1 = ((c/g_2), (b/g_2))$ и примените, например, теорему об однозначности разложения на простые множители.

17.2. Воспользуйтесь тем, что

$$\frac{(a/g_1)(c/g_2)}{(d/g_1)(b/g_2)} = \frac{ac}{db},$$

и примените задачу 17.1.

17.3. Для решения удобно применить теорему об однозначности разложения на простые множители. Число b делится на g_2, так как $g_2 \mid g_1$ и $g_1 \mid b$. Поэтому $g_2 \mid (d/g_1)\, b$, а так как $g_2 \mid t$, то $g_2 \mid (t, (d/g_1)\, b)$. Так как $((b/g_1), (d/g_1)) = 1 = (c, d)$, то $(t, (d/g_1)) = 1$, значит, $(t, b) = (t, (d/g_1)\, b)$ и $g_2 \mid (t, b)$. Но $tg_1 = ad + bc$, $(a, b) = 1$, следовательно, $(t, b) \mid d$, потому и $(t, b) \mid (d, b) = g_1$, откуда имеем, что $(t, b) \mid (t, g_1) = g_2$, а это вместе с тем, что $g_2 \mid (t, b)$, дает равенства $(t, b) = g_2$ и

$$(t/g_2, (d/g_1)(b/g_2)) = (t, (d/g_1)\, b)/g_2 = (t, b)/g_2 = 1.$$

17.4. Примените 17.3 и равенство

$$\frac{t/g_2}{(d/g_1)(b/g_2)} = \frac{ad + bc}{bd},$$

а также неравенства $g_2 \leq g_1 \leq b < 10^n$.

17.6. Применим равенство

$$\left(f_1 x^{[n/2]} + f_0\right)\left(g_1 x^{[n/2]} + g_0\right) =$$

$$= f_1 g_1 x^{2[n/2]} + ((f_1 + f_0)(g_1 + g_0) - f_1 g_1 - f_0 g_0) x^{[n/2]} + f_0 g_0,$$

где степени многочленов f_1 и g_1 меньше $]n/2[$, а степени многочленов f_0 и g_0 меньше $[n/2]$, и заметим, что для вычисления произведений f_1g_1, f_0g_0 требуется не более $M(]n/2[) + M([n/2])$ операций, для вычисления сумм $f_1 + f_0$, $g_1 + g_0$, $f_1g_1 + f_0g_0$ нужно не более $2[n/2]+2[n/2]-1$ операций (так как число операций равно наименьшему из количеств ненулевых коэффициентов у складываемых многочленов), для вычисления произведения $(f_1 + f_0)(g_1 + g_0)$ используется не более $M(]n/2[)$ операций, для вычисления разности $(f_1 + f_0)(g_1 + g_0) - f_1g_1 - f_0g_0$ достаточна $n-1$ операция, так как

$$(f_1 + f_0)(g_1 + g_0) - f_1g_1 - f_0g_0 = f_1g_0 + f_0g_1,$$

значит, степень этого многочлена равна $[n/2]+]n/2[-2 = n-2$, сложение многочленов f_0g_0 и $f_1g_1x^{2[n/2]}$ выполняется "бесплатно", так как они не имеют подобных членов, причем в их сумме отсутствует член вида $x^{2[n/2]-1}$, поэтому для сложения многочленов

$$f_0g_0 + f_1g_1x^{2[n/2]} \quad \text{и} \quad (f_1g_0 + f_0g_1)x^{[n/2]}$$

достаточно $n-2$ операции. В результате требуется дополнительно $4[n/2] + 2n - 4$ операции.

17.7. Для вычисления произведения двух многочленов степеней, меньших n, требуется n^2 попарных умножений их коэффициентов и для вычисления каждого из $2n-3$ коэффициентов, кроме старшего и свободного членов, требуются еще операции сложения в количестве на 1 меньше, чем число соответствующих слагаемых, поэтому общее число сложений на $2n-3$ меньше числа n^2-2 складываемых произведений.

17.8. Пусть $2^km = n$. Тогда неравенство

$$M(n) \leq 3^k(M(m) + 8m - 2) - 8n + 2$$

доказывается индукцией по k. База ($k = 1$) доказана в 17.6. Шаг индукции обосновывается тем же неравенством 17.6.

