МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

# ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

МОЩЕВИТИН
НИКОЛАЙ ГЕРМАНОВИЧ

МЕХМАТ МГУ

КОНСПЕКТ ПОДГОТОВЛЕН СТУДЕНТАМИ, НЕ ПРОХОДИЛ ПРОФ. РЕДАКТУРУ И МОЖЕТ СОДЕРЖАТЬ ОШИБКИ. СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ НА VK.COM/TEACHINMSU.

ЕСЛИ ВЫ ОБНАРУЖИЛИ ОШИБКИ ИЛИ ОПЕЧАТКИ, ТО СООБЩИТЕ ОБ ЭТОМ, НАПИСАВ СООБЩЕСТВУ VK.COM/TEACHINMSU.

БЛАГОДАРИМ ЗА ПОДГОТОВКУ КОНСПЕКТА
СТУДЕНТА ФИЗИЧЕСКОГО ФАКУЛЬТЕТА МГУ
**БУГАЯ ОЛЕГА АЛЕКСЕЕВИЧА**

# Содержание:

**Лекция 1** ..... **5**
1.1 Целая и дробная часть числа. ..... 5
1.2 Теоремы о делении с остатком. ..... 7
1.3 Алгоритмы Евклида. ..... 8
1.4 Проблема Зарембы. ..... 10
**Лекция 2** ..... **11**
2.1 Важная лемма. ..... 11
2.2 Утверждения и леммы, связанные с цепными дробями. ..... 11
2.3 Теорема о приближении. ..... 13
**Лекция 3** ..... **15**
3.1 Теорема Лагранжа о квадратичных иррациональностях. ..... 15
**Лекция 4** ..... **18**
4.1 Натуральные числа. ..... 18
4.2 Решето Эратосфена. ..... 18
4.3 Теоремы о простых числах. ..... 19
**Лекция 5** ..... **22**
5.1 Арифметические функции. ..... 22
5.2 Функция Мебиуса. ..... 23
**Лекция 6** ..... **25**
6.1 Формула Мебиуса. ..... 25
6.2 Сравнения и их свойства. ..... 26
6.3 Китайская теорема об остатках. ..... 27
**Лекция 7** ..... **29**
7.1 Классы вычетов. ..... 29
7.2 Сравнения и многочлены. ..... 30
7.3 Лемма Гензеля. ..... 31
**Лекция 8** ..... **33**
8.1 Лемма Гензеля. ..... 33
8.2 Квадратичные сравнения и символ Лежандра. ..... 34

8.3 Лемма Гаусса. ..... 36

**Лекция 9 ..... 37**

9.1 Квадратичный закон взаимности Гаусса и дополнительное соотношение. ..... 37

9.2 Показатель числа по модулю $m$. ..... 40

**Лекция 10 ..... 42**

10.1 Первообразный корень ..... 42

10.2 Критерий первообразного корня. ..... 43

10.3 Теоремы и утверждения, связанные с первообразным корнем. ..... 44

**Лекция 11 ..... 46**

11.1 Общая теорема и ее доказательство. ..... 46

## Лекция 1

### 1.1 Целая и дробная часть числа.

*Определение*. Если $x \in R$, то

1) Целая часть $x$, обозначаемая как $[x]$, будет равна $[x] = \max\{a \in Z, a \leq x\}$, $[-4{,}5] = -5$, т.е. $-5 = a \leq x = -4{,}5$;
2) Дробная доля $x$, обозначаемая как $\{x\}$, будет равна $\{x\} = x - [x]$.

*Замечание.*

$Z = \{0; \pm 1, \pm 2, \dots\}$
$N = \{1,2, \dots\}$
$N_0 = \{0,1,2, \dots\}$

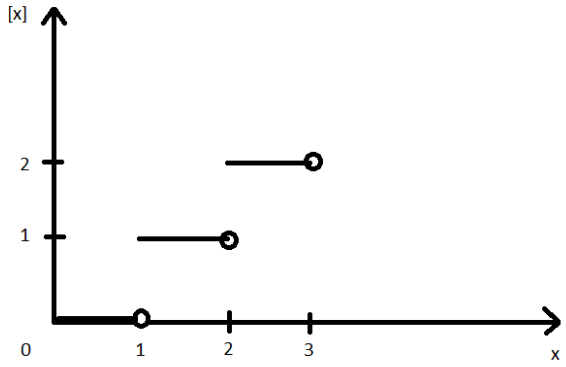



*Рис. 1.1. График зависимости целой части x от x (обратите внимание на выколотые точки).*

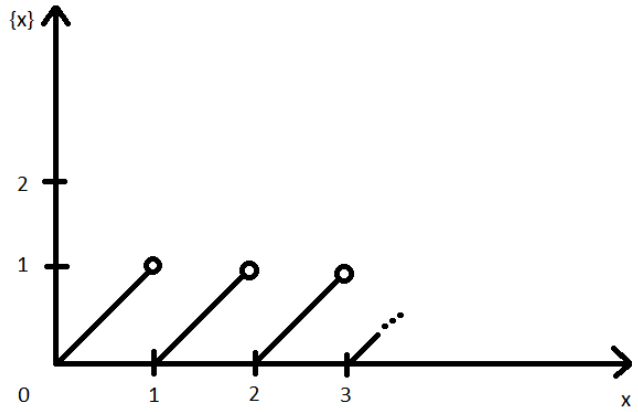



*Рис. 1.2. График зависимости дробной доли x от x.*



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Иногда целую часть $[x]$ обозначают как $\lfloor x \rfloor$, так как существует верхняя целая часть $\lceil x \rceil$.

По определению $\lceil x \rceil = \min\{a \in Z, a \geq x\}$.

$\lceil -4{,}5 \rceil = -4$; $\lceil 0 \rceil = 0$; $\lceil 0{,}5 \rceil = 1$.

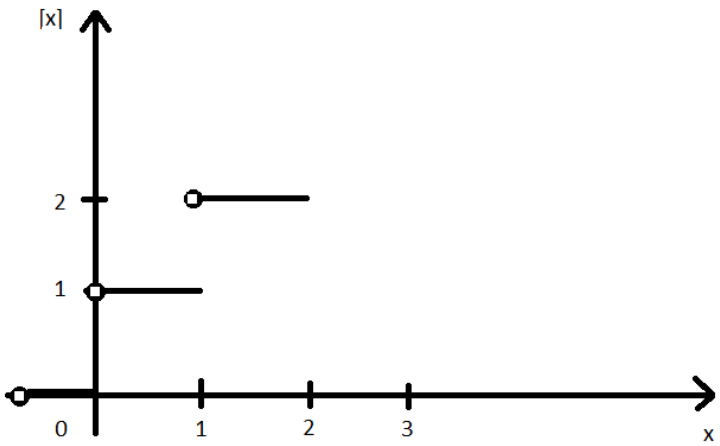



*Рис. 1.3. График зависимости верхней целой части x от x.*

*Определение.* Расстояние до ближайшего целого $||x|| = \min\limits_{a \in Z} |x - a|$.

*Замечание.*

$||x||$ - определено однозначно, но число $a$ (ближайшее целое) неоднозначно.

Например, для полуцелых чисел: для $x$= 3,5 $||x||$=0,5, но ближайшее целое либо $a = 3$, либо $a = 4$.

Выразим расстояние до ближайшего целого через дробную долю:

$$||x|| = \min(\{x\}, 1 - \{x\}) \quad (\mathbf{1})$$

Выразим верхнюю целую часть через нижнюю:

$$\lceil x \rceil = \begin{cases} \lfloor x \rfloor + 1, x \notin Z \\ \lfloor x \rfloor, x \in Z \end{cases} \quad (\mathbf{2})$$

Расстояние до ближайшего целого удовлетворяет неравенству треугольника:

$$||x + y|| \leq ||x|| + ||y|| \quad (\mathbf{3})$$

*Упражнение 1.*

1)Когда ближайшее целое к $x$ определено однозначно?

2)Если ближайшее целое однозначно, выразить его через $\lceil x \rceil$ и $\lfloor x \rfloor$.

*Упражнение 2.*



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Доказать неравенство треугольника

$$||x+y|| \leq ||x|| + ||y||$$

*Упражнение 3.*

Доказать, что для $\forall\, x \in R$ и $\forall\, a \in N$ $\left[\frac{[x]}{a}\right] = \left[\frac{x}{a}\right]$.

## 1.2 Теоремы о делении с остатком.

*Определение.* $a|b$ (читается "$a$ делит $b$", т. е. $a$ является делителем $b$), когда $\exists\ c \in Z : b = a * c$.

*Принцип Архимеда.* Во всяком непустом множестве натуральных чисел есть минимальный элемент.

Теорема 1 (об обычном делении с остатком). Если $a \in Z, b \in N$, то $\exists!\ q, r \in Z : a = bq + r, 0 \leq r < b$.

Доказательство.

<u>Существование.</u> Док-во выводится из принципа Архимеда. Рассмотрим множество $M = \{z \in N, \exists\, x \in Z: z = a - bx\}$. Необходимо проверить, что это множество непустое $M \neq \emptyset$ (для удовлетворения принципу Архимеда). Пусть $x_* = -|a| - 1$, заметим, что $b \in N$, поэтому $b \geq 1$. Запишем для него $z_* = a - bx_* = a + b * |a| + b \geq a + |a| + 1 \geq 1$, очевидно $a + |a| \geq 0$. Получили $z_* \geq 1 \Rightarrow z_* \in N$. Также был указан элемент $z_* = a - bx_* \in M \subset N$, значит $M \neq \emptyset$. Рассмотрим 2 случая:

1) $b|a$, т.е. $\exists\ q \in Z : a = bq$ и $\exists\, r = 0$.Отсюда $a = bq + r$, следовательно $\exists$ доказано. 2) $b \nmid a$. Рассмотрим $M$. Пусть $r = \min M$, который $\exists$ по принципу Архимеда. $r \in N$. *Утверждение.* $r < b$. Если $r = b$ $(r = a - bx)$, то $a = b(x+1)$, а значит $b|a$, но это не 2 случай. $\Rightarrow r \neq b$. Если $r > b$,рассмотрим $r' = r - b = a - b(x+1) \in N$, но тогда $r' < r$, что противоречит $r = \min M$. Значит, действительно $r < b$.

Полагаем $q = x$, $\Rightarrow a = bq + r$, $r \in N \Rightarrow \exists$ доказано. <u>Единственность.</u> Пусть $\exists a: a = bq + r = bq' + r'$. Докажем, что пара $(q, r) = (q', r')$. Запишем $r - r' = bq' - bq = bQ$, где $Q \in Z$. Получается $b|(r - r')$. Но $0 \leq r, r' \leq b - 1$, и, если $r \neq r'$, справедливы неравенства $1 \leq |r - r'| < b$, но из этого следует, что $b \nmid (r - r')$. Следовательно, $r = r'$, тогда $bq' = bq$ и $q' = q$. $\Rightarrow$ единственность доказана.

Теорема 2 (о делении с отрицательным остатком). Если $a \in Z, b \in N$, то $\exists!\ q', r' \in Z : a = bq' - r', 0 \leq r' < b$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

*Замечание.* Из Т.1 $\frac{a}{b} = q + \frac{r}{b}$ , $q = \left[\frac{a}{b}\right], \frac{r}{b} = \left\{\frac{a}{b}\right\}$. Из Т.2 $q' = \left[\frac{a}{b}\right]$.

Теорема 3 (о делении с остатком, связанным с ближайшим целым). Если $a \in Z, b \in N$, то $\exists!\ \ q'', r'' \in Z : a = bq'' + r'', \begin{cases} r' \in \left[-\frac{b-1}{2}, \frac{b-1}{2}\right],\ b - \text{нечет.} \\ r' \in \left[-\frac{b}{2}, \frac{b}{2}\right], b - \text{четн.} \end{cases}$.

*Упражнение.* Доказать теоремы 2,3.

**1.3 Алгоритмы Евклида.**

Алгоритм Евклида – это алгоритм нахождения наибольшего общего делителя двух чисел. Будем рассматривать $D(a,b)$: $\{z \in N: z|a, z|b\}$. Это множество непустое, так как содержит 1. Если $z \in D$, то $z \leq |a|, |b|$. Значит, $D$ ограниченное множество, а в ограниченном множестве есть максимальный элемент.

*Определение.* $\text{НОД}(a,b) = max\ D(a,b)$.

Лемма. Если $a = bq + r$, то $\text{НОД}(a,b) = \text{НОД}(b,r)$.( $a, q, r \in Z, b \in N$)

Доказательство. Если $\begin{cases} z|a \\ z|b \end{cases}$, то $z|r$. Если $\begin{cases} z|b \\ z|r \end{cases}$, то $z|a$. Тогда $D(a,b) = D(b,r)$ (множество общих делителей a, b совпадает с множеством общих делителей b, r) и $\max D(a,b) = \max D(b,r)$. И по определению $\text{НОД}(a,b) = \text{НОД}(b,r)$.

*Замечание.* Эта лемма верна для любого деления с остатком.

1)Обычный алгоритм Евклида.

$a = bq + r$ –обычное деление с остатком.

Сделаем замену $b = r_0, r = r_1, q = q_0$. Тогда $a = q_0 r_0 + r_1$, где $0 \leq r_1 \leq r_0$. Теперь будем делить $r_j$ на $r_{j+1}$ с остатком. Остаток – это натуральное число или ноль. Если остаток ноль, то алгоритм закончится, т.к. нельзя делить на ноль. На каждом шаге остаток уменьшается как минимум на единицу.

$a = q_0 r_0 + r_1$, где $0 \leq r_1 < r_0$.

$r_0 = q_1 r_1 + r_2$, где $0 \leq r_2 < r_1$.

….

$r_{j-1} = q_j r_j + r_{j+1}$, где $0 \le r_{j+1} < r_j$. **(4)**

$\exists n: r_{n+1} = 0$, т.е. $r_{n-1} = q_n r_n + r_{n+1}$, где $r_{n+1} = 0$.

Тогда утверждение алгоритма таково: НОД$(a, b) = r_n$ . **(5)**

*Замечание.* Обычно пишется $(a, b) =$ НОД$(a, b)$, если не возникает неопределенностей, так как в теории чисел почти не бывает векторов.

Т.е. $(a, b) = (a, r_0) = (r_0, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$

$(a, b) = (a, r_0)$ –по утверждению леммы. $(r_{n-1}, r_n) = r_n$ –если $r_n | r_{n-1}$, то НОД$(r_{n-1}, r_n) = r_n$. Таким образом, $r_n$ –последний не равный нулю остаток.

$$\frac{a}{b} = \frac{a}{r_0} = q_0 + \frac{r_1}{r_0} = q_0 + \frac{1}{r_0/r_1} = q_0 + \frac{1}{q_1 + r_2/r_1} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_n}}}} \quad \textbf{(6)}$$

Обозначим $q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_n}}}} = [q_0; q_1, \ldots, q_n]$ –обыкновенная цепная дробь,

где $q_0 = \left[\frac{a}{b}\right] \in Z$, $q_n = [\frac{r_{n-1}}{r_n}] \in N$ при $n > 1$ ($q_n$ называют неполным частным).

Справедливы следующие оценки: $\frac{r_1}{r_0} \in (0,1)$, $\frac{r_0}{r_1} > 1$.

*Следствие 1.* Если $\frac{a}{b} \in R, (a, b) = 1$, то оно представляется в виде обыкновенной цепной дроби $\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_n}}}} = [q_0; q_1, \ldots, q_n]$.

2) Алгоритм Евклида с минусом.

$$r_{j-1} = q_j r_j - r_{j+1}, \text{где } 0 \le r_{j+1} < r_j \quad \textbf{(7)}$$

$\exists m: r_{m+1} = 0$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

$a = bq - r = r_0 q_0 - r_1,$

$$\frac{a}{b} = q_0 - \frac{r_1}{r_0} = q_0 - \frac{1}{r_0/r_1} = q_0 - \frac{1}{q_1 - r_2/r_1} = q_0 - \frac{1}{q_1 - \frac{1}{q_2 - \frac{1}{q_3 - \ldots - \frac{1}{q_m}}}}. \quad \textbf{(8)}$$

$\frac{r_0}{r_1} > 1, q_0 = \left[\frac{a}{b}\right], q_1 = \left[\frac{r_0}{r_1}\right] \geq 2.$

В общем случае $m \neq n$ ($n$ из обычного алгоритма Евклида).

*Следствие 2.* Если $\frac{a}{b} \in R, (a, b) = 1$, то оно представляется в виде цепной дроби с минусами $\frac{a}{b} = q_0 - \frac{r_1}{r_0} = q_0 - \frac{1}{r_0/r_1} = q_0 - \frac{1}{q_1 - r_2/r_1} = q_0 - \frac{1}{q_1 - \frac{1}{q_2 - \frac{1}{q_3 - \ldots - \frac{1}{q_m}}}}$, где $q_0 \in Z, q_n \geq 2$ при $n > 1$.

