Московский физико-технический институт

факультет инноваций и высоких технологий

Основы комбинаторики и теории чисел

Лектор: А.М. Райгородский

конспект лекций

автор: Александр Марков

7 января 2017 г.

Оглавление

Глава 1

Теория множеств

1.1 Основы теории множеств

1.1.1 Основные понятия

В теории множеств множество принимается как *аксиоматическое* понятие, не сводимое к другим, а значит и строгого формального определения множества нет. Однако, можно использовать описательные формулировки, например "произвольный набор различных элементов, *мыслимый как единое целое*". Множества можно определить косвенно через аксиомы теории множеств, однако делать этого мы не будем. Удивительно, но элементы множества называются *элементами множества*. При этом определено отношение *принадлежности* $x \in A$, означающее что x является элементом множества A. При этом важно отметить, что добавление уже имеющегося во множестве элемента в множество не меняет самого множества. Для примера, записи $\{1, 2\} = \{1, 1, 2, 2, 2\} = \{2, 2, 1, 1, 1, \ldots\}$ считаются записями *одного и того же* множества.

Множество можно *задать* следующими способами:

1. $A = \{1, 2, 3\}$ — явно перечислить все элементы множества.

2. $A = \{x | 1 \leqslant x \leqslant 3 \wedge x \in \mathbb{Z}\}$ — *выделить* элементы, удовлетворяющие какому-то свойству из другого

множества.

Определение 1.1.1. Пусть даны два множества A, B. Тогда говорят, что A является *подмножеством* B, если $\forall a \in A : \ a \in B$. *Обозначение:* $A \subset B$.

Определение 1.1.2. Два множества A, B называются *равными*, если $\forall x : \ (x \in A) \Leftrightarrow (x \in B)$.

Заметим, что отношение "быть подмножеством"обладает следующими свойствами:

1. $A \subset A$
2. $A \subset B \wedge B \subset A \Rightarrow A = B$ — проверяется тривиально зная определния.
3. $A \subset B \wedge B \subset C \Rightarrow A \subset C$ — тоже очевидно.

При этом, ничего не запрещает множеству не содержать в себе элементов. Такое множество называется *пустым* множеством и обозначается $\varnothing$.

Утверждение 1.1.1.1. Пустое множество является подмножеством любого другого множества.

Доказательство. Предположим, что найдется множество A, такое что $\varnothing \nsubseteq A$. По определению это значит, что $\exists x \in \varnothing : \ x \notin A$, что противоречит тому, что в пустом множестве нет элементов. □

Определение 1.1.3. Пусть даны два множества A, B. Тогда

1. их объединением называется множество $A \cup B = \{x : \ x \in A \vee x \in B\}$, содержащее все элементы обоих множеств.
2. их пересечением называется множество $A \cap B = \{x : \ x \in A \wedge x \in B\}$, содержащее все элементы, лежащие в обоих множествах.
3. разностью множеств A и B называется множество $A \backslash B = \{x : \ x \in A \wedge x \notin B\}$, содержащее только те элементы, которые лежат в множестве A и не лежат в множестве B.
4. симметрической разностью называется множество $A \triangle B$, содержащее только элементы одного из множеств.

5. пусть дополнительно определено множество U, называемое *универсум*, заведомо содержащее все возможные элементы. Тогда множеством $\overline{A} = U \backslash A$ называется дополнение множества A.

Утверждение 1.1.1.2. Пустое множество единственно.

Доказательство. Заметим, что для любого множества A верно: $A \cap \varnothing = \varnothing$. Тогда предположим, что существует два пустых множества ε_1, ε_2. Имеем $\varepsilon_1 = \varepsilon_1 \cap \varepsilon_2 = \varepsilon_2$. □

Однако, у наивной теории множеств есть **огромный** недостаток: она *противоречива*.

1.1.2 Парадокс Рассела

Как будет показано дальше в курсе мат.логики, из противоречивой теории можно вывести все что угодно, поэтому недостаток действительно, достаточно существенный. Для примера рассмотрим следующую ситуацию, называемую *парадоксом Рассела*.

Заметим, что множества, условно, можно поделить на 2 части — которые содержат себя в качестве элемента (например, множество всех множеств), и которые не содержат себя в качестве элементов (например, множество всех натуральных чисел само не является натуральным числом). Рассмотрим множество $M = \{X : X \notin X\}$ — множество, элементами которого являются те и только те множества, которые не содержат себя в качестве своего элемента и спросим себя:

$$M \stackrel{?}{\in} M$$

Нетрудно проверить, что предположение $M \notin M$ влечет, что $M \in M$, и наоборот.

В данном парадоксе нет ошибки — он действительно доказывает противоречивость теории множеств. Есть несколько подходов к его исправлению. Например, в современной теории множеств (основанной на аксиоматике *Цермело-Френкеля*) идея заключается в том, что использовать можно лишь те множества, которые построены из уже существующих при помощи определенного набора аксиом.

1.1.3 Отображения и соответствия

Определение 1.1.4. *Кортеж* — упорядоченный набор элементов фиксированной длины. Кортежем длины 2 называется упорядоченная пара $(a,\, b) = \{\{a\},\, \{a,\, b\}\}$. Перебором случаев показывается, что $(a_1,\, b_1) = (a_2,\, b_2)$ если и только если $a_1 = a_2$ и $b_1 = b_2$.

Пусть T — кортеж длины n (т.е. содержащий n элементов). Тогда кортеж длины $n+1$, где на 1 месте стоит элемент a, а далее элементы T в таком же порядке называется множество $\{\{a\}, \{a, T\}\}$.

Замечание: Это не единственный способ дать определение кортежа.

Определение 1.1.5. Пусть даны множества A, B. Тогда их *декартовым произведением* называется множество $A \times B = \{(a, b) : a \in A \wedge b \in B\}$ всевозможных упорядоченных пар, где первый элемент лежит в A, а второй — в B.

Декартовой степенью множества A называется множество A^n всех кортежей длины n из элементов A.

Если отождествить элемент a и (a), а кортеж $(T_1, \ldots, T_k)$ с кортежем длины $n_{T_1} + \ldots + n_{T_k}$, то верны следующие свойства декартова произведения и степени (проверяются очевидно):

1. $A \times (B \times C) = (A \times B) \times C$
2. $A^n = A \times A \times \ldots \times A$ n раз
3. $A^n \times A^m = A^{n+m}$
4. $(A^n)^m = A^{nm}$

Определение 1.1.6. Пусть даны множества A, B. Тогда *соответствием* называется любое $F \subset A \times B$. Обозначение:

$$F : A \to B$$

Отображением называется однозначное соответствие, т.е. такое соответствие F, что

$$\forall a \in A \, \exists! b \in B : (a, b) \in F$$

Соответствие называется *инъективным*, если $\forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow F(a_1) \cap F(a_2) = \varnothing$. Инъективное отображение называется *инъекцией*, и в его случае определение записывается как $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$.

Соответствие называется *сюръективным*, если $\forall b \in B \, \exists a \in A : b \in F(a)$. Сюръективное отображение называется сюръекцией и для сюръекции верно $\forall b \in B \, \exists a \in A : b = f(a)$.

Определение 1.1.7. *Биекция* — отображение, являющееся одновременно сюръективным и инъективным.

Теорема 1.1.1. *f — биекция $\iff$ f — взаимно-однозначное соответствие.*

Доказательство. 1. Отображение однозначно по определнию.

2. Сюръективно $\iff$ каждому элементу из B в соответствие ставится $\geqslant 1$ элемент из A.

3. Инъективно $\iff$ каждому элементу из A в соответствие ставится $\leqslant 1$ элемент из B.

□

Зафиксируем множества A, B, $S \subset A$, $T \subset B$ и некоторое соответствие $F : A \to B$.

Определение 1.1.8. *Образом* множества S называется $F(S) = \{b \in B : \exists a \in S\, b \in F(a)\}$.

Прообразом множества T Называется $F^{-1}(T) = \{a \in A : F(a) \cap T \neq \varnothing\}$.

Теорема 1.1.2. *$F(S \cap T) = F(S) \cap F(T) \iff F$ инъективно.*

Доказательство. Если F не иъективно, то существуют a_1, a_2, такие что $F(a_1) \cap F(a_2) \neq \varnothing$. Положим $S = \{a_1\}$, $T = \{a_2\}$.

Если F инъекция, то $b \in F(S \cap T) \Rightarrow \exists a \in S \cap T : b \in F(a)$. Но $a \in S \cap T$ означает, что $a \in S$, $a \in T$, а значит $b \in F(S)$, $b \in F(T) \Rightarrow b \in F(S) \cap F(T)$.

С другой стороны, пусть $b \in F(S) \cap F(T)$. Тогда $\exists a_1 \in S : b \in F(a_1)$, $\exists a_2 \in T : b \in F(a_2)$. По определению инъективного соответствия это значит, что $a_1 = a_2 = a \in S \cap T \Rightarrow b \in F(S \cap T)$. □

Определение 1.1.9. Пусть $F : A \to B$ — соответствие. Тогда его *областью определения* называется $dom(F) = F^{-1}(B)$ — множество тех $a \in A$, для которых есть хотя бы один элемент из B. Его *областью значений* называется $ran(F) = F(A)$ — множество тех b, которым соответствует хотя бы один элемент из A.

Определение 1.1.10. Пусть $F : A \to B$, $S \subset A$. Тогда *сужением* F на S называется соответствие $F|_S : S \to B$ ($b \in F|_S(a) \iff a \in S \wedge b \in F(a)$). Относительно сужения F на S, отображение $F : A \to B$ называется *продолжением*.

Определение 1.1.11. Соответствие $F : A \to B$ называется *частично-заданной функцией*, если $F|_{dom(F)}$ — отображение.

Определение 1.1.12. Пусть $F : A \to B$, $G : B \to C$. Тогда их *композицей* называется соответствие $G \circ F : A \to C$, определяемое как $(G \circ F)(a) = G(F(a))$.

Утверждение 1.1.3.1. Пусть $H : W \to Q$, $G : V \to W$, $F : A \to V$. Тогда $H \circ (G \circ F) = (H \circ G) \circ F$

Доказательство. $\forall a \in A : H \circ (G \circ F)(a) = H((G \circ F)(a)) = H(G(F(a)))$. С другой стороны $(H \circ G) \circ F(a) = (H \circ G)(F(a)) = H(G(F(a)))$. □

Таким образом, соответствие ассоциативно. Однако, коммутативности композиции мешает *очень* многое. Так, если $C \neq A$, то композиция не определена, $C = A \neq B$, то $F \circ G : B \to B$, тогда как $G \circ F : A \to A$, а иначе можно придумать множество контрпримеров (пусть $F(x) = 2x$, $G(x) = x^2$).

Определение 1.1.13. *Тождественным* соответствием называется соответствие $id : A \to A$ со следующим свойством: $id(a) = a \forall a \in A$. Если $F : A \to B$, то *обратным* соответствием называется $F^{-1} : B \to A$, такое что $a \in F^{-1}(b) \iff b \in F(a)$.

Утверждение 1.1.3.2. (б/д)

$F^{-1} \circ F = id_A \iff F$ — инъективное и непустозначное. $F \circ F^{-1} = id_B \iff F$ — сюръективное. Оба утверждения верны в случае когда F — биекция.

1.1.4 Возведение множества в степень

Рассмотрим сначала мини-задачку: пусть в множестве A ровно n элементов, а в множестве B — k. Сколько существует различных функций из A в B? Нетрудно понять, что ответ это k^n (поймите это в качестве упражнения).

Определение 1.1.14. Пусть даны множества A, B. Тогда множеством B^A является множество всех *отображений* из A в B. Заметим, что если в B ровно 2 элемента, то это множество является *множеством всех подмножеств* множества A и называется *булеаном*. К тому же, если на A зафиксирован порядок, то это просто декартова степень.

Теорема 1.1.3. *Возведение в степень обладает следующими свойствами:*

1. $(A \times B)^C = A^C \times B^C$

2. *если* $B \cap C = \varnothing$, *то* $A^{B \cup C} = A^B \times A^C$

3. $(A^B)^C = A^{(B \times C)}$

Доказательство. 1. $f \in (A \times B)^C \Rightarrow f : C \to (A \times B)$, $f(c) = (a, b)$. Найдем $g : C \to A$ и $h : C \to B$, такие что $f(c) = (g(c), h(c))$.

2. $f : B \cup C \to A$, $g : B \to A$, $h : C \to A$. Положим $f(x) = \begin{cases} g(x), & x \in B \\ h(x), & x \in C \end{cases}$

3. Пусть $f : B \times C \to A$, $h : C \to A^B$, $g : B \to A$, $h(c) = g$. Тогда $f(b, c) = [h(c)](b) = g(b)$.

□

Отметим свойства, связанные с возведением в степень пустого множества:

$$\begin{cases} \varnothing^A = \varnothing, & A \neq \varnothing \\ A^{\varnothing} = \{\varnothing\} \\ \varnothing^{\varnothing} = \{\varnothing\} \end{cases}$$

1.2 Мощности множеств

Зачастую (почти всегда) полезно понимать, сколько элементов содержится в рассматриваемом множестве. Интуитивно понятно, как определить количество элементов в конечном множестве, однако для бесконечных множеств способ определить что-то подобное совсем не очевиден. Этот раздел посвящен такой характеристике множества, как *мощность*, и начнем мы его с рассмотрения конечных множеств.

Определение 1.2.1. Множество A содержит в себе 0 элементов, если $A = \varnothing$. Определение k-элементного множества далее продолжим по индукции, сказав, что множество A содержит в себе k элементов, если $\forall a \in A : A \backslash \{a\}$ содержит в себе $k - 1$ элемент. Множество называется *конечным*, если оно n-эементно для некоторого натурального n.

Утверждение 1.2.0.1. Введенное определение — корректно. То есть $\forall a_1 \neq a_2 \in A$ если $A \backslash \{a_1\} n-$элементое множество, то $A \backslash \{a_2\}$ — тоже.

Доказательство. Докажем индукцией по количеству элементов в A. База индукции: $A\backslash\{a_1\} = \varnothing \Rightarrow A = \{a_1\} \Rightarrow a_2 = a_1 \Rightarrow A\backslash\{a_2\} = \varnothing$.

Шаг индукции: предположим, что $a_1 \neq a_2$. По предположению индукции, $(A\backslash\{a_1\})\backslash\{a_2\} = A\backslash\{a_1, a_2\}$ является $n-1$-элементным множеством. Аналогично $(A\backslash\{a_2\})\backslash\{a_1\} = A\backslash\{a_1,\, a_2\}$ тоже $n-1$-элементное множество. Корректность теперь следует из того, что $a_1 \in A\backslash\{a_2\}$, а $a_2 \in A\backslash\{a_1\}$. □

Теорема 1.2.1. *Если A, B — конечные множества, то в них одинаковое число элементов тогда и только тогда когда существует биекция между A и B.*

Доказательство. $\Leftarrow$: индукцией по числу элементов.

$\Rightarrow$: очевидно □

Определение 1.2.2. Два множества A, B (конечных или бесконечных) называются *равномощными*, если существует биекция между A и B. Обозначение: $|A| = |B|$.

Заметим сразу, что отношение равномощности обладает следующими свойствами, каждое из которых следует из свойств биекции и композиции функций

1. $|A| = |A|$
2. $|A| = |B| \Rightarrow |B| = |A|$
3. $|A| = |B|,\ |B| = |C| \Rightarrow |A| = |C|$

Мы не дадим формального определения *мощности* множества (или, что то же самое, его *кардинального числа*), поскольку оно требует больших знаний теории множеств. Не строго говоря, можно сказать, что мощностью множества называется его *класс эквивалентности* в отношении равномощности (определение класса эквивалентности будет дано позже).

Доказательство. Множество A *менее мощно* чем множество B, если существует $B' \subset B :\ |A| = |B'|$. *Обозначение:* $|A| \leqslant |B|$. □

Нетрудно убедиться в следующих двух свойствах сравнения множеств по мощности:

1. $|A| \leqslant |A|$

2. $|A| \leqslant |B|$, $|B| \leqslant |C| \Rightarrow |A| \leqslant |C|$

Еще одно свойство занимает особое место в теории множеств.

Теорема 1.2.2. *(Кантора-Бернштейна)*

Если $|A| \leqslant |B|$, *а* $|B| \leqslant |A|$, *то* $|A| = |B|$.

Доказательство. По условию теоремы, существует две биекции $f : A_0 = A \to B_1 \subset B$, $g : B_0 = B \to A_1 \subset A$. Определим по индукции следующие множества: $A_{i+1} = g(B_i), B_{i+1} = f(A_i), C_i = A_i \backslash A_{i+1}, D_i = B_i \backslash B_{i+1}$, $C = \bigcap A_i$, $D = \bigcap B_i$. Тогда заметим, что множества C_i и C, D_i и D попарно не пересекаются. Более того, $A = C \cup C_1 \cup C_2 \cup \ldots$, $B = D \cup D_1 \cup D_2 \cup \ldots$. Построим биекцию $h : A \to B$.

$$h(x) = \begin{cases} f(x), & x \in C \vee x \in C_{2k+1},\ k \in \mathbb{N} \\ g^{-1}(x), & x \in C_{2k+2},\ k \in \mathbb{N} \end{cases}$$

□

Определение 1.2.3. Множество A называется *счетным*, если оно равномощно $\mathbb{N}$, т.е. все его элементы можно занумеровать натуральными числами.

Утверждение 1.2.0.2. 1. Если A конечно, а B счетно, то $A \cup B$ счетно.

2. Если A, B счетны, то $A \cup B$ счетны.

3. Если A_0, A_1, $\ldots$ — счетное число счетных множество, то $\bigcup\limits_{n=0}^{\infty} A_n$ — счетно.

