Дискретная математика, Коллоквиум 2

Балюк Игорь
@lodthe, GitHub

2019 — 2020

Материалы взяты из учебника Александра Рубцова.

Содержание

1 Определения

Контрольный вопрос на понимание определений включает в себя формулировку одного определения из списка ниже и контрольный вопрос по этому определению. Пример: «Определение полного прообраза. Пусть $f(x) = x^2$ — функция из $\mathbb{Z}$ в $\mathbb{Z}$. Найдите полный прообраз множества $\{1, 2, 3, 4\}$.

1. Деление целых чисел с остатком.

Говорят, что целое число a делится на целое число b, если $a = bk$ для некоторого целого числа k. В этом случае говорят также «a кратно b», и «b является делителем числа a».

Теперь определим деление остатком. Пусть b — целое положительное число. Деля на b с остатком, мы связываем предметы в пачки по b в каждой, пока это возможно: количество полных пачек называется частным (говорят ещё «неполное частное», чтобы отличать от частного как дроби), и сколько-то предметов останется, их количество и называют остатком.

Формально: разделить целое a на целое положительное b означает найти такое целое q (*частное*) и такое r (*остаток*), что

$$a = b \cdot q + r; \quad 0 \leqslant r < b.$$

2. Сравнения по модулю. Основные свойства.

Если два числа a и b дают одинаковые остатки при делении на положительное число N, то говорят, что они *сравнимы* по модулю N, и пишут $a \equiv b \pmod{N}$.

Эквивалентное определение: a и b сравнимы по модулю N, если разность $a - b$ делится на N.

Рассмотрим основные свойства:

1. $a \equiv b \pmod{c} \iff b \equiv a \pmod{c}$
2. $a \equiv b \pmod{c} \iff (a - x) \equiv (b - x) \pmod{c}$
3. $x \equiv a \pmod{m}, y \equiv b \pmod{m} \implies xy \equiv ab \pmod{m}$
4. $a \equiv 0 \pmod{c} \iff c \mid a$
5. $a \equiv b \pmod{d}, b \equiv c \pmod{d} \iff a \equiv c \pmod{d}$

Например, можно найти $2^{100} \bmod 7$ (остаток от деления 2^{100} на 7): поскольку $2^3 = 8 \equiv 1 \pmod{7}$, то $2^{99} = (2^3)^{33} \equiv 1^{33} = 1 \pmod{7}$, так что $2^{100} = 2^{99} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod{7}$.

3. Арифметика остатков (вычетов). Обратимые остатки (вычеты).

Остаток (вычет) по модулю N называется **обратимым**, если в произведении с каким-то другим остатком он даёт 1. Другими словами, a обратим, если уравнение $a \cdot x \equiv 1 \pmod{N}$ имеет решение.

4. Малая теорема Ферма.

Теорема. *Если p — простое число, то*

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

при любом a, не делящемся на p.

5. Функция Эйлера. Теорема Эйлера.

Теорема. *Пусть $N > 1$ — произвольное целое число, а $\varphi(N)$ равно количеству остатков среди $0, 1, \ldots, N - 1$, взаимно простых с N. Пусть a — один из этих остатков. Тогда*

$$a^{\varphi(N)} \equiv 1 \pmod{N}.$$

Функцию φ называют **функцией Эйлера** и традиционно обозначают буквой φ. Если N простое, то $\varphi(N) = N - 1$, и теорема Эйлера превращается в малую теорему Ферма.

6. Наибольший общий делитель. Алгоритм Евклида.

Наибольшим общим делителем (НОД) для двух целых чисел m и n называется наибольший из их общих делителей. Пример: для чисел 54 и 24 наибольший общий делитель равен 6.

Алгоритм Евклида помогает найти НОД двух целых чисел.