3)Алгоритм Евклида с ближайшими целыми.

$r_{j-1} = q_j r_j + \varepsilon_{j+1} r_{j+1}$, где $0 \leq r_{j+1} < \frac{r_j}{2}$, $\varepsilon_{j+1} = \begin{cases} +1 \\ -1 \end{cases}$. **(9)**

Приводит к разложению в цепную дробь такого вида

$$\frac{a}{b} = q_0 + \frac{\varepsilon_1}{q_1 + \frac{\varepsilon_2}{q_2 + \frac{\varepsilon_3}{q_3 + \ldots + \frac{\varepsilon_n}{q_n}}}} \quad (\mathbf{10})$$

**1.4 Проблема Зарембы.**

Гипотеза Зарембы утверждает, что $\forall b \in N\ \exists a \in N$ при условии $(a, b) = 1$: при разложении $\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_n}}}}$ в цепную дробь $\forall j\ q_j \leq 5$.

*Упражнение.* Решить проблему Зарембы в следующей формулировке. $\forall b \in N\ \exists a \in N$ при условии $(a, b) = 1$: при разложении $\frac{a}{b} = q_0 - \frac{1}{q_1 - \frac{1}{q_2 - \frac{1}{q_3 - \ldots - \frac{1}{q_n}}}}$ в цепную дробь $\forall j\ q_j \leq 5$.

Отличие в том, что первая формулировка – нерешенная математическая задача, а вторая может быть решена студентом.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

## Лекция 2

### 2.1 Важная лемма.

Лемма. Если $a|bc$ и $(a,b)=1$, то $a|c$.

Доказательство. (Через алгоритм Евклида).

Используя теорему о линейном представлении НОД,

$$(a,b)=1 \implies \exists\, x,y \in z : ax+by=1.$$

Очевидно, $acx+bcy=c$. $a|acx$ и из условия $a|bcy$. Тогда $a|(acx+bcy)=c. \implies a|c$.

$a_0 \in \mathrm{Z}, a_1, a_2, \dots, a_n \in N$.

$\frac{p_n}{q_n}=[a_0; a_1, a_2, \dots, a_n]$, $(p_n, q_n)=1$.

*Определение.* $\frac{p_n}{q_n}-$ подходящая дробь.

### 2.2 Утверждения и леммы, связанные с цепными дробями.

Лемма (о рекуррентных соотношениях). Если 1) $\begin{cases} p_{n+1}=a_{n+1}p_n+p_{n-1} \\ q_{n+1}=a_{n+1}q_n+q_{n-1} \end{cases}$, 2) $p_{n+1}\,q_n - q_{n+1}\,p_n=(-1)^n$, то $\frac{p_{n+1}}{q_{n+1}}=[a_0; a_1, a_2, \dots, a_{n+1}]$.

Доказательство. (по индукции)

Шаг индукции: по предположению индукции $\frac{p_{n+1}}{q_{n+1}}=\frac{a_{n+1}p_n+p_{n-1}}{a_{n+1}q_n+q_{n-1}}$.

Вместо $a_{n+1}$ подставим $a_{n+1}+\frac{1}{a_{n+2}}$. Тогда $\frac{p_{n+1}}{q_{n+1}}=\frac{(a_{n+1}+\frac{1}{a_{n+2}})p_n+p_{n-1}}{(a_{n+1}+\frac{1}{a_{n+2}})q_n+q_{n-1}}$.

Обоснование. Рассмотрим функцию $f(x)=a_0+\frac{1}{a_1+\dots+\frac{1}{a_n+\frac{1}{x}}}$.

Ясно, что функция имеет вид $f(x)=\frac{Ax+B}{Cx+D}$.

Исходя из этого предположения, имеет место запись $f(x)=a_0+\frac{1}{\frac{A_1x+B_1}{C_1x+D_1}}$.

$f(x)=a_0+\frac{1}{\frac{A_1x+B_1}{C_{1x+D_1}}}=f(x)=a_0+\frac{C_1x+D_1}{A_1x+B_1}=\frac{(A_1a_0+C_1)x+B_1a_0+D_1}{A_1x+B_1}=\frac{Ax+B}{Cx+D}$, где $A=A_1a_0+C_1, B=B_1a_0+D_1$, C=$A_1, D=B_1$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

По индукции в глубину этого выражения такая функция всегда записывается в виде $f(x)=\frac{Ax+B}{Cx+D}$. По предположению индукции $f(x)=\frac{xp_n+p_{n-1}}{xq_n+q_{n-1}}$ для $x=a_{n+1}\in N$. Мы знаем, что $f(x)=\frac{Ax+B}{Cx+D}=\frac{xp_n+p_{n-1}}{xq_n+q_{n-1}}$ для $x\in N$. Это верно и для любого вещественного $x$ из области определения, исходя из следующего. Запишем разность $\frac{Ax+B}{Cx+D}-\frac{xp_n+p_{n-1}}{xq_n+q_{n-1}}=\frac{\text{многочлен второго порядка}}{\text{какое}-\text{то выражение}}$. Так как для натуральных $x$ эта разность будет равна нулю, то многочлен второго порядка, стоящий справа у написанной выше разности, равен нулю как минимум в трех точках. Значит, этот многочлен тождественно равен нулю. Следовательно, $a_n$ у подходящей дроби может быть нецелым. Обоснование закончено.

По предположению индукции $\frac{p_{n+2}}{q_{n+2}}=\frac{a_{n+2}(a_{n+1}p_n+p_{n-1})+p_n}{a_{n+2}(a_{n+1}q_n+q_{n-1})+q_n}=\frac{a_{n+2}p_{n+1}+p_n}{a_{n+2}q_{n+1}+q_n}$. Если обе дроби несократимы, то $p_{n+2}=a_{n+2}p_{n+1}+p_n$, $q_{n+2}=a_{n+2}q_{n+1}+q_n$, но $(p_{n+2},q_{n+2})=1$ по определению. Докажем, что правая часть несократима. Обозначим $p^*,q^*$ за числитель и знаменатель соответственно. Рассмотрим $p^*q_{n+1}-q^*p_{n+1}=(a_{n+2}p_{n+1}+p_n)q_{n+1}-(a_{n+2}q_{n+1}+q_n)p_{n+1}=-(p_{n+1}q_n-q_{n+1}p_n)=-(-1)^n=(-1)^{n+1}$.Линейная комбинация $p^*,q^*$представляет собой единицу. Следовательно, $(p^*,q^*)=1$.

*Упражнение.* Проверить обоснование индукции для $n=1$.

Лемма. Для любой последовательности подходящих дробей выполнено:

1) $\frac{p_{2n}}{q_{2n}}$ –возрастает при $n\longrightarrow\infty$;
2) $\frac{p_{2n+1}}{q_{2n+1}}$ –убывает при $n\longrightarrow\infty$;
3) Любая честная дробь меньше любой нечетной;
4) $\left|\frac{p_n}{q_n}-\frac{p_{n+1}}{q_{n+1}}\right|=\frac{1}{q_nq_{n+1}}\to 0$ при $n\to\infty$;
5) $\exists\ \lim\limits_{n\to\infty}\frac{p_n}{q_n}$, который называется значением цепной дроби.

Доказательство. Рассмотрим разность через одну

1),2) $\frac{p_{n+2}}{q_{n+2}}-\frac{p_n}{q_n}=\frac{p_{n+2}q_n-q_{n+2}p_n}{q_nq_{n+2}}$. Числитель: $(a_{n+2}p_{n+1}+p_n)q_n-(a_{n+2}q_{n+1}+q_n)p_n=a_{n+2}(p_{n+1}q_n-q_{n+1}p_n)=a_{n+2}(-1)^n$, $>0$ при $n-$ четном, $<0$ при $n$ –нечетном.

3) $\frac{p_n}{q_n}-\frac{p_{n+1}}{q_{n+1}}=\frac{(-1)^{n+1}}{q_nq_{n+1}}$. Если следующая дробь нечетная, она больше всех предыдущих четных, если следующая четная, то она меньше всех предыдущих нечетных (по индукции).

4) $\left|\frac{p_n}{q_n}-\frac{p_{n+1}}{q_{n+1}}\right|=\left|\frac{(-1)^{n+1}}{q_nq_{n+1}}\right|=\frac{p_n}{q_n}-\frac{p_{n+1}}{q_{n+1}}=\frac{1}{q_nq_{n+1}}\to 0$ при $n\to\infty$;

5) Если подходящие дроби с четными номерами возрастают и они меньше любой нечетной дроби, то у нас есть возрастающая ограниченная последовательность, которая



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

имеет предел, по теореме Вейерштрасса (возрастающая ограниченная последовательность имеет предел). Аналогично для дробей с нечетными номерами. Из 4) следует, что пределы этих последовательностей совпадают.

*Следствие.* $q_{n+1} \geq q_n + p_{n-1}\ \forall\, n,\ q_n \geq (\frac{\sqrt{5}+1}{2})^{n-1}$.

*Упражнение.* Доказать, что $q_n \geq (\frac{\sqrt{5}+1}{2})^{n-1}$.

Утверждение. Если $\alpha \in R\backslash Q$ (вещественное иррациональное), то $\exists\, a_0 \in Z, a_1, \ldots \in N$: $\alpha$ есть значение формальной цепной дроби.

Доказательство. $[\alpha] = a_0$, $\alpha = a_0 + \{\alpha\} = a_0 + \frac{1}{\left[\frac{1}{\{\alpha\}}\right]+\{\frac{1}{\{\alpha\}}\}} = a_0 + \frac{1}{a_1+r_1}$, где $r_1 \in (0,1)$.

Тогда, если $\alpha = a_0 + \frac{1}{a_1+\ldots+\frac{1}{a_t+r_t}}$, $r_t \notin Q$, то $r_t = \frac{1}{\frac{1}{r_t}} = \frac{1}{\left[\frac{1}{r_t}\right]+\{\frac{1}{r_t}\}}$, $r_{t+1} = \{\frac{1}{r_t}\}$.

Докажем, что значение полученной цепной дроби есть $\alpha$. Запишем следующее равенство: $\frac{p_n}{q_n} = \frac{a_n p_{n-1}+p_{n-2}}{a_n q_{n-1}+q_{n-2}}$. Теперь вместо $a_n$ подставим $a_n + r_n$.

$\frac{(a_n+r_n)p_{n-1}+p_{n-2}}{(a_n+r_n)q_{n-1}+q_{n-2}} = \frac{p_n+r_n p_{n-1}}{q_n+r_n q_{n-1}}$. Проверим $\alpha - \frac{p_n}{q_n} = \frac{p_n+r_n p_{n-1}}{q_n+r_n q_{n-1}} - \frac{p_n}{q_n} = \frac{r_n(p_{n-1}q_n - q_{n-1}p_n)}{(q_n+r_n q_{n-1})q_n}$.

Тогда $\left|\alpha - \frac{p_n}{q_n}\right| = \frac{r_n}{(q_n+r_n q_{n-1})q_n} \to 0$.

*Упражнение.* Проблема единственности:

1) Доказать, что значение бесконечной цепной дроби всегда иррационально.
2) Доказать, что разные бесконечные дроби имеют разные значения.

Подсказка для 1).

$\alpha$ лежит между $\frac{p_n}{q_n}$ и $\frac{p_{n+1}}{q_{n+1}}$, т.е. $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$

Подсказка для 2).

Пусть $\alpha = [a_0; a_1, \ldots], \beta = [b_0; b_1, \ldots]$. Если $a_0 \neq b_0$, то $\alpha \neq \beta$, т.к. $[\alpha] \neq [\beta]$

*Упражнение.* Как выглядит множество тех $x \in R$: $x = [a_0; a_1, \ldots], a_0; a_1, \ldots, a_n \in N$?

**2.3 Теорема о приближении.**

Пусть $\alpha \in R\backslash Q$, где $\alpha = [a_0; a_1, \ldots, a_n, a_{n+1}, \ldots]$. Определим $\alpha_n = [a_n; a_{n+1}, a_{n+2}, \ldots] \notin Q$ – "хвост", ${\alpha_n}^* = [0; a_{n-1}, a_{n-2}, \ldots, a_1] \in Q$. Тогда $\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{{q_n}^2(\alpha_{n+1}+{\alpha_n}^*)}$, т.е.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

приближение числа рациональной дробью может быть записано с помощью этой формулы.

Доказательство. Рассмотрим $\frac{p_{n+1}}{q_{n+1}} = \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}}$. Подставим вместо $a_{n+1}$ в правую часть $\alpha_{n+1}$. Тогда $\alpha - \frac{p_n}{q_n} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(\alpha_{n+1}q_n + q_{n+1})} = \frac{(-1)^n}{{q_n}^2\left(\alpha_{n+1} + \frac{q_{n-1}}{q_n}\right)}$. Ясно, что $\frac{q_{n-1}}{q_n} = \frac{1}{\frac{q_{n-1}a_n + q_{n-2}}{q_{n-1}}} = \frac{1}{a_n + \frac{q_{n-2}}{q_{n-1}}}$. И так далее по индукции $\frac{q_{n-1}}{q_n} = {\alpha_n}^*$. Т.е. $\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{{q_n}^2(\alpha_{n+1} + {\alpha_n}^*)}$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

## Лекция 3

### 3.1 Теорема Лагранжа о квадратичных иррациональностях.

*Определение.* Квадратичная иррациональность $\alpha$– это иррациональное число, которое является корнем квадратного уравнения с целыми коэффициентами, т.е.

$\alpha \in R\backslash Q \ \exists\, A, B, C \ \in Z\ (A, B, C) \neq (0,0,0): A\alpha^2 + B\alpha + C = 0.$

*Определение.* Периодическая цепная дробь – это такая бесконечная цепная дробь $[a_0; a_1, \dots, a_n, a_{n+1}, \dots, a_{n+t}, a_{n+t+1}, \dots]$, что $\exists\, n, t : a_{n+t+j} = a_{n+j}\ \forall\, j\ \geq 0.$

$[a_0; a_1, \dots, a_n, a_{n+1}, \dots, a_{n+t}, a_{n+t+1}, \dots]$=$[a_0; a_1, \dots, a_{n-1}, \overline{a_n, \dots, a_{n+t-1}}]$. То, что под чертой называется «период», а все остальное до него называется «предпериод».

Теорема Лагранжа.

$\alpha$ является квадратичной иррациональностью тогда и только тогда, когда $\alpha$ – это периодическая цепная дробь.

Доказательство.

(1. Если период. ц. дробь, то кв. иррациональность - доказал Эйлер.2. Если кв. иррациональность, то период. ц. дробь – доказал Лагранжа.)

1)Сначала рассмотрим чисто периодический случай. $\alpha = \beta = [\overline{a_0; a_1, \dots, a_t}]$. используя «хвост», получаем $\alpha_{t+1} = \alpha$. Запишем подходящую $(t+1)$-ю дробь: $\frac{p_{t+1}}{q_{t+1}} = \frac{a_{t+1}p_t + p_{t-1}}{a_{t+1}q_t + q_{t-1}}$, заменяем $a_{t+1}$ на $\alpha_{t+1}$. $\frac{\alpha_{t+1}p_t + p_{t-1}}{\alpha_{t+1}q_t + q_{t-1}} = \alpha$, тогда $\alpha = \frac{\alpha p_t + p_{t-1}}{\alpha q_t + q_{t-1}}$. Получили уравнение $\alpha^2 q_t + \alpha(q_{t-1} - p_t) - p_{t-1} = 0$. $\alpha -$ б. ц. д. $\Longrightarrow\ \alpha \in R\backslash Q$ и $\alpha$ –корень квадратного уравнения. Значит $\alpha -$ это квадратичная иррациональность.

В случае $\alpha$ просто периодической. $\alpha = [a_0; \dots, a_{n-1}, \overline{a_n, \dots, a_{n+t-1}}]$. Также введем $\beta = [\overline{a_n; a_{n+1}, \dots, a_{n+t-1}}]$ - чисто периодическая, уже доказано, что это квадратичная иррациональность. $\beta$ это иррациональное число. $\beta = A + B\sqrt{D}$, $A, B \in Q, D \in N$.

$\frac{p_n}{q_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}$, чтобы получить $\alpha$ из $\beta$ надо в это выражение подставить $\beta$ вместо $a_n$. $\alpha = \frac{\beta p_{n-1} + p_{n-2}}{\beta q_{n-1} + q_{n-2}}$, $p, q\ \in Z$. После подстановки выражения для $\beta$ в $\alpha$ получаем $\alpha = A_1 + B_1\sqrt{D}, A_1, B_1 \in Q$. Ясно, что это корень какого-то квадратного уравнения с целыми коэффициентами. $\alpha$ иррациональное. Следовательно, $\alpha$ тоже квадратичная иррациональность.

