ГЛАВА 2. КОМБИНАТОРИКА

А. В. Яковлев

Как правило, все множества, встречающиеся в этой главе, конечны (если не оговорено противное). Количество элементов конечного множества M называется его порядком и обычно обозначается через $|M|$.

1. Простейшие комбинаторные задачи

1. Подстановки множества. Подстановкой конечного множества M называется любое биективное отображение множества M на себя.

Теорема. *Пусть M — конечное множество порядка $n \geq 1$. Тогда число P_n различных подстановок множества M равно $n! = 1 \cdot \ldots \cdot n$.*

Доказательство. Для $n = 1$ имеется единственное биективное отображение M на себя — тождественное отображение; поэтому $P_1 = 1$. Пусть $n > 1$ и уже доказано, что $P_{n-1} = (n-1)!$, и пусть $|M| = n$. Выберем какой-то элемент $a \in M$, и для любого элемента $b \in M$ обозначим через S_b множество тех подстановок, которые переводят a в b. Ясно, что множества S_b попарно не пересекаются, и что их объединение совпадает с множеством S всех подстановок множества M; поэтому $|S| = \sum\limits_{b \in M} |S_b|$.

Для любого $b \in M$, $b \neq a$, обозначим через σ_b подстановку, переставляющую элементы a и b и оставляющую на месте все остальные элементы множества M; через σ_a обозначим тождественную подстановку множества M. Пусть S' — множество подстановок множества из $n-1$ элементов $M \setminus \{a\}$; по предположению индукции $|S'| = (n-1)!$. Отображения $\alpha : S' \to S_b$, $\beta : S_b \to S'$, определенные формулами $\alpha(\sigma) = \sigma_b \sigma$, $\beta(\tau) = \sigma_b \tau$, взаимно обратны и потому биективны. Следовательно, каждое из n множеств S_b равномощно S' и состоит из $(n-1)!$ элементов. Таким образом, $|S| = \sum\limits_{b \in M} |S_b| = n(n-1)! = n!$.

2. Произведение биномов, отличающихся вторыми членами. Следующая формула очень часто встречается в различных вопросах комбинаторики.

Теорема. *Пусть I — конечное множество; тогда*

$$\prod_{i \in I} (1 + x_i) = \sum_{S \subseteq I} (\prod_{s \in S} x_s)$$

(произведение, соответствующее пустому множеству S, считается равным 1).

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TeX

Доказательство. Из коммутативности и ассоциативности сложения и умножения и из свойства дистрибутивности вытекает следующее правило перемножения сумм: в каждом сомножителе выберем по одному слагаемому, перемножим эти выбранные слагаемые и затем сложим такие произведения, составленные для всех выборов слагаемых в сомножителях. Применим это правило к нашему случаю. В каждом сомножителе $1 + x_i$ слагаемое можно выбрать двумя способами; для фиксированного выбора слагаемых обозначим через S множество тех индексов $i \in I$, для которых в сомножителе $1 + x_i$ выбрано второе слагаемое x_i. Если $j \notin S$, то в слагаемом $1 + x_j$ выбрано первое слагаемое 1. Ясно, что и обратно, любое подмножество $S \subseteq I$ отвечает, и притом единственному, выбору слагаемых. Произведение всех выбранных слагаемых равно $\prod\limits_{s\in S} x_s$, и для того, чтобы получить произведение интересующих нас биномов, надо сложить эти произведения, полученные для всех возможных выборов слагаемых, т.е. для всех подмножеств $S \subseteq I$:

$$\prod_{i\in I}(1 + x_i) = \sum_{S\subseteq I}(\prod_{s\in S} x_s)\,.$$

3. Число подмножеств конечного множества. Для конечного множества M, состоящего из $n \geq 1$ элементов обозначим через C_n^i количество подмножеств M, состоящих из i элементов $(0 \leq i \leq n)$. Полагая в формуле из предыдущего пункта $x_m = t$ для всех $m \in M$, находим:

$$(1+t)^n = \sum_{S\subseteq M}(\prod_{s\in S} t) = \sum_{S\subseteq M} t^{|S|} = \sum_{i=0}^{n}\sum_{\substack{S\subseteq M\\ |S|=i}} t^i = \sum_{i=0}^{n} C_n^i t^i.$$

Эта формула называется формулой бинома Ньютона; пользуясь ей, найдем явное выражение для C_n^i.

Теорема. *Количество C_n^i подмножеств порядка i множества, состоящего из $n \geq 1$ элементов, равно $\dfrac{n!}{i!(n-i)!}$, где $0! = 1! = 1$, $m! = 1 \cdot 2 \cdot \ldots \cdot m$ для натурального $m \geq 2$.*

Доказательство. Индукция по n; для $n = 1$ утверждение тривиально. Пусть уже доказано, что $C_n^i = \dfrac{n!}{i!(n-i)!}$ для любого i, $0 \leq i \leq n$. По формуле бинома Ньютона

$$\sum_{i=0}^{n+1} C_{n+1}^i t^i = (1+t)^{n+1} = (1+t)(1+t)^n = (1+t)\sum_{j=0}^{n} C_n^j t^j;$$

коэффициент при t^i в правой части этого соотношения равен 1 при $i = 0$ или $i = n+1$, и он равен $C_n^{i-1} + C_n^i$ при $1 \leq i \leq n$. Таким образом,

$$C_{n+1}^0 = 1 = \frac{(n+1)!}{0!(n+1-0)!}\,,$$

$$C_{n+1}^{n+1} = 1 = \frac{(n+1)!}{(n+1)!((n+1)-(n+1))!},$$

$C_{n+1}^{i} = C_n^{i-1} + C_n^i$ при $1 \le i \le n$. В последнем случае находим, пользуясь предположением индукции:

$$C_{n+1}^{i} = C_n^{i-1} + C_n^i = \frac{n!}{(i-1)!(n-i+1)!} + \frac{n!}{i!(n-i)!} =$$
$$\frac{n!}{(i-1)!(n-i)!}\Big(\frac{1}{n-i+1} + \frac{1}{i}\Big) = \frac{(n+1)!}{i!(n-i+1)!}.$$

2. Метод производящих рядов

1. Кольцо формальных степенных рядов. Пусть k — некоторое поле. Обозначим через $k[[t]]$ множество всевозможных бесконечных последовательностей $(a_0, a_1, \ldots)$, все компоненты которых a_i принадлежат полю k. Над элементами из $k[[t]]$ определим действия сложения и умножения. Пусть

$$f(t) = (a_0, a_1, \ldots), \quad g(t) = (b_0, b_1, \ldots,)$$

— два элемента из $k[[t]]$. Положим $f(t) + g(t) = (a_0 + b_0, a_1 + b_1, \ldots)$, а в качестве $f(t)g(t)$ возьмем последовательность $(c_0, c_1, \ldots)$, компоненты которой определены равенствами $c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0$.

Элементы из $k[[t]]$, вместо $(a_0, a_1, \ldots)$, обычно записывают в виде $a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \ldots$ или $\sum\limits_{i=0}^{\infty} a_i t^i$. Отметим при этом, что используемый в этих обозначениях знак суммы не имеет содержательного смысла: ведь сложить бесконечное число слагаемых невозможно. Этот знак следует воспринимать лишь как графический знак, позволяющий в более удобной форме записать последовательность $(a_0, a_1, \ldots)$. Элементы из $k[[t]]$ называются формальными степенными рядами; независимо от формы записи, формальный степенной ряд является лишь набором своих коэффициентов a_i.

Всякий многочлен $f(t) = a_0 + a_1 t + \cdots + a_n t^n$ можно рассматривать как формальный степенной ряд $\sum\limits_{i=0}^{\infty} a_i t^i$, в котором $a_i = 0$ при $i > n$. Таким образом, имеется естественное вложение кольца многочленов $k[t]$ в множество формальных степенных рядов $k[[t]]$. В частности, любой элемент a из поля k является многочленом нулевой степени и тоже может рассматриваться как степенной ряд: $a = a + 0 \cdot t + \ldots 0 \cdot t^n + \ldots$. В дальнейшем мы будем отождествлять многочлены с соответствующими им степенными рядами и, таким образом, считать, что $k \subset k[t] \subset k[[t]]$. Из определений действий над формальными степенными рядами сразу видно, что указанное вложение не нарушает действий над многочленами: результат сложения или умножения многочленов не зависит от того, рассматриваем мы их как многочлены из $k[t]$ или как формальные степенные ряды из $k[[t]]$.

Для формального степенного ряда $f(t) = \sum\limits_{i=0}^{\infty} a_i t^i$ и натурального числа n обозначим через $f_n(t)$ многочлен $f_n(t) = a_0 + a_1 t + \cdots + a_n t^n$. Из определений действий над формальными степенными рядами немедленно следует, что для любых $f(t), g(t) \in k[[t]]$ и любого натурального числа $m \leq n$ коэффициенты при t^m в формальных степенных рядах $f(t)+g(t)$, $f(t)g(t)$ совпадают с коэффициентами при t^m в многочленах $f_n(t)+g_n(t)$, $f_n(t)g_n(t)$. Отсюда легко получить, что действия над формальными степенными рядами обладают обычными свойствами: для любых $f(t), g(t), h(t) \in k[[t]]$ выполняются соотношения

(1) $f(t)+g(t)=g(t)+f(t)$;
(2) $f(t)+(g(t)+h(t))=(f(t)+g(t))+h(t)$;
(3) $f(t)+0=f(t)$;
(4) $f(t)+(-1)f(t)=0$;
(5) $f(t)g(t)=g(t)f(t)$;
(6) $f(t)(g(t)h(t))=(f(t)g(t))h(t)$;
(7) $f(t)\cdot 1=f(t)$;
(8) $f(t)(g(t)+h(t))=f(t)g(t)+f(t)h(t)$.

Действительно, для доказательства, например, свойства (8) достаточно доказать, что для любого натурального числа n коэффициенты при t^n в левой и правой частях равенства (8) совпадают; но, как отмечено выше, они соответственно совпадают с коэффициентами при t^n в многочленах $f_n(t)(g_n(t)+h_n(t))$, $f_n(t)g_n(t)+f_n(t)h_n(t)$, но последние два многочлена совпадают, поскольку, как известно, свойство (8) для них выполняется.

Таким образом, множество $k[[t]]$ является коммутативным ассоциативным кольцом с единицей. Более того, кольцо $k[[t]]$ является областью целостности, т.е. не имеет нетривиальных делителей 0. Действительно, пусть $f(t)=\sum\limits_{i=0}^{\infty} a_i t^i$, $g(t)=\sum\limits_{i=0}^{\infty} b_i t^i$ — ненулевые ряды из $k[[t]]$; тогда существуют такие номера m, n, что $a_i=0$ при $0 \leq i < m$, $b_j=0$ при $0 \leq j < n$, $a_m \neq 0$, $b_n \neq 0$. Отсюда следует, что коэффициент при t^{m+n} в ряде $f(t)g(t)$ равен $a_m b_n \neq 0$, а потому $f(t)g(t) \neq 0$.