Выберем k так, чтобы $2^k < n \leq 2^{k+1}$. Тогда если $3 \cdot 2^{k-1} < n$, то

$$M(n) \leq M\left(2^{k+1}\right) < 3^{k-1}(M(4) + 30) \leq 3^{k-1} \cdot 55 <$$

$$< 55 \cdot \left(\frac{n}{3}\right)^{\log_2 3} < \frac{35}{3}n^{\log_2 3}.$$

Если же $n \leq 3 \cdot 2^{k-1}$, то

$$M(n) \leq M\left(3 \cdot 2^{k-1}\right) < 3^{k-1}(M(3) + 22) \leq 3^{k-1} \cdot 35 \leq (35/3)n^{\log_2}.$$

17.9. С помощью 17.6 – 17.7 проверьте, что $M(n) < M_s(n)$ при $n = 6$ и $8 \leq n \leq 15$. Используя последнее утверждение как базу, докажите при $n \geq 8$ неравенство $M(n) < M_s(n)$ по индукции, осуществляя индукционный переход от n и $n+1$ к $2n$ и $2n+1$ с помощью 17.6 и неравенств

$$3M_s(n) + 8n - 4 = 3\left(n^2 + (n-1)^2\right) + 8n - 4 \leq 4n^2 + (2n-1)^2 = M_s(2n),$$

$$2M_s(n+1) + M_s(n) + 8n = 3M_s(n) + 16n - 4 \leq$$

$$\leq M_s(2n) + 8n = M_s(2n+1),$$

т. е. предполагая неравенство $M(n) < M_s(n)$ верным при $2^{k-1} \leq n < 2^k$, доказываем его справедливость при $2^k \leq n < 2^{k+1}$.

17.10. Разбейте интервал $2^k < n \leq 2^{k+3}$ на части $2^k < n \leq 3 \cdot 2^k$, $3 \cdot 2^k < n \leq 5 \cdot 2^k$, $5 \cdot 2^k < n \leq 7 \cdot 2^k$, $7 \cdot 2^k < n \leq 2^{k+3}$ и рассуждайте подобно 17.8.

17.11. Представьте многочлен степени, меньшей m, в виде

$$f_0 + f_1 x^n + \ldots + f_k x^{nk},$$

где $k =]m/n[- 1$, и степени многочленов f_i меньше n и, используя тождество

$$\left(f_0 + f_1 x^n + \ldots + f_k x^{nk}\right) g = \left(f_0 g + f_1 g x^n + \ldots + f_k g x^{nk}\right),$$

и неравенство $m/n \geq]m/n[- 1$, получите оценку

$$M(m,n) \leq]m/n[\, M(n) + (n-1)\,(]m/n[- 1) <$$

$$<]m/n[\, M(n) + m - m/n < mM(n)/n + m + M(n) =$$

$$= (mM(n)/n)\,(1 + n/M(n) + n/m).$$

17.12. Если при вычитании из k-й цифры уменьшаемого k-й цифры вычитаемого получается отрицательное число, то нужна еще операция прибавления к разности числа b – основания используемой системы счисления. Отсюда n дополнительных операций при выполнении вычитания.

17.13. Примените 17.12.

17.14. Применим тождества

$$\left(f_1 b^{]n/2[} + f_0\right)\left(g_1 b^{]n/2[} + g_0\right) =$$

$$= f_1 g_1 b^{2]n/2[} + (f_1 g_1 + f_0 g_0 - (f_1 - f_0)(g_1 - g_0))\, b^{]n/2[} + f_0 g_0,$$

где числа f_1 и g_1 – $[n/2]$-разрядные, а числа f_0 и g_0 соответственно $]n/2[$ -разрядные, и заметим, что для вычисления произведений $f_1 g_1$ и $f_0 g_0$ требуется $M(]n/2[) + M([n/2])$ операций, для вычисления разностей и суммы

$$f_0 - f_1, g_0 - g_1, f_1 g_1 + f_0 g_0$$

требуется не более

$$n\,(1 + [n/2] -]n/2[) + 2\,([n/2] +]n/2[- 1) + 2\,([n/2] +]n/2[) - 1 =$$

$$= 4n - 3 + n\,(1 + [n/2] -]n/2[)$$

операций, так как числа $f_1 g_1$ и $f_0 g_0$ имеют не более чем $2[n/2]$ и $2]n/2[$ разрядов соответственно, а в случае четного n нужно еще $2[n/2] = n$ операций для предварительного сравнения чисел (чтобы не вычитать из меньшего большее). Заметим далее, что для вычисления произведения $(f_1 - f_0)(g_1 - g_0)$ требуется не более $M(]n/2[) + 1$ операций (одна операция для вычисления знака у произведения), для вычисления разности

$$f_1 g_1 + f_0 g_0 - (f_1 - f_0)(g_1 - g_0) = f_1 g_0 + f_0 g_1$$

требуется не более $2]n/2[+ 1 + 2]n/2[- 1 = 4]n/2[$ операций, сложение чисел $f_0 g_0$ и $f_1 g_1 b^{2]n/2[}$ осуществляется "бесплатно" (записи этих чисел просто объединяются в одну запись), а для сложения чисел $f_1 g_1 b^{2]n/2[} + f_0 g_0$ и $(f_1 g_0 + f_0 g_1)\, b^{]n/2[}$