Лемма. Пусть $\alpha$ - значение бесконечной дроби $[a_0; a_1, \dots, a_n, \dots]$, тогда $\alpha\ \notin Q$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Доказательство. Предположим, что $\alpha = \frac{a}{b} \in R, a \in Z, b \in N, (a,b) = 1$. Рассмотрим $\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n]$. Рассмотрим (предполагая, что это не равно нулю) $\left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{a}{b} - \frac{p_n}{q_n}\right| \geq \frac{1}{bq_n}$. Справедливы следующие неравенства: $\frac{1}{bq_n} \leq \left|\frac{a}{b} - \frac{p_n}{q_n}\right| = |\alpha - \frac{p_n}{q_n}| \leq \frac{1}{q_n q_{n+1}}$. Т.е. $q_{n+1} \leq b\ \forall n$. Но $q_{n+1} \to \infty$, а $b$ – это знаменатель $\alpha$ (ограничено). Получаем противоречие. Значит, $\alpha$ –иррационально.

2) Дано $\alpha \in R \backslash Q, \exists\, A, B, C\ \in Z: A^2 + B^2 + C^2 \neq 0: A\alpha^2 + B\alpha + C = 0$. Надо доказать, что $\exists\, m, n\ \in N, m \neq n: \alpha_m = \alpha_n$ (хвосты). $\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$. Нужно написать уравнение, которому удовлетворяет $\alpha_n$: $A_n x^2 + B_n x + C_n = 0, A_n, B_n, C_n \in Z$. Получаем $A\left(\frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}\right)^2 + B\frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} + C = 0$.

$A_n = A{p_{n-1}}^2 + Bp_{n-1}q_{n-1} + C{q_{n-1}}^2$,

$B_n = 2Ap_{n-1}p_{n-2} + B(p_{n-1}q_{n-2} + q_{n-1}p_{n-2}) + 2Cq_{n-1}q_{n-2}$,

$C_n = A{p_{n-2}}^2 + Bp_{n-2}q_{n-2} + C{q_{n-2}}^2$.

Утв.1. ${B_n}^2 - 4A_nC_n = B^2 - 4AC$.

Получим уравнение $A_n{\alpha_n}^2 + B_n\alpha_n + C_n = 0$ из уравнения для предыдущего хвоста $A_{n-1}{\alpha_{n-1}}^2 + B_{n-1}\alpha_{n-1} + C_{n-1} = 0$. Нужно вместо $\alpha_{n-1}$ написать $a_{n-1} + \frac{1}{\alpha_n}$, тогда получится нужное уравнение. $A_{n-1}(a_{n-1} + \frac{1}{\alpha_n})^2 + B_{n-1}(a_{n-1} + \frac{1}{\alpha_n}) + C_{n-1} = 0$. $(A_{n-1}{a_{n-1}}^2 + B_{n-1}a_{n-1} + C_{n-1}){\alpha_n}^2 + (2A_{n-1}a_{n-1} + B_{n-1})\alpha_n + A_{n-1} = 0$. Считаем дискриминант: $(2A_{n-1}a_{n-1} + B_{n-1})^2 - 4A_{n-1}(A_{n-1}{a_{n-1}}^2 + B_{n-1}a_{n-1} + C_{n-1}) = {B_{n-1}}^2 - 4A_{n-1}C_{n-1}$.

Утв. 2. Последовательность $|B_n|$ ограничена.

$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_n q_{n-1}}$. Будем использовать с $k = n-1, k = n-2$. $p_k = \alpha q_k + \frac{\Theta_k}{q_{k+1}}$, где $|\Theta_k| < 1$. $B_n = 2A\left(\alpha\, q_{n-1} + \frac{\Theta_{n-1}}{q_n}\right)\left(\alpha q_{n-2} + \frac{\Theta_{n-2}}{q_{n-1}}\right) + B\left(\left(\alpha q_{n-1} + \frac{\Theta_{n-1}}{q_n}\right)q_{n-2} + q_{n-1}\left(\alpha q_{n-2} + \frac{\Theta_{n-2}}{q_{n-1}}\right)\right) + 2Cq_{n-1}q_{n-2} = 2Aq_{n-1}q_{n-2}\alpha^2 + 2Bq_{n-1}q_{n-2}\alpha + 2Cq_{n-1}q_{n-2} +$ ограниченная величина, при $n \to \infty$. $B_n = 2q_{n-1}q_{n-2}(A\alpha^2 + B\alpha + C) +$ ограниченная величина ( при $n \to \infty$) $= 0$. Следовательно, $B_n$ ограничено. $B_n = 0 + R, |R| \leq 4|A\alpha| + 2|A| + 2|B|$.

Утв. 3. $A_nC_n$ – ограничено.

$$A_nC_n = ({B_n}^2 - (B^2 - 4AC))/4$$



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Утв. 4. $|A_n|+|C_n| > 0$.

Утв. 5. $A_n, C_n$ −ограничены.

Утв. 6. Различных наборов $(A_n, B_n, C_n)$ −ограниченное число.

Утв. 7. Различных корней многочленов $A_n x^2 + B_n x + C_n = 0$ ограниченное число.

А хвостов $\alpha_n$ бесконечно. Значит, $\exists\, m \neq n\colon \alpha_n = \alpha_m$. Таким образом, цепная дробь периодична.

## Лекция 4

### 4.1 Натуральные числа.

Все натуральные числа разбиваются на три класса в зависимости от количества делителей.

Если $n \in N$ , то всегда $1|n, n|n$. Если $n = 1$, то это особый случай (у 1 ровно один делитель, а у всех остальных по крайней мере два делителя).

*Определение.* $n$ называется простым, если у него ровно два делителя.

Таким образом, $N = \{1\} \cup \{\text{простые числа}\} \cup \{\text{составные числа}\}$.

Лемма. Пусть $n -$ составное число и пусть множество $D -$ это множество всех делителей числа $n$. Возьмем такое множество $d$(оно не пустое) такое, что $\{d \in D, d > 1\}$. Тогда для $p = \min d$ выполнено следующее:

1) $p -$ простое;

2) $p^2 \leq n$.

Доказательство. Если $n -$ составное, то $n = ab$, где $a, b < n$ (из определения составного числа мы можем это утверждать). Для минимального делителя выполнено следующее $p \leq a, b$, тогда $p^2 \leq n$. Ясно, что $p$ простое. Если бы $p = uv$, где $u, v > 1$, то тогда бы $u|n$, а в этом случае $u < n$. Это противоречит минимальности $p$.

*Следствие.* У каждого натурального числа большего единицы есть простой делитель.

Доказательство. Если $n -$ простое, то оно само и есть простой делитель, если $n -$ составное, то у него есть простой делитель по доказанной выше лемме.

### 4.2 Решето Эратосфена.

Алгоритм выписывания простых чисел называется «решето Эратосфена».

Это алгоритм, который выписывает все простые числа $\leq n$.

В ходе алгоритма некоторые числа будут вычеркиваться, некоторые отмечаться, но будут оставаться не вычеркнутые и неотмеченные числа.

Алгоритм:

Выписываем числа 2 3 4 5 6 7 8 9 … $n$

1)Отмечаем 2.

2)Рассматриваем $2^2 = 4$. Зачеркиваем 4 и все, что больше 4 и кратно 2



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

3)Выбираем первое не вычеркнутое и неотмеченное, т.е. 3, и отмечаем его. Берем $3^2 = 9$. Вычеркиваем 9 и все, что больше 9 и кратно 3.

4) После некоторого количества итераций алгоритм можно представить в общем виде следующим образом: пусть у нас есть $p_1, \dots, p_k$ отмеченных чисел.

4.1) Если после того, как было получено $k$ этих чисел, не остается не вычеркнутых и неотмеченных, алгоритм заканчивается.

4.2) Если остаются неотмеченные и не вычеркнутые, берем число $p_{k+1}$(первое невычеркнутое) и продолжаем.

5) Вычисляем ${p_{k+1}}^2$

5.1) Если ${p_{k+1}}^2 > n$, то алгоритм кончается. После этого отмечаются все оставшиеся не вычеркнутые и не отмеченные числа.

5.2) Если ${p_{k+1}}^2 \leq n$, то вычеркиваем ${p_{k+1}}^2$ и все числа $> {p_{k+1}}^2$ и кратные $p_{k+1}$. После этого берем первое не вычеркнутое и неотмеченное и повторяем, начиная с пункта 4.

Утверждение алгоритма. Все отмеченные числа являются простыми.

Нужно доказать два утверждения:

1)Если число отмечено, то оно простое.

2)Если число простое, то оно отмечено.

Доказательство 1. Пусть $q$ −отмечено. Предположим, что оно составное. Если число $q$ составное, то по лемме у него есть минимальный простой делитель $p$: $p^2 \leq q$. Берем простой делитель, это простое число меньшее $n$. Значит, оно отмечено, потому что все простые числа отмечены. Оно могло быть отмечено двумя способами. Либо оно прошло через алгоритм и отметилось в его процессе, либо оно отметилось в последний момент (т.е. после окончания алгоритма). Если оно отметилось в последний момент, то $p^2 > n$. Но так как $p|q,\ p^2 \leq n$. Противоречие. Значит оно было отмечено в процессе алгоритма. Но при этом, когда отмечается $p$, вычеркивается $p^2$ и все, что больше $p^2$ и кратно $p$. В частности, было вычеркнуто $q$. Получили противоречие.

Доказательство 2. После того, как мы закончили алгоритм, все числа либо отмечены, либо вычеркнуты. Если число вычеркнуто, то оно не простое. Это значит, что если число простое, то оно не вычеркнуто. А если оно не вычеркнуто, то оно отмечено. Т.е. если число простое, то оно отмечено.

### 4.3 Теоремы о простых числах.

Теорема Евклида. Простых чисел бесконечно много.

Доказательство Евклида. Предполагаем противное. Пусть $p_1, \dots, p_t$ − все простые числа.

Рассмотрим выражение $n = p_1 * \ldots * p_t + 1$ –составное. У него есть простой делитель: $\exists\, p -$ простое: $p|n$. Тогда $\exists j: p = p_j$, так как нет других простых. Получается, что $p_j | p_1 * \ldots * p_t + 1 = A$, но $p_j | p_1 * \ldots * p_j * \ldots * p_t = B$. Тогда $p_j | (A - B) = 1$. Но это противоречие.

Рассмотрим $S_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$. Ясно, что $S_n$ неогр. при $n \to \infty$ ($\lim\limits_{n\to\infty} S_n = \infty$). Рассмотрим $P(x) = \sum_{p \le x} \frac{1}{p}$.

Также необходимо условие выпуклости графика функции $y(x) = -\log_2(1 - x)$,

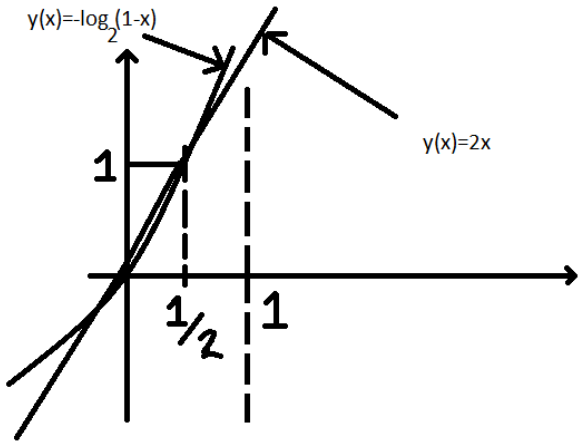



*Рис. 4.1. График функции* $y(x) = -\log_2(1 - x)$ *и* $y(x) = 2x$.

т.е. $2x \ge -\log_2(1 - x)$ при $x \in \left[0; \frac{1}{2}\right]$, и $1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots = \sum_{j=0}^{\infty} \frac{1}{p^j} = \frac{1}{1 - \frac{1}{p}} = f_p$

$p \le x$, $f_p > \sum_{j=0}^{\left[\frac{ln\, x}{ln\, p}\right]} \frac{1}{p^j}$. Пусть $k_p = [\frac{\ln x}{\ln p}]$. Пусть $\exists\, m \in N : m \le x$. Раскладываем $m$ на простые множители: $m = {p_1}^{\alpha_1} \ldots {p_t}^{\alpha_t}$. Тогда все простые множители будут в степенях не больших, чем $k_p (\alpha_i \le k_p\ \forall\, i \le t)$. Так как максимальная степень простого числа, не превосходящая $x$, это $k_p$. $p^{k_p} \le x \le p^{k_p + 1}$.

Если $p_1, \ldots, p_t -$ все простые $\le x$, то $\prod_{p \le x} f_p > \left(1 + \frac{1}{p_1} + \cdots + \frac{1}{{p_1}^{k_{p_1}}}\right) \ldots \left(1 + \frac{1}{p_t} + \cdots + \frac{1}{{p_t}^{k_{p_t}}}\right) \ge 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{[x]}$

Теорема. $P(x) \to \infty$ при $x \to \infty$.

$\prod_{p \le x} f_p \ge S_{[x]}$, после логарифмирования $\sum_{p \le x} \log_2 f_p \ge \log_2 S_{[x]}$. $\log_2 f_p = \log_2(\frac{1}{1 - \frac{1}{p}}) = -\log_2\left(1 - \frac{1}{p}\right) \le \frac{2}{p}$. $\sum_{p \le x} \frac{1}{p} \ge \frac{1}{2} \log_2 S_{[x]} \to \infty$ при $x \to \infty$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Основная теорема арифметики. Всякое натуральное число $n = p_1 \dots p_t$ $(n \geq 2)$ представляется в виде произведения простых, причем единственным образом (с точностью до порядка множителей).

Доказательство.

*Существование.* (индукция по $n$). Предположение индукции: доказано для всех $m \leq n - 1$. Если $n = p$(простое), то это и есть разложение на простые. Если $n$ −составное, то $n = ab$, где $a, b < n$, а для них по предположению индукции мы уже имеем разложение.

*Единственность.* (по индукции). Основание, n=2- ясно. Предположение индукции: $\forall m \leq n - 1$ −доказано. Предположим, что существует два различных разложения $n = p_1 \dots p_{t_1} = q_1 \dots q_{t_2}$. Утверждается, что $p_i \neq q_j$ $\forall i, j$. Иначе на $p_i = q_j$ можно сократить. В частности, $p_1 \neq q_1$, значит $(p_1, q_1) = 1$. Работает важная лемма: $p_1 | q_1 q_2 \dots q_{t_2}, (p_1, q_1) = 1$, значит $p_1 | q_2 \dots q_{t_2}$, тогда $q_2 \dots q_{t_2} = p_1 w, w \in N, w$ имеет разложение на простые $w = r_1 \dots r_s$. Тогда $n > m = q_2 q_3 \dots q_{t_2} = p_1 r_1 \dots r_s$. $p_1 \neq q_j$ . В левом разложении нет $p_1$, а в правом есть, получаем противоречие, так как $m < n$, а по предположению индукции для $m$ мы имеем единственность.

Каноническое разложение на простые множители принято записывать так: $n = {p_1}^{\nu_1} \dots {p_t}^{\nu_t}$.

*Определение.* $\nu_p(n) = \max\{k: p^k | n\}$.

Тогда $n = {p_1}^{\nu_1} \dots {p_t}^{\nu_t} = \prod_{p|n} p^{\nu_p(n)} = \prod_p p^{\nu_p(n)}$, так как если $p \nmid n$, то $\nu_p(n) = 0$.

*Упражнение.* Доказать, что

1)если $a | b \Leftrightarrow \forall\, p\ \nu_p(a) \leq \nu_p(b)$

2)если $\nu_p(ab) = \nu_p(a) + \nu_p(b)$

3) $\nu_p([a_1, \dots a_n]) = \max\limits_{1 \leq j \leq n} \nu_p(a_j)$, НОК

4) $\nu_p(\text{НОД}(a_1, \dots, a_n)) = \min\limits_{1 \leq j \leq n} \nu_p(a_j)$

Теорема. $\nu_p(n!) = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right]$.

Доказательство.

Лемма. Количество натуральных чисел $\leq x$ и кратных $m$ равно $\left[\frac{x}{m}\right]$.

Т.е. $\sum_{l: l \leq x, m|l} 1 = \left[\frac{x}{m}\right]$. $\nu_p(n!) = \sum_{j=2}^{n} \nu_p(j) = \sum_{j=2}^{n} \sum_{k: p^k | j} 1 = \sum_{k=1}^{\infty} \sum_{j: j \leq n, p^k | j} 1 =$ (по лемме) $\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

## Лекция 5

### 5.1 Арифметические функции.

*Определение.* Отображение $f: N \to C$(из натуральных чисел в комплексные) называется арифметической функцией.