В дальнейшем мы всегда будем называть $k[[t]]$ кольцом формальных степенных рядов от t над полем k.

2. Обратимые формальные степенные ряды. Над формальными степенными рядами можно производить многие операции, невозможные для многочленов. Здесь мы ограничимся лишь двумя примерами. Деление на многочлен и извлечение корней из многочленов возможно в кольце многочленов лишь в редких случаях; напротив, как мы покажем в этом и следующем пунктах, в кольце формальных степенных рядов эти операции почти всегда осуществимы.

Предложение. *Для того, чтобы для ряда $f(t)=\sum\limits_{i=0}^{\infty} a_i t^i$ существовал обратный ряд $g(t) \in k[[t]]$ необходимо и достаточно, чтобы свободный член a_0 ряда $f(t)$ был отличен от 0.*

Доказательство. Пусть $g(t)=\sum\limits_{i=0}^{\infty} b_i t^i$; для того чтобы выполнялось равенство $f(t)g(t)=1$, необходимо и достаточно, чтобы коэффициенты b_i формального ряда $g(t)$ удовлетворяли следующей системе уравнений:

$$\begin{aligned}
&1 = a_0 b_0,\\
&0 = a_0 b_1 + a_1 b_0,\\
&0 = a_0 b_2 + a_1 b_1 + a_2 b_0,\\
&\ \ \ldots\ldots\ldots\ldots\ldots\ldots\\
&0 = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0,\\
&\ \ \ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Но при $a_0 = 0$ эта система неразрешима, ибо ее первое уравнение превращается в неверное равенство $1 = 0 \cdot b_0 = 0$ при любом $b_0 \in k$. Напротив, при $a_0 \neq 0$ система разрешима: значения неизвестных b_i последовательно вычисляются по формулам

$$\begin{aligned}
&b_0 = 1/a_0,\\
&b_1 = -a_1 b_0/a_0,\\
&b_2 = -(a_1 b_1 + a_2 b_0)/a_0,\\
&\ \ \ldots\ldots\ldots\ldots\ldots\ldots\\
&b_n = -(a_1 b_{n-1} + \cdots + a_n b_0)/a_0,\\
&\ \ \ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Отметим один важный частный случай, когда деление можно выполнить явно:

$$\frac{1}{1-ct} = 1 + ct + c^2t^2 + \cdots + c^n t^n + \ldots.$$

Эта формула напоминает формулу для суммы бесконечной убывающей геометрической прогрессии; однако, в ее правой части стоит формальный степенной ряд, а не предел сумм начальных отрезков прогрессии. Для доказательства указанной формулы достаточно заметить, что при $n > 0$ в произведении $1 - ct$ на правую часть только произведения $-ct \cdot c^{n-1}t^{n-1}$ и $1 \cdot c^n t^n$ имеют относительно t степень n, и потому коэффициент при t^n в этом произведении равен $-c^n + c^n = 0$.

3. Бином Ньютона для формальных степенных рядов. В этом пункте мы воспользуемся соображениями, относящимися к математическому анализу, точнее, к теории рядов. Пусть $f(t) = \sum\limits_{i=0}^{\infty} a_i t^i \in \mathbb{R}[[t]]$ — формальный степенной ряд над полем вещественных чисел $\mathbb{R}$. Мы можем рассматривать его как функциональный ряд над полем вещественных чисел, и потому может оказаться, что он сходится в некоторой окрестности 0 к какой-то функции $\varphi(t)$. Как известно, в этом случае функция $\varphi(t)$ бесконечно дифференцируема в некоторой (возможно, меньшей) окрестности 0, и при этом $a_0 = \varphi(0)$, $a_i = \varphi^{(i)}(0)/i!$ при $i > 0$. Отсюда немедленно вытекает следующее утверждение.

Лемма 1. *Формальные степенные ряды над $\mathbb{R}$, которые в некоторой окрестности 0 сходятся к одной и той же функции, совпадают.*

Лемма 2. *Если формальные степенные ряды $f(t), g(t) \in \mathbb{R}$ сходятся в некоторых окрестностях 0 к функциям $\varphi(t)$, $\psi(t)$, то формальные степенные ряды $f(t)+g(t)$, $f(t)g(t)$ сходятся в некоторых окрестностях 0 к функциям $\varphi(t)+\psi(t)$, $\varphi(t)\psi(t)$.*

Доказательство. Пусть $f(t) = \sum\limits_{i=0}^{\infty} a_i t^i$, $g(t) = \sum\limits_{i=0}^{\infty} b_i t^i$; тогда

$$f(t)g(t) = \sum_{i=0}^{\infty}(\sum_{s=0}^{i} a_s b_{i-s})t^i.$$

В некоторых окрестностях нуля (возможно, меньших, чем исходные) ряды $f(t)$, $g(t)$ не просто сходятся, но сходятся абсолютно. Поэтому в пересечении этих окрестностей двойной ряд $\sum\limits_{r,s} a_r t^r \cdot b_s t^s$ сходится к функции $\varphi(t)\psi(t)$, причем его сумма не зависит от того, в каком порядке мы располагаем слагаемые и как мы их группируем. В частности, ряд

$$\sum_{i=0}^{\infty}(\sum_{r+s=i} a_s b_r)t^{r+s} = \sum_{i=0}^{\infty}(\sum_{s=0}^{i} a_s b_{i-s})t^i = f(t)g(t)$$

сходится к $\varphi(t)\psi(t)$.

Утверждение леммы, касающееся суммы рядов, тривиально.

Следствие. *Если формальные степенные ряды $f_1(t), \ldots, f_n(t) \in \mathbb{R}$ сходятся к функциям $\varphi_1(t), \ldots, \varphi_n(t)$ в некоторых окрестностях 0, и если $h(x_1, \ldots, x_n)$ — многочлен с вещественными коэффициентами, то формальный степенной ряд $h(f_1(t), \ldots, f_n(t))$ сходится к функции $h(\varphi_1(t), \ldots, \varphi_n(t))$ в некоторой окрестностях 0.*

Эти свойства позволяют широко использовать содержательные факты из анализа для получения формальных тождеств в $\mathbb{R}[[t]]$. Например, из того, что ряды Маклорена для функций $\sin t$, $\cos t$ сходятся к этим функциям, и из тождества $\cos^2 t + \sin^2 t = 1$ следует, что в кольце формальных степенных рядов справедливо равенство

$$(\sum_{i=0}^{\infty}(-1)^i \frac{t^{2i}}{(2i)!})^2 + (\sum_{i=0}^{\infty}(-1)^i \frac{t^{2i+1}}{(2i+1)!})^2 = 1.$$

Воспользуемся подобными соображениями для возведения формальных степенных рядов в дробные степени. Пусть a, $b > 0$ — целые числа, и пусть $f(t) \in \mathbb{R}[[t]]$ — формальный степенной ряд со свободным членом 1. Как обычно, через $(f(t))^{a/b}$ мы обозначаем такой формальный степенной ряд $g(t)$ со свободным членом 1, что $(f(t))^a = (g(t))^b$ при $a \geq 0$, и $(f(t))^{|a|}(g(t))^b = 1$ при $a < 0$. Такой степенной ряд (если он существует) единственен. Действительно, расширяя основное поле до поля комплексных чисел $\mathbb{C}$, заметим, что наряду с $g(t)$ тому же уравнению $(f(t))^a = (g(t))^b$ (соответственно, $(f(t))^{|a|}(g(t))^b = 1$) удовлетворяют еще и ряды $(\cos\frac{2\pi s}{b} + i\sin\frac{2\pi s}{b})g(t) \in \mathbb{C}[[t]]$, $s = 1, \ldots, b-1$, и, кроме этих b, других решений в области целостности $\mathbb{C}[[t]]$ это уравнение степени b не имеет. Остается заметить, что лишь у решения $g(t)$ свободный член равен 1.

Предложение. *Для любого рационального числа α и любого вещественного числа c существует формальный степенной ряд $(1+ct)^\alpha \in \mathbb{R}[[t]]$, и этот ряд имеет вид*

$$(1+ct)^\alpha = \sum_{i=0}^{\infty} \binom{\alpha}{i} c^i t^i, \quad \text{где } \binom{\alpha}{i} = \frac{\alpha(\alpha-1)\ldots(\alpha-i+1)}{i!}.$$

Доказательство. Из курса математического анализа известно, что указанный в формулировке предложения ряд $g(t)$ представляет ряд Маклорена для функции $(1+ct)^\alpha$, и что он сходится к функции $(1+ct)^\alpha$ в некоторой окрестности 0. Следовательно, если $\alpha = a/b$, где a, $b > 0$ — целые числа, то при $a \geq 0$ ряды $(g(t))^b$, $(1+ct)^a$ сходятся к одной и той же функции, а при $a < 0$ ряды $(f(t))^{|a|}(g(t))^b$, 1 сходятся к одной и той же функции. По лемме 1 отсюда следует, что формальные ряды $(g(t))^b$, $(1+ct)^a$ (соответственно, формальные ряды $(f(t))^{|a|}(g(t))^b$, 1) равны, т.е. что $g(t) = (1+ct)^\alpha$ в кольце формальных степенных рядов.

Замечание. Можно показать, что любой формальный степенной ряд со свободным членом 1 можно возвести в любую рациональную степень.

4. Производящие ряды. Числа Фибоначчи. Пусть $a_0, a_1, a_2, \ldots$ — некоторая последовательность, определенная при помощи какой-то процедуры; требуется найти явную формулу для n-го члена этой последовательности. Часто оказывается проще вычислить не каждый член последовательности по отдельности, а все вместе, сделав их коэффициентами формального степенного ряда $f(t) = \sum\limits_{i=0}^{\infty}$. Этот ряд называется производящим рядом для последовательности $a_0, a_1, a_2, \ldots$. Иногда его называют даже производящей функцией для последовательности, хотя ряд совсем не обязан сходиться и определять какую-то функцию. Проиллюстрируем применение производящих рядов на нескольких примерах.