требуется не более $2n-]n/2[+n+1-1=2n+[n/2]$ операций (так как число $f_1g_0+f_0g_1$ имеет не более $n+1$ разряда, а младшие $[n/2]$ разрядов числа f_0g_0 не участвуют в операциях). В результате требуется дополнительно

$$4n-3+n\,(1+[n/2]-]n/2[)+1+4]n/2[+2n+[n/2]=$$

$$=7n+3]n/2[+n\,(1+[n/2]-]n/2[)-2$$

операций.

17.15. Поступайте, как и в 17.10.

17.16. Согласно 17.13, $M_s(n)=5n^2-3n-2$. В частности, имеем $M(2)=12$, $M(3)=34$, $M(4)=66$, $M(5)=108$, $M(6)=160$, $M(7)=222$, $M(8)=294$. Применяя неравенства

$$M(2n)\leq 3M(n)+19n-2,\, M(2n+1)\leq 2M(n+1)+M(n)+17n+10,$$

проверьте, что для $n=8,9,\ldots,15$ справедливо неравенство $M(n)<M_s(n)$. Предполагая, что это неравенство верно при $n=2^{k-1},\ldots,2^k-1$, докажите, что оно верно и для $n=2^k,\ldots,2^{k+1}-1$, проверяя, что

$$M(2n)\leq 3M(n)+19n-2<$$

$$<3M_s(n)+19n-2=3\left(5n^2-3n-2\right)+19n-2<$$

$$<5\,(2n)^2-3\,(2n)-2=M_s(2n),$$

$$M(2n+1)\leq 2M(n+1)+M(n)+17n+10<$$

$$<2M_s(n+1)+M_s(n)+17n+10=$$

$$=2\left(5\,(n+1)^2-3\,(n+1)-2\right)+\left(5n^2-3n-2\right)+17n+10<$$

$$<5\,(2n+1)^2-3\,(2n+1)-2=M_s(2n+1).$$

17.17. Представим m-разрядное число в виде

$$\left(f_0+f_1b^n+\ldots+f_kb^{nk}\right),$$

где $k=]m/n[-1$ и числа f_i имеют не более n разрядов, и используя тождество

$$\left(f_0+f_1b^n+\ldots+f_kb^{nk}\right)g=\left(f_0g+f_1gb^n+\ldots+f_kgb^{nk}\right)=$$

$$=\left(f_0g+f_2gb^{2n}+\ldots+f_{2[k/2]}gb^{n2[k/2]}\right)+$$

$$+\left(f_1gb^n+f_3gb^{3n}+\ldots+f_{2]k/2[-1}gb^{n2]k/2[-1}\right)$$

и неравенство $m/n\geq\,]m/n[-1$, получим оценку

$$M(m,n)\leq\,]m/n[M(n)+2\,(m-n)-1+n\leq$$

$$\leq mM(n)/n+M(n)+2m-n+1<$$

$$<(mM(n)/n)\,(1+2n/M(n)+n/m),$$

так как числа в скобках вычисляются "бесплатно", младшие n разрядов числа f_0g не участвуют в нетривиальных операциях, а по старшим n разрядам

большего из чисел $f_{2[k/2]}g^{b^{n2[k/2]}}$ и $f_{2]k/2[-1}g^{b^{n2]k/2[-1}}$ проходит только перенос единицы (который скорее всего быстро затихает где-то в начале).