*Определение.* Пусть $f \not\equiv 0$ арифметическая функция и пусть для $\forall\, a, b \in N : (a, b) = 1$ выполняется $f(ab) = f(a)f(b)$. Тогда функция $f$ называется мультипликативной. Если же для всех $a, b \in N$ выполняется $f(ab) = f(a)f(b)$, то такая функция $f$ называется вполне мультипликативной.

Примеры.

1) $\tau(n) -$ количество делителей натурального числа $n$. $\tau(n) = \sum_{d|n} 1$

2) $\sigma(n) -$ сумма всех делителей $n$. $\sigma(n) = \sum_{\substack{d|n \\ d\in N}} d$

3) $\varphi(n)$ –количество натуральных чисел не превосходящих n, взаимно простых с $n$ (функция Эйлера).

Пусть $n = {p_1}^{\alpha_1} \dots {p_s}^{\alpha_s}$. Тогда $\tau(n) = \prod_{i=1}^{s}(1 + \alpha_i)$.

Предложение 1. Если $f -$ мультипликативная, то $f(1) = 1$.

Доказательство. $f(1^2) = f(1)^2$. $f(1)(f(1) - 1) = 0$. Если $f(1) = 0$, то $f(n) = f(n * 1) = f(n) * f(1) = 0$(предполагаем, что $f \not\equiv 0$) . Значит, $f(1) = 1$.

Предложение 2. Пусть $f -$ мультипликативная, тогда $\sum_{d|n} f(d) = \prod_{p|n}\left(1 + f(p) + f(p^2) + \ldots + f\left(p^{\nu_p(n)}\right)\right)$. Напоминание $\nu_p(n) = \max\{k \in Z \cup \{0\}: p^k | n\}$.

Доказательство. $\prod_{p|n}\left(1 + f(p) + f(p^2) + \ldots + f\left(p^{\nu_p(n)}\right)\right) = \prod_{i=1}^{s}\left(1 + f(p_i) + f({p_i}^2) + \ldots + f({p_i}^{\alpha_i})\right)$,считаем, что $n = {p_1}^{\alpha_1} \dots {p_s}^{\alpha_s}$. $\prod_{i=1}^{s}\left(1 + f(p_i) + f({p_i}^2) + \ldots + f({p_i}^{\alpha_i})\right) = \sum_{\substack{0 \le k_i \le \alpha_i \\ i=1,\dots,s}} f({p_1}^{k_1} \dots {p_s}^{k_s}) = \sum_{d|n} f(d)$.

*Следствие 1.* Если $f$ –мультипликативная функция, то $g(n) = \sum_{d|n} f(d)$ тоже мультипликативная функция.

Доказательство. Пусть $(m, n) = 1$, тогда $g(mn) = \sum_{d|mn} f(d) = \prod_{p|mn}\left(1 + f(p) + \ldots + f(p^{\nu_p(mn)})\right) = (\prod_{p|m}(1 + f(p) + \ldots + f(p^{\nu_p(m)}))) * (\prod_{p|n}(1 + f(p) + \ldots + f(p^{\nu_p(n)}))) = \sum_{d|m} f(d) \sum_{d|n} f(d) = g(m)g(n)$.

*Следствие 2.* Пусть $n = {p_1}^{\alpha_1} \dots {p_s}^{\alpha_s}$, тогда $\sigma(n) = \prod_{p|n} \frac{p^{\nu_p(n)+1} - 1}{p - 1}$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Доказательство. $\sigma(n) = \prod_{p|n}\left(1 + p + \ldots + p^{v_p(n)}\right) = \prod_{p|n} \frac{p^{v_p(n)+1}-1}{p-1}$.

Теорема 1. Пусть $g(n) = \sum_{d|n} f(d)$,тогда выполняется следующее утверждение: f является мультипликативной функцией тогда и только тогда, когда $g(n)$ мультипликативная.

Доказательство. Слева направо. Смотреть Следствие 1.

Справа налево. $g(n)$ −мультипликативная. По индукции.

Заметим, что $g(1) = f(1)$, т. е. $f(1) = 1$. Пусть $N$ − минимальное натуральное число такое, что $\exists\, m, n: (m, n) = 1, mn = N, f(mn) \neq f(m) * f(n)$. Тогда $g(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|n \\ d_2|m}} f(d_1 d_2)$. Если $d_1 d_2 \neq mn$, то $d_1 d_2 < mn$. $\sum_{\substack{d_1|n \\ d_2|m}} f(d_1 d_2) = f(mn) + \sum_{\substack{d_1|m \\ d_2|n \\ d_1 d_2 < mn = N}} f(d_1) f(d_2)$. $g(mn) = g(m) * g(n) = (\sum_{d_1|m} f(d_1))(\sum_{d_2|n} f(d_2)) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) = f(m) f(n) + \sum_{\substack{d_1|m \\ d_2|n \\ d_1 d_2 < mn = N}} f(d_1) f(d_2)$. Следовательно, $f(mn) = f(m) f(n)$.

Теорема 2. $\sum_{d|n} \varphi(d) = n$.

Доказательство. Рассмотрим рациональные числа $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}$ в несократимом виде. Тогда все знаменатели являются делителями $n$. С другой стороны, $\frac{k}{d}$ − несократимая дробь тогда и только тогда, когда $(k, d) = 1$. Количество чисел взаимно простых с $d$ от 1 до $d$ равно $\varphi(d)$. Следовательно, $\sum_{d|n} \varphi(d) = n$.

**5.2 Функция Мебиуса.**

*Определение.* $\mu(n) = \begin{cases} 1, n = 1 \\ 0, \exists p: p^2 | n \\ (-1)^k, \text{если } n = p_1 * \ldots * p_k \end{cases}$

Лемма 1. $\sum_{d|n} \mu(n) = \begin{cases} 1, n = 1 \\ 0, n \neq 1 \end{cases}$

Доказательство. Очевидно, что функция Мебиуса мультипликативная. Очевидно, что $\varepsilon(n) = \begin{cases} 1, n = 1 \\ 0, n \neq 1 \end{cases}$ − тоже мультипликативная. Достаточно доказать для $n = p^\alpha$. Т.к. если необходимо что-либо доказать про две мультипликативные функции (например, их равенство), то достаточно доказать, что они совпадают на простых степенях, потому что на все остальные натуральные числа они однозначно восстанавливаются. Но $\mu(1) = 1 = \varepsilon(1), \sum_{d|p^\alpha} \mu(d) = \mu(1) + \mu(p) + \ldots + \mu(p^\alpha) = 0$. Так как по определению функции



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Мебиуса, $\mu(1) = 1, \mu(p) = -1$, а все остальное равняется нулю. (Можно было воспользоваться предложением 2)

*Замечание.* По предложению $2\sum_{d|n}\mu(d) = \prod_{p|n}\left(\mu(1) + \mu(p) + \ldots + \mu\left(p^{\nu_p(n)}\right)\right)$. Это верно в том случае, если $n \neq 1$, иначе произведение будет пустым, а пустое произведение не будет равно 0.

Теорема. Если $g(n) = \sum_{d|n} f(d)$, то $f(n) = \sum_{d|n} g(d) * \mu(\frac{n}{d})$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

## Лекция 6

### 6.1 Формула Мебиуса.

Функция Мебиуса: $\mu(n) = \begin{cases} 1, n = 1 \\ 0,\ \exists\, p - \text{простое}: p^2|n \\ -1^r, n = p_1 \dots p_r \text{ (произведение различных простых)} \end{cases}$

Основное свойство функции Мебиуса: $\sum_{d|n} \mu(d) = \begin{cases} 1, n = 1 \\ 0, n > 1 \end{cases}$

$\sum_{d|n} \varphi(d) = n$, $\varphi(d)$ –Функция Эйлера. $\varphi(d)$ – количество натуральных чисел не превосходящих n, взаимно простых с $n$ $\{1 \le x \le d, (x, d) = 1\}$.

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

Доказательство. $\varphi(n) = \sum_{\substack{1 \le a \le n \\ (a,n)=1}} 1$ –считаем количество взаимно простых чисел с $n$. Введем $i(a) = \begin{cases} 1, (a, n) = 1 \\ 0, (a, n) > 1 \end{cases}$. Тогда $\varphi(n) = \sum_{a=1}^{n} i(a)$. В свою очередь $i(a) = \sum_{d|(a,n)} \mu(d)$. Если $(a, n) = 1$, то выражение равно 1, если $(a, n) > 1$ получается 0. Тогда $\varphi(n) = \sum_{a=1}^{n} \sum_{d|(a,n)} \mu(d) = \sum_{\substack{1 \le a \le n \\ d|a \\ d|n}} \mu(d)$. Дальше группируем все слагаемые с одинаковым значением $d$. $d$ в любом случае будет делить $n$. $d|a, a \le n$, тогда $a$ имеет вид $a = da_1, da_1 \le n$, т. е. $a_1 \le \frac{n}{d}$. Значит таких $a$ в точности $\frac{n}{d}$. $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$.

*Следствие 1.* $\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$

Доказательство. Если $n = {p_1}^{\alpha_1} \dots {p_t}^{\alpha_t}$ –каноническое разложение на множители, то правая часть$= n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_t}\right) = n\left(1 - \frac{1}{p_1} - \dots - \frac{1}{p_t} + \frac{1}{p_1 p_2} + \dots + \frac{1}{p_{t-1} p_t} \dots\right) = n \sum_{k=0}^{t} (-1)^k \sum_{i_1 < i_2 < \dots < i_k} \frac{1}{p_{i_1} p_{i_k}}$. С другой стороны, $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$. Если $d|n$, а $n$ разлагается на простые, то $d = {p_1}^{\beta_1} \dots {p_t}^{\beta_t}$. И если $\mu(d) \ne 0$, тогда $\beta_j \in \{0,1\}$, то $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n\left(1 - \frac{1}{p_1} - \dots - \frac{1}{p_t} + \frac{1}{p_1 p_2} + \dots + \frac{1}{p_{t-1} p_t} \dots\right)$.

*Следствие 2.* Функция Эйлера мультипликативная, т.е. если $(m, n) = 1$, то $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказательство. Из следствия 1.

Формула обращения Мебиуса. $f, g: N \to R$(можно в комплексные). $g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} g(d) \mu(\frac{n}{d})$



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Доказательство. Дано $g(d) = \sum_{k|d} f(k)$. Вычисляем правую часть выражения $f(n)$. Правая часть$= \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) = \sum_{d|n}(\sum_{k|\frac{n}{d}} f(k))\mu(d) = \sum_{\substack{d|n \\ k|\frac{n}{d}}} f(k)\mu(d)$. $\begin{cases} d|n \\ k|\frac{n}{d} \end{cases} \Leftrightarrow \begin{cases} k|n \\ d|\frac{n}{k} \end{cases}$

Т.е. $k\lambda = \frac{n}{d}, kd\lambda = n$. $\sum_{\substack{d|n \\ k|\frac{n}{d}}} f(k)\mu(d) = \sum_{k|n} f(k) \sum_{d|\frac{n}{k}} \mu(d) = f(n)$

Дано $f(d) = \sum_{k|d} g(k)\mu(\frac{d}{k})$. Преобразуем правую часть $g(n)$. $\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{k|\frac{n}{d}} g(k)\mu\left(\frac{n}{dk}\right) = \sum_{k|n} g(k) \sum_{d|\frac{n}{k}} \mu\left(\frac{n}{dk}\right) = \sum_{k|n} g(k) \sum_{d|\frac{n}{k}} \mu(d) = g(n)$

**6.2 Сравнения и их свойства.**

$a \equiv b(mod\ m)$ $a$ сравнимо с $b$ по модулю $m$ (иногда пишут $a \equiv b(m)$). Это означает, что $m|(a-b)$ или что у $a$ и $b$ одинаковые остатки по модулю $m$.

$1^0$. (Три свойства в одном пункте). Если $a \equiv b(m)$, а $b \equiv c(m)$, то $a \equiv c(m)$.

$a \equiv a(m)$.

$a \equiv b(m)$ тогда и только тогда, когда $b \equiv a(m)$.

$2^0$. Если $a \equiv b(m)$ и $c \equiv d(m)$, то $a \pm c \equiv b \pm d(m)$.

$3^0$. Если $a \equiv b(m)$ и $c \equiv d(m)$, то $ac \equiv bd(m)$.

Доказательство $3^0$. $a \equiv b(m)$ означает, что $b + \lambda m$, где $\lambda \in Z$. $c = d + \mu m$, где $\mu \in Z$. $ac = (b+\lambda m)(d+\mu m) = bd + \lambda md + b\mu m + \lambda\mu m^2 = bd + m(\lambda d + b\mu + \lambda\mu m)$. Т.е. $ac$ есть сумма $bd$ и целого кратного $m$: $m(\lambda d + b\mu + \lambda\mu m)$.

$4^0$. Если $a \equiv b(mod\ m)$ и $d|a, d|b, d|m$, то на $d$ можно сократить. $a = a_1 d, b = b_1 d, m = m_1 d$. Тогда $a_1 \equiv b_1(mod\ m)$.

Доказательство $4^0$. $a = b + \lambda m$, $a_1 d = b_1 d + \lambda\, m_1 d$, тогда $a_1 = b_1 + \lambda\, m_1$. Следовательно, $a_1 \equiv b_1(\, m_1)$.

$5^0$. Если $da \equiv db(mod\ m), (d, m) = 1$, то на $d$ можно сократить $a \equiv b(mod\ m)$.

Доказательство $5^0$. $da \equiv db(m)$, это значит, что $m|da - db = d(a-b)$, но $(m, d) = 1$. По важной лемме $m|a-b$, отсюда $a \equiv b(m)$.

$6^0$. Пусть $(a, m) = 1$, тогда $\exists x \in Z: ax \equiv 1(m)$.

Доказательство $6^0$. $(a, m) = 1$. По теореме о линейном представлении НОД $\exists x, y \in Z: ax + my = 1$, тогда $ax \equiv 1\ (m)$

*Замечание.* Если $ax \equiv 1(mod\ m), ax' \equiv 1(mod\ m)$, $(a, m) = 1$, следовательно $x \equiv x'(mod\ m)$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

*Упражнение.* Доказать замечание.

$7^0$. Пусть $(a,m)=1$, $b$ –произвольное, тогда $\exists x: ax \equiv b(mod\, m)$ и такое $x$ единственно по $mod\, m$, т.е. если $ax \equiv b(mod\, m)$ и $ax' \equiv b(mod\, m)$, то $x \equiv x'(mod\, m)$.

Доказательство $7^0$. Существование в 7 сразу следует из 6 (умножим на $b$).

Если $ax \equiv b(mod\, m)$, $ax' \equiv b(mod\, m)$, то $ax - ax' \equiv 0(mod\, m)$, т.е. $a(x-x') \equiv 0(mod\, m)$, $(a,m)=1$, по свойству 5 $x - x' \equiv 0(mod\, m)$ и единственность доказана.

$8^0$. Если $(a,m)=1$ и $a \equiv b(mod\, m)$, то $(b,m)=1$

Теорема Эйлера. Если $(a,m)=1$, то $a^{\varphi(m)} \equiv 1(mod\, m)$.

Доказательство. $\varphi(m) = |\{x \in N, x \le m, (x,m)=1\}$ –количество элементов в заданном множестве. Пусть $x_1, x_2, x_3, \dots, x_{\varphi(m)}$ – все числа из заданного выше множества. Рассмотрим $ax_1, ax_2, \dots, ax_{\varphi(m)}$. У этих чисел по $mod\, m$ есть остатки. $\forall\, 1 \le j \le \varphi(m)$ $ax_j = r_j(mod\, m$, где $r_j$ –остатки по $mod\, m, 0 \le r_j \le m-1$. $(x_j, m)=1$, $(a,m)=1$ значит $(ax_j, m)=1$. По свойству 8 получается, что $\forall\, 1 \le j \le \varphi(m)$ $(r_j, m)=1$. То есть $1 \le r_j \le (m-1)$: $(r_j, m)=1$. Докажем, что все числа $r_j$ различные, т.е. $r_j \ne r_i$ при $i \ne j$. Предположим, что $r_j$=$r_i$, тогда $ax_i \equiv r_i = r_j \equiv ax_j(mod\, m)$, т.е. $ax_i \equiv ax_j(mod\, m)$. $(a,m)=1$, по свойству 5 $x_i = x_j(mod\, m)$, но $1 \le x_j, x_i \le m$. Если два числа от 1 до m сравнимы по $mod\, m$, то они должны совпадать. Значит, $x_j = x_i$, тогда $j = i$, но все $x_j$ различны (т.е. если они совпадают, то $j = i$ ). Значит, все $r_j$ также различны.