В качестве первого примера рассмотрим последовательность чисел Фибоначчи, определяемую индуктивно по формулам:

$$a_0 = a_1 = 1, \quad a_n = a_{n-2} + a_{n-1} \text{ при } n \geq 2.$$

Таким образом, начало последовательности чисел Фибоначчи выглядит следующим образом:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Пусть $f(t) = \sum\limits_{i=0}^{\infty} a_i t^i$ — производящий ряд для последовательности Фибоначчи; тогда

$$\begin{aligned} t^2 f(t) &= \qquad a_0t^2 + a_1t^3 + \ldots + a_{n-2}t^n + \ldots \\ tf(t) &= a_0t + a_1t^2 + a_2t^3 + \ldots + a_{n-1}t^n + \ldots \end{aligned}$$

Складывая эти ряды и пользуясь тем, что $a_0 + a_1 = a_2$, $a_1 + a_2 = a_3$, ..., $a_{n-2} + a_{n-1} = a_n$, получаем:

$$t^2 f(t) + tf(t) = a_0t + a_2t^2 + a_3t^3 + \cdots + a_nt^n + \cdots = f(t) - a_0 - a_1t + a_0t = f(t) - 1;$$

отсюда следует, что

$$f(t) = \frac{1}{1 - t - t^2}.$$

Итак, мы вычислили производящий ряд последовательности Фибоначчи. Преобразуем это выражение, разложив получившуюся дробно-рациональную функцию в сумму простейших дробей. Пусть $\omega_1 = (1+\sqrt{5})/2$, $\omega_2 = (1-\sqrt{5})/2$ — корни трехчлена $z^2 - z - 1$; тогда $1 - t - t^2 = (1 - \omega_1 t)(1 - \omega_2 t)$ и

$$\sqrt{5}tf(t) = \frac{(\omega_1 t - \omega_2 t)}{1 - t - t^2} = \frac{(1-\omega_2 t) - (1 - \omega_1 t)}{(1-\omega_1 t)(1-\omega_2 t)} = \frac{1}{1 - \omega_1 t} - \frac{1}{(1 - \omega_2 t)} = \sum_{i=0}^{\infty} \omega_1^i t^i - \sum_{i=0}^{\infty} \omega_2^i t^i.$$

Сравнивая коэффициенты при t^{n+1} у формальных рядов, стоящих в левой и правой частях последнего равенства, находим, что $\sqrt{5}a_n = \omega_1^{n+1} - \omega_2^{n+1}$, т.е.

$$a_n = \frac{1}{\sqrt{5}}(\omega_1^{n+1} - \omega_2^{n+1}) = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1}).$$

5. Число решений уравнения $x_1 + \cdots + x_n = N$**.** Обозначим через a_N количество таких упорядоченных наборов неотрицательных целых чисел $x_1, \ldots, x_n$, что сумма всех чисел из набора равна N. Пусть $f(t) = \sum\limits_{i=0}^{\infty} a_i t^i$ — производящий ряд для последовательности $a_0, a_1, a_2, \ldots$. Покажем, что $f(t) = 1/(1-t)^n$. Действительно,

$$\frac{1}{(1-t)^n} = (\sum_{i=0}^{\infty} t^i)^n = (\sum_{x_1=0}^{\infty} t^{x_1}) \cdot \ldots \cdot (\sum_{x_n=0}^{\infty} t^{x_n}) = \sum_{x_1,\ldots,x_n} t^{x_1+\cdots+x_n} = \sum_{i=0}^{\infty} (\sum_{x_1+\cdots+x_n=i} t^i).$$

Таким образом, каждый упорядоченный набор неотрицательных целых чисел $x_1, \ldots, x_n$, сумма которого равна i, вносит в правую часть предыдущего равенства слагаемое t^i; поэтому общее число слагаемых вида t^i, т.е. коэффициент при t^i в правой части равенства, равно количеству a_i упорядоченных наборов неотрицательных целых чисел $x_1, \ldots, x_n$ с суммой i. Итак, формальный степенной ряд, стоящий в правой части равенства, совпадает с $f(t)$. Пользуясь доказанной выше формулой для степеней бинома, находим теперь:

$$\sum_{i=0}^{\infty} a_i t^i = f(t) = (1-t)^{-n} = \sum_{i=0}^{\infty} (-1)^i \binom{-n}{i} t^i.$$

Сравнивая коэффициенты при t^N, находим:

$$a_N = (-1)^N \binom{-n}{N} = (-1)^N \frac{(-n)(-n-1)\ldots(-n-N+1)}{N!} =$$
$$\frac{(N+n-1)(N+n-2)\ldots(n+1)n}{N!} = \binom{N+n-1}{N}.$$

6. Количество неассоциативных произведений. Пусть a, b, c — элементы некоторого множества, на котором определена бинарная операция умножения. Их произведение abc, вообще говоря, не определено: ведь наша операция бинарная, и мы каждый раз можем перемножить лишь два сомножителя. Поэтому под abc можно понимать два элемента нашего множества: произведение $(ab)c$ элемента ab на c и произведение $a(bc)$ элемента a на bc. Если умножение ассоциативно, как это бывает почти во всех привычных алгебраических системах, то оба этих элемента совпадают; однако при отсутствии ассоциативности они различны. Таким образом, существует два различных произведения трех элементов a, b, c (именно в таком порядке) — это произведения $a(bc)$ и $(ab)c$. Аналогично этому, четыре элемента можно перемножить пятью различными способами:

$$a(b(cd)),\ \ a((bc)d),\ \ (ab)(cd),\ \ (a(bc))d,\ \ ((ab)c)d.$$

В этом пункте мы ставим себе задачу сосчитать количество s_n неассоциативных произведений n элементов $a_1, \ldots, a_n$, $n \geq 1$. Из одного элемента a_1 можно составить лишь одно произведение a_1, а из двух элементов a_1, a_2 — тоже лишь одно произведение $a_1 a_2$. Таким образом, $s_1 = s_2 = 1$. Выше мы видели, что $s_3 = 2$, $s_4 = 5$. Дополним последовательность $s_1, s_2, \ldots$ начальным членом $s_0 = 0$ и рассмотрим производящий ряд $\sum\limits_{i=0}^{\infty} s_i t^i$.

Покажем, что при $n \geq 2$ выполняется соотношение

$$(*) \qquad s_n = s_1 s_{n-1} + s_2 s_{n-2} + \cdots + s_{n-1} s_1.$$

Действительно, при вычислении произведения n элементов на последнем шагу мы перемножаем два элемента xy, где для некоторого i, $1 \leq i \leq n-1$ элемент x является одним из s_i неассоциативных произведений элементов $a_1, \ldots, a_i$, а элемент y — одним из s_{n-i} неассоциативных произведений элементов $a_{i+1}, \ldots, a_n$. Таким образом, при фиксированном i имеется $s_i s_{n-i}$ различных неассоциативных произведений элементов $a_1, \ldots, a_n$, а общее количество всех таких произведений s_n равно $\sum\limits_{i=1}^{n-1} s_i s_{n-i}$, что мы и хотели доказать.

Добавляя в правую часть соотношения (*) два нулевых слагаемых, запишем его в виде

$$s_n = s_0 s_n + s_1 s_{n-1} + s_2 s_{n-2} + \cdots + s_{n-1} s_1 + s_n s_0.$$

Но правая часть последнего равенства — это в точности коэффициент при t^n в произведении формальных рядов $f(t) \cdot f(t)$. Таким образом, при $n \geq 2$ коэффициенты при t^n в рядах $f(t)$, $(f(t))^2$ совпадают. Но, очевидно, свободный член и коэффициент при t у ряда $(f(t))^2$ равны 0. Таким образом,

$$f(t) = s_1 t + (f(t))^2 = t + (f(t))^2.$$

Итак, формальный степенной ряд $f(t)$ является решением уравнения $z^2 - z + t = 0$. Но это уравнение имеет в области целостности $\mathbb{R}[[t]]$ в точности два решения

$$\frac{1 \pm \sqrt{1-4t}}{2} = \frac{1 \pm (1-4t)^{1/2}}{2} = \frac{1}{2}(1 \pm \sum_{i=0}^{\infty} (-4)^i \binom{1/2}{i} t^i).$$

Поскольку свободный член ряда $f(t)$ равен 0, этот ряд может совпадать только с решением, в котором из двух знаков $\pm$ выбран знак "минус". Итак, $f(t) = \frac{1}{2} \sum\limits_{i=0}^{\infty} (-1)^{i+1} 4^i \binom{1/2}{i} t^i$. Сравнивая коэффициенты при t^n в левой и правой частях этого равенства, находим:

$$s_n = \frac{1}{2}(-1)^{n+1} 4^n \binom{1/2}{n} = \frac{(-1)^{n+1} 4^n (1/2)(1/2-1)\ldots(1/2-n+1)}{2n!} = \frac{2^{n-1} \cdot 1 \cdot 3 \cdot \ldots \cdot (2n-3)}{n!}$$

(последнее преобразование выполнено в предположении $n \geq 2$). В частности,

$$s_2 = \frac{2 \cdot 1}{2!} = 1, \quad s_3 = \frac{2^2 \cdot 1 \cdot 3}{3!} = 2, \quad s_4 = \frac{2^3 \cdot 1 \cdot 3 \cdot 5}{4!} = 5,$$

что совпадает с непосредственно сосчитанными ранее значениями.

3. Теорема включения и исключения

1. Простейшие случаи. Напомним, что для конечного множества X мы обозначаем через $|X|$ порядок множества X, т.е. число его элементов.

Пусть A, B — конечные подмножества некоторого множества X; мы хотим сосчитать число элементов объединения $A \cup B$. Если мы сложим порядки множеств A и B, то элементы из пересечения $A \cap B$ будут сосчитаны дважды. Поэтому

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Аналогичная формула может быть получена и для трех конечных подмножеств A, B, C множества X. В сумме порядков этих множеств элементы из попарных пересечений сосчитаны дважды; но если мы рассмотрим разность

$$|A| + |B| + |C| - (|A \cap B| + |B \cap C| + |A \cap C|),$$

то увидим, что элементы из пересечения всех трех множеств остались не сосчитанными: мы их трижды учли в сумме $|A| + |B| + |C|$, но затем трижды выбросили из суммы. Таким образом,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|\,.$$

Наша цель — обобщить эти формулы на случай произвольного числа подмножеств. При этом нам удастся сформулировать основной результат так, что конечность подмножеств не будет предполагаться.

2. Характеристическая функция подмножества и её свойства. До конца параграфа зафиксируем множество X; все встречающиеся множества будут подмножествами X. Пусть $A \subseteq X$; характеристической функцией подмножества A называется функция $\chi_A : X \to \{0, 1\}$, определенная формулой

$$\chi_A(x) = \begin{cases} 1, & \text{если } x \in A, \\ 0, & \text{если } x \in X,\ x \notin A\,. \end{cases}$$

Отметим некоторые простые свойства характеристической функции.