17.18. Если обозначить через $\lambda(x)$ длину двоичной записи числа x, то будут справедливы соотношения

$$\lambda(x)+\lambda(y)-1\le\lambda(xy)\le\lambda(x)+\lambda(y),$$

$$m\lambda(x)-m+1\le\lambda(x^m)\le m\lambda(x),\quad \lambda\left(x^{1/m}\right)=]\lambda(x)/m[.$$

Выбрав n так, чтобы $2^{4n}<N$, и $n\to\infty$, и представив N в виде

$$(\ldots(a_1 2^n+a_2)2^n+\ldots+a_{l-1})2^n+a_l,$$

где $0\le a_i<2^n$, $l=[\log_2 N/n]+1$, определим последовательность

$$y_1=x^{a_1},\ y_2=x^{a_2}y_1^{2^n},\ \ldots,\ y_l=x^{a_l}y_{l-1}^{2^n},$$

тогда

$$y=y_l,\ y_{l-k}<y^{2^{-kn}},\ k=1,\ldots,l-1.$$

Используя 17.17, докажите, что последовательность $x^2,\ldots,x^{2^n}$ можно вычислить со сложностью

$$O\left(2^{2n}M(\lambda(x))\right)=O\left(2^{2n}M(\lambda(y))/N\right)=O\left(2^{-n}M(\lambda(y))\right).$$

Если задано число z, то вычислить $w=z^{2^n}$ можно со сложностью

$$\sum_{k=0}^{n-1}M\left(\lambda\left(z^{2^k}\right)\right)=\sum_{k=0}^{n-1}M\left(]2^{-n+k}\lambda(w)[\right)\le$$

$$\le\sum_{k=0}^{n-1}M\left([2^{-n+k}\lambda(w)]\right)+O\left(2^{-n+k}\lambda(w)\right)\le M(\lambda(w))+O(\lambda(w)).$$

Воспользуйтесь для этого неравенствами

$$M(n+1)\le M(n)+O(n),\ M\left(2^{-k}n\right)\le 2^{-k}M(n).$$

Применяя 17.17, покажите, что число y_k можно вычислить (в предположении, что задано число y_{k-1} и последовательность $x^2,\ldots,x^{2^n}$) со сложностью не выше

$$M(2^n\lambda(x))(1+\lambda(y_k)/(2^n\lambda(x)))+M(\lambda(y_k))+O(\lambda(y_k)).$$

Тогда сложность вычисления числа $y=x^N$ оценивается сверху величиной

$$\sum_{k=2}^{l}\frac{M(\lambda(y_k))+\lambda(y_k)M(2^n\lambda(x))}{2^n\lambda(x)}+O(\lambda(y_k))+$$

$$+M(2^n\lambda(x))l+O\left(2^{-n}M(\lambda(y))\right)\le$$

$$\le\sum_{k=2}^{l}]2^{(k-l)n}\lambda(y)[+M(2^n\lambda(x))\log_2 N+\sum_{k=2}^{l}M\left(]2^{(k-l)n}\lambda(y)[\right)+$$

$$+\frac{]2^{(k-l)n}\lambda(y)[M(2^n\lambda(x))}{2^n\lambda(x)} \leq \frac{(1+O(2^{-n}))\,\lambda(y)\,M(2^n\lambda(x))}{2^n\lambda(x)}+$$

$$+M(\lambda(y))+O(\lambda(y)) \leq (2+O(2^{-n}))\,(M(\lambda(y)))+O(\lambda(y)).$$

17.19. Для нахождения произведения неполного частного на делитель достаточно вычесть из делимого остаток.

17.20. Для нахождения остатка воспользуйтесь равенством $r = f - g[f/g]$ и тем фактом, что при вычитании все члены со степенями не ниже n-й сокращаются, поэтому для вычисления остатка достаточно найти разности n младших коэффициентов.

17.21. Представьте многочлен степени m в виде

$$f_0 + f_1 x^n + \ldots + f_k x^{nk},$$

где $k = [m/n]$, степени многочленов f_i меньше n, и используя тождество

$$f = f_0 + f_1 x^n + \ldots + f_k x^{nk} = f' + h_k g x^{n(k-1)} =$$

$$= \left(f_0 + f_1 x^n + \ldots + f_{k-2} x^{n(k-2)} + r_k x^{n(k-1)}\right) + h_k g x^{n(k-1)},$$

где $h_k = [(f_k x^n + f_{k-1})/g]$ – частное, а $r_k = f_k x^n + f_{k-1} - g h_k$ – остаток от деления $f_k x^n + f_{k-1}$ на g, сведите деление f на g к делению f' на g и получите неравенство

$$D(m,n) \leq D(nk+n-1,n) \leq D(nk-1,n) + D(2n-1,n),$$

из которого индукцией следует неравенство

$$D(m,n) \leq D(nk+n-1,n) \leq kD(2n-1,n) =$$

$$= D(2n-1,n)[m/n] < \frac{m}{n} D(n).$$

17.22. Первое из утверждений проверяется непосредственно, второе следует из первого, третье — из второго, четвертое — из первого.