Перемножим все сравнения с $r_j$. Тогда $a^{\varphi(m)} x_1 \dots x_{\varphi(m)} \equiv r_1 \dots r_{\varphi(m)}(mod\, m)$. Но $r_1 \dots r_{\varphi(m)}$ – это перестановка чисел $x_1 \dots x_{\varphi(m)}$. Вывод: $x_1 \dots x_{\varphi(m)} = r_1 \dots r_{\varphi(m)}$. Замечание. $(x_1 \dots x_{\varphi(m)}, m)=1$, так как $(x_j, m)=1$ $\forall\, j$. По свойству 5 на него можно сократить $x_1 \dots x_{\varphi(m)}$. Получается $a^{\varphi(m)} \equiv 1(mod\, m)$.

**6.3 Китайская теорема об остатках.**

Пусть $m_1, m_2, \dots, m_t$: $(m_i, m_j)=1$ $\forall\, i \ne j$ (попарно – взаимно простые). Рассмотрим следующую систему (китайская система): $\begin{cases} x \equiv b_1(mod\, m_1) \\ x \equiv b_2(mod\, m_2) \\ x \equiv b_3(mod\, m_3) \\ \dots \\ x \equiv b_t(mod\, m_t) \end{cases}$. Также рассмотрим $M = m_1 \dots m_t$, $M_j = M/m_j$, заметим, что $(M, M_j)=1$, тогда $\exists C_j: M_j C_j \equiv 1(mod\, m_j)$. $x^* = \sum_{j=1}^{t} M_j C_j b_j$. Утверждение теоремы: общее решение китайской системы $X \equiv x^*(mod\, M)$.

Доказательство.

1)$x^*$ –решение.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Рассмотрим $x^*$ по $mod\, m_k$. $M_j C_j \equiv \delta_{kj} (mod\, m_k)$, где $\delta_{kj} = \begin{cases} 1, k = j \\ 0, k \neq j \end{cases}$. Значит, $x^* \equiv b_k (mod\, m_k)$.

2)Ясно, что если $x$ и $x'$ –два решения, то $(x - x_j) \equiv 0 (mod\, m_j)\ \forall\, j$. Тогда $m_j | x - x'\ \forall\, j, (m_j, m_k) = 1$ при $k \neq j$. Значит, $m_1 \dots m_t | x - x'$, т.е. $x \equiv x' (mod\, M)$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

## Лекция 7

### 7.1 Классы вычетов.

Если $(a,m)=1$, то $a^{\varphi(m)} \equiv 1(mod\, m)$. Здесь $\varphi(m) = |\{x \in N: x \leq m, (x,m) = 1\}$ –функция Эйлера. $\varphi(p) = p-1$, если $p$ –простое. Частный случай теоремы Эйлера– это малая теорема Ферма, которая утверждает: если $(x,p)=1, p-$ простое, то $x^{p-1} \equiv 1(mod\, p)$.

*Следствие.* $x^p \equiv x(mod\, p), \forall\, x \in Z$, если $p-$ простое.

Если $a \equiv b(mod\, b)$, то сравнение задает отношение эквивалентности. А всякое отношение эквивалентности позволяет разбивать множество на классы эквивалентности.

Классы эквивалентности будут следующие: если есть $a \in Z$, то класс $\bar{a} = \{x \in Z: x \equiv a(mod\, m)\}$.

Операции:

*Определение.* Сумма и произведение классов эквивалентности – если есть класс $\bar{a}$ и класс $\bar{b}$, то $\bar{a} + \bar{b} = \overline{a+b}$ (класс элемента $a$+ класс элемента $b$=класс элемента $a+b$).

$\bar{a} * \bar{b} = \overline{ab}$.

*Утверждение*. Эти определения корректны.

Проверим это утверждение для произведения: если есть $a_1 \in \bar{a}, b_1 \in \bar{b}$, надо проверить, что $a_1 * b_1 \in \overline{a*b}$. $a_1 \equiv a(mod\, m), b_1 \equiv b(mod\, m)$, значит, $a_1 b_1 \equiv ab(mod\, m)$. Тогда $\overline{a_1 b_1} = \overline{ab}$.

*Утверждение.* Если есть $a$, то $\exists a^*: aa^* \equiv 1(mod\, m)$ тогда и только тогда, когда $(a,m) = 1$.

Доказательство. $aa^* \equiv 1(mod\, m)$, тогда $aa^* = 1 + \lambda m$. $\begin{cases} d|a \\ d|m \end{cases} \Longrightarrow d|1 \Longrightarrow (a,m) = 1$. В обратную сторону через линейное представление НОД.

*Определение.* Класс вычетов $A$ по $mod\, m$ обратим, если $\exists$ класс вычетов $B: A * B = \bar{1}$.

*Утверждение.* $A$ обратим по $mod\, d$ тогда и только тогда, когда $\exists x \in A: (x,m) = 1 \Leftrightarrow$ (далее другая формулировка)$\forall\, x \in A\ (x,m) = 1$.

Доказательство 1. $A = \bar{a}$. $\exists b: B = \bar{b}$, т.е. $a * b \equiv 1(mod\, m)$. Тогда $\exists\, a : (a,m) = 1$

Доказательство 2. Если $\exists x \in A: (x,m) = 1$, т.е. $A = \bar{x}$. Возьмем $y \in A$, тогда $y \equiv x(mod\, m)$. Тогда $y = x + \lambda m$, $(x,m) = 1$, тогда $(y,m) = 1$. В итоге $\forall y \in A\ (y,m) = 1$.

Функция Эйлера – это количество обратимых классов эквивалентности по $mod\, m$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

*Определение 1.* Множество $B \subset Z$ называется полной системой вычетов по $mod\ m$, если в $B$ имеется ровно по одному представителю из каждого класса вычетов.

Т.е. $B$ –полная система вычетов по $mod\ m$ тогда и только тогда, когда 1)$\forall x \in Z\ \exists b \in B: x \equiv b(mod\ m)$,2) $\forall\ b_1, b_2 \in B$(различные) $b_1 \not\equiv b_2(mod\ m)$.

Для любой полной системы вычетов по $mod\ m$ количество элементов $B$: $|B| = m$.

*Определение 2.* Множество $B \subset Z$ называется приведенной системой вычетов, если $b \subset B \Rightarrow (b, m) = 1$ и в $B$ имеется ровно по одному представителю из каждого обратимого класса вычетов по $mod\ m$.

$B$ – приведенная система вычетов $\Leftrightarrow$1) $\forall b \in B\ \ (b, m) = 1$ 2) $\forall x \in Z: (x, m) = 1\ \exists b \in B: x \equiv b(mod\ m)$ 3) $b_1, b_1 \in B$ различные , то $b_1 \not\equiv b_2(mod\ m)$.

Пример. Пусть $(m, n) = 1$, $B_m$ –какая- то приведенная система вычетов по $mod\ m$, $B_n$ –какая-то приведенная система вычетов по $mod\ n$. Рассмотрим множество $B = \{am + bn, a \in B_n, b \in B_m\}$.

Теорема. $B$ – это приведенная система вычетов по $mod\ mn$.

Доказательство.

1 условие: если $z \in B, z = am + bn$. $(z, m) = (bn, m)$. Если $(n, m) = 1$ и $(b, m) = 1$, то можно сократить: $(bn, m) = 1$. Значит, $(z, n) = 1$, так как $(am, n) = 1$.

2 условие: берем $x \in Z: (x, mn) = 1$. Ищем $z \in B: z \equiv x(mod\ mn)$. $z = am + bn, am + bn \equiv x(mod\ mn) \Leftrightarrow \begin{cases} am + bn \equiv x(mod\ m) \\ am + bn \equiv x(mod\ m) \end{cases} \Leftrightarrow \begin{cases} bn \equiv x(mod\ m) \\ am \equiv x(mod\ n) \end{cases}$, тогда $\exists b \in B_m, \exists a \in B_n$

3 условие: если $am + bn \equiv a'm + b'n(mod\ mn)$, то $am \equiv a'm(mod\ n), bn \equiv b'n(mod\ m)$. Так как $(m, n) = 1$, то $a \equiv a'(mod\ n), b \equiv b'(mod\ m)$. Но так как $a, b$ из приведенных систем в единственном количестве $a = a', b = b'$.

$|B| = |B_n||B_m|$=$\varphi(n)\varphi(m) = \varphi(mn)$

*Следствие.* $\varphi(mn) = \varphi(n)\varphi(m)$,если $(m, n) = 1$.

*Упражнение.* Пусть $B_n, B_m$ –полные системы вычетов по $mod\ m, n$. Как аналогично получить полную систему вычетов по $mod\ mn$?

**7.2 Сравнения и многочлены.**

Многочлен: $f(x) = a_n x^n + \ldots + a_1 x + a_0$, где $a_j \in Z$.

Пусть $m = p$ –простое. Рассмотрим $f(x) = x^p - x$ по $mod\ p$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

*Определение.* Многочлен по $mod\, m$ называется тождественно нулевым, если все его коэффициенты $a_j \equiv 0(mod\, m)$.

$f(x) = x^p - x$ –это не тождественно нулевой многочлен по $mod\, p$.

Теорема. Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0, a_n \not\equiv 0(mod\, p), p -$ простое, $n = \deg\, f(x)$, тогда $f(x)$ имеет не более $n$ различных корней по $mod\, p$.

Доказательство. Индукция по $n$. n=1- основание индукции. $f(x) = a_1 x + a_0, (a_1, p) = 1$, $a_1 x \equiv -a_0(mod\, p)$. Корни ищем в классах вычетов по $mod\, p$.

Шаг индукции: предположение индукции: у многочленов степени $\leq n-1$ корней не больше, чем степень. $(a_n, p) = 1$. Если у $f(x)$ нет корней, то доказывать нечего. Необходимо предположить, что корень $\exists$. Пусть $f(x_0) \equiv 0(mod\, p)$. $f(x) \equiv \big(f(x) - f(x_0)\big)(mod\, p) = a_n x^n + \ldots + a_1 x + a_0 - (a_n {x_0}^n + \ldots + a_1 x_0 + a_0) x_0 = (x - x_0) h(x)$, $h(x) = a_n(x^{n-1} + x^{n-2} x_0 + \ldots + {x_0}^{n-1}) + a_{n-1} * \ldots$ . Т.е. $f(x) \equiv (x - x_0) h(x)(mod\, p)$ (как функции).

Пусть $x_1 -$ корень $f(x)$, отличный от $x_0$, т.е. $x_1 \not\equiv x_0(mod\, p)$. $0 \equiv f(x_1) \equiv (x_1 - x_0) h(x_1)$(mod p), тогда $h(x_1) \equiv 0(mod\, p)$. $h$ –многочлен степени $\leq n-1$, для которого верно предположение индукции. Теорема док.

Рассмотрим $f(x) = x^{p-1} - 1, g(x) = (x-1)(x-2) \ldots (x-(p-1))$. Эти многочлены не тождественные нули.

После раскрытия скобок : $g(x) = x^{p-1} + \ldots$;

Рассмотрим $h(x) = f(x) - g(x)$. Тогда степень $h(x) \leq p - 2$.

$\forall x = 1, \ldots, p-1$ $h(x) \equiv 0(mod\, p)$, значит, у него $p-1$ корней. Тогда $h(x) -$ тождественно нулевой многочлен. Так как $h(x) -$ тождественно нулевой многочлен, то он и как функция тождественный ноль. $h(x) \equiv 0(mod\, p)\ \forall x \in Z$. Тогда $h(0) = 0$. Значит, $-1 \equiv (-1)(-2) \ldots (-(p-1))(mod\, p)$.

Если $p \geq 3$, то $p -$ нечет., четное число скобок. $-1 \equiv (p-1)!\,(mod\, p) -$ теорема Вильсона.

**7.3 Лемма Гензеля.**

$f(x) = a_n x^n + \ldots + a_1 x + a_0$. $(a_n, p) = 1$. Известно решение $f(x_1) = 0(mod\, p)$. Необходимо найти решение по $mod\, p^\alpha$ , $\alpha \geq 1$.

Лемма. Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0, a_j \in Z, a_n \not\equiv 0(mod\, p)$ и пусть $f(x_1) \equiv 0(mod\, p)$ и $f'(x_1) \not\equiv 0(mod\, p)$. Тогда $\forall\, \alpha \in N\ \exists!\ x_\alpha$ по $mod\, p^\alpha$: 1) $f(x_\alpha) \equiv 0(mod\, p^\alpha)$, 2) $x \equiv x_\alpha(mod\, p)$.

(иногда эту лемму называют леммой о подъеме решения.)



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Доказательство.

Основание очевидно при $\alpha = 1$. Шаг: получим из решения по $mod\, p^{\alpha}$ решение по $mod\, p^{\alpha+1}$. Решение $x_{\alpha+1}$ надо искать в виде $x_{\alpha+1} = x_{\alpha} + t * p^{\alpha}$.

$f(x_{\alpha+1}) = f(x_{\alpha} + t * p^{\alpha})$. $(x_{\alpha} + tp^{\alpha})^{k} \equiv {x_{\alpha}}^{k} + ktp^{\alpha}{x_{\alpha}}^{k-1}(mod\, p^{\alpha+1}), 2\alpha \geq \alpha + 1, \alpha \geq 1$. Тогда $f(x_{\alpha+1}) \equiv f(x_{\alpha}) + f'(x_{\alpha})tp^{\alpha}(mod\, p^{\alpha+1})$.

$f(x_{\alpha}) = \lambda p^{\alpha}$, так как $f(x_{\alpha}) \equiv 0(mod\, p^{\alpha})$по предположению индукции.

Сокращаем на $p^{\alpha}$: $0 \equiv \lambda + f'(x_{\alpha})t(mod\, p)$. Итак, лемма Гензеля доказана.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

## Лекция 8

### 8.1 Лемма Гензеля.

Теорема Эйлера. Если $(a, m) = 1$, то $a^{\varphi(m)} \equiv q(mod\ m)$.

Следствие- малая теорема Ферма. Если $p$ –простое, $p \nmid a$, то $a^{p-1} \equiv 1(mod\ p)$.

Многочлены $g(x) = x^{p-1} - 1, h(x) = (x-1)(x-2)\dots(x-(p-1))$ совпадают как многочлены по $mod\ p$. $g(x) - h(x) \equiv 0(mod\ p)$. Разложение многочлена $g(x)$ на линейные множители: $x^{p-1} - 1 = (x-1)(x-2)\dots(x-(p-1))$. Отсюда выводится теорема Вильсона при $x = 0$: $(p-1)! \equiv -1(mod\ p)$.

Теорема. $f(x) = f_n(x)x^n + \dots + f_0, f_j \in Z$. $f_n \not\equiv 0(mod\ p)$, тогда количество различных корней многочлена $f$ по $mod\ p$ не превосходит его степень $n = \deg f$. $p$ – простое.

Лемма Гензеля (лемма о «подъеме решения»). Пусть $f(x) \in Z[x]$.

Пусть $f(x_1) \equiv 0(mod\ p), p$ –простое и пусть $f'(x_1) \not\equiv 0(mod\ p)$. Тогда $\forall\ \alpha \in N\ \exists!\ x_\alpha$ по $mod\ p^\alpha$: 1) $x_\alpha \equiv 0(mod\ p^\alpha)$. 2) $x_\alpha \equiv x_1(mod\ p)$.

Доказательство. По индукции по $\alpha$.

Основание индукции $\alpha = 1$ –ясно. Шаг индукции: предполагаем для $\alpha$ доказано. Пусть $x^* \equiv x_1(mod\ p)$ корень $f(x)$, который 1) $f(x) \equiv 0(mod\ p^{\alpha+1})$, 2) $x \equiv x_1(mod\ p)$. Из 1) следует, что $f(x) \equiv 0(mop\ p^\alpha)$. Тогда, учитывая 2), по предположению индукции $x^* \equiv x_\alpha(mod\ p^\alpha)$. Решение $x^*$ должно иметь вид: $x^* = x_\alpha + tp^\alpha, t \in (mod\ p)$.

Преобразуем $f(x^*) = f(x_\alpha + tp^\alpha)$. $(x+y)^k = x^k + kx^{k-1}y + \dots$

$$f(x^*) = f(x_\alpha + tp^\alpha) = \overbrace{f_n {x_\alpha}^n + f_{n-1}{x_\alpha}^{n-1} + \dots + f_1{x_\alpha}^1 + f_0}^{f(x_\alpha)} +$$
$$tp^\alpha \overbrace{(nf_n{x_\alpha}^{n-1} + (n-1)f_{n-1}{x_\alpha}^{n-2} + (n-2)f_{n-2}{x_\alpha}^{n-3} + \dots + f_1)}^{f'(x_\alpha)} +$$

$\dots$ тут слагаемые вида $A * p^{2\alpha}$, где $A \in Z$. Сюда входят все степени $\geq 2$ с целыми коэффициентами.