- **Геометрическая интерпретация**. Пусть даны два отрезка длины a и b. Вычтем из большего отрезка меньший и заменим больший отрезок полученной разностью. Повторяем эту операцию, пока отрезки не станут равны. Если это произойдёт, то исходные отрезки соизмеримы, и последний полученный отрезок есть их наибольшая общая мера. Если общей меры нет, то процесс бесконечен и отрезки несоизмеримы.
- **Алгебраическая интерпретация**. Пусть нам даны два целых числа a и b. Вычтем из большего числа меньшее и заменим большее на полученную разность. Повторяем эту операцию, пока числа не станут равны. Последнее полученное число будет их наибольшим общим делителем. Это можно записать в виде следующей системы:

$$\begin{cases} a_0 = q_1 \cdot a_1 + a_2 \\ a_1 = q_2 \cdot a_2 + a_3 \\ \vdots \\ a_{k-2} = q_{k-1} \cdot a_{k-1} + a_k \\ a_{k-1} = q_k \cdot a_k. \end{cases}$$

  Тогда $q_k = \text{НОД}(a_0, a_1)$.

Алгоритм можно ускорить с помощью деления:

1. Большее число делим на меньшее.
2. Если делится без остатка, то меньшее число и есть НОД (следует выйти из цикла).
3. Если есть остаток, то большее число заменяем на остаток от деления.
4. Переходим к пункту 1.

7. Расширенный алгоритм Евклида нахождения решения линейного диофантова уравнения.

Линейное диофантово уравнение — уравнение вида $ax+by = c$. Решить диофантово уравнение означает найти все такие целые x, y, чтобы выполнялось равенство.

Если с делится на $\text{НОД}(a, b)$, ДУ имеет бесконечно много решений. В противном случае, оно не имеет решений вообще.

Если x_0, y_0 — какое-то частное решение диофантова уравнения, то тогда общее решение выражается следующим образом:

$$\begin{cases} x = x_0 + k \cdot \dfrac{b}{\text{НОД}(a,b)}, \quad k \in \mathbb{Z}, \\ y = y_0 - k \cdot \dfrac{a}{\text{НОД}(a,b)}, \quad k \in \mathbb{Z}, \end{cases}$$

Расширенный алгоритм Евклида — алгоритм, который находит НОДдвух чисел и коэффициенты, с помощью которых он выражается через эти числа, то есть такие x, y, что $ac+by = \text{НОД}(a, b)$. Чтобы получить решение диофантова уравнения, можно домножить x и y на $\dfrac{c}{\text{НОД}(a,b)}$.

Расширенный алгоритм Евклида представляет собой применение обычного алгоритма Евклида, а потом прохода «обратно», пользуясь следующим свойством: если пара (x_1, y_1) является решением уравнения $(b \bmod a) \cdot x_1 + a \cdot y_1 = \text{НОД}(a, b)$, то пара (x, y), такая что

$$\begin{cases} x = y_1 - \left\lfloor \dfrac{b}{a} \right\rfloor \cdot a \\ y = x_1 \end{cases}$$

является решением уравнения $ax + by = \text{НОД}(a, b)$.

Тем самым, надо выполнять алгоритм Евклида для чисел (a, b), а потом восстановить все предыдущие (x_k, y_k) зная (x_{k+1}, y_{k+1}).

8. Простые числа, формулировка основной теоремы арифметики.

Целое число $p > 1$ называется простым, если оно не разлагается в произведение меньших чисел (то есть не имеет положительных делителей, кроме 1 и p).

Теорема. *Всякое целое положительное число, большее 1, разлагается на простые множители, причём единственным образом: любые два разложения отличаются только перестановкой сомножителей.*

9. Равномощные множества.

Множество A называется равномощным множеству B, если существует биекция множества A в множество B.

10. Счётные множества.

Множество называется счётным, если оно равномощно множеству натуральных чисел $\mathbb{N}$.

11. Множества мощности континуум.

Множество имеет мощность **континуум**, если оно равномощно $\mathbb{R}$.