17.23. Непосредственно проверяется, что произведение правильной дроби на дробь, у которой степень числителя не больше степени знаменателя, будет правильной дробью. Тогда, согласно последнему пункту задачи 17.22, справедливо равенство

$$[R_1 R_2] = [R_1([R_2] + \{R_2\})] = [R_1[R_2] + R_1\{R_2\}] = [R_1[R_2]].$$

17.24. Воспользуйтесь вытекающим из 17.23 тождеством

$$\left[fg/x^{m-k+n}\right] = \left[\left[f/x^{m-k}\right] g/x^n\right],$$

где степени многочленов f и g равны m и n соответственно.

17.25. Воспользуйтесь вытекающим из 17.23 тождеством

$$[f/g] = [f/x^m\,[x^m/g]] = [f\,[x^m/g]/x^m],$$

где степени многочленов f и g равны m и n соответственно.

17.26. Первые два утверждения следуют из того, что при формальном добавлении к сомножителям старших членов с нулевыми коэффициентами произведение не меняется и при добавлении к делимому старших членов

с нулевыми коэффициентами частное и остаток тоже не меняются, так как коэффициенты частного и остатка выражаются в виде рациональных функций от коэффициентов делимого и делителя со знаменателями, являющимися степенями старшего коэффициента делителя.

Последнее утверждение следует из тождества

$$[x^m/g] = \left[\left[x^{n+m}/g\right]/x^n\right],$$

вытекающего из 17.23. Немонотонность по второму аргументу следует из того, что при $m < n$, очевидно, $D(m,n) = 0$.

17.27. Докажите, что произведение и частное двух многочленов существенно зависят от их коэффициентов.

17.28. Для доказательства равенства

$$P_{2k+1} = 2 \cdot x^{k+1} P_k - \left[P_k^2 g/x^{n-1}\right]$$

заметьте, что $P_k g = x^{k+n} - gr$, где $r = \left\{x^{k+n}/g\right\}$, и выведите с помощью 17.22 и 17.23 равенство

$$\left[P_k^2 g/x^{n-1}\right] = \left[P_k\left(x^{k+n} - gr\right)/x^{n-1}\right] =$$

$$= \left[P_k x^{k+1} - P_k gr/x^{n-1}\right] = P_k x^{k+1} - \left[P_k gr/x^{n-1}\right] =$$

$$= P_k x^{k+1} - \left[\left(x^{k+n}/g\right) gr/x^{n-1}\right] = P_k x^{k+1} - \left[x^{k+1} r\right],$$

из которых с помощью 17.22 немедленно следует, что

$$2 \cdot x^{k+1} P_k - \left[P_k^2 g/x^{n-1}\right] = 2 \cdot x^{k+1} P_k - P_k x^{k+1} + \left[x^{k+1} r\right] =$$

$$= P_k x^{k+1} + \left[x^{k+1} r\right] = \left[P_k x^{k+1} + x^{k+1} r\right] = \left[x^{k+1}(P_k + r)\right] =$$

$$= \left[x^{k+1}\left(\left[x^{k+n}/g\right] + \left\{x^{k+n}/g\right\}\right)\right] =$$

$$= \left[x^{k+1}\left(x^{k+n}/g\right)\right] = \left[x^{2k+1+n}/g\right] = P_{2k+1}.$$

17.29. Применим 17.26 и рассмотрим случай нечетного k. Получаем неравенство

$$R_k \leq R_{[k/2]} + M([k/2]) + M(2[k/2], n) + 2[k/2] + 2.$$

Далее при $2[k/2] < n$ воспользуемся 17.28, 17.24 и заметим, что для вычисления $\left[P_{[k/2]}^2 g/x^{n-1}\right]$ достаточно найти $2[k/2]+2$ старших коэффициента произведения $P_{[k/2]}^2 g$, что можно сделать со сложностью $M(2[k/2]+1, 2[k/2]) \leq M(k)$. В случае четного k последняя оценка заменяется на $M(2[k/2]) = M(k)$.

17.30. Первое равенство доказывается по индукции с помощью задачи 1.2. Второе равенство доказано в задаче 4.24.

17.31. Для доказательства первых двух неравенств воспользуйтесь тождеством

$$(f_1 x^n + f_0)(g_1 x^n + g_0) = f_1 g_1 x^{2n} + (f_1 g_0 + g_1 f_0) x^n + f_0 g_0,$$

где f_1 и g_1 – имеют степени m, а f_0 и g_0 – степени меньше n.