Доказательство. Нетрудно привести требуемые биекции в первых двух случаях. Доказательство третьего утверждения приводить здесь не будет, отметим лишь, что оно требует использование *аксиомы выбора.* □

Утверждение 1.2.0.3. $|\mathbb{N}^2| = |\mathbb{N}|$

Доказательство. Приведем явно биекцию: $F(m,\ n) = \frac{(m+n)(m+n+1)}{2} + n$. То, что это действительно биекция, проверяется разбором случаев. (своего рода это нумерация *уголком* натуральных чисел на числовой плоскости).

Замечание: приведенная биекция не единственная существующая. □

Следствие 1.2.1. $|\mathbb{N}^k| = |\mathbb{N}|$ — *индукция по* k.

Утверждение 1.2.0.4. $|\mathbb{N}^{\mathbb{N}}| \neq |\mathbb{N}|$.

Доказательство. Продемонстрируем в доказательстве этого утверждения идею, называемую *диагональный метод*:

С одной стороны ясно, что $|\mathbb{N}| \leqslant |\mathbb{N}^{\mathbb{N}}|$. Действительно, требуемая биекция есть $f(n) = \{n,\ n,\ \ldots\}$. Предположим, что $|\mathbb{N}^{\mathbb{N}}| = |\mathbb{N}|$. Занумеруем все последовательности натуральных чисел $d_0,\ d_1,\ \ldots$ и выпишем их в табличку. Пусть d_{ij} обозначает число в этой таблице, стоящее в i-той строке на j-том месте. Рассмотрим последовательность $\{x_n\}$ такую что $x_i = d_{ii} + 1$. Ясно, что это последовательность натуральных чисел, а значит, согласно нашему предположению, она имеет какой-то номер k и выписана в таблицу. С другой стороны, $x_k = d_{kk} + 1 = d_k \Rightarrow 1 = 0$. Противоречие. □

Приведенное выше утверждение показывает, что не все бесконечные множества являются счетными. Тогда встает вопрос: существует ли *наибольшая* мощность? То есть такое множество, что никакое другое множество не более мощно чем оно. Ответ на этот вопрос дает следующая теоерма.

Теорема 1.2.3. *(Кантора) Для любого множества* A *верно*

$$|2^A| > |A|$$

Доказательство. Понятно сразу, что 2^A не может быть менее мощно A, хотя бы потому что содержит в себе все одноэлементные множества. Предположим, что 2^A равномощно A и f это биекция между ними. Тогда $\forall x \in A:\ x \in f(x) \vee x \notin f(x)$. Рассмотрим множество $M = \{x \mid x \notin f(x)\} \subset A \Rightarrow \exists z \in A:\ f(z) = M$. Поступим аналогично ситуации в парадоксе Рассела и спросим себя, лежит ли z в M. Любое предположение приводит к противоречию. □

Определение 1.2.4. Множество называется *континуальным*, если оно равномощно $2^{\mathbb{N}}$.

Утверждение 1.2.0.5. $\mathbb{R}$ — континуально.

Доказательство. Любое действительное число представимо в виде бесконечной десятичной дроби. □

Лемма 1.2.4. *У любого бесконечного множества есть счетное подмножество.*

Доказательство. Выберем элемент $x \in A$ и дадим ему номер 0. Поскольку A бесконечно, то $A\backslash\{x_0\}$ тоже бесконечно. Выберем $y \in A\{x_0\}$ и дадим ему номер x_1. Будем делать так бесконечно много раз. □

Утверждение 1.2.0.6. Если A бесконечно, а B счетно, то $|A \cup B| = |A|$.

Доказательство. Пусть A' это счетное подмножество A, $T = A\backslash A'$. Тогда $A \cup B = (T \cup A') \cup B = T \cup (A' \cup B)$. Построим биекцию φ следующим образом: $\forall x \in T : \varphi(x) = x$. Далее

$$\forall x_n \in A' : \varphi(x_n) = \begin{cases} x_{\frac{n}{2}}, & 2 \mid n \\ \\ b_{\frac{n+1}{2}}, & 2 \nmid n \end{cases}.$$

□

Утверждение 1.2.0.7. $|\mathbb{R}| = |\mathbb{R}^2|$

Доказательство. Рассмотрим последовательность из нулей и единиц $a_0a_1\ldots$. Построим биекцию между $2^{\mathbb{N}}$ и $2^{\mathbb{N}} \times 2^{\mathbb{N}}$ следующим образом:

$$\varphi((a_0a_1\ldots)) = ((a_0a_2a_4\ldots), (a_1a_3a_5\ldots))$$

Ясно, что это требуемое отображение. □

Утверждение 1.2.0.8. $|\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|$

Доказательство. $|\mathbb{R}^{\mathbb{N}}| = |(2^{\mathbb{N}})^{\mathbb{N}}| = |2^{\mathbb{N}\times\mathbb{N}}| = |2^{\mathbb{N}}| = |\mathbb{R}|$ □

Утверждение 1.2.0.9. $|2^{\mathbb{R}}| = |\mathbb{R}^{\mathbb{R}}|$

Доказательство. $|\mathbb{R}^{\mathbb{R}}| = |(2^{\mathbb{N}})^{\mathbb{R}}| = |2^{\mathbb{N}\times\mathbb{R}}|$. Теперь покажем, что $\mathbb{N} \times \mathbb{R}$ равномощно $\mathbb{R}$:

$$|\mathbb{R}| = |\{1\} \times \mathbb{R}| \leqslant |\mathbb{N} \times \mathbb{R}| \leqslant |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$$

□

1.3 Отношения на множествах

Определение 1.3.1. *Свойством* называется произвольное подмножество A. *Бинарным отношением* называется любое подмножество A^2. Предикатом валентности k называется любое подмножество A^k. Будем рассматривать далее бинарные отношения. Пусть на A определено бинарное отношение R. Тогда будем писать xRy вместо $(x,\ y) \in R$.

Определение 1.3.2. Отношения бывают следующих видов

1. Рефлексивные: $\forall x \in A : xRx$. Примеры: равенство, подобие треугольников, быть подмножеством.
2. Симметричные $xRy \Rightarrow yRx$. Примеры: равенство, подобие, равномощность.
3. Антисимметричные $xRy \wedge yRx \Rightarrow x = y$. Примеры: быть подмножеством, отношение делимости на натуральных числах.
4. Транзитивные $xRy \wedge yRz \Rightarrow xRz$. Примеры: равенство, подобие треугольников.
5. Антитранзитивность $xRy \wedge yRz \Rightarrow \neg xRz$. Пример: xRy если x отец y.

Определение 1.3.3. Отношение называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Определение 1.3.4. Если на множестве A определено отношение эквивалентности $\sim$, то *классом эквивалентности* элемента $x \in A$ называется множество $K_x = \{a \in A : x \sim a\}$

Теорема 1.3.1. *(основная теорема об отношении эквивалентности)*

Если $\sim$ отношение эквивалентности на A, то тогда $A = \bigsqcup A_i$ таких что

1. $i \neq j \Rightarrow A_i \cap A_j = \varnothing$
2. $A_i \neq \varnothing$
3. $x \in A_i,\ y \in A_j,\ i \neq j \Rightarrow x \nsim y$
4. $x,\ y \in A_i \Rightarrow x \sim y$
5. $x \in A_i \Rightarrow A_i = K_x$

Доказательство. Сначала заметим, что $x \in K_x$ по рефлексивности. Далее, по транизитивности, $y \in K_x \Rightarrow K_y = K_x$. Отсюда в частности следует, что если $K_x \cap K_y \neq \varnothing$, то $K_x = K_y$. Тогда, положив A_i различными классами эквивалентности, получаем требуемое. □

Определение 1.3.5. *Фактор-множеством* называется множество всех классов эквивалентности.

Определение 1.3.6. Отношение называется отношением *частичного порядка*, если оно рефлексивно, антисимметрично и транзитивно. *Упорядоченным множеством* называется пара $(A, \leqslant_A)$ — множество и частичный порядок на нем.

Определение 1.3.7. *Изоморфизмом* упорядоченных множеств A и B называется биекция $f : A \to B$, сохраняющаяя порядок, т.е.

$$x \leqslant_A y \iff f(x) \leqslant_B f(y)$$

Множества называются изоморфными, если между ними существует изоморфизм. Обозначение: $A \simeq B$.

Определение 1.3.8. Частичный порядок называется *линейным порядком*, если любые два различных элемента множества сравнимы.

Определение 1.3.9. Элемент $x \in A$ называется *наибольшим*, если $\forall y \in A : \ y \leqslant x$. Элемент x называется *максимальным*, если не существует $a \in A : \ y > a$. Заметим сразу, что если x — наибольший, то он и максимальный. Обратное не верно.

Определение 1.3.10. Отношение называется отношением *строгого* порядка, если оно транзитивно и антирефлексивно.

Определение 1.3.11. Линейный порядок называется *плотным*, если $x < y \Rightarrow \exists z : \ x < z < y$.

Теорема 1.3.2. *Любые два счетных плотно линейно упорядоченных множества без наибольшего и наименьшего элементов изоморфны.*

Доказательство. Занумеруем $A = \{a_0, \ a_1, \ \ldots\}$, $B = \{b_0, \ b_1, \ \ldots\}$. Начнем строить изоморфизм f. Для начала, $f(a_0) = b_0$. Далее, пусть выбраны уже $f(a_0), \ \ldots, \ f(a_{n-1})$.

1. $a_n > \max\{a_0, \ \ldots, \ a_{n-1}\} \Rightarrow f(a_n) = b_{k(n)}$, где $k(n) = \min\{k : \ b_k > \max\{f(a_0), \ \ldots, \ f(a_{n-1})\}\}$
2. $a_n < \min\{a_0, \ \ldots, \ a_{n-1}\} \Rightarrow f(a_n) = b_{p(n)}$, где $p(n) = \min\{k : \ b_k < \min\{f(a_0), \ \ldots, \ f(a_{n-1})\}\}$
3. $a_j < a_n < a_i$, где $i, \ j < n$ и i это номер наибольшего a из выбранных, меньших чем a_n, а j — наименьшего a из выбранных, больших чем a_n. Тогда положим $f(a_n) = b_{m(n)}$, где $m(n) = \min\{m : \ f(a_i) < b_m < f(a_j)\}$

В первых двух случаях мы гарантированно найдем нужный b в силу того, что порядки не имеют наибольних и наименьшиъ элементов. В 3 случае используется плотность порядка.

По определению, f сохраняющая порядок инъекция. Докажем, что f это сюръекция. Пусть b_t такое, что t — минимальный номер элемента, которому ничего не соответствует. Пусть s таково, что если $f(a_n) \in \{b_0, \ldots, b_{t-1}\}$, то $n < s$. Зафиксируем s.

1. Если $b_t > \max\{f(a_0), \ldots, f(a_s)\}$ то $\exists p : a_p > \max\{a_0, \ldots, a_s\}$. Положим $p_m = \min\{p\} \Rightarrow f(a_{p_m}) = b_t$.

2. Если $b_t < \min\{f(a_0), \ldots, f(a_s)\}$ то $b_t = f(a_{p_m})$ где $p_m = \min\{q\, a_q < \min\{a_0, \ldots, a_s\}$.

3. Если $a_i < b_t < a_j$, то в качестве p_m можно взять наименьший номер элемента между a_i и a_j.

Из всего вышесказанного следует что $f(a_{p_m}) = b_t$ и f это сюръекция, а значит и биекция. $\square$

Глава 2

Комбинаторика

2.1 Основы комбинаторики

2.1.1 Базовые принципы

Предположим, что у нас имеются 2 множества (здесь и далее предполагаем, что рассматриваемые множества *конечны*, если не оговорено обратного) $A = \{a_1, a_2, \ldots, a_n\}$, $B = \{b_1, b_2, \ldots, b_m\}$.

1. *Правило суммы:* Количество способов выбрать один объект из A *или* B (в предположении, что $A \cap B = \varnothing$) равно $n + m$.

2. *Правило произведения:* Количество способов выбрать один объект из A и к нему в пару один объект из B равно nm.

3. *Принцип Дирихле:* Предположим, имеется n ящиков и $n+1$ кролик, которые сидят в этих ящиках. Тогда найдется ящик, в котором сидит $\geqslant 2$ кролика.

   Обобщенный принцип Дирихле: Если $nk+1$ разбит на n множеств, то хотя бы в одном множестве содержится $k + 1$ элемент.

Рассмотрим две задачи, иллюстрирующие принцип Дирихле:

Задача 1. Дан квадрат 2×2 и 5 точек внутри него. Необходимо доказать, что среди этих 5 точек найдется 2 такие, что расстояние между ними $\leqslant \sqrt{2}$.

Решение: Рассмотрим 4 квадратика 1×1. По принципу Дирихле, найдется квадратик, внутри или на границе которого 2 точки. Эти точки — искомые. $\square$

Задача 2. Пусть $\overline{x} = (x_1, \ldots, x_n)$ — последовательность чисел. Определим скалярное произведение $(\overline{x}, \overline{y}) = x_1y_1 + \ldots + x_ny_n$ стандартным образом. Рассмотрим множество

$$V = \{\overline{x} = (x_1, \ldots, x_8) : x_i \in \{-1, 0, 1\}, |\{i : x_i = \pm 1\}| = 4\}.$$

Пусть W это произвольное подмножество V, в котором никакие 2 вектора не имеют нулевое скалярное произведение. Вопрос: $|W| \leqslant ?$.

Решение: Разобьем множество V на подмножества-ящики. Первый ящик:

$$(1, 1, 1, 1, 0, 0, 0, 0)$$

$$(1, -1, -1, 1, 0, 0, 0, 0)$$

$$(1, -1, 1, -1, 0, 0, 0, 0)$$

$$(1, 1, -1, -1, 0, 0, 0, 0)$$

$$(0, 0, 0, 0, 1, 1, 1, 1)$$

$$(0, 0, 0, 0, 1, -1, -1, 1)$$

$$(0, 0, 0, 0, 1, -1, 1, -1)$$

$$(0, 0, 0, 0, 1, 1, -1, -1)$$

Второй ящик:

$$(1,\ -1,\ -1,\ -1,\ 0,\ 0,\ 0,\ 0)$$

$$(1,\ -1,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0)$$

$$(1,\ 1,\ -1,\ 1,\ 0,\ 0,\ 0,\ 0)$$

$$(1,\ 1,\ 1,\ -1,\ 0,\ 0,\ 0,\ 0)$$

$$(0,\ 0,\ 0,\ 0,\ 1,\ -1,\ -1,\ -1)$$

$$(0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ -1)$$

$$(0,\ 0,\ 0,\ 0,\ 1,\ 1,\ -1,\ 1)$$

$$(0,\ 0,\ 0,\ 0,\ 1,\ -1,\ 1,\ 1)$$

В качестве третьего "ящика"можно взять вектора из 1-го, умноженные на -1, а для четвертого — вектора второго. Нетрудно проверить, что любые 2 вектора из одного ящика компланарны. Таким образом, для каждой расстановки четырех нулей на 8 позиций-координат есть, своего рода, расстановка-дополнение, и каждой паре таких расстановок соответствует четыре ящика. Найдем количество ящиков.

Выбрать позиции для нулей — 70 способов (это будет позже понято). Значит, имеется 35 способов выбрать четверку нулей, а ящиков тогда $35 \cdot 4 = 140$. Два вектора не могут быть в одном ящике, а значит $|W| \leqslant 140$. □

2.1.2 Сочетания, размещения и перестановки

Пусть дано множество $A = \{a_1,\ \dots a_n\}$ из n объектов.

Определение 2.1.1. Произвольный *упорядоченный* набор (кортеж) из k элементов данного множества, среди которых *могут быть повторяющиеся*, называется размещением из n элементов по k с повторением. Соответственно, если элементы не могут повторяться, то набор называется размещением без повторений, или просто размещением из n по k.

Определение 2.1.2. Сочетанием из n элементов по k называется набор k элементов этого множества. Наборы, отличающиеся *только порядком* следования элементов считаются одинаковыми (этим

сочетание отличается от размещения). Соответственно, сочетания бывают с повторениями и без, в зависимости от того, разрешаем ли мы элементам набора повторяться или нет.

Обозначим за A_n^k, $\overline{A}_n^k$, C_n^k, $\overline{C}_n^k$ соответственно количество размещений без повторений, с повторениями, сочетаний без повторений и сочетаний с повторениями. Тогда справедлива следующее утверждение.

Утверждение 2.1.2.1.

$$\begin{aligned}
\overline{A}_n^k &= n^k \\
A_n^k &= \frac{n!}{(n-k)!} \\
C_n^k &= \frac{n!}{k!(n-k)!} \\
\overline{C}_n^k &= C_{n+k-1}^k
\end{aligned}$$

Доказательство. Первые три равенства достаточно очевидны. Докажем, для примера, второе из них: количество способов выбрать первый элемент размещения равно $|A| = n$. Количество способов выбрать второй элемент y равно $|A\backslash\{x\}| = n-1$, где x это первый выбранный элемент. По правилу умножения, количество способов выбрать пару элементов $(x,\ y)$ ровно $n(n-1)$. Рассуждая далее так же, получим требуемое равенство.

Покажем четвертое равенство. Зафиксируем некоторое сочетание с повторениями $(a_1,\ \ldots a_k)$ (некоторые элементы сочетания могут повторяться). Построим теперь последовательность из 0 и 1 по следующему правилу: вначале напишем 1 столько раз, сколько элемент a_1 встречается в сочетании (возможно, 0). После, поставим 0 и напишем 1 столько раз, сколько в сочетании встречается a_2 и так далее. В конце последовательности будет идти 1 столько раз, сколько в сочетании встречается a_n и 0 в конце ставить не будем. Легко понять, что по описанному алгоритму две одинаковые последовательности из 0 и 1 получаются только для совпадающих сочетаний. Заметим, что в каждой такой последовательности ровно k единиц и $n-1$ ноль. Значит, описанное выше отображение это биекция между сочетаниями с повторениями из n по k и последовательностями из 0 и 1 длины $n+k-1$ и содержащих ровно k единиц. Таких последовательностей ровно C_{n+k-1}^k □

Утверждение 2.1.2.2. 1. $C_n^k = C_n^{n-k}$

2. $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$

3. $C_n^0 + C_n^1 + \ldots + C_n^n = 2^n$

4. $(C_n^0)^2 + (C_n^1)^2 + \ldots + (C_n^n)^2 = C_{2n}^n$

Доказательство. 1. Выбрать k объектов из n это тоже самое, что отметить $n-k$ объектов, которые не будут выбранны.