12. Основные определения элементарной теории вероятностей: исходы, события, вероятность события.

Вероятностным пространством называется конечное множество U, его элементы называются **возможными исходами**. **Событием** называется произвольное подмножество $A \subseteq U$.

На вероятностном пространстве задана функция $Pr : U \to [0;1]$, такая что $\sum\limits_{x\in U} \Pr[x] = 1$. Функция Pr называется **вероятностным распределением**, а число $Pr[x]$ называется **вероятностью исхода** $x \in U$. Вероятностью события A называется число $Pr[A] = \sum\limits_{x\in A} \Pr[x]$.

13. Формулировка формулы включений и исключений для вероятностей.

В равновозможной модели для произвольных множеств $A_1, \dots, A_n \subseteq U$ верно

$$\Pr[A_1 \cup A_2 \cup \dots \cup A_n] = \sum_i \Pr[A_i] - \sum_{i<j} \Pr[A_i \cap A_j] + \dots = \sum_{\varnothing \neq I \subseteq \{1,2,\dots,n\}} (-1)^{|I|+1} Pr\left[\bigcap_{i\in I} A_i\right].$$

14. Условная вероятность.

Помимо вероятностей тех или иных событий бывает нужным говорить и о вероятностях одних событий при условии других. Неформально говоря, мы хотим определить вероятность выполнения события A в том случае, когда событие B выполняется.

В терминах вероятностного пространства определение этого понятия довольно естественное: нужно сузить вероятностное пространство на множество B. Так, для равновозможной модели мы получаем, что вероятность A при условии B есть просто $\dfrac{|A \cap B|}{|B|}$, то есть число благоприятных исходов поделенное на число всех исходов (после сужения всего вероятностного пространства до B).

В случае произвольного вероятностного пространства нужно учесть веса исходов, то есть нужно сложить вероятности исходов в $A \cap B$ и поделить на сумму вероятностей исходов в B.

Таким образом, мы приходим к формальному определению. **Условной вероятностью** события A при условии B называется число

$$\Pr[A \mid B] = \frac{Pr[A \cap B]}{\Pr[B]}.$$

15. Независимые события. Основные свойства независимых событий.

События A и B называются независимыми, если

$$\Pr[A] = \Pr[A \mid B].$$

Из определения условной вероятности мы сразу получаем эквивалентное определение независимостей событий. Событие A не зависит от события B, если

$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B].$$

16. Формула полной вероятности.

Лемма. *Пусть $B_1, B_2, \dots, B_n$ — разбиение вероятностного пространства, то есть $U = B_1 \cup B_2 \cup \dots \cup B_n$, где $B_i \cap B_j = \varnothing$ при $i \neq j$. Пусть также $Pr[B_i] > 0$ для всякого i. Тогда для всякого события A*

$$\Pr[A] = \sum_{i=1}^{n} \Pr[A \mid B_i] \cdot \Pr[B_i].$$

17. Случайная величина и математическое ожидание. Линейность математического ожидания.

Случайная величина — это числовая функция на вероятностном пространстве, то есть функция вида $\xi : U \to \mathbb{R}$. То есть, по сути, случайная величина — это обычная числовая функция, но теперь на её аргументах задано вероятностное распределение.

Математическим ожиданием случайной величины $\xi : U \to \mathbb{R}$ называется число

$$\mathrm{E}[\xi] = \sum_{u \in U} \xi(u) \cdot \Pr[u]$$

Лемма. *(линейность математического ожидания) Пусть $\xi : U \to \mathbb{R}$ и $g : U \to \mathbb{R}$ — две случайные величины на одном и том же вероятностном пространстве. Тогда*

$$E[f + g] = E[f] + E[g].$$

18. Формулировка неравенства Маркова.