1. *Характеристическая функция пересечения любых подмножеств множества X равна произведению характеристических функций этих множеств.*

Доказательство. Действительно, пусть $B = \bigcap\limits_{i \in I} A_i$; значение $\chi_B(x)$ характеристической функции пересечения равно 1 тогда и только тогда, когда элемент $x \in X$ принадлежит всем подмножествам A_i, т.е. когда $\chi_{A_i}(x) = 1$ для всех $i \in I$. Но последнее условие равносильно тому, что произведение всех чисел $\chi_{A_i}(x)$ равно 1 (заметим, что произведение сомножителей, каждый из которых равен 0 или 1, определено даже и тогда, когда этих сомножителей бесконечно много: оно равно 0, если хотя бы один из сомножителей равен 0, и равно 1, если все сомножители равны 1).

2. *Пусть $A \subseteq X$ и пусть $\bar{A}$ — дополнение в X подмножества A. Тогда $\chi_{\bar{A}}(x) = 1 - \chi_A(x)$ для всех $x \in X$.*

Доказательство. В самом деле, любой элемент $x \in X$ принадлежит одному и только одному из множеств A, $\bar{A}$, поэтому ровно одно из чисел $\chi_A(x)$, $\chi_{\bar{A}}(x)$ равно 0, а другое равно 1. Таким образом, для любого $x \in X$ выполняется равенство $\chi_A(x) + \chi_{\bar{A}}(x) = 1$.

3. *Пусть $\{A_i \,|\, i \in I\}$ — семейство подмножеств множества X, и пусть C — объединение всех множеств A_i. Тогда для любого $x \in X$ выполняется равенство*

$$1 - \chi_C(x) = \prod_{i \in I} (1 - \chi_{A_i}(x))\,.$$

Доказательство. Заметим, что дополнение $\bar{C}$ объединения C совпадает с пересечением дополнений $\bar{A}_i$ множеств A_i: элемент $x \in X$ не принадлежит объединению тогда и только тогда, когда он не принадлежит ни одному из множеств A_i. Поэтому наше утверждение непосредственно следует из свойств 1 и 2:

$$1 - \chi_C(x) = \chi_{\bar{C}}(x) = \prod_{i \in I} \chi_{\bar{A}_i}(x) = \prod_{i \in I} (1 - \chi_{A_i}(x))\,.$$

Как и выше, произведение в правой части имеет смысл даже при бесконечном числе сомножителей, так как каждый из этих сомножителей равен 0 или 1.

4. *Пусть A — конечное подмножество множества X. Тогда*

$$|A| = \sum_{x \in X} \chi_A(x)\,.$$

Доказательство. Это очевидно: $\chi_A(x)$ отличается от 0 только если $x \in A$; поэтому сумму (возможно, бесконечную) $\sum_{x \in X} \chi_A(x)$ можно заменить на сумму $|A|$ слагаемых $\sum_{x \in A} \chi_A(x)$, каждое из которых равно 1.

3. Теорема включения и исключения. Выведем теперь формулу для вычисления характеристической функции объединения конечного числа подмножеств.

Теорема включения и исключения для характеристических функций. *Пусть I — конечное множество, и пусть A_i, $i \in I$ — подмножества множества X. Пусть, далее, $C = \bigcup\limits_{i \in I} A_i$. Для подмножества $S \subseteq I$ обозначим через A_S пересечение $\bigcap\limits_{s \in S} A_s$. Тогда для любого элемента $x \in X$ справедливо равенство*

$$\chi_C(x) = \sum_{S \subseteq I, S \neq \varnothing} (-1)^{|S|+1} \chi_{A_S}(x) = \sum_{i=1}^{|I|} (-1)^{i+1} \sum_{S \subseteq I, |S| = i} \chi_{A_S}(x)\,.$$

Доказательство. Согласно свойству 3 характеристических функций подмножеств, мы имеем для любого $x \in X$:

$$1 - \chi_C(x) = \prod_{i \in I} (1 - \chi_{A_i}(x))\,.$$

Применяя к правой части этого равенства теорему о произведении биномов, отличающихся вторыми членами, получим:

$$1 - \chi_C(x) = \sum_{S \subseteq I} ((-1)^{|S|} \prod_{s \in S} \chi_{A_s}(x))\,.$$

Среди слагаемых правой части одно (то, которое отвечает пустому множеству) равно 1; сокращая его с 1 из левой части и замечая, что, по свойству 1 характеристической функции, $\prod\limits_{s \in S} \chi_{A_s}(x) = \chi_{A_S}(x)$, получаем требуемый результат.

Предположим теперь, что все подмножества A_i конечны; просуммируем значения всех частей полученного равенства по всем элементам $x \in X$. Согласно свойству 4 характеристической функции, мы получим следующий результат.

Теорема включения и исключения для порядков множеств. *Пусть I — конечное множество, и пусть A_i, $i \in I$ — конечные подмножества множества X. Тогда*

$$\left|\bigcup_{i\in I} A_i\right| = \sum_{S\subseteq I, S\neq\varnothing} (-1)^{|S|+1}\left|\bigcap_{s\in S} A_s\right| = \sum_{i=1}^{|I|}(-1)^{i+1}\sum_{S\subseteq I, |S|=i}\left|\bigcap_{s\in S} A_s\right|.$$

Для случаев, когда множество I состоит из двух или трех элементов, эта теорема превращается в уже доказанные соотношения

$$|A\cup B| = |A| + |B| - |A\cap B|\,,$$

$$|A\cup B\cup C| = |A| + |B| + |C| - |A\cap B| - |B\cap C| - |A\cap C| + |A\cap B\cap C|\,.$$

Можно бывает "сосчитать порядок" объединения подмножеств и тогда, когда подмножества бесконечны, но в некотором смысле измеримы; тогда надо считать не сумму всех значений характеристической функции, а интегрировать её. Эта форма теоремы включения и исключения широко используется в математике.

4. Применения теоремы включения и исключения..

1. Задача о шляпах. Пусть M — конечное множество, состоящее из n элементов. Мы видели, что число всех подстановок множества M равно $n!$; сосчитаем количество N тех из подстановок, которые оставляют неподвижным хотя бы один элемент.

Для каждого элемента m множества M обозначим через A_m множество всех подстановок, не двигающих элемент m. Пусть $S \subseteq M$; тогда пересечение $A_S = \bigcap_{s\in S} A_s$ состоит из всех подстановок, не двигающих элементы из S. Но любая подстановка $\sigma \in A_s$ отображает биективно дополнение $M \setminus S$ множества S на себя, т.е. ее ограничение σ' на $M\setminus S$ является подстановкой множества $M\setminus S$. Обратно, любая подстановка σ' множества $M\setminus S$ однозначно распространяется до подстановки σ всего множества M, не двигающей элементы из S, т.е. до элемента из A_S. Итак, число элементов множества A_S совпадает с числом подстановок множества $M\setminus S$, т.е. $|A_S| = (|M\setminus S|)! = (n-|S|)!$.

Объединение всех множеств A_m, $m\in M$, состоит в точности из тех подстановок, которые оставляют неподвижным хотя бы один элемент множества M; поэтому интересующее нас число N равно порядку этого объединения. Применяя теорему включения и исключения и пользуясь тем, что у множества M, состоящего из n элементов, имеется в точности C_n^i подмножеств S порядка i, находим:

$$N = \left|\bigcup_{m\in M} A_m\right| = \sum_{i=1}^{n}(-1)^{i+1}\sum_{\substack{S\subseteq M,\\ |S|=i}}|A_S| = \sum_{i=1}^{n}(-1)^{i+1}\sum_{\substack{S\subseteq M,\\ |S|=i}}(n-i)! =$$

$$\sum_{i=1}^{n}(-1)^{i+1}C_n^i(n-i)! = \sum_{i=1}^{n}(-1)^{i+1}\frac{n!}{i!(n-i!)}(n-i)! = n!\sum_{i=1}^{n}\frac{(-1)^{i+1}}{i!}.$$

Таким образом, отношение $N/n!$ числа подстановок, не двигающих хотя бы один элемент из множества M, к числу всех подстановок равно

$$\frac{1}{1!} - \frac{1}{2!} + \frac{1}{3!} - \cdots + (-1)^{n+1}\frac{1}{n!}.$$

При большом n это число мало отличается от $1 - 1/e = 1 - 1/2,71828... \approx 0,63212$.

Эта задача часто встречается в сборниках олимпиадных задач в разных вариантах; вот один из них. 100 джентльменов оставили при входе в клуб свои цилиндры. Однако, швейцар был навеселе, и при расставании раздал им их шляпы случайным образом. Какова вероятность того, что хотя бы один джентльмен вернулся домой в своем цилиндре? Как мы видели, эта вероятность весьма велика — почти две трети.

2. Теоретико-числовая функция Эйлера. Пусть $n \geq 1$ — натуральное число; обозначим через $\varphi(n)$ количество натуральных чисел m, взаимно простых с n и таких, что $1 \leq m \leq n$. Функция $\varphi(n)$ играет очень важную роль в теории чисел; она называется функцией Эйлера.

Выведем явную формулу для функции Эйлера. Пусть $P = \{p_1, \ldots, p_r\}$ — множество всех простых делителей числа n (если $n = 1$, то множество P пустое). Обозначим через A множество $\{1, \ldots, n\}$, через I — множество $\{1, \ldots, r\}$, и для $i \in I$ обозначим через A_i множество тех чисел из A, которые делятся на p_i. Число m взаимно просто с n тогда и только тогда, когда оно не делится ни на одно из чисел p_i, $i \in I$, т.е. когда оно не содержится ни в одном из множеств A_i, а значит, и в их объединении. Таким образом, $\varphi(n)$ равно числу элементов множества A, не принадлежащих $\bigcup\limits_{i\in I} A_i$, т.е. разности порядков множеств A, $\bigcup\limits_{i\in I} A_i$. Применяя теорему включения и исключения, находим:

$$\varphi(n) = n - \Big|\bigcup_{i\in I} A_i\Big| = n - \sum_{\substack{S\subseteq I\\ S\neq\emptyset}} (-1)^{|S|+1}\big|A_S\big|,$$

где $A_S = \bigcap\limits_{s\in S} A_s$ состоит из всех таких чисел, принадлежащих A, которые делятся на каждое из простых чисел p_s с номерами $s \in S$, а значит, и на их произведение $n_S = \prod\limits_{s\in S} p_s$. Таким образом, $A_S = \{n_S, 2n_S, \ldots, \dfrac{n}{n_S} n_S\}$, и потому число элементов множества A_S равно $n/n_S = n\prod\limits_{s\in S}\dfrac{1}{p_s}$. Итак,

$$\varphi(n) = n - \sum_{\substack{S\subseteq I\\ S\neq\emptyset}} (-1)^{|S|+1} n \prod_{s\in S}\frac{1}{p_s} = n\sum_{S\subseteq I}(-1)^{|S|}\prod_{s\in S}\frac{1}{p_s} = n\prod_{i\in I}(1 - \frac{1}{p_i})$$

(в последнем преобразовании использована формула для произведения биномов, отличающихся вторыми членами).