2. Рассмотрим множество $A = \{a_1, \ldots, a_n\}$. Количество k-сочетаний, содержащих a_1 равно C_{n-1}^{k-1} (т.к. необходимо выбрать еще $k-1$ элемент из оставшегося множества $\{a_2, \ldots, a_n\}$). Количество k-сочетаний, не содержащих a_1, равно C_{n-1}^k . Тогда количество всех сочетаний $C_n^k = C_n^{k-1} + C_{n-1}^{k-1}$

3. Число всех подмножеств n-элементного множества, очевидно, равно 2^n. С другой стороны, для каждого фиксированного $k \leqslant n$ число k-элементных подмножеств равно C_n^k .

4. Рассмотрим множество $A = \{a_1, \ldots, a_n, a_{n+1}, \ldots, a_{2n}\}$. Всего n-сочетаний ровно C_{2n}^n . С другой стороны, пусть k это число элементов в сочетании из множества $\{a_1, \ldots, a_n\}$. Тогда из второй половины множества A необходимо выбрать $n-k$ элементов, а количество n-сочетаний равно

$$C_{2n}^n = \sum_{k=0}^{n} C_n^k \, C_n^{n-k} = \sum_{k=0}^{n} (C_n^k)^2.$$

□

Задача: Пусть $A = \{1, \ldots, 30\}$, $M_1, \ldots, M_{15}$ — пятиэлементные сочетания без повторений из A. Верно ли, что элементы множества A можно раскрасить в два цвета так, чтобы для любых $M_1, \ldots, M_{15}$ каждое M_i было неодноцветно.

Решение: Всего раскрасок множества A в два цвета 2^{30}. Количество раскрасок, при которых одно конкретное M_i одноцветно есть $2 \cdot 2^{25} = 2^{26}$, т.к. нужно покрасить 25 элементов в 2 цвета 2^{25} способами, а потом в один из двух цветов элементы M_i. Тогда, количество раскрасок, при которых хотя бы одно из M_i одноцветно явно $< 15 \cdot 2^{26}$ (например, множества раскрасок при которых некоторые M_i одноцветны пересекаются по раскраске всех 30 элементов в один цвет). Очевидно, что $15 \cdot 2^{26} < 2^{30}$, а значит ответ на задачу *да*. □

Рассмотрим обобщение данной задачи. Положим $m(n) := \min\{s \in \mathbb{N} : \exists M_1, \ldots, M_s; \forall i\ |M_i| = n, \forall$ раскраски $M_1 \cup M_2 \cup \ldots \cup M_s$ в 2 цвета $\exists i : M_i$ одноцветно$\}$ (для примера, $m(2) = 3$). Решение в общем случае неизвестно, но получены следующие оценки:

$$\frac{1}{\sqrt{2}} \cdot \left(\frac{n}{\ln n}\right)^{1/2} 2^n \leqslant m(n) \leqslant \frac{e \ln 2}{4}(1 + \varphi(n))n^2 2^n$$

где $\varphi(n) \to 0$ при $n \to \infty$.

Предположим, что у нас имеется n_1 объект вида a_1, n_2 объектов вида a_2 ... n_k объектов вида a_k. Положим $n := n_1 + \ldots + n_k$. Обозначим за $P(n_1, \ldots, n_k)$ количество всевозможных перестановок, которые можно получить из этих n объектов.

Утверждение 2.1.2.3.

$$P(n_1, \ldots, n_k) = \frac{n!}{n_1! n_2! \ldots n_k!}.$$

Доказательство.

$$P(n_1, \ldots, n_k) = C_n^{n_1}\ C_{n-n_1}^{n_2}\ \ldots C_{n-n_1-\ldots-n_{k-1}}^{n_k}\ = \frac{n!}{n_1! n_2! \ldots n_k!}$$

□

Заметим, что справедлива *полиномиальная формула*

$$(x_1 + \ldots + x_k)^n = \sum_{\substack{(n_1, \ldots, n_k) \\ n_1 + \ldots + n_k = n}} P(n_1, \ldots, n_k) x_1^{n_1} \ldots x_k^{n_k}.$$

Действительно, $(x_1 + \ldots + x_k)^n = (x_1 + \ldots + x_n) \ldots (x_1 + \ldots + x_n)$. Каждый одночлен вида $x_1^{n_1} \ldots x_k^{n_k}$ встречается ровно $P(n_1, \ldots, n_k)$ т.к. необходимо выбрать n_1 различных скобок, из которых в произведение *идет* x_1, n_2 скобок для x_2 и так далее.

Следствие 2.1.1. $\sum\limits_{\substack{n_i \in \{0, \ldots, n\} \\ n_1 + \ldots + n_k = n}} P(n_1, \ldots, n_k) = k^n$

Утверждение 2.1.2.4. $C_{n+m}^n\ = C_{n+m-1}^{n-1}\ + C_{n+m-2}^{n-1}\ + \ldots + C_{n-1}^{n-1}$

Доказательство. Рассмотрим $n+1$ элементное множество. Количество m-сочетаний с повторениями из его элементов равно $\overline{C}_{n+1}^m = C_{n+m}^m\ = C_{n+m}^n$. С другой стороны, в каждом сочетании с повторениями, элемент a_1 встречается от 0 до m раз. Количество сочетаний с повторениями, в которых a_1 встречается ровно k раз равно $\overline{C}_{n-1}^{m-k} = C_{n+m-k-1}^{n-1}$. Суммируя по k от 0 до m получаем требуемое. □

Следствие 2.1.2. *1.* $n = 1$*: формула примет вид*

$$m + 1 = C_{m+1}^1 = C_m^0 + \ldots + C_0^0 = 1 + \ldots + 1$$

2. $n = 2$*:*

$$C_{m+2}^2 = C_{m+1}^1 + C_m^1 + \ldots + C_1^1$$
$$\frac{(m+1)(m+2)}{2} = (m+1) + m + (m-1) + \ldots + 2 + 1$$

а значит мы доказали формулу для суммы первых m *натуральных чисел.*

3. $n = 3$*:*

$$C_{m+3}^3 = C_{m+2}^2 + \ldots + C_2^2$$
$$\frac{(m+3)(m+2)(m+1)}{6} = \frac{(m+1)(m+2)}{2} + \frac{m(m+1)}{2} + \ldots + \frac{1 \cdot 2}{2} =$$
$$= \frac{(m+1)^2}{2} + \frac{m+1}{2} + \frac{m^2}{2} + \frac{m}{2} + \ldots + \frac{1^2}{2} + \frac{1}{2} =$$
$$= \frac{1}{2}\Big(1 + 2 + \ldots + (m+1) + 1^2 + 2^2 + \ldots + (m+1)^2\Big) =$$
$$= \frac{1}{2}\Big(\frac{(m+1)(m+2)}{2} + 1^2 + 2^2 + \ldots + (m+1)^2\Big) \Rightarrow$$
$$1^2 + 2^2 + \ldots + (m+1)^2 = \frac{(m+3)(m+2)(m+1)}{6} - \frac{(m+1)(m+2)}{2} = \frac{(m+1)(m+2)(2m+3)}{6}$$

то есть сумма квадратов первых m *натуральных чисел равна* $\dfrac{m(m+1)(2m+1)}{6}$

Продолжая дальше, можно получить формулу для суммы любых степеней первых натуральных чисел.

Утверждение 2.1.2.5. $C_n^0 - C_n^1 + C_n^2 - \ldots + (-1)^n C_n^n = \begin{cases} 1, & n = 0 \\ 0, & n > 0 \end{cases}$

Доказательство. $0 = (1-1)^n = \sum\limits_{k=0}^{n} C_n^k \, (-1)^k 1^{n-k}$ □

2.1.3 Формула включений и исключений

Теорема 2.1.1. *Пусть имеется множество из* N *объектов и некоторые свойства* $\alpha_1, \ldots, \alpha_n$*. Обозначим* α_k' *отрицание свойства* α_k*, т.е. элемент* a *удовлетворяет* α_k' *тогда и только тогда, когда он не удовлетворяет* α_k*. Пусть* $N(\alpha_i)$ *обозначает количество объектов, удовлетворяющих свойству*

α_i), $N(\alpha_i,\, \alpha_j)$ — *удовлетворяющих одновременно обоим свойствам* α_i, α_j ... $N(\alpha_1,\, \ldots,\, \alpha_n)$ — *удовлетворяющих всем свойствам. Тогда справедлива следующая формула, называемая формулой включений и исключений:*

$$N(\alpha_1',\, \alpha_2',\, \ldots \alpha_n') = N - N(\alpha_1) - \ldots - N(\alpha_n) + N(\alpha_1,\, \alpha_2) + \ldots + \\ + N(\alpha_{n-1},\, \alpha_n) - \ldots + (-1)^n N(\alpha_1,\, \ldots,\, \alpha_n)$$

Доказательство. Индукция по числу свойств. Для $n = 1 : N(\alpha_1') = N - N(\alpha_1)$. База доказана. Докажем переход индукции.

Предположим, что для всех $1 \leqslant k \leqslant n$ верно, что для любого N, любого множества из N объектов и любого набора свойств $\alpha_1, \ldots \alpha_k$ выполнена формула из условия теоремы. Рассмотрим только свойства $\alpha_1,\, \ldots,\, \alpha_n$. По предположению индукции, для них верна формула включений и исключений. (1)

Рассмотрим теперь только те объекты, которые обладают свойством α_{n+1}. К ним применимо предположение индукции (для $N = N(\alpha_{n+1})$), т.е.

$$N(\alpha_1',\, \ldots,\, \alpha_n',\, \alpha_{n+1}) = N(\alpha_{n+1}) - N(\alpha_1,\, \alpha_{n+1}) - \ldots + (-1)^n N(\alpha_1,\, \ldots,\, \alpha_n,\, \alpha_{n+1}). \text{ — (2)}$$

Имеем теперь, вычитая (2) из (1)

$$N(\alpha_1',\, \ldots,\, \alpha_n') - N(\alpha_1',\, \ldots,\, \alpha_n',\, \alpha_{n+1}) = N(\alpha_1',\, \ldots,\, \alpha_{n+1}') =$$

$$= N - N(\alpha_1) - \ldots - N(\alpha_n) + N(\alpha_1,\, \alpha_2) + \ldots + N(\alpha_{n-1},\, \alpha_n) - \ldots + (-1)^{n+1} N(\alpha_1,\, \ldots,\, \alpha_n,\, \alpha_{n+1})$$

□

Следствие 2.1.3. $\sum\limits_{k=0}^{n} C_n^k\ (-1)^k (n-k)^m = 0,\ m < n$

Доказательство. Рассмотрим $\{a_1,\, \ldots,\, a_n\}$ и выберем все $\overline{A}_n^m$ размещения из n по m с повторениями. Объектами, к которым будем применять формулу включений-исключений будем считать эти размещения, т.е. $N = n^m$. Скажем, что размещение обладает свойством α_i, если оно не содержит a_i.

$$N(\alpha_i) = (n-1)^m \qquad N(\alpha_i,\, \alpha_j) = (n-2)^m$$

$$N(\alpha_1',\, \ldots,\, \alpha_m') = 0, \text{ так как } m < n$$

Применяя формулу включений-исключений, получаем требуемое равенство. □

Следствие 2.1.4. *(задача о беспорядках)*

Рассмотрим следующую задачу: имеется n человек и n мест в аудитории. Сколько имеется способов рассадить людей так, чтобы никто не сидел на своем месте?

Решение: В качестве объектов будем рассматривать перестановки людей $N = n!$. Пусть α_i означает, что i-тый человек при данной перестановки сидит на своем месте. Тогда

$$N(\alpha'_1, \ldots, \alpha'_n) = n! - C_n^1\ (n-1)! + C_n^2\ (n-2)! - \ldots + (-1)^n C_n^n\ 0! = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n \frac{1}{n!})$$

Устремляя $n \to \infty$, получаем ответ $\frac{n!}{e}$. □

2.2 Функция Мёбиуса

2.2.1 Функция Мёбиуса и ее свойства

Определение 2.2.1. Функция Мёбиуса $\mu : \mathbb{N} \to \mathbb{N}$ определена следующим образом:

$$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^s, & n = p_1 p_2 \ldots p_s \\ 0, & \text{иначе} \end{cases}$$

Утверждение 2.2.1.1. Сумма значений функции Мёбиуса на делителях числа, отличного от единицы, равна 0.

$$\sum_{d\,|\,n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n \geqslant 2 \end{cases}$$

Доказательство. Случай $n = 1$ очевиден. Предположим теперь, что $n \geqslant 2$. Тогда $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$. Если $d \mid n$, то тогда $d = p_1^{\beta_1} \ldots p_s^{\beta_s}$, $\forall i \quad 0 \leqslant \beta_i \leqslant \alpha_i$.

Если $\beta_i \geqslant 2$, то, по определению функции Мёбиуса, $\mu(d) = 0$. Исходя из этих соображений, перепишем сумму:

$$\sum_{d\,|\,n} \mu(d) = \sum_{\substack{d = p_1^{\beta_1} \ldots p_s^{\beta_s} \\ \forall i\ 0 \leqslant \beta_i \leqslant 1}} \mu(d) = \sum_{k=0}^{s} \sum_{\substack{d = p_1^{\beta_1} \ldots p_s^{\beta_s} \\ \text{ровно } k \text{ из } \beta_i \text{ равны } 1}} \mu(d) = \sum_{k=0}^{s} (-1)^k C_s^k$$

□

Утверждение 2.2.1.2.

$$\varphi(n) = \sum_{d \mid n} \mu(\tfrac{n}{d})d$$

где $\varphi(n)$ это *функция Эйлера*, т.е. количество натуральных чисел, меньших n и взаимно простых с n.

Доказательство. Заметим, что утверждение 2.2.1.1 можно переписать как $\sum\limits_{d \mid n} \mu(d) = \lfloor \frac{1}{n} \rfloor$. Обозначим наибольший общий делитель чисел n и k как $(n,\ k)$. Имеем

$$\varphi(n) = \sum_{k=1}^{n} \lfloor \frac{1}{(n,\ k)} \rfloor = \sum_{k=1}^{n} \big(\sum_{d \mid (n,\ k)} \mu(d) \big) = \sum_{k=1}^{n} \sum_{\substack{d \mid n \\ d \mid k}} \mu(d) =$$

$$= \sum_{d \mid n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d \mid n} \mu(d) \big(\sum_{q=1}^{n/d} 1 \big) = \sum_{d \mid n} \mu(d) \frac{n}{d}$$

□

Теорема 2.2.1. *(формула обращений Мёбиуса)*

Пусть $f : \mathbb{N} \to \mathbb{R}$, $g : \mathbb{N} \to \mathbb{R}$ *две функции, причем* $f(n) = \sum\limits_{d \mid n} g(d)$. *Тогда*

$$g(n) = \sum_{d \mid n} \mu(d) f(\frac{n}{d}) = \sum_{d \mid n} \mu(\frac{n}{d}) f(d) \qquad (1)$$

Доказательство. Преобразуем сумму справа от знака равенства в *(1)*:

$$\sum_{d \mid n} \mu(d) f(\frac{n}{d}) = \sum_{d \mid n} \mu(d) \big(\sum_{d' \mid \frac{n}{d}} g(d') \big) =$$

$$= \sum_{dd' \mid n} \mu(d) g(d') = \sum_{dd' \mid n} \mu(d') g(d) =$$

$$= \sum_{d \mid n} g(d) \big(\sum_{d' \mid \frac{n}{d}} \mu(d') \big) =$$

$$= g(n) \sum_{d' \mid 1} \mu(d') + \sum_{\substack{d \mid n \\ d < n}} g(d) \big(\sum_{d' \mid \frac{n}{d}} \mu(d') \big) = g(n)$$

□

2.2.2 Количество циклических последовательностей

Приведем пример использования формулы обращения Мёбиуса. Пусть дано множество $\{b_1,\ \ldots,\ b_r\}$, которые мы будем называть *алфавитом*. Словом длины n назовем произвольное n-размещение с повторениями из элементов алфавита (таким образом, слов длины n ровно r^n).

Скажем, что слово $a_1a_2\dots a_n$ является *циклическим*, если мы отождествляем все слова $a_1a_2\dots a_n = a_2a_3\dots a_{n-1}a_n = \dots = a_na_1\dots a_{n-1}$. Например, в алфавите из букв { Ж, А, Б } есть циклическое слово ЖАБА = АБАЖ = БАЖА = АЖАБ. Обозначим за $T_n(r)$ количество всех различных циклических слов длины n в алфавите из r символов. Задача: найти это число.

Решение: Назовем *периодом* циклического слова такое $\min d \geqslant 1$, что после d циклических сдвигов на 1 символ слово переходит в себя.

Лемма 2.2.2. *Любой период d делит n.*

Доказательство. Предположим, что $n = dq + r$, $0 < r < d$. Тогда сдвинем слово q раз на d символов. Оно перешло в само себя. Сдвинем теперь слово на r символов. Так как всего мы сдвинули слово на n символов, то оно перешло само в себя, а значит r — минимальное число, после которого слово переходит в само себя. Противоречие с определением периода. □

Следствие 2.2.1. *Любая циклическая последовательность длины n и периода d имеет вид*

$$A = a_1a_2\dots a_da_1\dots a_d\dots a_1\dots a_d$$

т.е. состоит из $\frac{n}{d}$ повторяющихся блоков длины d. Это следует из предыдущей леммы и того факта, что после d сдвигов буква a_i переходит в a_{d+i}.

Пусть V это множество всех линейных последовательностей (т.е. не циклических. Например, ЖАБА и БАЖА считаются разными) длины n. Положим $d_1, \dots d_s$ — все делители n. Тогда $V = V_1 \sqcup V_2 \sqcup \dots \sqcup V_s$, где V_i — множество линейных последовательностей с периодом d_i.