Теорема (Неравенство Маркова) Пусть ξ — случайная величина, принимающая только **неотрицательные** значения. Тогда для всякого $x > 0$ верно

$$\Pr[\xi \geqslant x] \leqslant \frac{\mathrm{E}[\xi]}{x}.$$

То есть, вероятность того, что случайная величина ξ сильно больше своего математического ожидания, не слишком велика (заметим, что лемма становится содержательной, когда $x > \mathrm{E}[\xi]$).

19. Определение схемы в некотором функциональном базисе. Представление схем графами.

Полным базисом называется набор связок, если через эти связки выражается любая булева функция.

Стандартным базисом назовём набор из операций конъюнкция (И), дизъюнкция (ИЛИ) и отрицание (НЕ).

Булевой схемой от переменных $x_1, \ldots, x_n$ мы будем называть последовательность булевых функций $g_1, \ldots, g_s$, в которой всякая g_i получается из предыдущих функций последовательности и переменных применением одной из логических операций из выбранного базиса для этой схемы.

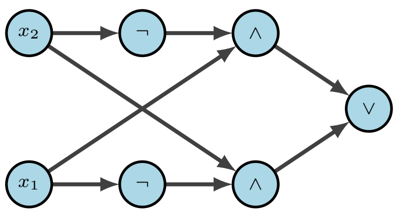
В булевой схеме задано некое число $m \geqslant 1$ и члены последовательности $g_{s-m+1}, \ldots, g_s$ называются **выходами схемы**. Число m называют числом выходов схемы.

Мы говорим, что схема вычисляет булеву функцию $f : \{0,1\}^n \to \{0,1\}^m$, если для всякого $x \in \{0,1\}^n$ верно $f(x) = (g_{s-m+1}(x), \ldots, g_s(x))$.

Размером схемы называют число s.

Рассмотрим представление схемы графом:

Рис. 1: Схема функции $x_1 \oplus x_2$



20. Полный базис. Примеры полных и неполных базисов.

Полным базисом называется набор связок, если через эти связки выражается любая булева функция.

Стандартным базисом назовём набор из операций конъюнкция (И), дизъюнкция (ИЛИ) и отрицание (НЕ).

Примеры полных базисов:

1. Базис $\{\wedge, \vee, \neg\}$ полный, так как всякую булеву функцию можно выразить через ДНФ.

2. Базис $\{\neg, \wedge\}$ полный, так как $x_1 \vee x_2 = \neg(\neg x_1 \wedge \neg x_2)$.
3. Базис $\{\neg, \vee\}$ полный, так как $x_1 \wedge x_2 = \neg(\neg x_1 \vee \neg x_2)$.
4. Базис $\{|\}$ (штрих Шеффера) полный, так как $\neg x = x \mid x$ и $x_1 \wedge x_2 = \neg(x_1 \mid x_2) = (x_1 \mid x_2) \mid (x_1 \mid x_2)$.
5. Базис $\{1, \oplus, \wedge\}$ полный, так как всякую булеву функцию можно выразить многочленом Жегалкина.

Примеры неполных базисов:

1. Базис $\{\wedge, \vee\}$ неполный, так как он монотонный.
2. Базис $\{\oplus, \wedge\}$.
3. Базис $\{\vee, \rightarrow\}$.

21. Полином Жегалкина (в стандартном виде).

Многочленом Жегалкина называется формула вида

$$\bigoplus_{S \subseteq \{1,\dots,n\}} a_S \bigwedge_{i \in S} x_i, \quad a_S \in \{0,1\}.$$

Примеры многочлена Жегалкина:

$$1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus (x_1 \wedge x_2) \oplus (x_1 \wedge x_3) \oplus (x_2 \wedge x_3) \oplus (x_1 \wedge x_2 \wedge x_3);$$
$$x_3 \oplus (x_1 \wedge x_3) \oplus (x_2 \wedge x_3) \oplus (x_1 \wedge x_2 \wedge x_3).$$

Для простоты чтения $\wedge$ можно опускать:

$$1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3;$$

22. Схемная сложность функции (размер схемы).