$\alpha \geq 1$, следовательно $2\alpha \geq \alpha + 1$.

Получаем $f(x_\alpha + tp^\alpha) \equiv (f(x_\alpha) + tp^\alpha f'(x_\alpha))(mod\ p^{\alpha+1})$. Цель состоит в том, чтобы найти все $t$ по $mod\ p$: $f(x_\alpha + tp^\alpha) \equiv 0(mod\ p^{\alpha+1})$. Дано $f(x_\alpha) \equiv 0(mod\ p^\alpha)$.

$\frac{f(x_\alpha)}{p^\alpha} \in Z$. $f(x_\alpha) + tp^\alpha f'(x_\alpha) \equiv 0(mod\ p^{\alpha+1})$ –все члены сравнения и модуль делятся на $p^\alpha$. Значит, можно сократить. Сокращаем на $p^\alpha$. $\frac{f(x_\alpha)}{p^\alpha} + tf'(x_\alpha) \equiv 0(mod\ p)$. По свойству сравнений $\exists!\ t$ по $mod\ p$ удовлетворяющее этому сравнению.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

*Упражнение.* Как формулируется утверждение для случая $f'(x_1) \equiv o(mod\ p)$, $\alpha = 2$.

*Замечание.* О сравнениях $f(x) \equiv 0(mod\ m)\ (*), f(x) \in Z[x], m = m_1 \dots m_t, (m_i, m_j) = 1$.

Как, зная решения каждого сравнения $f(x) \equiv 0(mod\ m_j)$, получить все решения сравнения **(*)**?

Если $x_j -$ это решение $f(x_j) \equiv 0(mod\ m_j)$, то $x^*$, определяемое из китайской системы $\begin{cases} x^* \equiv x_1(mod\ m_1) \\ \dots \\ x^* \equiv x_t(mod\ m_t) \end{cases}$, будет решением (*) и все решения имеют такой вид. Если есть система сравнений $\begin{cases} f(x) \equiv 0(mod\ m_1) \\ \dots \\ f(x) \equiv 0(mod\ m_t) \end{cases}$, то из условия $(m_i, m_j) = 1 \Leftrightarrow f(x) \equiv 0(mod\ m)$.

*Следствие.* Если $f(x) \equiv 0(mod\ m_j)$ имеет $N_j$ решений $1 \le j \le t$, тогда сравнение $f(x) \equiv 0(mod\ m_1 \dots m_t)$, где $(m_j, m_i) = 1$ имеет число решений $N_1 * \dots * N_t$.

**8.2 Квадратичные сравнения и символ Лежандра.**

$x^2 \equiv a(mod\ p)(*)$. $p -$ простое, $p \ge 3$

*Определение.* $a$ называется квадратичный вычет по $mod\ p$, если $a \not\equiv 0(mod\ p)$ и (*) разрешима.

*Определение.* $a$ называется квадратичный невычет по $mod\ p$, если $a \not\equiv 0(mod\ p)$ и (*) не разрешима.

Символ Лежандра $\left(\frac{a}{p}\right) = \begin{cases} 0, a \equiv 0(mod\ p) \\ 1, a - \text{квадратичный вычет по } mod\ p \\ -1, a - \text{квадратичный невычет по } mod\ p \end{cases}$

Свойства символа Лежандра.

$1^0$. Если $a \equiv b(mod\ p)$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Очевидно.

$2^0$. Теорема Эйлера. $a -$ квадратичный вычет $\Leftrightarrow \left(\frac{a}{p}\right) = 1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1(mod\ p)$

$3^0$. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(mod\ p), \frac{(p-1)}{2} \in Z$

$4^0$. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

$5^0$. Квадратичный закон взаимности Гаусса. Если $p, q \ge 3$ различные простые, то



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

$$\left(\frac{p}{q}\right) * \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} * \frac{q-1}{2}}$$

$6^0$. Дополнительное соотношение. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Очевидно, что из 3 следует 4. $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = (a)^{\frac{p-1}{2}}(b)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(mod\ p)$, $\left(\frac{ab}{p}\right) - \left(\frac{a}{b}\right)\left(\frac{b}{p}\right) \equiv 0(mod\ p), p \geq 3$. Следовательно, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

*Свойство 2*. Теорема Эйлера. $a$ −квадратичный вычет тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.

Доказательство. 1)Док-во ⇒ .

$a$ −квадратичный вычет, значит $(a, p) = 1$ и $\exists x: x^2 \equiv a(mod\ p)$. Следовательно, $(x, p) = 1$. По малой теореме Ферма $x^{(p-1)} \equiv 1(mod\ p)$. $x^{p-1} = x^{2*\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.

Док-во ⇐.

2)Дано $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.

$\pm 1, \pm 2, \pm 3, \dots, \pm\frac{p-1}{2}$ −приведенная система вычетов по $mod\ p$.

Возведем все в квадрат: $1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$. Получили все возможные квадраты по $mod\ p$. Т.е. это все квадратичные вычеты по $mod\ p$.

Утверждение. Это все <u>различные</u> квадратичные вычеты.

Док-во утв. Пусть $1 \leq i < j \leq \frac{p-1}{2}$: $i^2 \equiv j^2(mod\ p)$. Возьмем два различных числа из этого набора и предположим, что они совпадают по $mod\ p$. $i^2 \equiv j^2(mod\ p)$.

$j^2 - i^2 \equiv 0(mod\ p)$ или $(j-i)(j+i) \equiv 0(mod\ p)$. $0 < j - i < \frac{p-1}{p}, 2 \leq j + i \leq (p-1)$. По важной лемме либо $p|j-i$, либо $p|j+i$. Но в промежутках выше нет чисел, делящихся на $p$. Поэтому такого $1 \leq i < j \leq \frac{p-1}{2}$: $i^2 \equiv j^2(mod\ p)$ быть не может. Утв. доказано.

Рассмотрим многочлен $f(x) = x^{\frac{p-1}{2}} - 1$. $\deg f = \frac{p-1}{2}$. Все квадратичные вычета являются корнями $f(x)$, причем они различны. Их $\frac{p-1}{2}$(у многочлена корней ≤степень многочлена).

Свойство доказано.

*Свойство 3*. 1 случай. $a \equiv 0(mod\ p)$ − все ясно.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

2 случай. 2.1. $a -$ квадратичный вычет. $a^{\frac{p-1}{2}} \equiv 1(mod\, p) = \left(\frac{a}{p}\right)(mod\, p)$

2.2. $a$ –квадратичный невычет. Тогда $(a, p) = 1$. По малой теореме Ферма $a^{p-1} - 1 \equiv 0(mod\, p)$. Разложим на множители $\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0(mod\, p)$. По важной лемме либо

$a^{\frac{p-1}{2}} - 1 \equiv 0(mod\, p)$, либо $a^{\frac{p-1}{2}} + 1 \equiv 0(mod\, p)$. 1 это $a^{\frac{p-1}{2}} \equiv 1(mod\, p)$, 2 это $a^{\frac{p-1}{2}} \equiv -1(mod\, p)$. Но по условию $a -$ квадратичный невычет. Значит, он не может удовлетворять 1 уравнению, потому что этому равенству удовлетворяют только вычеты.

Вывод. $a^{\frac{p-1}{2}} \equiv -1(mod\, p)$. Тогда $\left(\frac{a}{p}\right) = -1$. Когда $a$ –квадратичный невычет, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(mod\, p)$.

*Упражнение.* Доказать, что вычетов и невычетов по $mod\, p, p \geq 3$ одинаковое количество.

**8.3 Лемма Гаусса.**

Лемма.

$\pm 1, \pm 2, \pm 3, \dots, \pm \frac{p-1}{2} (**)$ –приведенная система вычетов по $mod\, p$. Запишем из нее только абсолютные величины $1,2,3, \dots, \frac{p-1}{2}$. Есть число $a : (a, p) = 1$ и необходимо понять вычет оно или невычет. Сделаем следующее: $1 * a = \varepsilon_1 r_1, 2 * a = \varepsilon_2 r_2, \dots, \frac{p-1}{2} * a = \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}$, все это по $mod\, p$. $r_j \in \left\{1,2, \dots, \frac{(p-1)}{2}\right\}, \varepsilon_j \in \{+1, -1\}$. Тогда $\left(\frac{a}{p}\right) = \prod_{j=1}^{\frac{p-1}{2}} \varepsilon_j$.

Доказательство. Перемножим. $a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! = \prod_{j=1}^{\frac{p-1}{2}} \varepsilon_j \prod_{j=1}^{\frac{p-1}{2}} r_j$.

Тогда $r_j$ –это перестановка чисел $1,2,3, \dots, \frac{p-1}{2}$. На них сокращаем. Получаем $a^{\frac{p-1}{2}} = \prod_{j=1}^{\frac{p-1}{2}} \varepsilon_j$. По критерию Эйлера $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$. Итак, $\left(\frac{a}{p}\right) = \prod_{j=1}^{\frac{p-1}{2}} \varepsilon_j$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

## Лекция 9

### 9.1 Квадратичный закон взаимности Гаусса и дополнительное соотношение.

$p \geq 3$ –простое.

$x^2 \equiv a(mod\ p) \quad (*)$

*Опр.* $a -$ квадратичный вычет, если $(a,p) = 1$ и (*) разрешима.

*Опр.* $a -$ квадратичный невычет, если $(a,p) = 1$ и (*) неразрешима.

Символ Лежандра $\left(\frac{a}{p}\right) = \begin{cases} 0, p|a \\ 1, a - \text{квадратичный вычет} \\ -1, \text{квадратичный невычет} \end{cases}$

Свойства символа Лежандра.

Если $a \equiv b(mod\ p)$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Теорема Эйлера. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(mod\ p)$. Из этого $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Дополнительное соотношение. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Теорема. (Квадр. з. взаимности Гаусса.)

$p, q \geq 3$, (различные, но в записанном виде верно и для одинаковых) простые, тогда $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Лемма Гаусса. $\pm 1, \pm 2, \pm 3, \dots, \pm\frac{p-1}{2}$ –приведенная система вычетов по $mod\ p$. Запишем половину этой приведенной системы в столбик, помножим на $a$. Пусть $(a,p) = 1$.

$\begin{matrix} 1*a \equiv \varepsilon_1 r_1 (mod\ p) \\ 2*a \equiv \varepsilon_2 r_2 (mod\ p) \\ \dots \\ \frac{p-1}{2}*a \equiv \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}} (mod\ p) \end{matrix}$, где $\varepsilon_j \in \{-1,1\}, r_j \in \left\{1,2,\dots,\frac{p-1}{2}\right\}$ –модули минимального остатка.

Тогда $\left(\frac{a}{p}\right) = \prod_{j=1}^{\frac{p-1}{2}} \varepsilon_j$.

Доказательство. Перемножим полученную систему. $a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! = \prod_{j=1}^{\frac{p-1}{2}} \varepsilon_j \prod_{j=1}^{\frac{p-1}{2}} r_j\ (mod\ p)$.

Утв. $r_1, r_2, \dots, r_{\frac{p-1}{2}} -$ это перестановка чисел $1,2,\dots,\frac{p-1}{2}$. Для каждого $r_j$ справедливо $1 \leq r_j \leq \frac{p-1}{2}$. Все $r_j$ различны. Действительно, если $r_j = r_i$, то $\pm ia \equiv ja(mod\ p)$. Но $(a,p) = 1$ и на $a$ можно сократить (по важной лемме): $\pm i \equiv j(mod\ p)$. $i \pm j \equiv 0(mod\ p), 1 \leq i,j \leq$



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

$\frac{p-1}{2}, 2 \le i+j \le (p-1)$. В этом промежутке нет чисел делящихся на p, поэтому $(i+j,p)=1$. Тогда $i-j \equiv 0(mod\, p)$. Тогда $i \equiv j(mod\, p)$. Следовательно, они совпадают $i=j$.

Вывод. $\prod_{j=1}^{\frac{p-1}{2}} r_j = \left(\frac{p-1}{2}\right)!$

Заметим, что $\left(\frac{p-1}{2}, p\right) = 1$. Тогда $a^{\frac{p-1}{2}} = \prod_{j=1}^{\frac{p-1}{2}} \varepsilon_j\, (mod\, p)$. Но $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)(mod\, p)$ по теореме Эйлера. Следовательно, $\left(\frac{a}{p}\right) = \prod_{j=1}^{\frac{p-1}{2}} \varepsilon_j$.

*Следствие.* $t = \#\{1 \le j \le \frac{p-1}{2} : \varepsilon_j = -1\}$. $t$ –количество элементов в указанном множестве. Тогда $\left(\frac{a}{p}\right) = (-1)^t$.

*Замечание.* $\frac{p^2-1}{8} \in Z$. $\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8}$, $p$ –нечетное. В числителе стоят два подряд идущих четных числа. Одно из них делится на 4, другое делится на 2.

Доказываем квадратичный закон и дополнительное деление с остатком.

Рассмотрим обычное деление с остатком. $\frac{ak}{p} = \left[\frac{ak}{p}\right] + \left\{\frac{ak}{p}\right\}$. Умножим на $p$. $ak = p\left[\frac{ak}{p}\right] + p\left\{\frac{ak}{p}\right\}$. $ak - p\left[\frac{ak}{p}\right] = \underbrace{p\left\{\frac{ak}{p}\right\}}_{r^*}$ –это остаток от деления $ak$ на $p$ в обычном делении с остатком. $1 \le r^* \le p-1$. $ak - p\left[\frac{ak}{p}\right] = p\left\{\frac{ak}{p}\right\} = \begin{cases} r_k, & \text{если } \varepsilon_k = 1 \\ p - r_k, & \text{если } \varepsilon_k = -1 \end{cases}$. Если $r^* \ge \frac{p+1}{2}$, то $r^* - p = r_k$, тогда обычный остаток $r^* = p - r_k$.

Перепишем. Если $r^* \ge \frac{p+1}{2}$, то $r^* = p - r_k, \varepsilon_k = -1$. $p\left\{\frac{ak}{p}\right\} = \begin{cases} r_k\ (\text{если } \varepsilon_k = 1) = \varepsilon_k * r_k \\ p - r_k\ (\text{если } \varepsilon_k = -1) = p + \varepsilon_k r_k \end{cases}, 1 \le k \le \frac{p-1}{2}$.

Посчитаем следующее: $\sum_{k=1}^{\frac{p-1}{2}} k = \frac{1}{2}\frac{p-1}{2}\left(\frac{p-1}{2}+1\right) = \frac{p^2-1}{8}$.

Сложим все выражения для $p\left\{\frac{ak}{p}\right\}$: $a\frac{p^2-1}{8} - p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right] = tp + \sum_{k=1}^{\frac{p-1}{2}} \varepsilon_k r_k$ .

Рассмотрим это равенство по $mod\ 2$. $a\frac{p^2-1}{8} - p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right] \equiv tp + \sum_{k=1}^{\frac{p-1}{2}} \varepsilon_k r_k\ (mod\ 2)$.

$p \equiv 1(mod\ 2)$, $+1 \equiv -1(mod\ 2)$. $\varepsilon_k \equiv 1(mod\ 2)$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Тогда $\sum_{k=1}^{\frac{p-1}{2}} \varepsilon_k r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} r_k (mod\ 2) \equiv \sum_{k=1}^{\frac{p-1}{2}} k\ (mod\ 2) = \frac{p^2-1}{8}$. И получим $a\frac{p^2-1}{8} - \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ak}{p}\right] \equiv t + \frac{p^2-1}{8} (mod\ 2)$.

Или (напоминание $+1 \equiv -1 (mod\ 2)$) $(a-1)\frac{p^2-1}{8} + \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ak}{p}\right] \equiv t (mod\ 2)$. Обозначим $S_a = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ak}{p}\right]$.