Положим $W_i :=$ множество всех линейных последовательностей длины d_i и периода d_i. Из следствия 2.2.1 следует, что $|V_i| = |W_i|$. Пусть $U_i :=$ множество циклических последовательностей, которые получаются из последовательностей W_i циклическим сдвигом. Тогда

$$d_i|U_i| = |W_i|$$

Рассмотрим функцию $m(d_i) = |U_i|$. Для нее верно, что $d_im(d_i) = |W_i|$, а значит

$$r^n = d_1m(d_1) + \dots + d_sm(d_s) = \sum_{d\,|\,n} d \cdot m(d)$$

Рассмотрим функции $f(n) := r^n$, $g(n) := n \cdot m(n)$ и применим к ним формулу обращения Мёбиуса. Тогда

$$n \cdot m(n) = \sum_{d \mid n} \mu(d) r^{\frac{n}{d}} \Rightarrow m(n) = \frac{1}{n} \sum_{d \mid n} \mu(d) r^{\frac{n}{d}}$$

По следствию 2.2.1 циклические последовательности длины n и периода d отождествляются с последовательностями длины d и периода d,а значит

$$\begin{aligned} T_r(n) = \sum_{d \mid n} m(d) &= \sum_{d \mid n} \frac{1}{d} \Big(\sum_{d' \mid d} \mu(d') r^{\frac{d}{d'}} \Big) = \\ &= \sum_{\substack{d \mid n \\ d' \mid d}} \frac{r^{\frac{d}{d'}}}{\frac{d}{d'}} \frac{\mu(d')}{d'} = [k := \frac{d}{d'}] = \\ &= \sum_{d' k \mid n} \frac{r^k}{k} \frac{\mu(d')}{d'} = \sum_{k \mid n} \frac{r^k}{k} \sum_{d' \mid \frac{n}{k}} \frac{\mu(d')}{d'} = \\ &= \sum_{k \mid n} \frac{r^k}{k} \frac{\varphi(\frac{n}{k})}{\frac{n}{k}} = \frac{1}{n} \sum_{k \mid n} r^k \varphi(\frac{n}{k}) \end{aligned}$$

где φ — функция Эйлера. □

2.2.3 Обращение Мёбиуса на ЧУМах

Напомним, что частично упорядоченным множеством называется пара $(A, \leq_A)$ — множество и частичный порядок на нем.

Определение 2.2.2. Пусть дан ЧУМ $(P, \leq_P)$.Определим функцию Мёбиуса $\mu(x, y)$; $x \leq y$ на нем следующим образом:

1. $\mu(x, x) = 1$
2. $\mu(x, y) = -\sum\limits_{x \leq z < y} \mu(x, z)$ для $x \prec y$.

Утверждение 2.2.3.1. Рассмотрим ЧУМ $(\mathbb{N}, \mid)$. Тогда, если $d \mid n$, то $\mu(\frac{n}{d}) = \mu(d, n)$, т.е. определение обощенной функции Мёбиуса корректно.

Доказательство. Достаточно показать, что $\mu(1, n) = \mu(n)$ (диаграммы Хассе). Покажем это

1. $n = 1 :\ \mu(1) = 1 = \mu(1, 1)$
2. $n = p$ — простое. Тогда $\mu(p) = -1 = -\mu(1, 1) = \mu(1, p)$
3. $n = p^2$. Тогда $\mu(p^2) = 0$; $\mu(1, p^2) = -(\mu(1,1) + \mu(1, p)) = 0$. Аналогично для степеней $\geqslant 2$.

4. $n = p_1 p_2 \dots p_s$, $\mu(n) = (-1)^s$. Докажем, что $\mu(1,\ n) = (-1)^s$ индукцией по s. База при $s = 1$ уже доказана. Переход:

$$\mu(1,\ p_1 p_2 \dots p_s) = -\big(\mu(1,\ 1) + \mu(1,\ p_1) + \dots + \mu(1,\ p_1) + \mu(1,\ p_1 p_2) + \dots + \mu(1,\ p_{s-1} p_s) + \\ + \dots + \mu(1,\ p_1 \dots p_{s-1}) + \dots + \mu(1,\ p_2 \dots p_s)\big) = -\left(1 - C_s^1\ + C_s^2\ - \dots + (-1)^{s-1} C_s^{s-1}\ \right)$$

Заметим, что если к выражению в скобках прибавить $(-1)^s C_s^s\ = (-1)^s$, то вся сумма будет равна 0. А значит выражение в скобках равно $(-1)^{s+1}$. Что и требовалось.

5. $\gcd(n,\ m) = 0 \Rightarrow \mu(1,\ nm) = \mu(1,\ n) \cdot \mu(1,\ m)$ — без доказательства.

□

Теорема 2.2.3. *(Обобщенная формула обращения Мёбиуса, б/д)*

Пусть $(P,\ \preceq_P)$ — *ЧУМ, причем каждый его элемент имеет лишь конечное число предшественников. Пусть даны две функции* $g : P \to \mathbb{R}$ *и* $f : P \to \mathbb{R}$, $f(y) = \sum\limits_{x \preceq y} g(x)$. *Тогда*

$$g(y) = \sum_{x \preceq y} \mu(x,\ y) f(x)$$

Приведем пример использования обобщенной формулу обращения Мёбиуса. Сначала опишем ЧУМ $(P,\ \preceq_P)$.

Рассмотрим произвольные множества $S_1, \dots, S_n$ конечной мощности и $\Omega := S_1 \cup \dots \cup S_n$. Рассмотрим произвольное индексное множество $J \subseteq \{1,\ \dots n\}$. Тогда определим элемент ЧУМа $P = \bigcap\limits_{j \in J} S_j$ (для $J = \varnothing$ положим $P := \Omega$). Как множества некоторые элементы ЧУМа могут совпадать, но мы все равно будем различать их по множеству индексов J, из которого они получились. Скажем, что $P \preceq P' \Leftrightarrow J' \subseteq J$.

Пусть $f : P \to \mathbb{R}$, $f(P) = |P|$ и $g : P \to \mathbb{R}$, $g(P) =$ количество элементов из P, которые не принадлежат ни одному $P' \preceq P$.

Утверждение 2.2.3.2. $f(P) = \sum\limits_{P' \preceq P} g(P')$ — очевидно из определения ЧУМ и функций f, g.

Применим формулу обращения Мёбиуса. Тогда $g(P) = \sum\limits_{P' \preceq P} \mu(P',\ P) f(P')$

Утверждение 2.2.3.3. $\mu(P',\ P) = (-1)^{|J| - |J'|}$

Доказательство. Индукция по $k := |J| - |J'|$. База для $k = 0$ очевидна. Предположим, что утверждение верно для $k = n$ и докажем для $k = n + 1$.

Пусть $P \preceq P'' \prec P' \Rightarrow J' \subset J'' \subseteq J$. Пусть $J' = \{i_1, \ldots, i_s\}$, $J = \{i_1, \ldots, i_s, j_1, \ldots, j_{n+1}\}$. Тогда $J'' = \{i_1, \ldots, i_s\} \cup I$, где $\varnothing \subset I \subseteq \{j_1, \ldots, j_{n+1}\}$, $|I| = i$. Тогда, по предположению индукции, $\mu(P, P'') = (-1)^{|J|-|J''|} = (-1)^{n+1+s-s-i} = (-1)^{n+1-i}$. Количество различных I мощности i равно C_{n+1}^i . Имеем, аналогично 2.2.3

$$-\sum_{P \preceq P'' \prec P} \mu(P, P'') = -\big(C_{n+1}^1 \, (-1)^{n+1-1} + C_{n+1}^2 \, (-1)^{n+1-2} + \\ + \ldots + (-1)^{n+1-n-1} C_{n+1}^{n+1} \big) = (-1)^{n+1} = (-1)^k$$

□

Тогда для $P = \Omega : \; g(P) = 0$, т.к. $\varnothing$ вложено в любое множество. Поэтому

$$0 = \sum_{P \preceq \Omega} |P| \mu(P, \Omega) = |\Omega| + |S_1| \mu(S_1, \Omega) + \ldots + |S_n| \mu(S_n, \Omega) + \\ + |S_1 \cap S_2| \mu(S_1 \cap S_2, \Omega) + \ldots + |S_1 \cap S_2 \cap \ldots \cap S_n| \mu(S_1 \cap \ldots \cap S_n, \Omega)$$

Перенося все слагаемые, кроме первого, в другую часть равенства, получаем формулу включений-исключений.

2.3 Разбиение чисел на слагаемые

Рассмотрим натуральное число $n \in \mathbb{N}$. Задача разбиения числа на слагаемые заключается в количестве способов представить n в виде суммы $n = x_1 + \ldots + x_t$, где каждое $x_i \in \mathbb{N}$, с некоторыми дополнительными условиями. Мы рассмотрим здесь два вида подобной задачи.

2.3.1 Задача о попойке

Формулировка: найти количество *упорядоченных* разбиений числа n на слагаемые, которые могут принимать значения только из множества $\{n_1, \ldots, n_k\}$. Обозначим это количество за $f(n; n_1, \ldots, n_k)$.

Утверждение 2.3.1.1. $f(n; n_1, \ldots, n_k) = \sum_{i=1}^{k} f(n - n_i; n_1, \ldots, n_k)$

Доказательство. Положим $V :=$ множество всех упорядоченных разбиений числа n на слагаемые, $V_i :=$ множество тех разбиений, где первое слагаемое равно n_i.

$$V = V_1 \sqcup \ldots \sqcup V_k \Rightarrow |V| = |V_1| + \ldots + |V_k|$$

Заметим теперь, что $|V_i| = f(n - n_i;\ n_1, \ldots,\ n_k)$. Зададим начальные условия

$$\begin{cases} f(0;\ n_1,\ \ldots,\ n_k) = 1 \\ \\ f(-n;\ n_1,\ \ldots,\ n_k) = 0 \end{cases}$$

□

Следствие 2.3.1. $f(n;\ 1,\ 2,\ \ldots, n) = 2^{n-1}$

Доказательство. Докажем индукцией по n. База $n = 1$ ясна. Переход:

$$f(n;\ 1,\ \ldots,\ n) = f(n-1;\ 1,\ \ldots,\ n) + f(n-2;\ 1,\ \ldots,\ n) + \ldots + f(n-n;\ 1,\ \ldots,\ n) =$$

$$= 2^{n-2} + 2^{n-3} + \ldots + 2^0 + 1 = 2^{n-1} - 1 + 1 = 2^{n-1}$$

□

2.3.2 Задача о капусте

Формулировка: найти количество *неупорядоченных* разбиений числа n на слагаемые, которые могут принимать значения только из множества $\{n_1,\ \ldots,\ n_k\}$. Обозначим это количество за $F(n;\ n_1,\ \ldots,\ n_k)$.

Ясно сразу, что $F(n;\ n_1,\ \ldots,\ n_k) < f(n;\ n_1,\ \ldots,\ n_k)$.

Утверждение 2.3.2.1. $F(n;\ n_1,\ \ldots,\ n_k) = F(n;\ n_2,\ \ldots,\ n_k) + (n - n_1;\ n_1,\ \ldots,\ n_k)$

Доказательство. $V = V_1 \sqcup V_2$, где V_1 это те разбиения, которые не содержат слагаемого n_1, а V_2 — которые содержат хотя бы одно такое слагаемое. □

Положим $p(n) := F(n;\ 1,\ 2,\ \ldots n)$

Теорема 2.3.1. *(Харди-Рамануджан, б/д)*

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2/3}\sqrt{n-1/24}}$$

2.3.3 Диаграммы Юнга

Определение 2.3.1. *Диаграммой Юнга* этого разбиения называется конечный набор ячеек или клеток, выровненных по левой границе, в котором длины строк образуют невозрастающую последовательность (каждая строка такой же длины как предыдущая, или короче).

Набор чисел, состоящий из длин строк, задает разбиение некоторого положительного числа n, которое равно общему числу ячеек диаграммы.

Докажем с помощью диаграмм Юнга некоторые утверждения, связанные с неупорядоченными разбиениями числа на слагаемые.

Утверждение 2.3.3.1. Количество неупорядоченных разбиений числа n на не более k слагаемых равно количество разбиений числа $n + k$ на ровно k слагаемых.

Доказательство. Очевидно, что существует биекция между разбиениями числа на слагаемыми и диаграммами Юнга. Пусть $n = x_1 + \ldots + x_t$ — некоторое разбиение числа n на $\leqslant k$ слагаемых. Рассмотрим его диаграмму Юнга. Припишем слева к ней столбец высотой k. У полученной диаграммы ровно $n + k$ ячеек и k строк, а значит, она задает разбиение числа $n+k$ на k слагаемых. Заметим теперь, что разные диаграммы Юнга для разбиений n переходят при такой операции в разные диаграммы для разбиений $n + k$. □

Утверждение 2.3.3.2. Количество неупорядоченных разбиений числа n на не более k слагаемых равно количесту разбиений числа $n + \frac{k(k+1)}{2}$ на ровно k различных слагаемых.

Доказательство. Рассмотрим диаграмму Юнга некоторого разбиения числа n. "Припишем"к ней "прямоугольный треугольник содержащий $\frac{k(k+1)}{2}$ ячеек (длина первой строки k и высота первого столбца k). Полученное отображение — биекция между рассматриваемыми в условии разбиениями. □

Определение 2.3.2. Рассмотрим диаграмму Юнга τ, содержащую k строк. *Двойственной* диаграммой Юнга к диаграмме τ называется диаграмма Юнга, содержащая k столбцов, причем высота i-го столбца в этой диаграмме равна длине i-той строки в диаграмме τ.

Утверждение 2.3.3.3. Количество неупорядоченных разбиений числа n на не более k слагаемых равно количеству неупорядоченных разбиений числа n на слагаемые, каждое из которых $\leqslant k$.

Доказательство. Требуемая биекция переводит диаграмму Юнга в двойственную ей диаграмму. $\square$

Задача Эйлера. Рассмотрим бесконечное произведение

$$(1-x)(1-x^2)\dots(1-x^k)\dots = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + \dots \quad (1)$$

Эйлером было доказано, что все числа, стоящие в показателях, имеют вид $\frac{3q^2 \pm q}{2}$.

Заметим теперь, что $(-x^{n_1}) \cdot (-x^{n_2}) \cdot \ldots \cdot (-x^{n_k}) = a \cdot x^n \Leftrightarrow n = n_1 + \ldots + n_k$, а коэффицент при x^n в (1) равен количеству неупорядоченных разбиений числа n на четное число слагаемых (n_1) за вычетом количества неупорядоченных разбиений числа n на нечетное число слагаемых (n_2). Тогда результат, полученный Эйлером, можно сформулировать так:

$$n_1 - n_2 = \begin{cases} (-1)^q, & n = \dfrac{3q^2 \pm q}{2} \\ 0, & \text{иначе} \end{cases}$$

2.4 Линейные рекуррентные соотношения

Определение 2.4.1. Последовательность $\{y_n\}$ удовлетворяет линейному рекуррентному соотношению порядка k с постоянными коэффицентами $a_0, \ldots, a_k \in \mathbb{R}$, если $a_0,\ a_k \neq 0$ и $\forall n$:

$$a_k y_{n+k} + a_{k-1} y_{n+k-1} + \ldots + a_0 y_n = 0$$

Линейные рекуррентные соотношения интересны тем, что для всех таких соотношений существует алгоритм, который позволяет выразить y_n как функцию от n. Рассмотрим случай, когда последовательность удовлетворяет соотношению второго порядка.

Определение 2.4.2. Характерестическим уравнением линейного рекуррентного соотношения второго порядка с коэффицентами $a_2,\ a_1,\ a_0$ называется уравнение $a_2x^2 + a_1x + a_0 = 0$.

Теорема 2.4.1. *Рассмотрим рек. соотношение $a_2y_{n+2} + a_1y_{n+1} + a_0y_n = 0$. Если λ_1 и λ_2 — различные корни характеристического уравнения этого соотношения, то*

1. *$\forall c_1,\ c_2 \in \mathbb{C}$ последовательность $y_n = c_1\lambda_1^n + c_2\lambda_2^n$ удовлетворяет этому соотношению.*

2. *Если последовательность* $\{y_n\}$ *удовлетворяет этому рек.соотношению, то* $\exists c_1,\ c_2 \in \mathbb{C}:\ y_n = c_1\lambda_1^n + c_2\lambda_2^n$.

Доказательство. 1. Просто подставим $y_{n+2},\ y_{n+1},\ y_n$ в рек. соотношение. Получим:

$$c_1\lambda_1^n(a_2\lambda_1^2 + a_1\lambda_1 + a_0) + c_2\lambda_2^n(a_2\lambda_2^2 + a_1\lambda_2 + a_0) = 0$$

2. Пусть последовательность $\{y_n\}$ удовлетворяет рек.соотношени. Составим систему уравнений

$$\begin{cases} c_1 + c_2 = y_0 \\ c_1\lambda_1 + c_2\lambda_2 = y_1 \end{cases}$$

Пусть $c_1^*,\ c_2^*$ это ее решения. Рассмотрим последовательность $y_n^* = c_1^*\lambda_1^n + c_2^*\lambda_2^n$. Согласно пункту 1. она удовлетворяет этому соотношению. При этом, $y_0^* = y_0,\ y_1^* = y_1$. Значит, $\forall n : y_n = y_n^*$

□

Теорема 2.4.2. *Рассмотрим рек. соотношение* $a_2y_{n+2} + a_1y_{n+1} + a_0y_n = 0$. *Если* $\lambda_1 = \lambda_2 = \lambda$ *— корень характеристического уравнения этого соотношения кратности 2, то*

1. $\forall c_1,\ c_2 \in \mathbb{C}$ *последовательность* $y_n = (c_1n + c_2)\lambda^n$ *удовлетворяет этому рек. соотношению.*

2. *Если последовательность* $\{y_n\}$ *удовлетворяет этому рек.соотношению, то* $\exists c_1,\ c_2 \in \mathbb{C}:\ y_n = (c_1n + c_2)\lambda^n$.