Схемная сложность булева отображения $f : \{0,1\}^n \to \{0,1\}^m$ (в частности, булевой функции) — это наименьший размер (количество присваиваний) схемы, вычисляющей это выражение.

2 Вопросы на знание доказательств

1. Сравнение $ax \equiv 1 \pmod N$ имеет решение тогда и только тогда, когда НОД$(a, N) = 1$.

Теорема. *Сравнение $ax \equiv 1 \pmod N$ имеет решение тогда и только тогда, когда НОД$(a, N) = 1$.*

Доказательство. Докажем теорему в обе стороны.

- $\Leftarrow$: Пусть НОД$(a, N) = 1$. Следовательно, $\exists k_1, k_2 : k_1 a + k_2 N = 1$ (следует из алгоритма Евклида). Вычислим остаток при делении на N обеих частей:

$$\begin{cases} k_1 a + k_2 N & \equiv k_1 a \pmod N \\ 1 & \equiv 1 \pmod N \end{cases}$$
$$\Downarrow$$
$$k_1 a \equiv 1 \pmod N.$$

Следовательно, k_1 и есть искомый x, при котором $ax \equiv 1 \pmod N$.

- $\Rightarrow$: Пусть $\exists x : ax \equiv 1 \pmod N$. Тогда $\exists t : ax - tN = 1$. Требуется доказать, что в этом случае НОД$(a, N) = 1$. Докажем от противного.

Пусть НОД$(a, N) = d > 1$. Тогда $\exists k_1, k_2 : a = k_1 d$ и $N = k_2 d$. Подставим эти произведения в выражение

$$k_1 dx - k_2 dt = 1 \implies d(k_1 x - k_2 t) = 1.$$

Это возможно только при $d = 1$. Следовательно, НОД$(a, N) = 1$.

■

2. Малая теорема Ферма.

Теорема. *Если p — простое число, то*

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

при любом a, не делящемся на p.

Доказательство.

Сначала докажем нужную для доказательства лемму.

Лемма. *Умножение остатков $1, 2, \dots, p-1$ на a даст те же остатки, но в другом порядке.*

Доказательство. Докажем от противного. Пусть нашлись каких-то два числа ax и ay, дающих одинаковый остаток при делении на p (x, y — остатки). Тогда $a \cdot (x - y)$ делится на p, что невозможно (так как a не делится на p). Тогда нет совпадающих остатков, так как произведений и остатков $p - 1$. ■

Рассмотрим произведение $a, 2a, 3a, \dots, (p-1)a$. Тогда

$$a \cdot 2a \cdot \dots \cdot (p-1)a \equiv a^{p-1} \cdot (p-1)! \pmod p.$$

С другой стороны, по лемме это эквивалентно $(p-1)!$ по модулю p (произведение остатков в другом порядке). Тогда $a^{p-1} \equiv 1 \pmod p$, что и требовалось доказать. ■

3. **Теорема Эйлера.**

Теорема. *Пусть $N > 1$ — произвольное целое число, а $\varphi(N)$ равно количеству остатков среди $0, 1, \dots, N-1$, взаимно простых с N. Пусть a — один из этих остатков. Тогда*

$$a^{\varphi(N)} \equiv 1 \pmod N.$$

Доказательство. Заметим, что достаточно рассматривать остаток от деления a на n.

Рассмотрим граф, где каждой вершине соответствует какой-то остаток, взаимно простой с n, а ребром из x в y будем называть преобразование $x \to y$. Тогда в графе будет $\varphi(n)$ вершин. Так как a взаимно просто с n, то

- Для каждой вершины графа x получаем, что ax взаимно просто с n (так как x взаимно просто с n по построению). Из этого следует, что всегда возможно провести ребро $x \to ax$, если его нет.
- Уравнение $ax \equiv b \pmod n$ имеет единственное решение (по модулю n) для любого b. Из этого следует, что из каждой вершины графа выходит ровно одно ребро и в каждую вершину входит ровно одно ребро.