Теорема. *Пусть множество A представлено в виде объединения конечного числа подмножеств B_1,...,B_n. Для того чтобы существовали попарно различные элементы $a_1, \ldots, a_n \in A$, такие что $a_i \in B_i$ для любого i, $1 \leq i \leq n$, необходимо и достаточно, чтобы для любого подмножества Γ множества $\{1, \ldots, n\}$ в объединении $\bigcup\limits_{i \in \Gamma} B_i$ тех из подмножеств B_i, номера которых принадлежат Γ, содержалось не меньше элементов, чем в множестве Γ.*

Доказательство. Необходимость условия очевидна. Действительно, пусть $a_1, \ldots, a_n \in A$ — элементы, удовлетворяющие требованиям теоремы; тогда для любого подмножества $\Gamma = \{i_1 < \cdots < i_s\}$ множества $\{1, \ldots, n\}$ объединение $B_{i_1} \cup \cdots \cup B_{i_s}$ содержит по крайней мере s различных элементов $a_{i_1}, \ldots, a_{i_s}$.

Докажем теперь достаточность условия теоремы. Пусть $A = B_1 \cup \cdots \cup B_n$ и пусть для любого подмножества Γ множества $\{1, \ldots, n\}$ в объединении $\bigcup\limits_{i \in \Gamma} B_i$ тех из подмножеств B_i, номера которых принадлежат Γ, содержится не меньше элементов, чем в множестве Γ. Применяя это условие к одноэлементным множествам $\Gamma = \{i\}$ мы видим, что каждое из множеств B_i содержит хотя бы один элемент, и потому непусто. Дальнейшие рассуждения ведем индукцией по n; если $n = 1$, то $A = B_1 \neq \varnothing$, и поэтому существует элемент $a_1 \in A = B_1$.

Пусть для всех $m < n$ уже доказано, что если $A = B_1 \cup B_2 \cup \cdots \cup B_m$, и для любых $1 \leq i_1 < i_2 < \cdots < i_k \leq m$ объединение множеств B_{i_1}, B_{i_2},..., B_{i_k} содержит не меньше k элементов, то существуют различные элементы $b_1 \in B_1$,..., $b_m \in B_m$. Докажем утверждение для n множеств. Пусть множество A представлено в виде объединения подмножеств B_1,...,B_n и пусть выполнено условие теоремы. Наши рассуждения разбиваются на два случая.

Случай 1. Для любого $k < n$ объединение любых k различных из множеств B_1, B_2,..., B_n содержит строго больше k элементов. Это, в частности, означает, что каждое из множеств B_i состоит не меньше чем из двух элементов. Выберем произвольный элемент $b_n \in B_n$; возможно, элемент b_n принадлежит и каким-то другим из множеств B_i. Для $i < n$ обозначим через B'_i подмножество B_i, состоящее из всех элементов множества B_i, отличных от b_n. Таким образом, $B'_i = B_i$, если $b_n \notin B_i$, и B'_i получается из B_i выбрасыванием элемента b_n в противном случае.

Проверим, что для множества $A' = \bigcup\limits_{i=1}^{n-1} B'_i$ и его подмножеств B'_1,...,B'_{n-1} выполнены условия теоремы. Действительно, для любых $1 \leq i_1 < i_2 < \cdots < i_k \leq n-1$ объединение множеств B'_{i_1},..., B'_{i_k} или совпадает с объединением множеств B'_{i_1},..., B'_{i_k} (если это последнее объединение не содержит b_n), или получается из него выбрасыванием единственного элемента b_n. Поэтому число элементов множества $B'_{i_1} \cup \cdots \cup B'_{i_k}$ отличается от числа элементов множества $B_{i_1} \cup \cdots \cup B_{i_k}$ не больше, чем на 1. Но в нашем случае множество $B_{i_1} \cup \cdots \cup B_{i_k}$ содержит строго больше, чем k элементов; поэтому множество $B'_{i_1} \cup \cdots \cup B'_{i_k}$ состоит не меньше, чем из k элементов, в чем мы и хотели убедиться.

По предположению индукции, достаточность условий теоремы справедлива для множества A' и его подмножеств B'_1,...,B'_{n-1}; поэтому существуют различные элементы $b_1 \in B'_1 \subseteq B_1$, ..., $b_{n-1} \in B'_{n-1} \subseteq B_{n-1}$. Но $b_n \in B_n$, и поэтому элементы b_1,..., b_{n-1}, b_n являются представителями всех множеств B_1,..., B_{n-1}, B_n. Они попарно различны: все элементы b_1,..., b_{n-1} отличны от b_n, и они были выбраны так, что попарно не совпадают. Итак, для этого случая утверждение теоремы доказано.

Случай 2. Существуют $k < n$ различных из множеств B_1,..., B_n, объединение которых состоит из k элементов. Обозначим через m разность $n - k$. Перенумеровав, если надо, множества B_i, добьемся того, чтобы объединение именно последних k множеств $C = B_{m+1} \cup \cdots \cup B_n$ состояло из k элементов. Пусть $A' = A \setminus C$, $B'_i = B_i \setminus C$ $(1 \le i \le m)$; иначе говоря, каждое множество B'_i получается из B_i выбрасыванием всех элементов, принадлежащих множеству C. Ясно, что $A' = B'_1 \cup \cdots \cup B'_m$.

Покажем, что для множеств B'_i выполнены условия теоремы. Действительно, пусть $1 \le i_1 < \cdots < i_p \le m$; тогда

$$B'_{i_1} \cup \cdots \cup B'_{i_p} = (B_{i_1} \cup \cdots \cup B_{i_p}) \setminus C = (B_{i_1} \cup \cdots \cup B_{i_p} \cup C) \setminus C =$$
$$(B_{i_1} \cup \cdots \cup B_{i_p} \cup B_{m+1} \cup \cdots \cup B_n) \setminus C\,.$$

По условию теоремы, число элементов множества $B_{i_1} \cup \cdots \cup B_{i_p} \cup B_{m+1} \cup \cdots \cup B_n$ не меньше чем $p + (n - m) = p + k$. Но множество C состоит ровно из k элементов; поэтому число элементов множества

$$B'_{i_1} \cup \cdots \cup B_{i_p} = (B_{i_1} \cup \cdots \cup B_{i_p} \cup B_{m+1} \cup \cdots \cup B_n) \setminus C$$

не меньше $(p + k) - k = p$.

Поскольку $m < n$, $k < n$, мы можем применить предположение индукции к множествам $A' = B'_1 \cup \cdots \cup B'_m$ и $C = B_{m+1} \cup \cdots \cup B_n$. Существуют, таким образом, различные элементы $b_1 \in B'_1 \subseteq B_1$, ..., $b_m \in B'_m \subseteq B_m$ и различные элементы $b_{m+1} \in B_{m+1}$, ..., $b_n \in B_n$. Но все элементы b_1,...,b_m не принадлежат C, а элементы b_{m+1},...,b_n, наоборот, содержатся в C. Следовательно, все элементы b_1,...,b_m, b_{m+1},...,b_n различны, и они являются представителями всех множеств B_1,...,B_m, B_{m+1},...,B_n.

Теорема полностью доказана. В следующих параграфах мы приведем несколько ее приложений.

5. Теорема об одновременном выборе представителей для двух разбиений множества

Разбиением множества называется его представление в виде объединения попарно непересекающихся множеств. Если A — некоторое множество и B — его подмножество, то элемент $a \in A$ называется представителем подмножества B, если $a \in B$.

Теорема. *Пусть $A = B_1 \cup \cdots \cup B_n = C_1 \cup \cdots \cup C_n$ — два разбиения множества A. Для того чтобы существовали элементы $a_1, a_2, \ldots, a_n \in A$, которые были бы представителями как всех множеств первого разбиения, так и всех множеств второго разбиения, необходимо выполнение двух условий:*

(1) *для любого $k \le n$ и для любых k из множеств B_1, ..., B_n их объединение содержит целиком не больше k из множеств C_1, ..., C_n;*

(2) *для любого* $k \leq n$ *и для любых* k *из множеств* C_1, ..., C_n *их объединение содержит целиком не больше* k *из множеств* B_1, ..., B_n,

и достаточно выполнения любого одного из этих условий.

Доказательство. Необходимость очевидна. Пусть, например, $B_{i_1} \cup \dots \cup B_{i_k} \supseteq C_{j_1} \cup \dots \cup C_{j_p}$, где $1 \leq i_1 < \dots < i_k \leq n$, $1 \leq j_1 < \dots < j_p \leq n$, $k < p$. Тогда объединение $k < p$ множеств B_{i_1}, ..., B_{i_k} содержало бы p представителей a_{s_1}, ..., a_{s_p} множеств C_{j_1},..., C_{j_p} и потому хотя бы одно из множеств B_{i_1}, ..., B_{i_k} содержало бы по меньшей мере два из элементов a_1, a_2,..., a_n, а это, в соответствии с принципом Дирихле, противоречит тому, что элементы a_1, a_2,..., a_n представляют все множества B_1, ..., B_n.

Докажем теперь достаточность условия (2) (достаточность условия (1) доказывается аналогично). Обозначим через M множество $\{1, 2, \dots, n\}$ и для каждого i, $1 \leq i \leq n$ обозначим через K_i подмножество множества M, состоящее из всех таких индексов $j \in M$, что непусто пересечение $B_i \cap C_j$.

Покажем, что для подмножеств $K_1, \dots, K_n$ выполняются условия теоремы о выборе различных представителей в подмножествах. Действительно, пусть объединение k из подмножеств K_s состоит меньше чем из k элементов. Перенумеровав множества B_i, добьемся того, чтобы из меньшего, чем k, числа элементов состояло объединение $K_1 \cup \dots \cup K_k$; перенумеровав теперь множества C_j, добьемся, чтобы $K_1 \cup \dots \cup K_k = \{1, \dots, p\}$, $p < k$. Это означает, что множества $B_1, \dots, B_k$ имеют непустые пересечения только с множествами $C_1, \dots, C_p$, и потому объединение p множеств $C_1, \dots, C_p$ полностью содержит в себе $k > p$ множеств $B_1, \dots, B_k$; но это противоречит условию (2).