Доказательство. 1.

$$a_2(c_1(n+2) + c_2)\lambda^{n+2} + a_1(c_1(n+1) + c_2)\lambda^{n+1} + a_0(c_1n + c_2)\lambda^n = c_1n\lambda^n(a_2\lambda^2 + \\ + a_1\lambda + a_0) + c_2\lambda^n(a_2\lambda^2 + a_1\lambda + a_0) + \lambda^{n+1}c_1(2a_2\lambda + a_1) = 0$$

где равенство последней скобки нулю можно проверить, например, посчитав производную.

2. Пусть последовательность $\{y_n\}$ удовлетворяет рек.соотношени. Составим систему уравнений

$$\begin{cases} c_2 = y_0 \\ (c_1 + c_2)\lambda = y_1 \end{cases}$$

Пусть $c_1^*,\ c_2^*$ это ее решения. Рассмотрим последовательность $y_n^* = (c_1^*n + c_2^*)\lambda^n$. Согласно пункту 1. она удовлетворяет этому соотношению. При этом, $y_0^* = y_0,\ y_1^* = y_1$. Значит, $\forall n : y_n = y_n^*$

□

Теорема 2.4.3. *(Для общего случая, б/д)*

Рассмотрим рек. соотношение k-го порядка. Пусть $a_k x^k + \ldots + a_0 = 0$ *— его характерестическое уравнение. Пусть у него имеется ровно k корней с учетом кратности. Пусть* $\mu_1, \ldots, \mu_r$ *это все различные корни этого уравнения,* $m_1, \ldots, m_r$ *это их кратности, а* $P_1(n), \ldots, P_r(n)$ *это произвольные многочлены от n степеней* $m_1 - 1, \ldots, m_r - 1$*. Тогда*

$$y_n = P_1(n)\mu_1^n + \ldots + P_r(n)\mu_r^n.$$

2.5 Формальные степенные ряды

Определение 2.5.1. Пусть даны числа $a_0, a_1, \ldots$. *Формальным степенным рядом* называется *картинка* (формальное алгебраическое выражение) вида $\sum\limits_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots$. Два ф.с.р называются равными, если $\forall n : \ a_n = b_n$.

На множестве ф.с.р определены следующие операции:

1. Сложение: пусть A и B это два ф.с.р с коэффицентами $\{a_n\}$, $\{b_n\}$. Тогда их суммой называется ф.с.р C, такой что $c_n = a_n + b_n$.

2. Вычитание: пусть A и B это два ф.с.р с коэффицентами $\{a_n\}$, $\{b_n\}$. Тогда их разностью называется ф.с.р C, такой что $c_n = a_n - b_n$.

3. Умножение на число: $\alpha \in \mathbb{C}$, A — ф.с.р. Тогда $\alpha A = C$ — ф.с.р, такой что $c_n = \alpha a_n$.

4. Произведение: пусть A и B это два ф.с.р с коэффицентами $\{a_n\}$, $\{b_n\}$. Тогда их произведением называется ф.с.р C, такой что $c_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$ (перемножаются такие коэффиценты, что сумма степеней x при них равна n).

5. Деление: пусть A и B это два ф.с.р с коэффицентами $\{a_n\}$, $\{b_n\}$ и $b_0 \neq 0$. Тогда их частным называется ф.с.р $C = A/B$, такой что $A = BC$, т.е.

$$a_0 = c_0 b_0$$

$$a_1 = c_0 b_1 + c_1 b_0$$

$$\ldots$$

Пример 2.5.0.1. $A = 1,\ B = 1 - x$. Тогда

$$C = \frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots$$

Ф.с.р полезны тем, что с их помощью можно доказывать различные комбинаторные тождества. Рассмотрим пример, иллюстрирующий это.

Пример 2.5.0.2.

$$\left(\frac{1}{1-x^2}\right)^2 = \frac{1}{(1-x)^2} \cdot \frac{1}{(1+x)^2}$$

Левая часть равенства:

$$\left(\frac{1}{1-x^2}\right)^2 = (1 + x^2 + x^4 + \dots)^2 = 1 + 2x^2 + 3x^4 + \dots + (n+1)x^{2n} + \dots$$

С другой стороны рассмотрим ряды в правой части равенства

$$\left(\frac{1}{1-x}\right)^2 = (1 + x + x^2 + \dots)^2 = 1 + 2x + 3x^2 + \dots + (n+1)x^n + \dots$$
$$\left(\frac{1}{1+x}\right)^2 = (1 - x + x^2 - \dots)^2 = 1 - 2x + 3x^2 - \dots + (-1)^n(n+1)x^n + \dots$$

Тогда коэффицент при x_n в их произведении равен коэффицентру при x_n в ф.с.р. слева от равенства и равен

$$1 \cdot (-1)^n(n+1) + 2(-1)^{n-1}n + \dots + (n+1) \cdot 1 \cdot (-1)^0 = \begin{cases} 0, & n = 2k+1 \\ n+1, & n = 2k \end{cases}$$

Определение 2.5.2. Обозначим $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n$ — ф.с.р. Ряд называется *сходящимся* в точке $x = x_0$, если существует конечный предел $\lim\limits_{k\to\infty} \sum\limits_{n=0}^{k} a_n x_0^n = f(x_0)$.

Пример 2.5.0.3. $a_n = 1$. Тогда $f(x) = \sum\limits_{n=0}^{\infty} x^n$, что сходится при $|x| < 1$ и расходится при $|x| \geqslant 1$.

Пример 2.5.0.4. $a_n = 2^n$. Тогда $f(x) = \sum\limits_{n=0}^{\infty} 2^n x^n$, что сходится при $|x| < \frac{1}{2}$ и расходится при $|x| \geqslant \frac{1}{2}$.

Пример 2.5.0.5. $a_n = 2^n,\ 2 \mid n;\ a_n = 3^n,\ 2 \nmid n$. Тогда сходится при $|x| < \frac{1}{3}$ и расходится при $|x| > \frac{1}{3}$.

Теорема 2.5.1. *(Коши-Адамара, б/д)*

Радиусом сходимости ряда $f(x)$ называется число ρ, определяемое как

$$\rho = \frac{1}{\overline{\lim\limits_{n\to\infty}} \sqrt[n]{|a_n|}}$$

Тогда при $|x| < \rho$ степенной ряд сходится, при $|x| > \rho$ ряд расходится, а при $|x| = \rho$ ряд может как сходиться, так и расходиться. Множество $\{x : |x| < \rho\}$ называется кругом сходимости ряда.

Теорема 2.5.2. *(б/д)*

Внутри круга сходимости степенной ряд можно дифференцировать почленно, причем его производная выражается формулой

$$f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}$$

2.5.1 Производящие функции

Определение 2.5.3. Пусть $\{a_n\}$ — числовая последовательность. Тогда ее *производящей функцией* называется степенной ряд $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n$.

Пример 2.5.1.1. Найдем производящую функцию для последовательности биномиальных коэффициентов.

$$f(x) = \sum_{k=0}^{n} C_n^k \, x^k = (1+x)^n$$

Теперь посчитаем значение функции $F(x) = \sum\limits_{k=0}^{n} k^2 C_n^k \, (\frac{2}{3})^k$. Для начала заметим, что $f(x)$ сходится в любой точке, а значит в любой точке $\mathbb{R}$ существует ее производная. Тогда

$$x\left(xf'(x)\right)' = x(x'f'(x) + xf''(x)) = x(f'(x) + xf''(x)) = x\sum_{k=1}^{n} k^2 C_n^k \, x^{k-1} = \sum_{k=0}^{n} k^2 C_n^k \, x^k$$

Таким образом $F(x) = x(f'(x) + xf''(x)) = xk(1+x)^{k-1} + x^2 k(k-1)(1+x)^{k-2}$, а значит

$$F(\frac{2}{3}) = \frac{2}{3} \cdot n \cdot \left(\frac{4}{3}\right)^{n-1} + \frac{4}{9} n(n-1) \cdot \left(\frac{4}{3}\right)^{n-2}$$

Определение 2.5.4. Последовательность чисел Фибоначчи определяется следующим образом: $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ при $n \geqslant 2$. Найдем ее производящую функцию:

$$f(x) = \sum_{n=0}^{\infty} F_n x^n$$

$$xf(x) = \sum_{n=0}^{\infty} F_n x^{n+1}$$

$$x^2 f(x) = \sum_{n=0}^{\infty} F_n x^{n+2}$$

$$xf(x) + x^2 f(x) = F_0 x + (F_1 + F_2)x^2 + (F_2 + F_1)x^3 + \ldots = f(x) - F_1 x - F_0 = f(x) - x \Rightarrow$$

$$\Rightarrow xf(x) + x^2 f(x) = f(x) - x \Rightarrow f(x) = \frac{x}{1 - x - x^2}$$

2.5.2 Числа Каталана

Определение 2.5.5. Числами Каталана называется последовательность натуральных чисел, заданная следующим образом: $T_0 = 1$, $T_n = T_{n-1}T_0 + \ldots + T_0T_{n-1} = \sum\limits_{i=0}^{n-1} T_iT_{n-i-1}$.

Полезным (и не сложным) упражнением будет показать, что n-ое число Каталана равно количеству

1. правильных скобочных последовательностей длины $2n$.

2. способов соединения $2n$ точек на окружности n непересекающимися хордами.

3. разбиений выпуклого $(n+2)$-угольника на треугольники непересекающимися диагоналями.

В каждом случае индукцией по n доказывается, что количество способов сделать это удовлетворяет рекуррентному соотношению для чисел Каталана.

Утверждение 2.5.2.1.

$$T_n = \frac{1}{n+1}C_{2n}^n$$

Доказательство. Докажем это утверждение с помощью производящих функций. Для начала найдем явный вид производящей функции чисел Каталана

$$f(x) = T_0 + T_1x + T_2x^2 + \ldots$$

$$(f(x))^2 = T_0^2 + (T_0T_1 + T_1T_0)x + \ldots + (T_0T_n + \ldots + T_nT_0)x^n = T_1x + T_2x^2 + \ldots \Rightarrow$$

$$x\,(f(x))^2 = f(x) - T_0 = f(x) - 1 \Rightarrow$$

$$f(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

подставим $x = 0$: $xf(x) = \dfrac{1 - \sqrt{1-4x}}{2}$

Далее, раскроем $(1+x)^{1/2}$ по биному Ньютона для обобщенной степени:

$$
\begin{aligned}
&(1+x)^{1/2} = 1 + C^1_{1/2}\, x + C^2_{1/2}\, x^2 + \ldots + C^n_{1/2}\, x^n \\
&\text{где } C^k_{1/2} = \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\ldots\left(\frac{1}{2}-n+1\right)}{n!} \\
&= \frac{\frac{1}{2}\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\cdots\left(-\frac{2n-3}{2}\right)}{n!} \\
&= \frac{2^{-n}(-1)^{n-1}\cdot 1\cdot 3\cdot\ldots\cdot(2n-3)\cdot 2\cdot 4\cdot\ldots\cdot(2n-2)}{n!\cdot 2\cdot 4\cdot\ldots\cdot(2n-2)} \\
&= \frac{2^{-n}(-1)^{n-1}(2n-2)!}{n!2^{n-1}(n-1)!} = 2^{1-2n}(-1)^{n-1}C^{n-1}_{2n-2}\,\frac{1}{n}
\end{aligned}
$$

Тогда коэффицент при x^n в $\sqrt{1-4x}$ равен $(-4)^n\cdot 2^{1-2n}\cdot(-1)^{n-1}C^{n-1}_{2n-2}\cdot\frac{1}{n} = -\frac{2}{n}C^{n-1}_{2n-2} = -2T_{n-1}$, а $T_n = \frac{1}{n+1}C^n_{2n}$ □

Глава 3

Теория чисел

3.1 Основы теории чисел

Здесь и далее p будет обозначать нечетное простое число, а $\gcd(a,\ b)$ — НОД чисел a и b.

Определение 3.1.1. Пусть $a,\ b \in \mathbb{Z};\ m \in \mathbb{N}_+$. Говорят, что a *сравнимо* с b по *модулю* m если$(a-b)\vdots m$. *Обозначение:* $a \equiv b \pmod{m}$. Очевидно, что $(a-b)\vdots m \iff a$ и b дают одинаковые остатки при делении на m.

Заметим, что отношение $\equiv$ это отношение эквивалентности, а значит $\mathbb{Z}$ распадается на классы эквивалентности.

Определение 3.1.2. *Вычетом* по модулю m называется любой представитель класса эквивалентности, содержащей данный остаток при делении на m.

Полной системой вычетов называется любой набор из m всевозможных вычетов. *Приведенной системой вычетов* называется множество тех вычетов из полной системы, которые взаимно просты с m.

Определение 3.1.3. Функцией Эйлера $\varphi : \mathbb{N} \to \mathbb{N}$ называется функция, равная размеру приведенной системы вычетов по модулю n.

Теорема 3.1.1. *(малая теорема Ферма)*

Если p — простое, то $a^p \equiv a \pmod p$

Доказательство. Приведем два доказательства.

1. $(\underbrace{1 + \ldots + 1}_{a \text{ раз}})^p = \underbrace{1^p + \ldots + 1^p}_{a \text{ раз}} + \sum P(n_1, \ldots, n_a) \equiv a \pmod p$ т.к. $P(n_1, \ldots, n_a) = \frac{p!}{n_1! \ldots n_a!}$ где $n_i < p \Rightarrow \gcd(n_1! \ldots n_a!, p) = 1$.

2. Пусть a — взаимно просто с p. Рассмотрим полную систему вычетов по модулю p.

   Утверждение 3.1.0.1. Если элементы полной системы вычетов умножить на a, то снова получится полная система вычетов

   Доказательство. Предположим, что какие-то два элемента ax_i, ax_j совпали. Тогда $a(x_i - x_j) \vdots p \Rightarrow x_i \equiv x_j \pmod p$, что не так. Противоречие □

   Тогда рассмотрим полные системы вычетов $\{1, \ldots, p-1\}$ и $\{a, 2a, \ldots, (p-1)a\}$. Перемножим все числа в них:

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod p \Rightarrow 1 \equiv a^{p-1} \pmod p$$

   □

Теорема 3.1.2. *(теорема Эйлера)*

Пусть $\gcd(a, m) = 1$. Тогда $a^{\varphi(m)} \equiv 1 \pmod m$

Доказательство. Доказательство аналогично второму доказательству малой теоремы Ферма, с той лишь разницей, что испольуется приведенная система вычетов. □

3.2 Проблема Эрдеша-Гинзубрга-Зива

3.2.1 Одномерный случай

Определение 3.2.1 (Формулировка)**.** Пусть даны наборы из d целых чисел и фиксированное число n. При каком наимешьшем числе наборов $m = m(n)$ среди них гарантированно найдется n наборов, таких что сумма чисел в каждой из d позиций этих наборов делиться на n.

Теорема 3.2.1. *(ЭГЗ, $d = 1$)*

Пусть p — простое число. Тогда среди любых $2p-1$ целых чисел найдется p чисел, таких что их сумма делится на p.

Доказательство. Для начала покажем, что $2p-2$ числа не хватит. Действительно, простеший контр-пример: $p-1$ ноль и $p-1$ единица. Теперь перейдем к доказательству, что $2p-1$ чисел достаточно.

Утверждение 3.2.1.1. $C_{2p-1}^{p} \equiv 1 \pmod{p}$

Доказательство.

$$C_{2p-1}^{p} = \frac{(2p-1)!}{p!(p-1)!} = \frac{(2p)!}{p!p!} \cdot \frac{1}{2} = \frac{1}{2} C_{2p}^{p}$$

Рассмотрим $(1+1)^{2p}$. По биному Ньютона:

$$C_{2p}^{0} + \ldots + C_{2p}^{2p} \equiv 1 + 1 + C_{2p}^{p} \equiv 4^p \equiv 4 \text{ (м.т.Ф.)} \Rightarrow C_{2p}^{p} \equiv 2 \pmod{p}$$

а значит $C_{2p-1}^{p} \equiv 1 \pmod{p}$. □

Утверждение 3.2.1.2. Для любого $q \in \{1, \ldots, p-1\}$ $C_{2p-1-q}^{p-q} \equiv 0 \pmod{p}$

Доказательство. При таком q выполнены неравенства $2p-1-q \geqslant p$; $p-q \leqslant p-1$. А значит

$$C_{2p-1-q}^{p-q} = \frac{(2p-1-q)!}{(p-q)!(p-1)!} \equiv 0 \pmod{p}$$

поскольку числитель делится на p, а знаменатель взаимнопрост с p. □

Докажем теорему от противного. Предположим, что $m(p) > 2p-1$. Это означает, что найдется $a_1, a_2, \ldots, a_{2p-1}$ чисел, таких что $\forall I \subset \{1, \ldots, 2p-1\} : |I| = p : \sum\limits_{i \in I} a_i \not\equiv 0 \pmod{p}$. Положим

$$S := \sum_{\substack{I \subset \{1, \ldots, 2p-1\} \\ |I| = p}} \left(\sum_{i \in I} a_i \right)^{p-1}$$

по малой теореме Ферма, $(\sum a_i)^{p-1} \equiv 1 \pmod{p}$ а значит $S \equiv C_{2p-1}^{p} \equiv 1 \pmod{p}$.

С другой стороны, $\left(\sum\limits_{i \in I} a_i \right)^{p-1}$ есть сумма выражений вида $a_{i_1}^{\alpha_{i_1}} a_{i_2}^{\alpha_{i_2}} \ldots a_{i_q}^{\alpha_{i_q}}$. Каждое такое выражение возникает в S столько раз, сколько таких $I \subset \{1, \ldots, 2p-1\}$, $|I| = p : \{i_1, \ldots, i_q\} \subset I$, а их ровно C_{2p-1-q}^{p-q}, где $1 \leqslant q \leqslant p-1$. Тогда каждый коэффицент в S имеет вид C_{2p-1-q}^{p-q}, а значит делится на p. Но тогда $S \equiv 0 \pmod{p}$. Противоречие. □

Заметим, что, хоть мы и привели доказательство для случая простого числа, теорема верна для произвольного натурального n.