Тогда граф обязан разбиться на циклы, так как иначе процесс умножения можно продолжать сколь угодно долго и условие на количество ребер нарушится.

Пусть k — степень такая, что $a^k \equiv 1 \pmod n$. Заметим, что она существует, так как для единицы существует цикл:

$$1 \to a \to a^2 \to \dots \to a^k.$$

Докажем, что все циклы имеют одинаковую длину. Очевидно, что длину, большую k цикл иметь не может (так как $b \cdot a^k \equiv b \pmod n$ и цикл замкнётся). Пусть для какого-то b есть цикл длины $l < k$.

Тогда $b \cdot a^l \equiv b \pmod n$ и (так как b взаимно просто с n, то у него есть обратный элемент) $a^l \equiv 1 \pmod n$.

Приходим к противоречию. Тогда $\varphi(n) = km$ для какого-то m и

$$a^{\varphi(n)} \equiv a^{km} \equiv 1^m = 1 \pmod n,$$

что и требовалось доказать. ■

4. **Корректность алгоритма Евклида и расширенного алгоритма Евклида.**

Теорема (Алгоритм Евклида) Пусть a, b — целые числа, не равные одновременно нулю. Определим последовательность чисел:

$$a \geqslant b > r_1 > r_2 > \dots > r_n,$$

где $\forall k : r_k$ — это остаток от деления r_{k-2} на r_{k-1}. Тогда НОД(a, b) равен последнему ненулевому члену этой последовательности, то есть r_n.

Доказательство. Пусть $a = b \cdot q + r$. Тогда требуется доказать, что НОД$(a, b) =$ НОД(b, r):

1. Пусть d — любой общий делитель чисел a и b, необязательно наибольший, тогда $a = t_1 \cdot d$ и $b = t_2 \cdot d$, где t_1, t_2 — целые числа.
2. Тогда d также является общим делителем чисел b и r, так как b делится на d по определению, а $r = a - b \cdot q = t_1 \cdot d - t_2 \cdot d \cdot q = d \cdot (t_1 - t_2 \cdot q)$.
3. Верно и обратное: пусть d — общий делитель b и r, то есть $b = t_2 \cdot d$ и $r = t_3 \cdot d$. Тогда b делится на d по определению, и $a = q \cdot b + r = q \cdot t_2 \cdot d + t_3 \cdot d = d \cdot (q \cdot t_2 + t_3)$.
4. Следовательно, все общие делители пар чисел (a, b) и (b, r) совпадают. В частности, совпадает и наибольший общий делитель.

Алгоритм конечный, так как за одну итерацию одно из чисел становится меньше своего предыдущего значения, причем могут получаться только неотрицательные числа. ∎

Теорема (Расширенный алгоритм Евклида) Пусть a, b — целые числа, $d =$ НОД(a, b). Тогда существуют x, y, такие что $ax + by = d$.

Доказательство.

1. Пусть $a = b \cdot q + r$. Из доказательства алгоритма Евклида известно, что НОД$(a, b) =$ НОД(b, r). Воспользуемся этим свойством, чтобы найти x и y.
2. Пусть x' и y' — числа, такие что $bx' + ry' =$ НОД(a, b). Заметим, что r можно выразить с помощью арифметических операций через a и b:
$$r = a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b.$$
3. Подставим полученное в уравнение:
$$bx' + ry' = bx' + \left(a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b\right) \cdot y' = bx' + ay' - \left\lfloor \frac{a}{b} \right\rfloor \cdot b \cdot y' = ay' + b \cdot \left(x' - \left\lfloor \frac{a}{b} \cdot y' \right\rfloor\right).$$
4. С одной стороны: НОД$(a, b) = ay' + b \cdot \left(x' - \left\lfloor \frac{a}{b} \right\rfloor \cdot y'\right)$.