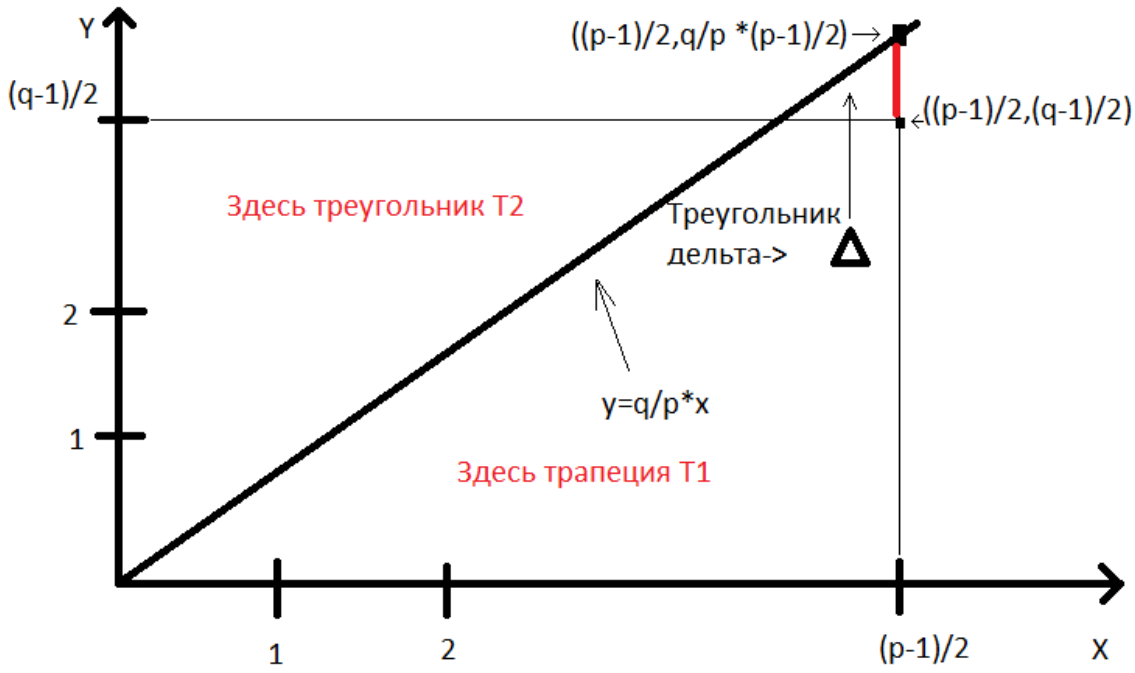
Рассмотрим случай, когда $a = 2$. Тогда $S_2 = 0$. Значит, $t \equiv \frac{p^2-1}{2} (mod\ 2)$. Получили $\left(\frac{2}{p}\right) = (-1)^t$. Дополнительное соотношение доказано.

Рассмотрим случай, когда a –нечетное. Обозначим $a = q$. Тогда $t \equiv \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] (mod\ 2)$.

Получится $\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right]}$. В свою очередь $\left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]}$

*Замечание.* Геометрический смысл сумм $\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right], \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]$.

Пусть $p > q$. Посмотрим прямую $y = \frac{q}{p}x$. Нужно определить то, где расположена точка $\left(\frac{p-1}{2}, \frac{q-1}{2}\right)$ –выше или ниже прямой $y = \frac{q}{p}x$.






МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

*Рис. 9.1 – Вспомогательный график.*

Получим $\frac{q-1}{2} < \frac{q}{p}\frac{p-1}{2} = \frac{q}{2}\frac{p-1}{p} < \frac{q}{2}$, так как

$p(q-1) < q(p-1)$

$pq - p \vee pq - q$

$-p \vee -q$

$-p < -q$, так как $p > q$.

В треугольнике дельта нет целых точек. Также расстояние обозначенное на рис. 9.1 не превосходит $\frac{1}{2}$.

$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right]$ –количество целых точек без учета нулевых точек в области $1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q}{p}x$ (в трапеции T1 (которая получается между прямой $y = \frac{q}{p}x$ и осью координат (даже если брать начало трапеции от $y = 0$, а не от $y = 1$, ничего не изменится-целая часть 0 все равно 0), так как в дельта нет целых точек). Причем на прямой $y = \frac{q}{p}x, 1 \le x \le \frac{p-1}{2}$, также целых точек нет.

$\sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]$ –количество целых точек в треугольнике T2.

Тогда $\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}$. Это количество целых точек в прямоугольнике $1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}$.

Вывод. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{qk}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}}\left[\frac{pj}{q}\right]} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

**9.2 Показатель числа по модулю $m$.**

Если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 (mod\ m)$. (теорема Эйлера).

*Определение.* Пусть $(a, m) = 1$, тогда $ord_m a = \min\{x \in N: a^x \equiv 1(mod\ m)\}$ (Это множество не пусто, так как есть $\varphi(m)$) есть показатель числа $a$ по $mod\ m$.

Теорема. Если $(a, m) = 1, a^z \equiv 1(mod\ m), z \in N$, то $ord_m a | z$.

Доказательство. Пусть $\nu = ord_m a$. Разделим $z$ на $\nu$ с остатком. Тогда $z = \nu q + r, 0 \le r < \nu. a^z \equiv 1(mod\ m)$, но также $a^z \equiv a^{\nu q + r}(mod\ m) \equiv (a^\nu)^q a^r (mod\ m) \equiv a^r (mod\ m)$ ($a^\nu = 1$, потому что $\nu$ это показатель), $a^r \equiv 1(mod\ m)$, а $r < \nu$ –таких натуральных чисел нет, потому что $\nu$ минимальное. Значит, $r = 0$. Т.е. $\nu | z$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

*Следствие.* $\forall\, a\colon (a,m) = 1 \;\; ord_m a | \varphi(m)$.

## Лекция 10

### 10.1 Первообразный корень.

Если $(a,m)=1$, то $a^{\varphi(m)}\equiv 1(mod\ m)$. (теорема Эйлера).

Рассмотрим множество $\Omega_a=\{x\in N: a^x\equiv 1(mod\ m)\}$, $\Omega_a\neq\emptyset$.

*Определение.* Показателем $a$ по $mod\ m$ называется минимальный элемент множества $\Omega_a$ $ord_m a=\min\Omega_a$.

Показатель—это такая минимальная натуральная степень, что если возвести в эту степень, то получится 1 по модулю m.

Теорема. Если $(a,m)=1, a^x\equiv 1(mod\ m), x\in N$, то $ord_m a|x$.

Доказательство. Обозначим $\nu=ord_m a$. Делим $x$ на $\nu$ с остатком. $x=\nu q+r, 0\le r<\nu$.

Если $r=0$, то все доказано. Рассмотрим $r\neq 0, 1\le r<\nu$. Тогда можно записать $a^x=a^{\nu q+r}$. Но $a^x\equiv 1(mod\ m), a^\nu\equiv 1(mod\ m)$,значит, $a^{\nu q}\equiv 1(mod\ m)$. Следовательно, $a^r=1(mod\ m)$, а $1\le r<\nu$. Но $\nu$ —минимальное. Противоречие.

Следствие. $ord_m a|\varphi(m)$ всегда.

Свойства показателя:

Утв. 1. Если $ord_m a=bc$, то $ord_m(a^b)=c$. $a^{bc}\equiv 1(mod\ m)$ и ни в какой меньшей степени оно не является 1.

Утв. 2. Если $ord_m a=x, ord_m b=y, (x,y)=1$, то $ord_m ab=xy$.

Доказательство. Надо показать, что $(ab)^{xy}\equiv 1(mod\ m)$. Это ясно, так как $(ab)^{xy}=\underbrace{(a^x)}_{\equiv 1(mod\ m)}{}^y\underbrace{(b^y)}_{\equiv 1(mod\ m)}{}^x\equiv 1(mod\ m)$. Докажем, что если $(ab)^z\equiv 1(mod\ m)$, то $x|z, y|z$. Так как $(x,y)=1$, то $xy|z$ и утв. 2 будет доказано.

Итак, $(ab)^z\equiv 1(mod\ m)$, возведем выражение в степень $x$: $(ab)^{zx}\equiv 1(mod\ m)$. $a^x\equiv 1(mod\ m)$, сокращаем на $a$. $b^{zx}\equiv 1(mod\ m)$, а $ord_m b=y$. По теореме (доказанной выше в этой лекции) $y=ord_m b|zx$. $y|zx, (x,y)=1$, тогда по важной лемме $y|z$.

Аналогично $(ab)^{zy}\equiv 1(mod\ m), a^{zy}\equiv 1(mod\ m)$. Тогда $x=ord_m a|zy$. Отсюда по важной лемме $x|z$.

*Определение.* Пусть $(g,m)=1$. $g$ называется первообразным корнем по $mod\ m$, если $ord_m g=\varphi(m)$.

Теорема. Пусть $m=p$ —простое, тогда $\exists g$ —первообразный корень по $mod\ m$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

1.

Доказательство.

Для $p = 2$ теорема очевидна. И пусть далее $p$ −нечетное простое. Рассмотрим приведенную систему вычетов по $mod\, p$: $1,2,\dots,p-1$. Рассмотрим также их показатели: $\nu_1 = ord_p 1 = 1, \nu_2 = ord_p 2, \nu_3 = ord_p 3, \dots, \nu_{p-1} = ord_p(p-1) = 2$. Пусть $\tau$ −наименьшее общее кратное всех возможных показателей. Рассмотрим многочлен $f(x) = x^\tau - 1$. $f(x)$ по $mod\, p$ имеет $p-1$ корень. $(p-1)$ − количество различных корней $\leq \tau$ − степень многочлена $f$. $\nu_j | \varphi(m)\ \forall\, j\ 1 \leq j \leq (p-1)$. Наименьшее общее кратное делит любое общее кратное. $\varphi(m)$ −общее кратное чисел $\nu_1, \dots, \nu_{p-1}$. Тогда $\tau | \varphi(m) = \varphi(m) = p-1$. Тогда $\tau \leq p-1$. Следовательно, $\tau = p-1$. Разложим его на простые множители: $\tau = p-1 = {q_1}^{\alpha_1} * \dots * q^{\alpha_t}$ −каноническое разложение на простые множители.

Сформулируем ряд утверждений, из которых получится доказательство теоремы:

1)$\forall\, j \in \{1,\dots,t\}\ \exists\, a_j$: $ord_p a_j \equiv 0\left(mod\, {q_j}^{\alpha_j}\right)$. Если ${q_j}^{\alpha_j}$ встретилось в наименьшем общем кратном, то оно встретилось в каком-то $\nu$, т.е. ${q_j}^{\alpha_j} |\, ord_p a_j$.

2)$\forall\, j \in \{1,\dots,t\}\ \exists\, b_j$: $ord_p b_j = {q_j}^{\alpha_j}$. $ord_p a_j = {q_j}^{\alpha_j} * w_j, w_j \in Z$. Тогда $b_j = {a_j}^{w_j}$.

3)$({q_j}^{\alpha_j}, {q_i}^{\alpha_i}) = 1$, если $i \neq j$. Возьмем $g = \prod_{j=1}^{t} b_j$. Тогда $ord_p g = \prod_{j=1}^{t} {q_j}^{\alpha_j} = p-1$.

Теорема. Первообразные корни существуют только по модулям вида $2,4,p^\alpha, p \geq 3, \alpha \in N$ и $2p^\alpha$.( обозначим эти модули как (*))

Если $m \in N, m > 1$ не имеет вид (*), то есть три возможности 1) $\exists\, p, q$ −различные, нечетные, простые : $pq|m$.

2)$m = 2^\alpha p^\beta, \alpha \geq 2, \beta \geq 1, p \geq 3$

3) $m = 2^\alpha, \alpha \geq 3$. (обозначим эти три возможности как (**))

*Замечание.* Если $m \in N, m > 1$, то либо удовлетворяет (*), либо удовлетворяет (**)

**10.2 Критерий первообразного корня.**

Критерий первообразного корня.

Пусть $(a, m) = 1$. Рассмотрим $\varphi(m)$. Тогда $a$ −является первообразным корнем по $mod\, m$ тогда и только тогда, когда $\forall q$ −простого: $q|\varphi(m)$ выполнено $\frac{a^{\varphi m}}{q} \not\equiv 1(mod\, m)$

Доказательство критерия.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Если $a$ −первообразный корень, то $ord_m a = \varphi(m)$. Тогда $\frac{a^{\varphi(m)}}{q} \not\equiv 1(mod\, m)$. Ясно, что если $q > 1$ и $q|\varphi(m)$, то $a^{\frac{\varphi(m)}{q}}$ не ноль, так как $\frac{\varphi(m)}{q} < \varphi(m)$.

$a^{\varphi(m)} \equiv 1(mod\, m)$ (теорема Эйлера). Если $ord_m a = \nu$, то $\nu|\varphi(m)$. Если $\nu < \varphi(m)$, то $\exists\, q -$ простое и $q|\varphi(m) : \nu|\frac{\varphi(m)}{q}$. Тогда $a^\nu \equiv 1(mod\, m)$ и $a^{\frac{\varphi(m)}{q}} \equiv 1(mod\, m)$. Противоречие. Значит, $\nu = \varphi(m)$.

**10.3 Теоремы и утверждения, связанные с первообразным корнем.**

Теорема. Первообразные корни существуют только по модулям вида $2,4,p^\alpha, p \geq 3, \alpha \in N$ и $2p^\alpha$.( обозначим эти модули как (*))

Доказательство. Если $m = 2$, то $g = 1$ −первообразный корень. $m = 4, g = 3$ −п.к.

$m = 8,\ \varphi(8) = 4$. Если $(a, 8) = 1$,то $a$ −нечетное. Тогда $a^2 \equiv 1(mod\, 8)$. $\forall\, a$ −нечетного $ord_8 a = 1$ или 2 По модулю 8 не существует первообразного корня. (эта теорема в этой лекции не будет доказана до конца. Лишь необходимые для этого утверждения и теоремы.) Сформулируем необходимую для доказательства теорему.

Теорема. Пусть $p$ −нечетное простое. 1) Пусть $g$ −первообразный корень по $mod\, p$. Тогда либо $g^{p-1} \not\equiv 1(mod\, p^2)$, либо $(g+p)^{p-1} \not\equiv 1(mod\, p^2)$.

2)Обозначим $g_1 = \begin{cases} g, \text{если } g^{p-1} \not\equiv 1(mod\, p^2) \\ g + p. \text{если } g^{p-1} \equiv 1(mod\, p^2) \end{cases}$. Заметим, что всегда выполняется $g_1^{p-1} \not\equiv 1(mod\, p^2)$. Тогда $\forall \alpha \in N\ \ g_1$ будет первообразным корнем по модулю $p^\alpha$.

Доказательство 1.

Предположим, что $g^{p-1} \equiv 1(mod\, p^2)$. Рассмотрим $(g+p)^{p-1} \equiv \underbrace{g^{p-1}}_{\equiv 1(mod\, p^2)} + \underbrace{\underbrace{(p-1)g^{p-2}}_{\not\equiv 0(mod\, p)} p}_{\not\equiv 0(mod\, p^2)}\ (mod\, p^2) \not\equiv 1(mod\, p^2)$. Тогда утверждение 1 доказано.

Доказательство 2.

Надо доказать, что $ord_{p^\alpha} g_1 = \varphi(p^\alpha). \varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Пусть $q$ −простое и $q|\varphi(p^\alpha)$. Тогда либо $q = p$, либо $q|(p-1)$. Для $q|p-1$ $g_1^{\left(\frac{\varphi(p^\alpha)}{q}\right)} = {g_1}^{p^{\alpha-1}\frac{p-1}{q}}.{g_1}^{\frac{p-1}{q}} \not\equiv 1(mod\, p)$. $a^p \equiv a(mod\, p)$. ${g_1}^{p^{\alpha-1}\frac{p-1}{q}} \equiv {g_1}^{\frac{p-1}{q}} \not\equiv 1(mod\, p)$. Тогда ${g_1}^{p^{\alpha-1}\frac{p-1}{q}} \not\equiv 1(mod\, p^\alpha)$. Для простых: $q|(p-1)$ критерий выполнен автоматически. А для $q = p$: $g_1^{\frac{\varphi(p^\alpha)}{p}} \not\equiv 1(mod\, p^\alpha)$, т.е. ${g_1}^{p^{\alpha-2}(p-1)} \not\equiv 1(mod\, p^\alpha)$. Если это доказать, то будет доказано, что $g_1$ −первообразный корень.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

По критерию $g_1$ –это первообразный корень по модулю $p^2$. Докажем, что $g_1$ это первообразный корень по модулю $p^\alpha, \alpha \geq 2$.

Утв. ${g_1}^{p^\beta(p-1)} \equiv 1 + c_\beta p^{\beta+1}\left(mod\ p^{\beta+2}\right)$, где $c_\beta \not\equiv 0(mod\ p)$.

Доказательство утв. По индукции.

$(g_1^{p^\beta(p-1)})^p = (1 + c_\beta p^{\beta+1} + Ap^{\beta+2})^p \equiv 1 + p\left(c_\beta p^{\beta+1} + Ap^{\beta+2}\right)\left(mod\ p^{\beta+3}\right) \equiv 1 + c_\beta p^{\beta+2}(mod\ p^{\beta+3})$.

Основание индукции. Шаг индукции $\beta = 0 \longmapsto \beta = 1$.

В разложении по биному Ньютона далее будет $\left(c_\beta p^{\beta+1} + Ap^{\beta+2}\right)^2$. И необходимо, чтобы это делилось на $p^{\beta+3}$: $p^{\beta+3} | \left(c_\beta p^{\beta+1} + Ap^{\beta+2}\right)^2$.

$\left(c_\beta p^{\beta+1} + Ap^{\beta+2}\right)^2$. Необходимо, чтобы выполнялось $2\beta + 2 \geq \beta + 3$, т.е. $\beta \geq 1$.