3.2.2 Двумерный случай

Определение 3.2.2 (Формулировка)**.** Пусть даны пары целых чисел и фиксированное число n. При каком наимешьшем числе пар $m = m(n)$ среди них гарантированно найдется n пар, таких что сумма чисел в каждой позиции этих пар делиться на n.

Сначала немного об истории теоремы. В 1983 году А.Кемниц предложил естественное обобщение проблемы Эрдеша-Гинзбурга-Зива. Как уже можно догадаться, он предложил рассматривать вместо целых чисел *пары* целых чисел. Нетрудно видеть, что $m(n) > 4n - 4$. Действительно, рассмотрим множество, содержащая по $n - 1$ набору видов (1, 0), (0, 0), (0, 1), (1, 1). Очевидно, что в таком множестве нет подмножества мощности n с суммой элементов, делящейся на n.

Кемниц выдвинул гипотезу, что $m(n) = 4n - 3$ и проверил ее для некоторых малых значений n. Однако доказательство этой гипотезы затянулось. Н.Алон и М.Дубинер в 1993 году доказали, что $m \leqslant 6n - 5$. В 2000 году Л.Роньяи установил неравенство $m \leqslant 4n - 2$, и лишь в 2003 году Х.Райхер "дожал"доказательство, показав, что $m \leqslant 4n-3$. Однако, в данном разделе мы изложим доказательство *Роньяи*, считающееся некоторыми одним из самых изящных рассуждений в комбинаторике. Но для начала докажем несколько вспомогательных теорем.

Теорема 3.2.2. *(Шевалле)*

Пусть $F(x_1, \ldots, x_n)$ — многочлен от n переменных, коэффициенты которого являются вычетами по некоторому простому модулю p и $\deg F < n$. Тогда количество различных (по модулю p) решений сравнения $F(x_1, \ldots, x_n) \equiv 0 \pmod p$ делится на p.

Доказательство. Если $F(x_1, \ldots, x_n) \equiv 0 \pmod p$, то оно же и в $p - 1$ степени будет сравнимо с 0, а это значит, что число решений этого сравнения равно

$$\sum_{x_1=1}^{p} \sum_{x_2=1}^{p} \cdots \sum_{x_n=1}^{p} \left(1 - (F(x_1, \ldots, x_n))^{p-1}\right)$$

Если S делится на p то и

$$S - pn = \sum_{x_1=1}^{p} \sum_{x_2=1}^{p} \dots \sum_{x_n=1}^{p} (F(x_1, \dots, x_n))^{p-1}$$

тоже делится на p.

$(F(x_1, \dots, x_n))^{p-1}$ есть некоторый многочлен степени $\leqslant (n-1)(p-1)$. Как известно, любой многочлен это сумма одночленов. Покажем, что $\sum\limits_{x_1=1}^{p} \dots \sum\limits_{x_n=1}^{p} x_1^{\beta_1} \dots x_n^{\beta_n} \equiv 0 \pmod p$ для $\sum\limits_{i=1}^{n} \beta_i \leqslant (n-1)(p-1)$. Это будет означать, что каждый отдельный одночлен делится на p, а значит и S делится на p.

$\sum\limits_{x_1=1}^{p} \dots \sum\limits_{x_n=1}^{p} x_1^{\beta_1} \dots x_n^{\beta_n} = \left(\sum\limits_{x_1=1}^{p} x_1^{\beta_1}\right) \dots \left(\sum\limits_{x_n=1}^{p} x_n^{\beta_n}\right) = S^*$. Рассмотрим случаи:

1. Существует i, такое что $\beta_i = 0$. Тогда $\sum\limits_{x_i=1}^{p} x_i^{\beta_i} = p \equiv 0 \pmod p$ и $S^* \equiv 0 \pmod p$.

2. Если $p = 2$, то $\sum \beta_i \leqslant n-1 \Rightarrow \exists i : \beta_i = 0$ и сведено к случаю 1).

3. Если $p \geqslant 3$ и $\forall i \ \beta_i \neq 0$. Тогда из того, что степень многочлена $\leqslant (n-1)(p-1)$, а слагаемых в $\sum\limits_{i=1}^{n}$ следует, что $\exists \beta_i : 1 \leqslant \beta_i \leqslant p-2$. Тогда существует число a, такое что $a^{\alpha_i} \not\equiv 1 \pmod p$ (например, можно взять *первообразный корень по этому модулю*, их существование будет доказано позже). Имеем

$$a^{\beta_i} \underbrace{\sum_{x_i=1}^{n} x_i^{\beta_i}}_{S_i} = \sum_{x_i=1}^{n} (a \cdot x_i)^{\beta_i} \equiv \underbrace{\sum_{y_i=1}^{p} y_i^{\alpha_i}}_{S_i} \text{ т.к. } a^{\beta_i} \cdot x_i \text{ пробегает всю систему вычетов}$$

$$\Rightarrow a^{\beta_i} S_i \equiv S_i \Rightarrow S_i(a^{\beta_i} - 1) \equiv 0 \pmod p \Rightarrow S_i \equiv 0 \pmod p$$

откуда следует, что $S^* \equiv 0 \pmod p$. Теорема доказана. □

Теорема 3.2.3. *(Варнинг, б/д)*

Если в условии теоремы Шевалле набор $(0, \dots, 0)$ *является решением сравнения, то есть и нетривиальное решение.*

Теорема 3.2.4. *(Обобщенная теорема Варнинга, б/д)*

Пусть $F_1(x_1, \dots, x_n), \dots, F_k(x_1, \dots, x_n)$ *— многочлены с коэффициентами — вычетами по простому модулю* p*. Пусть сумма их степеней меньше* n*. Тогда, если набор* $(0, \dots, 0)$ *является решением*

системы

$$\begin{cases} F_1(x_1,\ \ldots,\ x_n) \equiv \pmod p \\ \ldots \\ F_k(x_1,\ \ldots,\ x_n) \equiv 0 \pmod p \end{cases}$$

то существует и нетривиальное решение этой системы.

Лемма 3.2.5. *Пусть* $(a_1,\ b_1),\ \ldots,\ (a_{3p},\ b_{3p})$ *— наборы, такие что* $\sum\limits_{i=1}^{3p} a_i \equiv \sum\limits_{i=1}^{3p} b_i \equiv 0 \pmod p$. *Тогда существует множество* $J \subset \{1,\ \ldots,\ 3p\}$ *мощности* p, *такое что* $\sum\limits_{i\in I} a_i \equiv \sum\limits_{i\in I} b_i \equiv 0 \pmod p$.

Доказательство. Рассмотрим многочлены

$$\begin{cases} F_1(x_1,\ \ldots,\ x_n) = \sum\limits_{i=1}^{3p-1} a_i x_i^{p-1} \\ F_2(x_1,\ \ldots,\ x_n) = \sum\limits_{i=1}^{3p-1} b_i x_i^{p-1} \\ F_3(x_1,\ \ldots,\ x_n) = \sum\limits_{i=1}^{3p-1} x_i^{p-1} \end{cases}$$

Очевидно, что они удовлетворяют условию обобщенной теоремы Варнинга, а значит существует нетривиальное решение системы $(x_1,\ \ldots,\ x_{3p-1})$.

Рассмотрим множество $I = \{i \in \{1, \ldots, 3p-1\} : x_i \not\equiv 0 \pmod p\}$. Поскольку решение нетривиальное, $I \neq \varnothing$. Из F_1 следует, что $\sum\limits_{i\in I} a_i \equiv 0$. Из F_2 следует тоже самое про b_i. Из F_3 следует, что $|I| \equiv 0 \pmod p \Rightarrow |I| = p,\ 2p$. Если $|I| = p$ то $J = I$. Если же $|I| = 2p$, то $J = \{1,\ 2,\ \ldots,\ 3p\}\backslash I$. □

Теорема 3.2.6. *(Роньяи, случай простого числа)*

$$m(p) \leqslant 4p - 2,\ \textit{где}\ p\ -\ \textit{простое.}$$

Доказательство. Предположим противное. Тогда среди любых $m := 4p-2$ наборов $(a_1, b_1), \ldots (a_m, b_m)$ не существует подмножества мощности p, сумма элементов в котором делится на p по каждой координате. Согласно лемме 3.2.5, не существует тогда и набора мощности $3p$, обладающего таким же свойством.

Пусть $\sigma_k(x_1,\ \ldots,\ x_n)$ — симметрический многочлен. Определим многочлен F:

$$F(x_1,\ \ldots,\ x_m) = \left(\left(\sum_{i=1}^{m} a_i x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{m} b_i x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{m} x_i\right)^{p-1} - 1\right)\left(\sigma_p(x_1,\ \ldots,\ x_m) - 2\right)$$

Пусть $\overline{x}:\ \forall i\ x_i \in \{0,\ 1\}$.

1. Если $\sum\limits_{i=1}^{m} x_i \in \{p,\ 3p\}$ то первая или втарая скобка сравнима с 0.
2. Если $\sum\limits_{i=1}^{m} x_i = 2p$, то $\sigma_p(\overline{x}) = C_{2p}^{p} \equiv 2 \pmod p \Rightarrow$ 4-ая скобка сравнима с 0.
3. Если $\sum\limits_{i=1}^{m} x_i$ не делится на p, то третья скобка сравнима с 0
4. Если $\sum\limits_{i=1}^{m} x_i = 0$ то $F(0,\ \ldots,\ 0) = 2$.

Раскроем все скобки и заменим в каждом одночлене степень входящих в него x_i на 1 (т.к. $1^a = 1$). Получим новый многочлен F', степень которого не больше степени F, который обнулятся на всех наборах, где есть хотя бы одна единица, а на всех остальных $F' = 2$.

Утверждение 3.2.2.1. (б/д) $F' = 2(1 - x_1)(1 - x_2)\ldots(1 - x_m)$

Тогда $deg\, F' = m = 4p-2 \leqslant deg\, F = (p-1)+(p-1)+(p-1)+p = 4p-3 < 4p-2$. Противоречие. □

3.3 Распределение простых

(Напомним, что p — это простое число)

3.3.1 Немного фактов

Определение 3.3.1. Функция $\pi(x) : \mathbb{N} \to \mathbb{N}$ равна *количеству* простых чисел, меньше либо равных x.

Теорема 3.3.1. *(постулат Бертрана, б/д)*

Для любого x на отрезке $[x,\ 2x]$ найдется хотя бы одно простое число.

Интересен вопрос, как быстро должна рости функция, чтобы на отрезке $[x,\ x + f(x)]$ для любого x существовало хотя бы одно простое число. Доказано, что существует такая константа $c \in \mathbb{R}$, что $f(x) = cx^{0,525}$.

Гипотеза: $f(x) = c \ln^2 x$.

Кроме этого известно, что $\pi(x) \sim \frac{x}{\ln x}$ при $x \to \infty$ (т.е. предел отношения этих функций равен 1).

3.3.2 Теорема Чебышева

Теорема 3.3.2. *Существуют числа* $a,\ b \in \mathbb{R},\ 0 < a < b$ *такие что*

$$\frac{ax}{\ln x} \leqslant \pi(x) \leqslant \frac{bx}{\ln x}$$

Доказательство. Заметим, что $\pi(x) = \sum\limits_{p \leqslant x} 1$. Определим теперь две дополнительные функции ($\mathbb{P}$ — множество простых чисел):

$$\theta(x) = \sum_{p \leqslant x} \ln p$$

$$\psi(x) = \sum_{\substack{p \in \mathbb{P},\ \alpha \in \mathbb{N}: \\ p^\alpha \leqslant x}} \ln p$$

Для примера найдем $\psi(x)$ при $x = 10$:

$$\psi(10) = \ln 2 + \ln 2 + \ln 2 + \ln 3 + \ln 3 + \ln 5 + \ln 7$$

Утверждение 3.3.2.1.

$$\psi(x) = \sum_{p \leqslant x} \left[\frac{\ln x}{\ln p}\right] \ln p$$

Доказательство. Очевидно из определения □

Введем следующие обозначения:

$$\lambda_1 = \overline{\lim_{x \to \infty}} \frac{\theta(x)}{x} \quad \lambda_2 = \overline{\lim_{x \to \infty}} \frac{\psi(x)}{x} \quad \lambda_3 = \overline{\lim_{x \to \infty}} \frac{\pi(x)}{x/\ln x}$$

$$\mu_1 = \underline{\lim_{x \to \infty}} \frac{\theta(x)}{x} \quad \mu_2 = \underline{\lim_{x \to \infty}} \frac{\psi(x)}{x} \quad \mu_3 = \underline{\lim_{x \to \infty}} \frac{\pi(x)}{x/\ln x}$$

Лемма 3.3.3. $\lambda_1 = \lambda_2 = \lambda_3; \quad \mu_1 = \mu_2 = \mu_3$

Доказательство. Очевидно, что $\frac{\theta(x)}{x} \leqslant \frac{\psi(x)}{x} \Rightarrow \lambda_1 \leqslant \lambda_2$.

$$\psi(x) = \sum_{p \leqslant x} \left[\frac{\ln x}{\ln p}\right] \ln p \leqslant \sum_{p \leqslant x} \frac{\ln x}{\ln p} \cdot \ln p = \ln x \sum_{p \leqslant x} 1 = \ln x \cdot \pi(x)$$

$$\Rightarrow \frac{\psi(x)}{x} \leqslant \frac{\pi(x) \cdot \ln x}{x} \Rightarrow \lambda_2 \leqslant \lambda_3$$

Пусть $\alpha \in (0,\ 1)$. Тогда

$$\theta(x) = \sum_{p \leqslant x} \ln p \geqslant \sum_{x^\alpha \leqslant p \leqslant x} \ln p > \sum_{x^\alpha \leqslant p \leqslant x} \ln x^\alpha = \alpha \ln x \sum_{x^\alpha \leqslant p \leqslant x} 1 = \alpha \ln x \left(\pi(x) - \pi(x^\alpha)\right) \geqslant \alpha \ln x \left(\pi(x) - x^\alpha\right)$$

откуда следует, что

$$\frac{\theta(x)}{x} > \alpha \ln x \left(\frac{\pi(x)}{x} - x^{\alpha-1} \right) = \alpha \left(\frac{\pi(x)}{x/\ln x} - x^{\alpha-1} \ln x \right)$$

Устремляя $x \to \infty$, получим, что $\lambda_1 \geqslant \alpha\lambda_3$. Но тогда

$$\sup_{\alpha \in (0,\,1)} \alpha\lambda_1 \geqslant \sup_{\alpha \in (0,\,1)} \alpha\lambda_3 \Rightarrow \lambda_1 \geqslant \lambda_3$$

а значит $\lambda_1 = \lambda_2 = \lambda_3$.

Абсолютно аналогично, $\mu_1 = \mu_2 = \mu_3$ □

Докажем, что $\frac{\pi(x)}{x/\ln x} \leqslant 4 \ln 2$ Рассмотрим C_{2n}^n . Очевидно, что $C_{2n}^n < 2^{2n}$. Тогда

$$C_{2n}^n = \frac{(2n)!}{n!n!} \geqslant \prod_{n \leqslant p \leqslant 2n} p \Rightarrow \prod_{n \leqslant p \leqslant 2n} p < 2^{2n}$$

Логарифмируя обе части неравенства, получаем, что $\sum\limits_{n \leqslant p \leqslant 2n} \ln p < 2n \ln n$, что означает, что

$$\theta(2n) - \theta(n) < 2n \ln 2$$

Сложим такие неравенства для $n = 1,\ 2,\ \ldots,\ 2^k$ (помня, что $\theta(1) = 0$), где k определим позже.

Получим $\theta(2^{k+1}) < 2(2^{k+1} - 1) \ln 2 < 2^{k+2} \ln 2$. Для произвольного x подберем k так, что $2^k \leqslant x < 2^{k+1}$. Тогда имеем

$$\theta(x) \leqslant \theta(2^{k+1}) < 2^{k+2} \ln 2 = 2^k 4 \ln 2 < x \cdot 4 \ln 2 \Rightarrow \frac{\theta(x)}{x} \leqslant 4 \ln 2 \Rightarrow \lambda_3 \leqslant 4 \ln 2$$

Докажем теперь, что $\frac{\pi(x)}{x} \geqslant \ln 2$:

$$\underbrace{C_{2n}^0 + \ldots + C_{2n}^{2n}}_{2n+1} = 2^{2n} \Rightarrow C_{2n}^n > \frac{2^{2n}}{2n+1}$$

Определим $\alpha_p :=$ степень, в которой p входит в каноническое разложение C_{2n}^n

$$\alpha_p = \left[\frac{2n}{p}\right] + \left[\frac{2n}{p^2}\right] + \ldots - 2\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2} + \ldots\right]\right) = \left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right) + \left(\left[\frac{2n}{p^2}\right] - 2\left[\frac{n}{p^2}\right]\right) + \ldots$$

используя неравенство $[2x] - 2[x] \leqslant 1$, получаем, что $\alpha_p \leqslant \left[\frac{\ln 2n}{\ln p}\right]$. Тогда

$$C_{2n}^n \leqslant \prod_{p \leqslant 2n} p^{\alpha_p} \leqslant \prod_{p \leqslant 2n} p^{\left[\ln 2n / \ln p\right]} = exp\left(\sum_{p \leqslant 2n} \left[\frac{\ln 2n}{\ln p} \ln p\right] \cdot \ln p \right) = e^{\psi(2n)}$$

Прологарифмируем неравенство $\frac{2^{2n}}{2n+1} \leqslant C_{2n}^n \leqslant e^{\psi(2n)} \Rightarrow \psi(2n) \geqslant 2n \ln 2 - \ln(2n+1)$.