Согласно теореме о выборе различных представителей в подмножествах, существуют различные числа $i_1, i_2, \dots, i_n \in M$, такие что $i_s \in K_s$ для любого s. Это означает, что непусты все пересечения $B_1 \cap C_{i_1}$, $B_2 \cap C_{i_2}$, ..., $B_n \cap C_{i_n}$; выберем в каждом из них по элементу $a_1 \in B_1 \cap C_{i_1}$, $a_2 \in B_2 \cap C_{i_2}$, ..., $a_n \in B_n \cap C_{i_n}$. Элементы $a_1, a_2, \dots, a_n$ являются представителями всех множеств $B_1, B_2, \dots, B_n$; поскольку элементы $i_1, i_2, \dots, i_n \in M = \{1, 2, \dots, n\}$ различны, они составляют перестановку множества $\{1, 2, \dots, n\}$, и потому элементы a_1, $a_2, \dots, a_n$ являются также представителями всех множеств $C_1, C_2, \dots, C_n$.

Теорема полностью доказана.

Условия этой теоремы выполняются автоматически, если все подмножества B_i, C_j состоят из одинакового числа элементов. Пример такой ситуации доставляется теорией групп. Пусть G — конечная группа и H — её подгруппа; тогда группа G разбивается в объединение попарно непересекающихся левых классов смежности G по H и в объединение попарно непересекающихся правых классов смежности G по H, причем число элементов в каждом из этих классов (левом или правом) одно и то же: оно равно порядку подгруппы H. По доказанной теореме, мы можем выбрать такие элементы $g_1, \dots, g_n \in G$, которые являлись бы одновременно представителями всех левых и всех правых классов смежности.

6. Латинские прямоугольники

Пусть M — конечное множество, состоящее из n элементов. Латинским прямоугольником над множеством M называется прямоугольная таблица, в каждой строке которой встречаются по одному разу все элементы множества M, и в каждом столбце которой любой элемент из M встречается не более одного раза. Таким образом, число столбцов латинского прямоугольника равно n, а число строк не превосходит n. Немного иначе латинский прямоугольник определяется так: все его элементы принадлежат M, ни в одной строке нет одинаковых элементов, ни в одном столбце нет одинаковых элементов, причем в любой строке (но не в столбце!) встречаются все элементы множества M.

Теорема. *Пусть M — конечное множество, состоящее из n элементов, и пусть A — латинский прямоугольник над M, состоящий из m строк и n столбцов. Если $m < n$, то к прямоугольнику A можно приписать еще одну строку так, чтобы получившийся $(m+1) \times n$ прямоугольник снова был латинским.*

Доказательство. Для каждого i, $1 \leq i \leq n$, обозначим через $K_i \subset M$ множество всех элементов множества M, не содержащихся в i-м столбце латинского прямоугольника A. Покажем, что для подмножеств $K_1, \ldots, K_n$ выполняются условия теоремы о выборе различных представителей в подмножествах.

Действительно, все элементы множества M встречаются по одному разу в каждой из m строк прямоугольника A, а в каждом столбце прямоугольника A любой элемент из M встречается не более одного раза. Следовательно, каждый из элементов множества M встречается ровно в $n-m$ из дополнений K_i столбцов прямоугольника A. Пусть объединение $U = K_{i_1} \cup \cdots \cup K_{i_k}$ каких-то k из множеств K_i состоит из p элементов. Поскольку каждый из этих p элементов входит не более чем в $n-m$ из множеств $K_{i_1}, \ldots, K_{i_k}$, сумма $k(n-m)$ порядков этих множеств не больше, чем $p(n-m)$. Таким образом, $k(n-m) \leq p(n-m)$, т.е. $k \leq p$, в чем мы и хотели убедиться.

Таким образом, к подмножествам $K_1, \ldots, K_n$ можно применить теорему о выборе различных представителей в подмножествах. Согласно этой теореме, существуют различные элементы $a_1, \ldots, a_n \in M$, такие что $a_1 \in K_1, \ldots, a_n \in K_n$. Ясно, что если мы добавим к латинскому прямоугольнику A строку $(a_1, a_2, \ldots, a_n)$, то мы снова получим латинский прямоугольник. Теорема доказана.

Применяя эту теорему несколько раз, получим

Следствие 1. *Каждый латинский прямоугольник может быть дополнен до латинского квадрата.*

Если множество M непусто, то, расставив элементы этого множества в каком-то порядке, мы получим латинский прямоугольник над множеством M из одной строки. Применив теперь следствие 1, получим

Следствие 2. *Над любым непустым множеством существуют латинские квадраты.*

7. Теорема Кёнига

1. Граничный ранг матрицы. Пусть A — числовая матрица. Её граничным рангом называется наибольшее число r, такое что существуют r ненулевых элементов матрицы, лежащих в разных строках и разных столбцах. То, что мы употребляем здесь слово "ранг", оправдывается следующим соображением. Перманентом квадратной матрицы порядка n называется сумма $n!$ всевозможных произведений элементов матрицы, взятых по одному из каждой строки и каждого столбца. Мы видим, что перманент очень похож на определитель; различие состоит только в том, что в перманент каждое произведение входит со знаком " + ", а в определитель некоторые произведения входят со знаком " + ", а другие — со знаком " − ". Если все элементы матрицы неотрицательны, то перманент этой матрицы отличен от 0 тогда и только тогда, когда можно выбрать n ненулевых элементов матрицы, лежащих в разных строках и разных столбцах. В этих терминах граничный ранг вещественной матрицы, все элементы которой неотрицательны, может быть определен как наибольшее число r, такое что в матрице существует квадратная подматрица порядка r с ненулевым перманентом. Напомним, что если в этом определении вместо перманента участвует определитель, то мы придем к обычному рангу матрицы. Очевидно, ранг матрицы не больше граничного ранга, и они действительно могут не совпадать: ранг матрицы

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

равен 1, а её граничный ранг равен 2.

2. Теорема Кёнига. Рядами матрицы называются её строки и столбцы. Мы будем интересоваться минимальным количеством рядов, содержащих все отличные от 0 элементы матрицы A. Например, все ненулевые элементы матрицы

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

входят в два ряда: первую строку и первый столбец; если бы разрешалось использовать только строки или только столбцы, то для включения всех отличных от 0 элементов нам понадобилось бы 3 ряда.

Теорема Кёнига. *Граничный ранг числовой матрицы совпадает с наименьшим числом рядов, в которых содержатся все ненулевые элементы матрицы.*

Доказательство. Обозначим через r_1 граничный ранг матрицы A, а через r_2 — наименьшее количество рядов, содержащих все ненулевые элементы матрицы A. Нам надо доказать два неравенства: $r_1 \leq r_2$ и $r_2 \leq r_1$. Первое из них тривиально: если r_1 отличных от 0 элементов матрицы лежат в разных строках и разных столбцах, то каждый ряд может содержать только один из этих элементов, и для того, чтобы включить в себя лишь эти элементы (не говоря уже об остальных ненулевых элементах матрицы), понадобится не меньше r_1 рядов. Докажем второе неравенство.

Пусть все ненулевые элементы матрицы A содержатся в r_2 рядах, из которых p строк и $q = r_2 - p$ столбцов. Очевидно, ни r_1, ни r_2 не меняются при перестановке строк и столбцов матрицы; поэтому, не умаляя общности, мы можем считать, что все отличные от 0 элементы матрицы A содержатся в первых p строках и первых q столбцах, т.е. что матрица A имеет вид

$$A = \begin{pmatrix} F & B \\ C & \mathbb{O} \end{pmatrix} ,$$

где B — матрица, состоящая из p строк, C — матрица из q столбцов и $\mathbb{O}$ — нулевая матрица.

Обозначим через $J = \{q+1, q+2, \dots, n\}$ множество номеров (в матрице A) столбцов матрицы B. Для каждого из индексов i, $1 \le i \le p$, обозначим через $K_i \subseteq J$ множество номеров тех столбцов, в которых в i-й строке матрицы B стоят ненулевые элементы. Покажем, что для любого $k \le p$ число элементов объединения любых k из множеств K_i не меньше k. Действительно, в противном случае существовали бы такие индексы $1 \le i_1 < \dots < i_k \le p$, что число ℓ элементов объединения $U = K_{i_1} \cup \dots \cup K_{i_k}$ меньше k. Это означает, что в строках матрицы B с номерами $i_1, \dots, i_k$ ненулевые элементы есть лишь в столбцах с номерами из U. Пусть $U = \{j_1 < \dots < j_\ell\}$. Заменим в нашей системе рядов матрицы A строки с номерами $i_1, \dots, i_k$ на столбцы с номерами $j_1, \dots, j_\ell$. Нетрудно видеть, что новая система рядов снова содержит все ненулевые элементы матрицы A; действительно, элементы из матриц F и C входят в первые q столбцов, те ненулевые элементы матрицы B, которые не попали в строки с номерами $i_1, \dots, i_k$, содержатся в оставшихся $p-k$ строках, а ненулевые элементы из строк с номерами $i_1, \dots, i_k$ входят в столбцы с номерами $j_1, \dots, j_\ell$. Но число рядов в новой системе равно $q + (p-k) + \ell < p + q = r_2$, а это противоречит тому, что число r_2 равно наименьшему числу рядов, содержащих все ненулевые элементы матрицы A.

Таким образом, для множеств K_i выполнены условия теоремы о выборе различных представителей в подмножествах. Согласно этой теореме, существуют различные номера $s_1 \in K_1, \dots, s_p \in K_p$. Это означает, что элементы матрицы A, лежащие в 1-й строке и s_1-м столбце, 2-й строке и s_2-м столбце, $\dots$, p-й строке и s_p-м столбце отличны от 0; ясно, что все эти элементы принадлежат матрице B. Таким образом, в матрице B нашлись p ненулевых элементов, лежащих в разных строках и разных столбцах. Точно так же, в матрице C существуют q ненулевых элементов, лежащих в разных строках и разных столбцах. Очевидно, что все эти $p+q = r_2$ ненулевых элементов лежат в разных строках и разных столбцах матрицы A, и потому их количество r_2 не больше, чем граничный ранг r_1 матрицы A. Итак, мы убедились в том, что $r_2 \le r_1$, что завершает доказательство теоремы Кёнига.

3. Применение теоремы Кёнига: матрицы с равными суммами по всем вертикальным рядам и по всем горизонтальным рядам. Квадратная матрица, в каждой строке и в каждом столбце которой есть ровно одна единица, а все остальные элементы равны 0, называется матрицей перестановки, или перестановочной матрицей. Вот все перестановочные матрицы порядка 3:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Пусть единственная единица расположена в 1-й строке перестановочной матрицы на i_1-м месте, во второй — на i_2-м месте, ... , в n-й — на i_n-м месте. Поскольку в каждом столбце перестановочной матрицы может быть только одна единица, номера столбцов i_1, i_2, ... , i_n попарно различны; следовательно, они образуют перестановку . Отсюда и название таких матриц — перестановочные матрицы. Всего перестановочных матриц порядка n столько же, сколько перестановок множества $\{1, 2, \ldots, n\}$, т.е. $n!$.