Биномиальный коэффициент при втором слагаемом $C_p^2 = \frac{p(p-1)}{2}$.

Если $p > 2$, то $p | C_p^2$, а если $p = 2$, то не делит.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

## Лекция 11

### 11.1 Общая теорема и ее доказательство.

$m \geq 2, m \in N, (a, m) = 1$

*Определение.* $\nu$ –показатель $a$ по $mod\ m$, $\nu = ord_m a = min\{\, x \in N: a^x \equiv 1(mod\ m)\}$

Теорема. Если $a^\mu \equiv 1(mod\ m)$и $\mu \in N,$ то $ord_m a | \mu$

*Следствие.* $ord_m a | \varphi(m)$.

*Определение.* $g$ называется первообразным корнем по $mod\ m$, если $ord_m g = \varphi(m)$. $(g, m) = 1$.

Критерий первообразного корня.

Пусть $(g, m) = 1$, тогда $\nu -$ первообразный корень по $mod\ m$ тогда и только тогда, когда $\forall q$ –простого: $q | \varphi(m)$ выполняется $g^{\frac{\varphi(m)}{q}} \not\equiv 1(mod\ m)$.

Теорема. Если $m = p$ –простое, то по $mod\ m$ $\exists$ первообразный корень.

Теорема. Первообразные корни существуют только по модулям вида $2,4, p^\alpha, 2p^\alpha, p \geq 3 -$ простое, $\alpha \in N$. (обозначим эти модули как (*))

Доказательство. Выпишем необходимые для доказательства теоремы утверждения.

Утв. 1. Пусть $g -$ первообразный корень по $mod\ p$, тогда либо $g^{p-1} \not\equiv 1(mod\ p^2)$, либо $(g + p)^{p-1} \not\equiv 1(mod\ p^2)$.

Утв. 2. Пусть $g$ –первообразный корень по $mod\ p$. Обозначим $g_1 = \begin{cases} g, \text{если } g^{p-1} \not\equiv 1(mod\ p^2) \\ g + p, \text{если } g^{p-1} \equiv 1(mod\ p^2) \end{cases}$. Тогда $g_1$ –это первообразный корень по $mod\ p^\alpha\ \forall\ \alpha \geq 1$.

Утв. 3. Пусть $g_1$ –это первообразный корень по $mod\ p^\alpha$. Обозначим $g_2 = \begin{cases} g_1, \text{если } g_1 - \text{нечетн.} \\ g_1 + p^\alpha, \text{если } g_1 - \text{четно} \end{cases}$, тогда $g_2$ –это первообразный корень по $mod\ 2p^\alpha$.

Утв. 4. Если $\exists p, q$ –различные, нечетные, простые: $pq | m$, то по $mod\ m$ $\nexists$ первообразных корней.

Утв. 5. Если $m = 2^\alpha p^\beta, \beta \geq 1, \alpha \geq 2, p$ –нечетное простое, то по $mod\ m$ $\nexists$ первообразных корней.

Утв. 6. По $mod\ m = 2^\alpha, \alpha \geq 3$ $\nexists$ первообразных корней.

Из утверждений 2,3 получается следующее: если $m$ имеет вид (*), то по $mod\ m$ $\exists$ первообразные корни.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Из утверждений 4,5,6 получается следующее: если $m$ не имеет вид (*), то по $mod\ m \nexists$ первообразных корней.

Доказательство утв. 1.

Пусть $g^{p-1} \equiv 1(mod\ p^2)$. $(g+p)^{p-1} \equiv \underbrace{g^{p-1}}_{\equiv q(mod\ p^2)} + \underbrace{(p-1)pg^{p-2}}_{\not\equiv 0(mod\ p^2)}(mod\ p^2)$.

Доказательство утв. 2.

Пусть $g_1$ –такой первообразный корень по $mod\ p$, что $g_1^{p-1} \not\equiv 1(mod\ p^2)$. Хотим проверить для него критерий первообразного корня по $mod\ p^\alpha$. $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Возьмем простой делитель $q|\varphi(p^\alpha)$. Либо $q|(p-1)$, либо $q = p$.

1)Если $q|(p-1)$, то $g_1^{\frac{p-1}{q}} \not\equiv 1(mod\ p)$. Но $x^p \equiv x(mod\ p)$. Следовательно, $g_1^{p^{\alpha-1}*\frac{p-1}{q}} \equiv g_1^{\frac{p-1}{q}} \not\equiv 1(mod\ p)$. Итак, $g_1^{\frac{\varphi(p^\alpha)}{q}} \not\equiv 1(mod\ p^\alpha)$. Для таких простых критерий выполнен автоматически.

2)Вспомогательное утверждение. $\forall \beta \geq 0, \beta \in N$ $g_1^{p^\beta(p-1)} \equiv 1 + c_\beta p^{\beta+1}(mod\ p^{\beta+2})$, где $(c_\beta, p) = 1$.

Доказательство вспомогательного утверждения. По индукции по $\beta$.

Основание индукции $\beta = 0$. Шаг индукции. Надо от $\beta$ перейти к $\beta + 1$.

$g_1^{p^\beta(p-1)} = 1 + c_\beta p^{\beta+1} + A_\beta p^{\beta+2}, A_\beta \in Z$. Возводим в степень $p$: $g_1^{p^{\beta+1}(p-1)} = (1 + c_\beta p^{\beta+1} + A_\beta p^{\beta+2})^p$.

Пишем бином Ньютона: $g_1^{p^{\beta+1}(p-1)} = (1 + c_\beta p^{\beta+1} + A_\beta p^{\beta+2})^p = 1 + p(c_\beta p^{\beta+1} + A_\beta p^{\beta+2}) + \frac{p(p-1)}{2}(c_\beta p^{\beta+1} + A_\beta p^{\beta+2})^2 + \cdots$. Если обозначить $X = c_\beta p^{\beta+1} + A_\beta p^{\beta+2}$, то по биному будет следующее $1 + px + \frac{p(p-1)}{2}X^2 + X^3 w, w \in Z$.

$p^{\beta+1}|X$. $p^{3(\beta+1)}|X^3, \beta \geq 0, 3(\beta+1) \geq \beta + 3$, тогда $p^{\beta+3}|X^3$.

Получаем $g_1^{p^{\beta+1}(p-1)} = (1 + c_\beta p^{\beta+1} + A_\beta p^{\beta+2})^p = 1 + p(c_\beta p^{\beta+1} + A_\beta p^{\beta+2}) + \frac{p(p-1)}{2}(c_\beta p^{\beta+1} + A_\beta p^{\beta+2})^2 (mod\ p^{\beta+3})$.

$p > 2$, $p|\frac{p(p-1)}{2}$. Смотрим за слагаемым с $X^2$. $p^{2(\beta+1)}|X^2$. В свою очередь $p^{2(\beta+1)+1}|\frac{p(p-1)}{2}X^2$. А $p^{\beta+3}|p^{2\beta+3}, \beta \geq 0$.



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
ФОНД ВОЛЬНОЕ ДЕЛО
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

$g_1^{p^{\beta+1}(p-1)} \equiv 1 + p\left(c_\beta p^{\beta+1} + A_\beta p^{\beta+2}\right)\left(mod\ p^{\beta+3}\right) \equiv 1 + c_\beta p^{\beta+2}(mod\ p^{\beta+3})$. $c_\beta = c_{\beta+1}$
Шаг индукции завершен. Вспомогательное утверждение доказано.

$\frac{\varphi(p^\alpha)}{p} = p^{\alpha-2}(p-1)$. В том утверждение надо взять $\beta = \alpha - 2$.

Получаем $g_1^{p^{\alpha-2}(p-1)} \equiv 1 + cp^{\alpha-1}(mod\ p^\alpha) \not\equiv 1(mod\ p^\alpha)$. При $q = p$ критерий проверен.

Таким образом, утв. 2. доказано.

Доказательство утв. 3.

Если $p$ –нечетное простое, то $\varphi(2p^\alpha) = \varphi(p^\alpha)$. $\varphi(2) = 1$

Представим, что $g_1$ –это первообразный корень по $mod\ p^\alpha$, тогда $g_1 + p^\alpha$ –тоже первообразный корень по $mod\ p^\alpha$, значит, $g_2$ –это первообразный корень по $mod\ p^\alpha$, причем нечетный. Тогда $(g_2, 2p^\alpha) = 1$ и можно говорить о его показателе $\nu = ord_{2p^\alpha} g_2$. $g_2^\nu \equiv 1(2p^\alpha)$, тогда $g_2^\nu \equiv 1(mod\ p^\alpha)$. Тогда $\nu \geq ord_{p^\alpha} g_2 = \varphi(p^\alpha) = \varphi(2p^\alpha)$. Но, с другой стороны, $\nu \leq \varphi(2p^\alpha)$. Тогда $ord_{2p^\alpha} g_2 = \varphi(2p^\alpha)$. Т.е. $g_2$ –это первообразный корень по $mod\ 2p^\alpha$.

Доказательство утв. 4.

Если есть два простых различных нечетных числа делителя $m$, то $m$ имеет вид: $m = p^\alpha q^\beta A, (A, pq) = 1, p, q \geq 3$ – различные. Тогда $\varphi(m) = \varphi(p^\alpha)\varphi(q^\beta)\varphi(A)$, но $\varphi(p^\alpha), \varphi\left(q^\beta\right)$ –четные. $\varphi(p^\alpha) = p^{\alpha-1}(p-1), (p-1)$ –четное.

Рассмотрим $k = \text{НОК}\left[\varphi(p^\alpha), \varphi\left(q^\beta\right), \varphi(A)\right] \leq \varphi(p^\alpha)\varphi\left(q^\beta\right)\varphi(A) = \frac{1}{2}\varphi(m)$. Теорема Эйлера: если $(a, m) = 1$, то $a^{\varphi(p^\alpha)} \equiv 1(p^\alpha)$, $a^{\varphi(q^\beta)} \equiv 1\left(q^\beta\right)$, $a^{\varphi(A)} \equiv 1(A)$. $a$ нужно возвести в такую степень, чтобы были 1 по всем модулям. Такой степенью будет степень НОК. $a^{\text{НОК}[\varphi(p^\alpha), \varphi(q^\beta), \varphi(A)]} \equiv 1(mod\ m)$. $\forall a: (a, m) = 1\ a^k \equiv 1(mod\ m), k \leq \frac{\varphi(m)}{2}$.

Вывод. $\nexists$ числа с показателем $\varphi(m)$ по $mod\ m$. Утв. 4 доказано.

Доказательство утв. 5.

$\varphi(2^\alpha) = 2^{\alpha-1}, \varphi\left(p^\beta\right) = p^{\beta-1}(p-1)$. Они оба четные. $k = \text{НОК}\left[\varphi(2^\alpha), \varphi\left(p^\beta\right)\right] \leq \frac{\varphi(2^\alpha)\varphi(p^\beta)}{2} = \frac{\varphi(2^\alpha p^\beta)}{2}$. Если $\left(a, 2^\alpha p^\beta\right) = 1$, то $a^{\varphi(2^\alpha)} \equiv 1(mod\ 2^\alpha)$, $a^{\varphi(p^\beta)} \equiv 1(mod\ p^\beta)$.

Тогда $a^k \equiv 1(mod\ 2^\alpha)$, $a^k \equiv 1(mod\ p^\beta)$. И получается $a^k \equiv 1(mod\ 2^\alpha p^\beta)$.

Но $k \leq \frac{\varphi\left(2^\alpha p^\beta\right)}{2}$. Тогда какое бы мы $a$ взаимно простое с $2^\alpha p^\beta$ не взяли, оно будет в степени $k$ единицей. А это меньше, чем функция Эйлера. Утв. 5 доказано.

Утв. 6.1. $ord_{2^\alpha}5 = 2^{\alpha-2}$

Утв. 6.2. Множество $B = \{(-1)^u 5^v, 0 \le u \le 1, 0 \le v \le 2^{\alpha-2} - 1\}$ –это приведенная система вычетов по $mod\ 2^\alpha$. Т.е. если $(a, 2^\alpha) = 1$, то $\exists\, u, v\ (0 \le u \le 1, 0 \le 2^{\alpha-2} - 1)$: $a \equiv (-1)^u 5^v (mod\ 2^\alpha)$.

*Замечание.* Из 6.1,6.2 следует 6.

Доказательство утв. 6.1.

$ord_{2^\alpha}5 = \nu | \varphi(2^\alpha) = 2^{\alpha-1}$. Значит, $\nu$ должно иметь вид $\nu = 2^\beta$.

Утв. $5^{2^\beta} = 1 + c_\beta 2^{\beta+2}, c_\beta$ –нечетное.

Доказательство утв. По индукции. Основание индукции $5 = 5^{2^0} = 1 + 4 = 1 + c_0 2^2$.

Шаг индукции. Возводим в степень 2. $5^{2^{\beta+1}} = \left(1 + c_\beta 2^{\beta+2}\right)^2 = 1 + c_\beta 2^{\beta+3} + c_\beta^2 2^{2(\beta+2)} = 1 + c_{\beta+1} 2^{\beta+3}, c_{\beta+1} = c_\beta + c_\beta^2 2$ –нечетное. Доказано.

Подставляем $\beta = \alpha - 2$. Получаем $5^{2^{\alpha-2}} = 1 + c_\beta 2^\alpha \equiv 1 (mod\ 2^\alpha)$. Подставляем $\beta = \alpha - 3$. $5^{2^{\alpha-3}} = 1 + c_\beta 2^{\alpha-1}, c_\beta \not\equiv 0 (mod\ 2)$. $5^{2^{\alpha-3}} \not\equiv 1 (mod\ 2^\alpha)$.

Вывод. $ord_{2^\alpha}5 = 2^{\alpha-2}$. Утв. 6.1 доказано.

Доказательство утв. 6.2.

В определении множества $B$ написано $2^{\alpha-1} = \varphi(2^\alpha)$ чисел. Все они нечетные, т.е. взаимно просты с $2^\alpha$. Достаточно доказать, что все эти числа различны по $mod\ 2^\alpha$.

Может ли выполняться следующее $5^{v_1} \equiv 5^{v_2} (mod\ 2^\alpha)$, где $v_1 \ne v_2, 0 \le v_j \le 2^{\alpha-2} - 1$?

Не может. Пусть $v_1 < v_2$, тогда $5^{v_2 - v_1} \equiv 1 (mod\ 2^\alpha)$. Но если $v_1 \ne v_2$, $0 < v_2 - v_1 < 2^{\alpha-2}$. Так как $0 < v_2 - v_1 < ord_{2^\alpha}5$. Тогда этого быть не может.

Аналогично, не может быть $-5^{v_1} \equiv -5^{v_2} (mod\ 2^\alpha)$.

Но также не может быть $5^{v_1} \equiv -5^{v_2} (mod\ 2^\alpha), \alpha \ge 3$. Так как $\alpha \ge 3$, из этого следовало бы равенство по $mod\ 4$. $5^{v_1} \equiv -5^{v_2} (4)$, получилось $1 \equiv -1 (mod\ 4)$, что неверно.

Утв. 6.2 доказано.

6.1, 6.2 верны для $\alpha = 2$. А при выводе из них утв. 6 мы использовали, что $\alpha \ge 3$.

**Литература по курсу “Элементы теории чисел”. Мощевитин Н. Г.**

**Рекомендации лектора:**

1. Нестеренко Ю. В. Теория чисел. – М.: Академия, 2008. http://mmmf.msu.ru/lect/nesterenko/mainnth.pdf

2. Бухштаб А. А. Теория чисел. – М.: Просвещение, 1966. https://ikfia.ysn.ru/wp-content/uploads/2018/01/Buhshtab1966ru.pdf

3. Виноградов И. М. Основы теории чисел. – М.: Наука ,1981. http://mathscinet.ru/files/VinogradovIM.pdf

**Дополнительная литература:**

4. Арнольд И. В. Теория чисел. – М.: ЛЕНАНД, 2017. http://i.uran.ru/webcab/system/files/bookspdf/teoriya-chisel/teoriya.pdf

5. Боревич З. И., Шафаревич И. Р. Теория чисел. – М.: Наука, 1985. https://urss.ru/cgi-bin/db.pl?lang=Ru&blang=ru&page=Book&id=243548

6. Гаусс К. Ф. Труды по теории чисел. – М.: Изд-во АН СССР, 1959. https://djvu.online/file/aW0RTccrPVZ4i

7. Сизый С. В. Лекции по теории чисел. – М.: Физматлит, 2008. http://www.allmath.ru/highermath/algebra/theorychisel-ugu/

8. Э. Ландау. Основы анализа. – М.: ИЛ, 1947. https://ikfia.ysn.ru/wp-content/uploads/2018/01/Landau1947ru.pdf

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