17.32. Из 17.29 и 17.30 вытекают неравенства

$$R_{[k]_{i-1}} - R_{[k]_i} \leq M([k]_i) + M(2[k]_i) + 2[k]_i + 2,$$

где $[k]_i = [k/2^i]$, $0 \le i \le m$. Складывая их и используя неравенства

$$M([k]_i) \le \mathbb{M}([k]_i) \le 2^{-i}\mathbb{M}(2^i[k]_i) \le 2^{-i}\mathbb{M}(k), \quad M(1) \ge R(1),$$

и соотношения 17.30, получаем оценку

$$R_k \le 3\mathbb{M}(k) + 2k - 2\nu(k) + 2[\log_2 k].$$

17.33. Примените 17.32.

17.34. Примените 17.33, 17.20, 17.25, 17.31.

17.35. Воспользуйтесь 17.34 и 17.21.

17.36. Примените 17.20, 17.25, 17.33, 17.11.

17.37. В случае $s = 0$ доказательство основано на использовании очевидных тождеств

$$[x^k f/gx^k] = [f/g], \quad gx^k\left\{x^k f/gx^k\right\} = x^k\left(g\{f/g\}\right).$$

Случай $s > 0$ сводится к рассмотренному с помощью 17.26.

17.38. Докажите неравенство

$$D(nk, n) \le D(nk - n - 1, n) + D(2n, n)$$

и примените 17.21, 17.37.

17.39. Примените 17.22 и заметьте, что у дроби $R_1/([R_2]R_2)$ степень числителя не больше степени знаменателя согласно условию задачи, откуда вытекает, что $R_1\{R_2\}/([R_2]R_2)$ — правильная дробь.

17.40. Примените 17.39.

17.41. Примените 17.40 и 17.38.

17.42. Воспользуйтесь 17.41, 17.37. Тогда

$$M(n) \le 2D(n) + D(2n) + \le 2D(2n).$$

17.43. Примените 17.41.

17.44. Положим $z'_{2k-1} = 2z_k - q_{2k+2}z_k^2$, тогда

$$0 \le z'_{2k-1} - 2z_k + qz_k^2 = (q - q_{2k+2})z_k^2 \le 2^{-2k-2} \cdot 4 = 4^{-k}.$$

Так как

$$|1 - qz_k| \le 2^{-k}q,$$

то

$$0 \le 1/q - 2z_k + qz_k^2 = (1 - qz_k)^2/q \le 4^{-k}q \le 4^{-k},$$

поэтому

$$\left|z'_{2k-1} - 1/q\right| \le 4^{-k}.$$

В силу неравенства $q_{2k+2} \ge 1/2$ имеем

$$z'_{2k-1} = 2z_k - q_{2k+2}z_k^2 \le 2z_k - z_k^2/2 = 2 - (2 - z_k)^2/2 \le 2.$$

Отсюда и из соотношения

$$\left|z'_{2k-1} - z_{2k-1}\right| = \left|z'_{2k-1} - \left\{\left\{z'_{2k-1}2^{2k-1}\right\}\right\}2^{1-2k}\right| \le 4^{-k}$$

следует, что

$$z_{2k-1} = \left\{\left\{z'_{2k-1}2^{2k-1}\right\}\right\}2^{1-2k} \le 2,$$

$$|z_{2k-1} - 1/q| \le |z'_{2k-1} - 1/q| + 4^{-k} \le 2^{-2k+1}.$$

17.45. Достаточно рассмотреть случай нечетного k. Воспользуйтесь задачей 17.44, фактом, что сложение и вычитание n-разрядных чисел выполняется со сложностью $O(n)$, и оценкой

$$M(n+1) \le M(n) + O(n).$$

17.46. Рассуждайте так же, как в решении задачи 17.32. Докажите по индукции равенство $[k]_i = [(k-2)/2^i] + 2$, где $[k]_i = [[k]_{i-1}]_1$, $[k]_1 = [k/2] + 1$.

17.47. Действительно, если при $q = 2^{-n}Q$

$$|z_{k-1} - 1/q| \le 2^{-k+1},$$

то

$$\left|2^{k-1}z_{k-1} - 2^{n+k-1}/Q\right| \le 1,$$

а так как Q не степень двойки, то $2^{n+k-1}/Q$ не является конечной двоичной дробью, поэтому $[2^{n+k-1}/Q] = 2^{k-1}z_{k-1}$ либо $2^{k-1}z_{k-1} - 1$. Сравнивая $2^{k-1}z_{k-1}Q$ с 2^{n+k-1}, находим $[2^{n+k-1}/Q]$ точно. Для этого нужно дополнительно $M(k,n) + 2k$ операций.