Теорема. *Пусть A — квадратная матрица порядка n с вещественными неотрицательными компонентами. Обозначим через S_i сумму элементов i-й строки матрицы A, а через T_j сумму элементов j-го столбца матрицы A. Если $S_1 = S_2 = \cdots = S_n$ и $T_1 = T_2 = \cdots = T_n$, то матрица A может быть представлена в виде*

$$A = \alpha_1 P_1 + \alpha_2 P_2 + \cdots + \alpha_m P_m\,,$$

где P_1, P_2, ... , P_m — перестановочные матрицы, а α_1, α_2, ... , α_m — неотрицательные вещественные числа.

Доказательство. Пусть $S_1 = S_2 = \cdots = S_n = p$, $T_1 = T_2 = \cdots = T_n = q$. Тогда сумма всех элементов матрицы равна, с одной стороны, $S_1 + S_2 + \cdots + S_n = np$, а, с другой стороны, эта же сумма равна $T_1 + T_2 + \cdots + T_n = nq$. Таким образом, $np = nq$, т.е. $p = q$. Следовательно, сумма элементов каждого ряда матрицы равна p.

Найдем граничный ранг r матрицы A. По теореме Кёнига, все ненулевые элементы матрицы A содержатся в r рядах этой матрицы. Но элементы матрицы неотрицательны, а сумма элементов каждого ряда равна p; поэтому сумма всех ненулевых элементов матрицы, а значит, и сумма всех элементов матрицы, не превосходит rp (эта сумма могла бы быть и меньше rp, потому что некоторые из ненулевых элементов считались бы дважды — в строке и столбце, если они входят в число r выбранных рядов). Но мы видели, что сумма всех элементов матрицы равна np; итак, $np \le rp$ и, если матрица A ненулевая, $n \le r$. Поскольку, очевидно, $r \le n$, мы доказали, что граничный ранг любой ненулевой матрицы, удовлетворяющей условиям теоремы, равен n.

Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}.$$

Будем доказывать теорему индукцией по числу ненулевых элементов матрицы A. Если ненулевых элементов вообще нет, т.е. если A — нулевая матрица, то утверждение теоремы тривиально. Пусть $A \neq 0$ и пусть теорема уже доказана для матриц с меньшим числом ненулевых элементов. Поскольку матрица A ненулевая, её граничный ранг равен n, и потому найдутся n ненулевых элементов матрицы A, лежащих в разных строках и разных столбцах. Таким образом, найдется перестановка $i_1, i_2, \dots, i_n$ множества $\{1, 2, \dots, n\}$, такая что числа $a_{1i_1}, a_{2i_2}, \dots, a_{ni_n}$ отличны от 0. Пусть $\alpha_1 > 0$ — наименьшее из этих чисел, и пусть P_1 — перестановочная матрица, отвечающая перестановке $i_1, i_2, \dots, i_n$. Ясно, что сумма элементов каждого ряда матрицы $A - \alpha_1 P_1$ равна $p - \alpha_1$, так что эта матрица снова удовлетворяет условиям теоремы. Но в матрице $A - \alpha_1 P_1$ число ненулевых элементов хотя бы на 1 меньше, чем в матрице A; применяя к $A - \alpha_1 P_1$ предположение индукции, найдем перестановочные матрицы $P_2, \dots, P_m$ и неотрицательные вещественные числа $\alpha_2, \dots, \alpha_m$, такие что

$$A - \alpha_1 P_1 = \alpha_2 P_2 + \cdots + \alpha_m P_m ,$$

т.е. $A = \alpha_1 P_1 + \alpha_2 P_2 + \cdots + \alpha_m P_m$. Теорема доказана.

4. Задача о выборе партнеров. Применяя теорему из предыдущего пункта, легко получить решение одной комбинаторной задачи, которую удобно сформулировать как задачу о выборе танцевальных партнеров.

На танцевальном вечере собрались n девушек и n юношей; каждая девушка знакома ровно с $k \geq 1$ юношами, а каждый юноша — ровно с k девушками. Доказать, все юноши могут одновременно пригласить девушек на танец так, чтобы каждая пара состояла из знакомых друг с другом молодых людей.

Действительно, занумеруем всех юношей числами от 1 до n, и всех девушек тоже занумеруем числами от 1 до n. Пусть A — квадратная матрица порядка n, на пересечении i-й строки и j-го столбца которой стоит 1, если i-й юноша знаком с j-й девушкой, и стоит 0, если они не знакомы. Сумма элементов каждой строки равна k, и сумма элементов каждого столбца равна k; поэтому мы находимся в ситуации предыдущего пункта. Из доказательства приведенной там теоремы следует, что граничный ранг матрицы A равен n, и потому можно выбрать в матрице n единиц, стоящих в разных строках и разных столбцах. Если выбранная в i-й строке единица стоит в столбце с номером s_i, то $s_1, \dots, s_n$ — перестановка множества $\{1, \dots, n\}$; ясно, что условия задачи будут удовлетворены, если для каждого i юноша с номером i пригласит на танец девушку с номером s_i.

8. Теорема Рамсея

Теорема Рамсея. *Пусть $r \geq 2$ — натуральное число, и пусть $q_1, q_2, \dots, q_m \geq r$ — некоторый набор натуральных чисел. Тогда существует такое число $R = R_m(r; q_1, q_2, \dots, q_m) \geq 1$, зависящее только от чисел r, q_1, q_2, ..., q_m, что если M — множество, число элементов которого не меньше R, и множество $P_r(M)$ подмножеств множества M, состоящих из r элементов, представлено в виде объединения m попарно не пересекающихся подмножеств Q_1, Q_2,...,Q_m,* *то существуют подмножество $A \subseteq M$ и номер i, $1 \le i \le m$, такие что число элементов множества B равно q_i и все подмножества порядка r множества B принадлежат множеству Q_i.*

Прежде, чем переходить к доказательству, условимся для натурального числа p называть p-подмножествами любые подмножества, состоящие из p элементов.

Доказательство. Простейшие случаи. Если $r = 1$, то мы можем взять в качестве $R_m(1; q_1, ..., q_m)$ число $q_1 + ... + q_m - m$. Действительно, множество $P_1(M)$ одноэлементных подмножеств множества M — это само множество M, и потому в этом случае надо найти подмножество $A \subseteq M$, состоящее из q_i элементов, все элементы которого принадлежат множеству $Q_i \subseteq P_1(M) = M$. Если этого нельзя сделать ни для одного i, то каждое множество Q_i состоит не больше чем из $q_i - 1$ элементов, откуда следует, что в множестве $M = Q_1 \cup Q_2 \cup \cdots \cup Q_m$ не больше, чем $(q_1 - 1) + (q_2 - 1) + \cdots + (q_m - 1) = R_m(1; q_1, ..., q_m)$ элементов.

Пусть теперь $m = 2$ и одно из чисел q_1, q_2 равно r; покажем, что тогда в качестве $R_2(r; q_1, q_2)$ подойдет второе из этих чисел, уменьшенное на 1. Действительно, пусть, например, $q_1 = r$, а число элементов множества M не меньше q_2. Множество $P_r(M)$ r-элементных подмножеств множества M разбито в объединение подмножеств Q_1 и Q_2. Если множество Q_1 непусто, то существует r-элементное подмножество $A \in Q_1$ множества M; оно удовлетворяет требованиям, так как состоит из $q_1 = r$ элементов, а его единственное r-элементное подмножество A принадлежит Q_1. Если же множество Q_1 пусто, то $P_r(M) = Q_2$; в множестве M не меньше q_2 элементов, поэтому в нем можно выбрать q_2-элементное подмножество A, и все r-элементные подмножества A принадлежат $P_r(M) = Q_2$.

Доказательство в случае $m = 2$. Мы будем строить числа $R_2(r; q_1, q_2)$, удовлетворяющие требованиям теоремы Рамсея, индукцией по r; при $r = 1$ эти числа уже построены. Пусть $r \ge 2$, и пусть числа $R_2(r - 1; q_1', q_2')$ уже построены для всех $q_1', q_2' \ge r - 1$. В свою очередь, числа $R_2(r; q_1', q_2')$ будут строиться индукцией по $q_1' + q_2'$. Мы уже знаем все числа $R_2(r; r, q)$ и $R_2(r; q, r)$; пусть $q_1 > r$, $q_2 > r$, и пусть уже известны все $R_2(r; q_1', q_2')$ с $q_1' + q_2' < q_1 + q_2$. Покажем, что тогда можно положить

$$R_2(r; q_1, q_2) = R_2(r - 1; R_2(r; q_1 - 1, q_2) + 1, R_2(r; q_1, q_2 - 1) + 1) + 1\,.$$

Пусть M — множество, число элементов которого больше этого числа. Возьмем произвольный элемент $a \in M$ и обозначим через M' множество всех элементов из M, отличных от a. Разобьем множество $(r - 1)$-подмножеств $P_{r-1}(M')$ в объединение двух непересекающихся множеств Q_1' и Q_2' следующим образом. Пусть $A \subseteq M'$ — подмножество M', состоящее из $r - 1$ элементов; тогда $A \cup \{a\}$ — подмножество M, состоящее из r элементов, т.е. $A \cup \{a\} \in P_r(M) = Q_1 \cup Q_2$. Обозначим через Q_1' множество всех тех подмножеств $A \in P_{r-1}(M')$, для которых $A \cup \{a\} \in Q_1$, а через Q_2' обозначим множество всех тех подмножеств $A \in P_{r-1}(M')$, для которых $A \cup \{a\} \in Q_2$. Ясно, что $P_{r-1}(M') = Q_1' \cup Q_2'$ и что множества Q_1' и Q_2' не пересекаются.

Число элементов множества $M' = M \setminus \{a\}$ не меньше чем

$$R_2(r; q_1, q_2) - 1 = R_2(r-1; R_2(r; q_1 - 1, q_2) + 1, R_2(r; q_1, q_2 - 1) + 1).$$

По предположению индукции, все числа $R_2(r-1; q_1', q_2')$ удовлетворяют требованиям теоремы. Поэтому существует или подмножество D множества M', состоящее из $R_2(r; q_1 - 1, q_2) + 1$ элементов, все $(r-1)$-подмножества которого принадлежат Q_1', или подмножество $E \subseteq M'$, состоящее из $R_2(r; q_1, q_2 - 1) + 1$ элементов, все $(r-1)$-подмножества которого принадлежат Q_2'. Дальнейшие рассуждения в обоих случаях аналогичны, поэтому без ущерба для полноты доказательства ограничимся первым из них.