Для произвольного x подберем n так, что $2n \leqslant x \leqslant 2(n+1)$ (в частности, $2n > x-2$). Для таких n и x имеем

$$\psi(x) \geqslant \psi(2n) \geqslant 2n\ln 2 - \ln(2n+1) > (x-2)\ln 2 - \ln(x-1) \Rightarrow \frac{\psi(x)}{x} > \ln 2 - \frac{2\ln 2}{x} - \frac{\ln(x-1)}{x}$$

устремляя $x \to \infty$, получаем, что $\lambda_3 = \lambda_2 \geqslant \ln 2$. Аналогичные рассуждения для μ_2 и μ_1. □

3.4 Квадратичные вычеты и невычеты

3.4.1 Определения и свойства

Теорема 3.4.1. *Рассмотрим сравнение $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \equiv 0 \pmod p$, где все a_i — целые. Тогда, если это сравнение имеет $n+1$ различное решение (по модулю p), то $\forall i\ a_i \equiv 0 \pmod p$.*

Доказательство. Представим f в виде $f(x) = a_n(x-x_1)\ldots(x-x_n) + b_1(x-x_1)\ldots(x-x_{n-1}) + \ldots + b_{n-1}(x-x_1) + b_n$. Подставляя последовательно $x_1, \ldots, x_{n+1}$ получаем, что $b_n, b_{n-1}, \ldots, a_n \equiv 0 \pmod p$, а т.к. $a_i = \alpha_1 a_n + \beta_1 b_1 + \ldots + \beta_n b_n$, то $a_i \equiv 0 \pmod p$. □

Определение 3.4.1. Пусть p — нечетное простое число. Если $(a,\ p) = 1$ и сравнение $x^2 \equiv a \pmod p$, то a называется *квадратичным вычетом* по модулю p. В противном случае a называется *невычетом*.

Для каждого a, при которых это сравнение разрешимо, существует два корня: $+x_0$ и $-x_0 \Rightarrow$ количетсво кв. вычетов $\leqslant \frac{p-1}{2}$. С другой стороны, если при каком-то a имеется 4 решения, то по теореме 3.4.1 $1 \equiv 0 \pmod p$, а значит количество вычетов $\geqslant \frac{p-1}{2}$, а это означает, что количество вычетов и невычетов в точности $\frac{p-1}{2}$.

Теорема 3.4.2. *Если a — квадратичный вычет, то*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p,$$

иначе

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Доказательство.

$$a^{p-1} \equiv 1 \pmod p \Rightarrow a^{p-1} - 1 \equiv 0 \Rightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Обе скобки не могут одновременно делится на p (иначе их разность бы делилась на p), а значит ровно одна из них делится на p. При этом, если $a \equiv x^2 \pmod{p}$, то $a^{\frac{p-1}{2}} \equiv x^{2 \cdot \frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ □

Утверждение 3.4.1.1. Пусть a — квадратичный вычет по модулю нечетного простого числа p. Тогда a является квадратичным вычетом по модулю p^l для любого натурального l.

Доказательство. Рассмотрим решение сравнения $x^2 \equiv a \pmod{p}$. Тогда $x^2 = a + mp \pmod{p^2}$ для некоторого m. Положим $y = x + zp$ для некоторого z. Тогда $y^2 \equiv x^2 + 2xzp \equiv a + (m + 2xz)p \pmod{p^2}$. Положим $z = m(2x)^{-1} \pmod{p}$ (очевидно, что p не может делить 2 и x, а значит число $2x$ обратимо в $\mathbb{Z}_p$). Тогда $y^2 \equiv a \pmod{p^2} \Rightarrow a$ является квадратичным вычетом по модулю p^2. Аналогичные рассуждения обобщаются по индукции для доказательства для произвольной степени p. □

Утверждение 3.4.1.2. (б/д)

Если $a \equiv 1 \pmod{8}$, то a является квадратичным вычетом по модулю 2^k.

Утверждение 3.4.1.3. (б/д)

Пусть $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$. Тогда, если a является квадратичным вычетом по каждому из модулей $p_1^{\alpha_1}, \dots, p_n^{\alpha_n}$, то a является квадратичным вычетом по модулю m.

3.4.2 Символ Лежандра

Определение 3.4.2. Пусть $(a,\ p) = 1$. *Символом Лежандра* называется число

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ — квадратичный вычет,} \\ -1, & \text{иначе} \\ 0, & (a,\ p) \neq 1 \text{ (иногда)} \end{cases}$$

Достаточно очевидны следующие свойства символа Лежандра

1. $\left(\frac{1}{p}\right) = 1$
2. $\left(\frac{a}{p}\right) = a^{(p-1)/2}$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

4. $\left(\dfrac{a+kp}{p}\right) = \left(\dfrac{a}{p}\right)$
5. $\left(\dfrac{a^2}{p}\right) = 1$

Теорема 3.4.3.

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

Доказательство. Положим $p_1 := \frac{p-1}{2}$. Рассмотрим $a:\ (a,\ p) = 1$. Пусть

$$a \cdot 1 = \varepsilon_1 \cdot r_1$$

$$a \cdot 2 = \varepsilon_2 \cdot r_2$$

$$\dots$$

$$a \cdot p_1 = \varepsilon_{p_1} \cdot r_{p_1}$$

где $\varepsilon_i = \pm 1$, $r_i = \min\{a \cdot i \bmod p, -a \cdot i \bmod p\}$ — то есть минимальное по абсолютному значению сравнимое с $a \cdot i$ число, взятое с нужным знаком. Тогда

$$a^{p_1} \cdot (1 \cdot 2 \cdot \ldots \cdot p_1) \equiv \varepsilon_1 \cdot \ldots \cdot \varepsilon_{p_1} \cdot (r_1 \cdot \ldots \cdot r_{p_1}).$$

Из выбора r_i, их можно сократить с произведением $(1 \cdot \ldots \cdot p_1)$, а значит

$$a^{p_1} \equiv \varepsilon_1 \cdot \ldots \cdot \varepsilon_{p_1}.$$

Рассмотрим ε_x, где $x \in \{1,\ \ldots,\ p_1\}:\ \exists k \in \mathbb{N}:\ kp \leqslant ax \leqslant (k+1)p$. Тогда $\varepsilon_x = 1$ если x на координатной прямой находится ближе к kp, и -1 иначе:

$$\left\{\frac{ax}{p}\right\} \leqslant \frac{1}{2} \Rightarrow \varepsilon_x = 1$$

поэтому (нетрудно проверить), что ε_x можно переписать следующим образом:

$$\varepsilon_x = (-1)^{\left[2 \cdot \left\{\frac{ax}{p}\right\}\right]} = (-1)^{\left[\frac{2ax}{p} - 2\left[\frac{ax}{p}\right]\right]} = (-1)^{\left[\frac{2ax}{p}\right]}$$

а значит $\left(\dfrac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1}\left[2ax/p\right]}$.

Если a нечетное, то $a + p$ — четное. Тогда:

$$\left(\frac{2a}{p}\right) = \left(\frac{4\left(\frac{a+p}{2}\right)}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]} = (-1)^{\sum\limits_{x=1}^{p_1}[ax/p]+x} = (-1)^{\frac{p_1(p_1+1)}{2} + \sum\limits_{x=1}^{p_1}[ax/p]}$$

Взяв $a = 1$ и подставив $p_1 = \frac{p-1}{2}$ получаем требуемое (т.к. целая часть равна 0 для любого x из пределов суммирования). □

Теорема 3.4.4. *(квадратичный закон взаимности)*

Пусть p и q различные нечетные простые числа. Тогда

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

Доказательство. Рассмотрим множество $S = \{(qx, py) : x = 1, \ldots, \frac{p-1}{2}; y = 1, \ldots, \frac{q-1}{2}\}$. $|S| = \frac{p-1}{2} \cdot \frac{q-1}{2}$.

Если $qx = py$, то $q \mid py$ что невозможно. Поэтому $S = S_1 \sqcup S_2$, где $S_1 = \{(qx,\, py) : qx < py\}$, $S_2 = \{(qx,\, py) : qx > py\}$. Поскольку $S = S_1 \sqcup S_2$, то $|S| = |S_1| + |S_2|$.

Найдем $|S_1|$: так как $qx < py$, то $x \leqslant \left[\frac{py}{q}\right] \Rightarrow (-1)^{|S_1|} = (-1)^{\sum\limits_{y=1}^{q}[py/q]} = \left(\frac{p}{q}\right)$. Аналогично $(-1)^{|S_2|} = \left(\frac{q}{p}\right)$, откуда следует, что

$$(-1)^{|S|} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = (-1)^{|S_1|} \cdot (-1)^{|S_2|} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$$

□

3.5 Первообразные корни и индексы

3.5.1 Первообразные корни

Определение 3.5.1. Минимальная натуральная степень γ, в которой число a сравнимо с 1 по модулю m назовем *показателем a* по модулю m.

Утверждение 3.5.1.1. Если γ — показатель a по модулю m, то $\gamma \mid \varphi(m)$.

Доказательство. Пусть $\varphi(m) = \gamma k + r$, $0 < r < \gamma$. По теореме Эйлера

$$1 \equiv a^{\varphi(m)} \equiv a^{\gamma k + r} \equiv a^r$$

что противоречит минимальности γ. □

Определение 3.5.2. Число g называется *первообразным корнем* по модулю m, если $(g,\, m) = 1$ и минимальная (не нулевая) степень, в которой g сравнимо с 1 по модулю m равна $\varphi(m)$.

Теорема 3.5.1. *(о существовании первообразных корней)*

Первообразные корни существуют только по модулям 2, 4, p, p^α, $p^{2\alpha}$, *где* p — *любое нечетное простое число,* $\alpha \in \mathbb{N}$.

Доказательство. $1:2$) Тривиально так как $\varphi(2) = 1$.

$2:4$) Число 3 является первообразным корнем по модулю 4.

$3:p$) Обозначим за δ_i показатель числа i для $i \in \{1, \ldots, p-1\}$. Определим $\tau := [\delta_1, \ldots, \delta_{p-1}]$ — наименьшее общее кратное этих чисел. Поскольку $\tau \geqslant 2 \Rightarrow \tau = q_1^{\alpha_1} \ldots q_k^{\alpha_k}$. Поскольку τ делится на любое δ_i, то $\forall i = 1, \ldots, k\ \exists \delta \in \{\delta_1, \ldots, \delta_{p-1}\} :\ \delta = a q_i^{\alpha_i}$, где $(a,\ q_i) = 1$. Пусть x_i это число, чей показатель δ_i, a_i из утверждения выше.

Утверждение 3.5.1.2. Показатель $x_i^{a_i}$ равен $q_i^{\alpha_i}$.

Доказательство. От противного □

Положим $g := x_1^{a_1} \ldots x_k^{a_k}$. Нетрудно проверить, что показатель числа g это в точности τ. Тогда

1. По определению показателя $\tau \leqslant p-1$
2. Рассмотрим сравнение $x^\tau \equiv 1 \pmod p$. По определнию τ все числа от 1 до $p-1$ являются его решениями, но $p \nmid 1$, а значит $p - 1 \leqslant \tau$ по теореме 3.4.1.

откуда следует, что $\tau = p-1$ и это показатель g.

$4:p^\alpha, 2p^\alpha$) Пусть g — первообразный корень по модулю p, чье существование доказано в предыдущем пункте.

Лемма 3.5.2.

$$\exists t :\ (g+pt)^{p-1} = 1 + pu, \quad \text{где } (u,\ p) = 1$$

Доказательство.

$$\begin{aligned}(g+pt)^{p-1} &= g^{p-1} + (p-1)ptg^{p-2} + p^2 a = \\ &= \underbrace{1 + pb}_{g^{p-1} \equiv 1} + (p-1)ptg^{p-2} + p^2 a = \\ &= 1 + p(b + \underbrace{(p-1)g^{p-2}}_{\text{в.п. с } p} t + pa) = 1 + p(b + ct + a)\end{aligned}$$

поскольку ct любое, то просто подберем t так, чтобы $b + ct + pa$ не делилось на p (т.к. ct пробегает всю систему вычетов) $\square$

$\varphi(p^\alpha) = (p-1)p^{\alpha-1}$. Покажем, что число $g + pt$ из леммы имеет $(p-1)p^{\alpha-1}$ в качестве показателя.

Пусть δ — показатель $g + pt$. Тогда $(g+pt)^\delta \equiv 1 \pmod{p^\alpha} \Rightarrow (g+pt)^\delta \equiv 1 \pmod{p} \Rightarrow p - 1 \mid \delta$.

С другой стороны, т.к. δ показатель, то он делит $\varphi(p^\alpha) = (p-1)p^{\alpha-1} \Rightarrow \delta = (p-1)p^\beta$. Имеем

$$(g+pt)^{p-1} = 1 + pu$$

$$(g+pt)^{(p-1)p} = (1+pu)^p = 1 + p^2u + p^3a = 1 + p^2u_1, \;\; (u_1,\, p) = 1$$

$$(g+pt)^{(p-1)p^\beta} = 1 + p^{\beta+1}u_\beta, \;\; (u_\beta,\, p) = 1$$

С одной стороны, $\beta \mid \alpha - 1$. Но т.к. δ это показатель g, то $p^{\beta+1}u_\beta \mid p^\alpha \Rightarrow \beta + 1 \mid \alpha$. Это означает, что $\beta = \alpha - 1 \Rightarrow \delta = (p-1)p^{\alpha-1}$

Для $2p^\alpha$: $\varphi(2p^\alpha) = \varphi(p^\alpha)$. Возьмем g — показатель по p^α. Если он оказался четным, то возьмем новый $\tilde{g} = g + p^\alpha$.

Несуществование по модулю 2^α, $\alpha \geqslant 3$) По индукции по t легко доказать, что

$$(2k+1)^{2^{t-2}} = 1 + 2^t a$$

но $\varphi(2^\alpha) = 2^{\alpha-1}$, а любое нечетное число сравнимо с 1 по модулю 2^α в двое меньшей степени.

Несуществование по произвольному модулю) Пусть $m = 2^\alpha p_1^{s_1} \dots p_\alpha^{s_\alpha}$. Рассмотрим a — взаимно простое с m. Пусть $\delta = [\varphi(2^\alpha),\, \varphi(p_1^{\alpha_1}), \dots,\, \varphi(p_s^{\alpha_s})]$. Тогда $a^g \equiv 1$, но $g < \varphi(m)$. $\square$

3.5.2 Системы индексов

Определение 3.5.3. *Индексом* числа a по модулю m по основанию g называется такое число γ, что $g^\gamma \equiv a \pmod{p}$. Обозначение: $\gamma = \mathrm{ind}_g a$

Сначала покажем, как строить системы индексов.

Пусть $m = 2^\alpha$. $5 = 1 + 4$, $5^2 = 1 + 8 + 16 = 1 + 8t_1$, $\dots$, $5^{2^{\alpha-3}} = 1 + 2^{\alpha-1}t_{\alpha-3}$, где $\forall i\, (t_i,\, 2) = 1$. Тогда

все числа

$$5^1,\ 5^2,\ 5^3,\ \ldots,\ 5^{2^{\alpha-2}}$$

$$-5^1,\ -5^2,\ -5^3,\ \ldots,\ -5^{2^{\alpha-2}}$$

различные по модулю 2^α среди одной строки, а числа среди разных строк различны, так как они различны по модулю 4. Это означает, что если a из приведенной системы вычетов по модулю 2^α, то существует такие γ_0, γ_1 что $a = (-1)^{\gamma_0}5^{\gamma_1}$, где $\gamma_0 \in \{0, 1\}$, $\gamma_1 \in \{1, 2, \ldots, 2^{\alpha-2}\}$. Тогда (γ_0, γ_1) называется системой индексов по модулю 2^α.

Пусть теперь $m = 2^\alpha p_1^{\alpha_1} \ldots p_s^{\alpha_s}$. Тогда системой индексов называется набор $(\gamma_0; \gamma_1; \mathrm{ind}_{p_1^{\alpha_1}} a; \ldots; \mathrm{ind}_{p_s^{\alpha_s}} a)$

3.6 Диофантовы приближения

3.6.1 Теорема Дирихле

Теорема 3.6.1. *(Дирихле)*

Если α иррациональное, то существует бесконечно много различных несократимых дробей $\frac{p}{q}$, таких что

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{q^2}$$

Замечание: Для рациональных чисел теорема неверна (если вы хотите проверить это, покажите сначала, что знаменатели таких дробей ограничены).

Доказательство. Пусть $Q \in \mathbb{N}_+$. Разобьем отрезок $[0, 1]$ на Q частей. Рассмотрим числа $\{\alpha\}, \{2\alpha\}, \ldots, \{(Q+1)\alpha\}$. По принципу Дирихле среди существует два различных x_1, x_2, таких что $\{\alpha x_1\}$, $\{\alpha x_2\}$ лежат в одном отрезке $\left[\frac{k}{Q};\ \frac{k+1}{Q}\right]$.

Это означает, что

$$|\{\alpha x_1\} - \{\alpha x_2\}| = |\alpha(x_1 - x_2) - ([\alpha x_1] - [\alpha x_2])| < \frac{1}{Q}$$

Положим $q_1 := (x_1 - x_2) < Q$, $p_1 := ([\alpha x_1] - [\alpha x_2])$. Тогда

$$|\alpha q_1 - p_1| < \frac{1}{Q} \Rightarrow |\alpha - \frac{p_1}{q_1}| < \frac{1}{Qq_1} \leqslant \frac{1}{q_1^2}$$

. Возьмем теперь Q такое, что $|\alpha q_1 - p_1| > \frac{1}{Q}$ и просто напросто найдем новые p_2 и q_2 по той же процедуре. $\square$

3.6.2 Цепные дроби

Определение 3.6.1. *Цепной дробью* называется число $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}} = [a_0;\, a_1\, a_2,\, \dots,\, a_n]$.

Канонической записью цепной дроби называется запись, получаемая по индукции: $[a_0] = \frac{a_0}{1}, [a_0; a_1, \dots, a_n] = a_0 + \frac{1}{[a_1;\, a_2,\, \dots,\, a_n]}$ Числа a_i называются *неполными частными*, а дробь $[a_0;\, a_1,\, \dots,\, a_k] = \frac{p_k}{q_k}$ — k-той *подходящей* дробью.