17.48. Примените 17.46 и 17.47.

17.49. Применим задачи 17.47 – 17.48 и воспользуемся равенством $[f/g] = [f[2^{m-1}/g]/2^{m-1}] + \alpha$, где f — m-разрядное, а g — n-разрядное двоичные числа, а $\alpha = 0, 1$ или 2, вытекающим из неравенства

$$0 \le f/g - (f/2^{m-1})[2^{m-1}/g] \le f/2^{m-1} < 2.$$

Для точного вычисления $[f/g]$ остается найти разность

$$f - g[f[2^{m-1}/g]/2^{m-1}],$$

сравнить ее с числами g и $2g$ и в зависимости от результата, возможно, прибавить к числу $[f[2^{m-1}/g]/2^{m-1}]$ единицу или двойку. Но таким образом получается лишь оценка

$$D(m,n) \le R(m,n) + M(m, m-n) + M(n, m-n) + O(m).$$

Чтобы получить лучшую оценку, достаточно вместо числа $[2^{m-1}/g]$ взять число $a = 2^{k-1}z_{k-1}$, где $k = m - n$, на вычисление которого требуется R_{k-1} операций, и такое, что $[2^{m-1}/g]$ равно a или $a - 1$.

Действительно,

$$\left|f[2^{m-1}/g]/2^{m-1} - fa/2^{m-1}\right| \le f/2^{m-1} < 2,$$

$$\left|fa/2^{m-1} - [f/2^{m-k-1}]a/2^k\right| < a/2^k \le 1,$$

значит,

$$\left|[f[2^{m-1}/g]/2^{m-1}] - [[f/2^{m-k-1}]a/2^k]\right| \le 3,$$

на вычисление произведения $[f/2^{m-k-1}]a$ достаточно $M(k)$ операций, так как числа $[f/2^{m-k-1}]$ и a являются k-разрядными, а вычисление чисел $[f/2^{m-k-1}]$ и $b = [[f/2^{m-k-1}]a/2^k]$ делается "бесплатно" (если числа a или $[f/2^{m-k-1}]$ имеют

больше, чем k разрядов, то они являются степенями двойки, и произведение $[f/2^{m-k-1}]a$ тоже вычисляется "бесплатно").

Из доказанных неравенств следует, что $[f/g] = b + \beta$, где $\beta = -3, \ldots, 5$, и произведение gb равно числу $g[f/g]$ или отличается от него на βg. Для точного вычисления $[f/g]$ и $g[f/g]$ достаточно сравнить $gb - f$ с числами ig, где $i = -2, \ldots, 4$ и закончить доказательство также, как и выше. Сложность выполнения указанных действий не выше

$$M(k) + M(n,k) + 2m - 1 + m + 2n + 6(n+2) + k + 1$$

(так как числа $\pm g$, $\pm 2g$, $4g$ вычисляются "бесплатно", а сравнение $gb - f$ с нулем не нужно, ибо уже сравнили f с gb). Остается применить 17.45.

17.50. Первое из утверждений следует из того, что при формальном добавлении к сомножителям старших разрядов с нулевыми цифрами произведение не меняется.

Монотонность $R(m,n)$ по первому аргументу выводится с помощью вытекающего из 1.2 тождества $[[2f/g]/2] = [f/g]$. Аналогично доказывается монотонность $D(m,n)$ по первому аргументу. Немонотонность по второму аргументу следует из того, что при $m < n$, очевидно, $D(m,n) = 0$. Доказательство неравенства в случае $s = 0$ основано на применении очевидных тождеств

$$[2^k f/2^k g] = [f/g], \quad 2^k g\left\{2^k f/2^k g\right\} = 2^k\left(g\{f/g\}\right).$$

Случай $s > 0$ сводится к рассмотренному с помощью монотонности $D(m,n)$ по первому аргументу.

17.51. Докажите, что произведение и частное двух чисел существенно зависит от их цифр.

17.52. Поступайте аналогично 17.21.

17.53. Примените 17.49 и 17.17.