Число элементов множества D больше $R_2(r; q_1 - 1, q_2)$, и по предположению индукции число $R_2(r; q_1 - 1, q_2)$ удовлетворяет требованиям теоремы; поэтому существует или подмножество A' множества D, состоящее из $q_1 - 1$ элементов, все r-подмножества которого принадлежат Q_1, или подмножество B множества D, состоящее из q_2 элементов, все r-подмножества которого принадлежат Q_2. Во втором из этих подслучаев подмножество $B \subseteq M$ именно такое, как требуется в теореме; в первом же подслучае требованиям теоремы удовлетворяет множество $A = A' \cup \{a\}$. Действительно, множество A состоит из q элементов, и все его r-подмножества, не содержащие элемента a, принадлежат Q_1; покажем, что и r-подмножества, содержащие a, тоже принадлежат Q_1. В самом деле, пусть X — r-подмножество A, такое что $a \in A$; тогда $X' = X \setminus \{a\}$ — $(r-1)$-подмножество $A' \subseteq D$. Но все $(r-1)$-подмножества D принадлежат Q_1'; поэтому $X' \in Q_1'$, а это, по определению Q_1', означает, что $X = X' \cup \{a\} \in Q_1$.

Этим завершается доказательство теоремы в случае $m = 2$.

Доказательство в общем случае. Пусть теперь $m \geq 3$ и пусть удовлетворяющие требованиям теоремы Рамсея числа $R_{m-1}(r; q_1, \ldots, q_{m-1})$ уже построены для всех r, q_1, ..., q_{m-1}. Положим

$$R_m(r; q_1, \ldots, q_{m-1}, q_m) = R_2(r; R_{m-1}(r; q_1, \ldots, q_{m-1}) + 1, q_m)$$

и покажем, что эти числа удовлетворяют требованиям теоремы Рамсея. Пусть M — множество из большего числа элементов, и пусть $P_r(M) = Q_1 \cup \cdots \cup Q_{m-1} \cup Q_m$ — разбиение множества r-подмножеств $P_r(M)$ в объединение m попарно не пересекающихся подмножеств. Обозначим через S объединение $Q_1 \cup \cdots \cup Q_{m-1}$; тогда $P_r(M) = S \cup Q_m$ — разбиение $P_r(M)$ в объединение двух не пересекающихся подмножеств. Поскольку число элементов множества M больше, чем

$$R_m(r; q_1, \ldots, q_{m-1}, q_m) = R_2(r; R_{m-1}(r; q_1, \ldots, q_{m-1}) + 1, q_m),$$

по теореме Рамсея, которая для $m = 2$ уже доказана, существует или подмножество $B \subseteq M$, число элементов которого равно $R_{m-1}(r; q_1, \ldots, q_{m-1}) + 1$, а все r-подмножества принадлежат S (т.е. $P_r(B) \subseteq S$), или подмножество $A \subseteq M$, состоящее из q_m элементов, все r-подмножества которого принадлежат Q_m. Во втором случае требуемое теоремой подмножество уже найдено; разберемся теперь с первым случаем.

Обозначим через Q'_i $(1 \leq i < m)$ пересечение множества Q_i с множеством $P_r(B)$ r-подмножеств множества B; ясно, что $P_r(B) = Q'_1 \cup \dots \cup Q'_{m-1}$ — разбиение множества $P_r(B)$ в объединение $m-1$ попарно не пересекающихся подмножеств. Число элементов множества B больше $R_{m-1}(r; q_1, \dots, q_{m-1})$; поэтому по теореме Рамсея, которая предположением индукции считается в этом случае справедливой, существует подмножество $A \subseteq B \subseteq M$ и индекс i, $1 \leq i < m$, такие что множество A состоит из q_i элементов, и все r-подмножества A содержатся в $Q'_i \subseteq Q_i$. Итак, и в этом случае нашлось требуемое теоремой Рамсея подмножество.

Теорема Рамсея полностью доказана.

9. Приложения теоремы Рамсея

1. Задача о раскрашенных многоугольниках. На плоскости выбраны N точек общего положения (это значит, что никакие три из них не лежат на одной прямой). Все $N(N+1)/2$ отрезков раскрашены в один из трех цветов: красный, зеленый или синий. Мы говорим, что многоугольник с вершинами в выбранных точках красный, если все его стороны и диагонали окрашены в красный цвет; аналогично определяются зеленые и синие многоугольники. Требуется доказать, что если число N достаточно велико, то существует красный четырехугольник или зеленый пятиугольник или синий семиугольник с вершинами в выбранных точках.

Эта задача олимпиадного типа дает пример непосредственного применения теоремы Рамсея. Пусть M — множество выбранных точек; в нашем случае множество $P_2(M)$ пар элементов из M представляет собой множество отрезков, соединяющих точки, и оно уже разбито в объединение трех не пересекающихся множеств $Q_{\text{к}}$, $Q_{\text{з}}$, $Q_{\text{с}}$, состоящих из соответственно красных, зеленых или синих отрезков. Пусть $N > R_3(2; 4, 5, 7)$; по теореме Рамсея существует подмножество $A \subseteq M$, состоящее из 4 элементов, все 2-подмножества которого принадлежат $Q_{\text{к}}$, или подмножество $B \subseteq M$, состоящее из 5 элементов, все 2-подмножества которого принадлежат $Q_{\text{з}}$, или подмножество $C \subseteq M$, состоящее из 7 элементов, все 2-подмножества которого принадлежат $Q_{\text{с}}$. Иначе говоря, это означает, что из точек множества M можно составить красный четырехугольник или зеленый пятиугольник или синий семиугольник.

2. Существование выпуклых многоугольников с вершинами в больших множествах точек общего положения.

Теорема. *Пусть $n \geq 3$ — натуральное число. Существует натуральное число $E(n)$, зависящее только от n, такое что если на плоскости выбрано множество точек, находящихся в общем положении, состоящее из $N > E(n)$ точек, то существует выпуклый n-угольник, все вершины которого принадлежат выбранному множеству.*

Напомним, что N точек находятся в общем положении, если никакие три из них не лежат на одной прямой.

Доказательство. Пусть S — множество точек общего положения на плоскости. Разобьем множество $P_4(S)$ подмножеств множества S, состоящих из четырех элементов, в объединение двух подмножеств Q_1 и Q_2 следующим образом.

Четверка F точек из S попадает в множество Q_1, если точки из F являются вершинами выпуклого четырехугольника, и она попадает в Q_2, если это не так, т.е. если одна из точек множества F лежит внутри треугольника, образованного остальными точками множества F. Пусть число точек множества S больше числа $E(n) = R_2(4; n, 5)$. По теореме Рамсея существуют n точек множества S, любые 4 из которых являются вершинами выпуклого четырехугольника, или 5 точек из S, никакие 4 из которых не являются вершинами выпуклого четырехугольника. Теорема вытекает теперь непосредственно из двух лемм, первая из которых утверждает, что второй случай невозможен, а вторая — что n-угольник, получающийся в первом случае, выпуклый.

Лемма 1. *Из любых 5 точек общего положения на плоскости найдутся четыре, лежащие в вершинах выпуклого четырехугольника.*

Лемма 2. *Пусть любые четыре из n точек общего положения на плоскости являются вершинами выпуклого четырехугольника. Тогда эти n точек представляют собой вершины выпуклого n-угольника.*

Доказательства обеих лемм используют понятие выпуклой оболочки конечного множества точек S. Под выпуклой оболочкой множества S мы понимаем выпуклый многоугольник с вершинами из S, содержащий все точки из S. Существует лишь конечное число несамопересекающихся многоугольников с вершинами в конечном множестве S точек общего положения на плоскости; выберем из них многоугольник P наибольшей площади. Если бы многоугольник P не был выпуклым или если бы не все точки множества S содержались в нем, то, как нетрудно видеть, площадь многоугольника P можно было бы увеличить, а это противоречит выбору P. Итак, P — выпуклая оболочка множества S. Тем самым, мы доказали, что выпуклая оболочка конечного множества точек общего положения на плоскости всегда существует.

Доказательство леммы 1. Пусть заданы пять точек общего положения на плоскости. Их выпуклая оболочка может быть 5-угольником, 4-угольником или треугольником. В первых двух случаях какие-то четыре из точек — вершины выпуклого четырехугольника; поэтому остается рассмотреть случай, когда выпуклая оболочка является треугольником, а две из точек D и E лежат внутри этого треугольника. Проведем через точки D и E прямую; поскольку она пересекает границу треугольника, одна из его вершин A лежит по одну сторону от прямой, а две другие B и C — по другую. Один из четырехугольников $BCDE$, $BCED$ несамопересекающийся и ясно, что он выпуклый.

Доказательство леммы 2. Достаточно доказать, что выпуклая оболочка n точек плоскости, удовлетворяющих требованиям леммы, является n-угольником. Пусть эта выпуклая оболочка $A_1A_2\ldots A_m$ представляет собой выпуклый m-угольник с $m < n$ сторонами. В нашем множестве, состоящем из n точек, найдется хотя бы еще одна точка B, отличная от вершин A_1, A_2, $\ldots$, A_m выпуклой оболочки. Она лежит внутри многоугольника $A_1A_2\ldots A_m$ и потому попадает внутрь одного из треугольников $A_1A_2A_3$, $A_1A_3A_4$, $\ldots$, $A_1A_{n-1}A_n$. Пусть точка B лежит внутри треугольника $A_1A_iA_{i+1}$, $2 \le i \le n-1$; тогда точки A_1, A_i, A_{i+1}, B не могут быть вершинами выпуклого четырехугольника, а это противоречит предположению леммы 2. Лемма доказана.

3. "Одноцветные" решения уравнения $x + y = z$.

Теорема. *Пусть множество натуральных чисел $\mathbb{N}$ разбито в объединение r подмножеств $Q_1, \ldots, Q_r$ (т.е. множество $\mathbb{N}$ "раскрашено в n различных цветов"). Тогда существуют числа x, y, z, принадлежащие одному и тому же из множеств Q_i и такие, что $x + y = z$ (иначе говоря, существует "одноцветные" решения уравнения $x + y = z$).*

Доказательство. Разобьем множество пар натуральных чисел в объединение r подмножеств $U_1, \ldots, U_r$, считая, что $\{i, j\} \in U_i$ тогда и только тогда, когда абсолютная величина разности этих чисел $|i - j|$ принадлежит множеству Q_i $i = 1, 2, \ldots, r$. По теореме Рамсея, если $N > R_r(2; 3, 3, \ldots 3)$, то среди натуральных чисел $1, 2, \ldots, N$ найдется такая тройка чисел, все 2-подмножества которой принадлежат одному и тому же из множеств U_i. Пусть $a < b, c$ — эта тройка чисел; тогда все числа $x = b - a$, $y = c - b$, $z = c - a$ принадлежат множеству Q_i, и $x + y = (b - a) + (c - b) = c - a = z$.