Теорема 3.6.2. *Для числителей и знаменателей подходящих дробей верны следующие соотношения:*

$$\begin{cases} p_k = a_k p_{k-1} + p_{k-2} \\ q_k = a_k q_{k-1} + q_{k-2} \end{cases}$$

Доказательство. Доказательство индукцией по k. База индукции: $p_0 = a_0$, $p_1 = a_0 a_1 + 1$, $p_2 = a_2(a_0 a_1 + 1) + a_0$; $q_0 = 1$, $q_1 = a_1$, $a_2 = a_1 a_2 + 1$ — считаются руками. Далее докажем переход индукции.

$$[a_0;\, a_1,\, \dots,\, a_{k+1}] = \frac{p_{k+1}}{q_{k+1}}$$
$$[a_1;\, a_2,\, \dots,\, a_{k+1}] = \frac{p^*_{k+1}}{q^*_{k+1}}$$
$$[a_0;\, a_1,\, \dots,\, a_{k+1}] = a_0 + \frac{1}{\frac{p^*_{k+1}}{q^*_{k+1}}} = \frac{a_0 p^*_{k+1} + q^*_{k+1}}{p^*_{k+1}}$$

Тем самым получены следующие соотношения

$$\begin{cases} p_{k+1} = a_0 p^*_{k+1} + q^*_{k+1} \\ q_{k+1} = p^*_{k+1} \end{cases}$$

Тогда, применяя предположение индукции для $[a_1;\, a_2,\, \dots,\, a_{k+1}]$, имеем для q_{k+1}

$$q_{k+1} = p^*_{k+1} = a_{k+1} p^*_k + p^*_{k-1} = a_{k+1} q_k + q_{k-1}$$

и чуть сложнее для p_{k+1}

$$p_{k+1} = a_0(a_{k+1} p^*_k + p^*_{k-1}) + a_{k+1} q^*_k + q^*_{k-1} = a_{k+1}(a_0 p^*_k + q^*_k) + (a_0 p^*_{k-1} + q^*_{k-1}) = a_{k+1} p_k + p_{k-1}$$

□

Следствие 3.6.1. *Умножим первое равенство на q_{k-1}, второе на p_{k-1} и вычтем второе из первого. Получим*

$$p_k q_{k-1} - q_k p_{k-1} = p_{k-2} q_{k-1} - p_{k-1} q_{k-2}(1).$$

Если обозначить $r_k := p_k q_{k-1} - q_k p_{k-1}$, то это значит, что для последовательности r_k верно

$$r_k = -r_{k-1}$$

Легко посчитать, что $r_1 = p_1 q_0 - q_1 p_0 = (a_0 a_1 + 1) - a_1 a_0 = 1$, а это значит, что $(p_k,\ q_k) = 1$.

Более того, умножив равенство (1) на $\dfrac{1}{q_k q_{k-1}}$ получим

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k+1}}{q_k q_{k-1}}$$

которое означает, что дроби с нечетными номерами больше чем дроби с четными номерами.

Следствие 3.6.2. *Умножим первое равенство на q_{k-2}, второе на p_{k-2} и снова найдем их разность:*

$p_k q_{k-2} - q_k p_{k-2} = a_k(p_{k-1} q_{k-2} - q_{k-1} p_{k-2}) = a_k(-1)^k$.

Умножив полученное на $\dfrac{1}{q_k q_{k-2}}$ имеем

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_{k-2} q_k}$$

откуда следует, что дроби с нечетными номерами убывают, а дроби с четными — возрастают.

Определение 3.6.2. Число α равно *бесконечной цепной дроби* $[a_0;\ a_1,\ \ldots,\ a_n,\ \ldots]$, если $\alpha = \lim\limits_{n\to\infty} \frac{p_n}{q_n}$, если этот предел существует и конечен.

Встает вопрос: как разложить число в цепную дробь?. На самом деле довольно просто:

$$a = [a] + \{a\} = [a] + \frac{1}{\frac{1}{\{a\}}} = \ldots$$

Утверждение 3.6.2.1. (б/д) Описанный процесс согласуется с определением значения цепной дроби.

Теорема 3.6.3. *(теорема Дирихле)*

Доказательство через цепные дроби.

Доказательство. Пусть дроби $\frac{p_n}{q_n}$ приближают α. Тогда

$$\left|\alpha - \frac{p_{2k-1}}{q_{2k-1}}\right| \leqslant \left|\frac{p_{2k}}{q_{2k}} - \frac{p_{2k-1}}{q_{2k-1}}\right| = \frac{1}{q_{2k}q_{2k-1}} < \frac{1}{q_{2k-1}^2}$$

□

Теорема 3.6.4. *(б/д)*

Для любого иррационального числа α существует бесконечно много различных несократимых дробей $\frac{p}{q}$, таких что

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{\sqrt{5}q^2}$$

Теорема 3.6.5. *(б/д)*

Если $\alpha = \frac{1+\sqrt{5}}{2}$, то для любого положительного ε неравенство

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{(\sqrt{5}+\varepsilon)q^2}$$

имеет лишь конечное число решений в p, q.

Если в условиях теоремы убрать из рассмотрения $\frac{1+\sqrt{5}}{2}$ и эквивалентные ему по сходимости, то новой границей будет

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{\sqrt{8}q^2}$$

Повторим еще раз. Получим новую оценку:

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{5}{\sqrt{271}} \cdot \frac{1}{q^2}$$

Продолжая выбрасывать числа из рассмотрения, получим последовательность констант, каждый раз ограничивая апроксимацию $\{c_n\}$. Полученная последовательность называется *спектром Лагранжа*, причем $\lim\limits_{n\to\infty} c_n = \frac{1}{3}$

Теорема 3.6.6. *Пусть $\psi(q)$ — любая функция, принимающая только положительные значения и монотонно стремящаяся к бесконечности. Тогда существует иррациональное число α, что для него существует бесконечно много различных дробей $\frac{p}{q}$, таких что*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\psi(q)}$$

Доказательство. Заметим, что $q_{2k} = a_{2k}q_{2k-1} + q_{2k-2} \geqslant a_{2k}$. Построим α так, чтобы его неполные частные с четными номерами были больше, чем $\psi(q_{2k-1})$. Тогда

$$\left|\alpha - \frac{p_{2k-1}}{q_{2k-1}}\right| \leqslant \frac{1}{q_{2k-1}q_{2k}} \leqslant \frac{1}{a_{2k}} < \frac{1}{\psi(q_{2k-1})}$$

т.к. ψ монотонно возрастает, то a_{2k} тоже, а значит предел $\frac{p_k}{q_k}$ конечен. □

Теорема 3.6.7. *(Гипотеза Бахвалова-Коробова-Зарембы)*

Для любого натурального числа p существует число $a \in \{1, \ldots, p\}$: такое, что у $\frac{a}{p}$ не превосходят 5.

3.6.3 Алгебраические и трансцендетные числа

Определение 3.6.3. Число a называется *алгебраическим*, если оно является корнем некоторого многочлена с рациональными коэффицентами. Множество алгебраических чисел образует поле.

Множество алгебраических чисел счетно, а значит существует не алгебраические числа. Если число a не является алгебраическим, то оно называется *трансцендентным.*

Теорема 3.6.8. *(Лиувилль, б/д)*

Если α — алгебраическое число, причем минимальная степень многочлена, корнем которого является α равна n, то тогда существует число $c = c(\alpha)$, такое что неравенство

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{c}{q^n}$$

имеет лишь конечное число различных решений $\frac{p}{q}$.

Построим явно пример трансцендентного числа: воспользуемся теоремой 3.6.6 и будем строить число для, например, $psi(q_n) = e^{q_n}$. Тогда с некоторого n аппроксимация будет лучше, чем та, которой нет по теореме Лиувилля.

Теорема 3.6.9. *(Гельфонд, б/д)*

Пусть α, β — алгебраические числа, причем $\alpha \neq 0, 1$, а β иррациональное. Тогда α^β трансцендентное.

Докажем, что e^π трансцендентное. Предположим, что e^π алгеброическое. Тогда $(e^\pi)^i = -1$ — алгебраическое. Противоречие с теоремой Гельфонда.

Известно, что числа e, π, $\pi \pm e^\pi$, $\pi \cdot e^\pi$ — трансцендентные. Однако это практически всё, что известно. Например, про число $\pi + e$ неизвестно даже, иррационально ли оно.

3.7 Геометрия чисел

3.7.1 Теоремы Миньковского на плоскости

Определение 3.7.1. Назовем фигуру на плоскости *простой*, если она состоит из конечного числа попарно непересекающихся прямоугольников. Определим площадь простой фигуры как сумму площадей состовляющих ее прямоугольников (площадь прямоугольника равна произведению его сторон).

Рассмотрим теперь ограниченное множество точек плоскости Ω. Определим *нижнюю меру* $\mu_*(\Omega)$ как супремум суммы площадей всех простых фигур, целиком содержащихся в Ω. Определим *верхнюю меру* $\mu^*(\Omega)$ как инфимум суммы площадей всех простых фигур, целиком содержащих Ω. Тогда, если $\mu_*(\Omega) = \mu^*(\Omega) = S$, то множество Ω называется *измеримым*, а S — его площадью (краткое описание меры Жордана). Если верхняя и нижняя меры не совпадают, то множество называется *неизмеримым*.

Пример неизмеримого множества: рациональные точки квадрата единичной площади. Нижняя мера равна 0, а верхняя — 1.

Определение 3.7.2. Множество Ω называется *выпуклым*, если $\forall x,\ y \in \Omega$ отрезок, соединяющий их, целиком лежит в Ω.

Определение 3.7.3. Зафиксируем на плоскости некоторую систему координат $O(0,\ 0)$. Если для любого $x \in \Omega$ точка $-x$ тоже содержится в Ω, то Ω называется *центрально симметрическим*.

Теорема 3.7.1. *Если Ω — выпуклое центрально симметричное тело с площадью $S > 4$, то в Ω есть нетривиальные целые точки*

Доказательство. Пусть $\mathbb{Z}^2$ это множество всех точек с целыми координатами, $p \in \mathbb{N}$. Определим множество $\frac{1}{p}\mathbb{Z}^2$ как множество точек вида $\left(\frac{a}{p},\ \frac{b}{p}\right)$, $(a,\ b) \in \mathbb{Z}^2$.

Рассмотрим множество $\Omega \cap \frac{1}{p}\mathbb{Z}^2$. Положим $N_p := |\Omega \cap \frac{1}{p}\mathbb{Z}^2|$. Поскольку площадь одной точки равна $\frac{1}{p^2}$, то

$$\frac{N_p}{p^2} \to S \text{ при } p \to \infty \Rightarrow \exists p : \frac{N_p}{p^2} > 4 \Rightarrow N_p > 4p^2 = (2p)^2$$

Определим на $\frac{1}{p}\mathbb{Z}^2$ отношение эквивалентности $\sim$:

$$\left(\frac{a_1}{p}, \frac{a_2}{p}\right) \sim \left(\frac{b_1}{p}, \frac{b_2}{p}\right) \iff a_1 \equiv b_1,\ a_2 \equiv b_2 \pmod{2p}$$

Количество классов эквивалентостей равно $(2p)^2$. Поскольку $N_p > (2p)^2$, то в $\Omega \cap \frac{1}{p}\mathbb{Z}^2$ есть две разные точки $A = \left(\frac{a_1}{p}, \frac{a_2}{p}\right)$ и $B = \left(\frac{b_1}{p}, \frac{b_2}{p}\right)$, лежащие в одном классе эквивалентности $A \sim B$. Из центральной симметрии следует, что $-B \in \Omega$, а из выпуклости, что середина C отрезка $[A, -B] \in \Omega$.

Рассмотрим точку C:

$$C = \left(\frac{a_1 - b_1}{2p}; \frac{a_2 - b_2}{2p}\right) \in \mathbb{Z}^2$$

поскольку числитель каждой дроби $\equiv 0 \pmod{2p}$. □

Теорема 3.7.2. *(теорема Минъковского)*

Пусть Ω выпуклое, центрально симметричное замкнутое тело (содержит свои границы) с площадью $S \geqslant 4$. Тогда в Ω есть нетривиальная целая точка.

Доказательство аналогично предыдущему случаю.

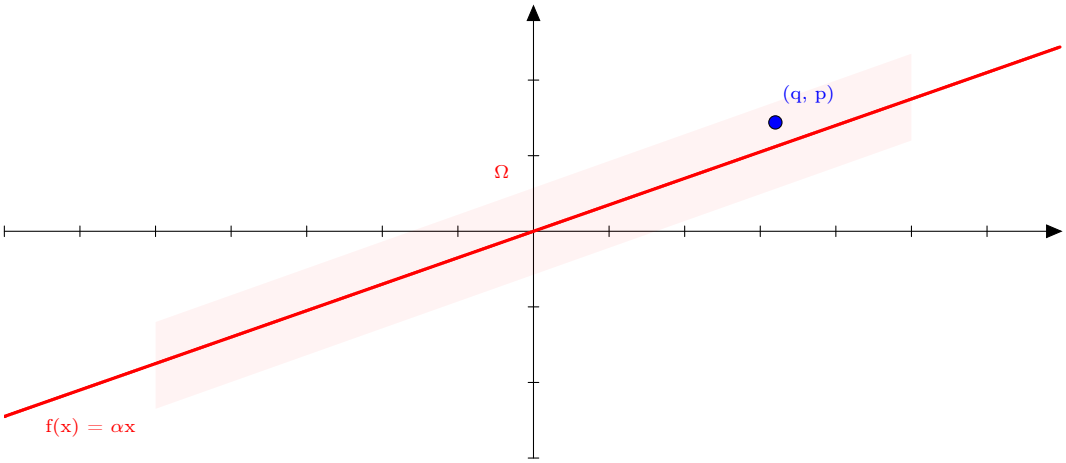
Теорема 3.7.3. *(теорема Дирихле)*

Доказательство из теоремы Минъковского.

Доказательство. Пусть $\Omega = \{(x, y) : |\alpha x - y| \leqslant \frac{1}{Q},\ -Q \leqslant x \leqslant Q\}$. Тогда Ω выпуклое и центрально симметричное. $S(\Omega) = 2Q \cdot \frac{2}{Q} = 4 \Rightarrow \exists (q, p) \in \Omega \cap \mathbb{Z}^2 \backslash \{(0, 0)\}$. Для этой точки

$$|\alpha q - p| \leqslant \frac{1}{Q},\ |q| \leqslant Q \Rightarrow \left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{Qq} \leqslant \frac{1}{q^2}$$

Для нахождения новых точек построим новый параллелограмм для бОльшего значения Q так, чтобы уже рассмотренная точка (q, p) не попала в него, при этом сохранив его площадь. □



3.7.2 Теорема Миньковского в пространстве $\mathbb{R}^n$

Определение 3.7.4. *Каноническим параллелепипедом* в пространстве $\mathbb{R}^n$ называется множество точек $\{x \in \mathbb{R}^n : a_i \leqslant x_i \leqslant b_i\}$. Простым телом называется объединение некоторого конечного числе непересекающихся параллелепипедов. Мерой параллелепипеда называется произведение $\prod_{i=1}^{n}(b_i - a_i)$. В остальном определение меры аналогично плоскому случаю.

Теорема 3.7.4. *(теорема Миньковского)*

Пусть Ω — выпуклое центрально симметричное замкнутое тело с мерой $\mu(\Omega) \geqslant 2^n$. Тогда в Ω есть нетривиальная целая точка.

Доказательство аналогично плоскому случаю.

3.7.3 Решетки и теоремы Миньковского

Определение 3.7.5. Решеткой Λ на плоскости называется множество точек $\{a_1\vec{e_1} + a_2\vec{e_2};\ a_1,\ a_2 \in \mathbb{Z}\}$, где $\vec{e_1}$, $\vec{e_2}$ это базис в $\mathbb{R}^2$. Например, стандартная целочисленная решетка получается если в качестве базиса выбрать $\vec{e_1} = (1,\ 0)^T$, $\vec{e_2} = (0,\ 1)^T$.

У каждой решетки есть ячейки, на которые она "разбивает"плоскость. Эти ячейки называются *фундаментальными областями* решетки Λ.

Мера фундаментальной области решетки называется ее *определителем* $\det\Lambda$.

Теорема 3.7.5. *(Миньковский)*

Пусть Λ — решетка на плоскости, а Ω — ц/с выпуклое тело с $\mu(\Omega) > 4 \det \Lambda$. Тогда

$$\Omega \cap \Lambda \backslash \{0\} \neq \varnothing$$

Определение 3.7.6. Решетка Λ в $\mathbb{R}^n$ определяется аналогично плоскому случаю. Определитель решетки равен $|\det(e_1, \ldots, e_n)|$

Теорема 3.7.6. *(Миньковский)*

Пусть Λ — решетка в $\mathbb{R}^n$, Ω — выпуклое ц/с тело с $\mu(\Omega) > 2^n \det \Lambda$. Тогда

$$\Omega \cap \Lambda \backslash \{0\} \neq \varnothing$$

Определение 3.7.7. *Критическим детерминантом* множества Ω называется $\inf\{\det \Lambda : \Lambda \cap \Omega \backslash \{0\} = \varnothing\} = \Delta(\Omega)$

Теорема 3.7.7. *(Миньковский)*

Пусть Ω такое же как и раньше с $\dfrac{\mu(\Omega)}{\Delta(\Omega)} \leqslant 2^n$. Тогда верно все то же самое.

Теорема 3.7.8. *(1945, Миньковский-Главка, б/д)*

Пусть Ω — произвольное измеримое множество. Тогда

$$\frac{\mu(\Omega)}{\Delta(\Omega)} \geqslant 1$$

Теорема 3.7.9. *(1960-е, Шмидт, б/д)*

Пусть Ω — произвольное измеримое множество. Тогда

$$\frac{\mu(\Omega)}{\Delta(\Omega)} \geqslant cn, \text{ где } c > 0$$