17.54. Воспользуйтесь 17.53 и 17.52 и проверьте, что

$$D(2n,n) \leq 5\mathbb{M}(n) + O(n), \quad D(m,n) <$$

$$< mD(2n,n)/n < 5m\mathbb{M}(n)/n + O(n).$$

17.55. Из утверждений 17.49 и 17.17 следуют неравенства

$$D(m,n) < 4\mathbb{M}(m-n) + M(n,m-n) + O(m) <$$

$$< \frac{nM(m-n)}{m-n} + 4\mathbb{M}(m-n) + O(m).$$

17.56. Заметьте, что

$$AB + 1 > \frac{2^{3n-1}A}{[2^{3n-1}/B]} \geq AB,$$

так как

$$(AB+1)\left(\frac{2^{3n-1}}{B} - 1\right) = A \cdot 2^{3n-1} + \frac{2^{3n-1}}{B} - 1 - AB > A \cdot 2^{3n-1}$$

в силу неравенств

$$AB \leq 2^{2n} - 1 \leq \frac{2^{3n-1}}{B} - 1.$$

17.57. Пусть f – $(2n+2)$-разрядное, а g – $(n+1)$-разрядное числа. Положим

$$q = [f/g],\ \ r = f - qg,\ \ q_1 = [[f/4]/[g/2]],\ \ r_1 = [f/4] - q_1[g/2],$$

тогда числа q_1 и $q_1[g/2]$ вычисляются со сложностью $D(n) + O(n)$, а значит, и число $2q_1g$, равное $4q_1[g/2]$ при четном g и $4q_1[g/2] + 2q_1$ при нечетном g, вычисляется со сложностью $D(n) + O(n)$. Так как согласно

$$q_1 = [[f/4]/[g/2]] = [f/4[g/2]],$$

то

$$-2 < 2q_1 - q < \frac{f}{2[g/2]} - \frac{f}{g} + 1 \le \frac{f}{2g[g/2]} + 1 < 5,$$

значит, $-2g < 2q_1g - qg < 5g$, $-5g < f - 2q_1g < 3g$. Сравнивая число $f - 2q_1g$ с числами $-4g, -3g, \ldots, 2g$, представляем его в виде $sg + r$, где $s = -5, \ldots, 2$, и со сложностью $O(n)$ находим остаток r и частное $q = 2q_1 + s$.

17.58. Примените 17.57, 17.56, 17.52 и заметьте, что последние три цифры числа AB можно определить за $O(1)$ операций по последним трем цифрам чисел A и B, поэтому, зная число $[2^{4n-1}/D]$, для нахождения произведения AB достаточно за $O(1)$ операций найти разность $[2^{4n-1}/D]$ и AB (вычитая остаток от деления $[2^{4n-1}/D]$ на 8 из остатка от деления AB на 8) и потом за $O(n)$ операций само число AB. Воспользуйтесь также 17.52 и заметьте, что число C вычисляется со сложностью не выше

$$2R(4n, n) + O(n) \le 2D(4n, n) + O(n) \le$$

$$\le 6D(2n, n) + O(n) = 6D(n) + O(n),$$

число D — со сложностью не выше

$$D(3n+1, n+1) + O(n) \le 2D(2n+1, n+1) + O(n) =$$

$$= 2D(n+1) + O(n),$$

и, наконец, число $[2^{4n-1}/D]$, согласно 17.50, вычисляется со сложностью не выше

$$\max\{R(4n, 2n), R(4n, 2n+1)\} \le$$

$$\le \max\{R(4n, 2n), R(4n+1, 2n+1)\} \le$$

$$\le R(4n+1, 2n+1) \le R(4n+2, 2n+1) \le D(2n+1).$$

17.59. Примените 17.57, 17.58, 17.51.

17.60. Примените 17.57 и 17.58.

17.66. Для вычисления $\sqrt{x}$ с заданной точностью примените рекуррентную последовательность $z_{n+1} = z_n(3 - xz_n^2)/2$, $z_0 = 1$ и в качестве искомого приближения возьмите xz_n.

ОГЛАВЛЕНИЕ

ВЫСШАЯ МАТЕМАТИКА

Под общей редакцией
академика Российской Академии наук
В.А. Садовничего

Архипов Г.И., Садовничий В.А., Чубариков В.Н.
Лекции по математическому анализу

Виноградов И.М.
Элементы высшей математики (Аналитическая геометрия. Дифференциальное исчисление. Основы теории чисел)

Привалов И.И.
Введение в теорию функций комплексного переменного

Садовничий В.А.
Теория операторов

Нечаев В.И.
Элементы криптографии (Основы теории защиты информации)

ISBN 5-06-003613-8