   С другой стороны: НОД$(a, b) = ax + by$. Отсюда получаем, что $x = y'$ и $y = x' - \left\lfloor \frac{a}{b} \right\rfloor \cdot y'$.
5. Таким образом, зная x' и y', такие что $bx' + ry' =$ НОД(a, b), можно на каждом шаге алгоритма Евклида получить x и y, такие что $ax + by =$ НОД(a, b).
   Для случая, когда $r = 0$, разложение очевидно: $x' = 1, y' = 0$. Из него можно получить остальные коэффициенты.

∎

5. Основная теорема арифметики.

Теорема. *Всякое целое положительное число, большее* 1*, разлагается на простые множители, причём единственным образом: любые два разложения отличаются только перестановкой сомножителей.*

Доказательство.

- **Существование**. Докажем существование разложения числа n на простые множители, предполагая, что оно уже доказано для любого другого числа, меньшего n. Если n — простое, то существование доказано. Если n — составное, то оно может быть представлено в виде произведения двух чисел a и b, каждое из которых больше 1, но меньше n. Числа a и b либо являются простыми, либо могут быть разложены в произведение простых (уже доказано ранее). Подставив их разложение в $n = a \cdot b$, получим разложение исходного числа n на простые.
- **Единственность**. Пусть некоторое число N имеет два разложения:
$$N = p_1 \cdot p_2 \cdot \dots \cdot p_n = q_1 \cdot q_2 \cdot \dots \cdot q_m.$$
  Сократим общие сомножители, если они есть. Если сократится не всё, то получим два разложения одного числа, не имеющих общих сомножителей (для удобства оставим n и m):
$$p_1 \cdot p_2 \cdot \dots \cdot p_n = q_1 \cdot q_2 \cdot \dots \cdot q_m.$$

Докажем следующее утверждение: если p — простое число, то произведение чисел, каждое из которых не делится на p, не может делиться на p. Действительно, если $a \not\equiv 0 \pmod p$ и $b \not\equiv 0 \pmod p$, то и $a \cdot b \not\equiv 0 \pmod p$.

Правая часть равенства выше — это произведение чисел, каждое из которых не делится на p_1, следовательно, все произведение не делится на p_1. Приходим к противоречию, когда $q_1 \cdot \dots \cdot q_m = n$, но $n \not\equiv 0 \pmod{p_1}$. Следовательно, разложение числа N на простые множители единственно.

■

6. Китайская теорема об остатках.

Теорема. *Пусть числа $m_1, m_2, \dots, m_k$ попарно взаимно просты. Рассмотрим следующую систему сравнений:*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Определим целые числа M, M_i, b_I следующим образом:

$$M = \prod_{i=1}^{k} m_i; \quad M_i = \frac{M}{m_i}; \quad M_i \cdot b_i \equiv a_i \pmod{m_i}, 1 \leqslant i \leqslant k.$$

После чего определим x_0 следующим образом:

$$x_0 = \sum_{i=1}^{k} M_i \cdot b_i.$$

Тогда множество целых чисел, удовлетворяющих системе сравнений, составляет класс вычетов $x \equiv x_0 \pmod M$.

Доказательство. Так как НОД$(M_i, m_i) = 1$ по построению, а значит, существует обратный к M_i по модулю m_i. Тогда $b_i \equiv a_i \cdot M_i^{-1} \pmod{m_i}$ и x_0 также существует.

Покажем, что x_0 соответствует системе сравнений. Так как $m_i \mid M_j$ при $j \neq i$, то $x_0 \equiv M_i \cdot b_i \equiv a_i \pmod{m_i}$ для $1 \leqslant i \leqslant k$. Тогда систему можно переписать в следующем виде:

$$\begin{cases} x \equiv x_0 \pmod{m_1} \\ x \equiv x_0 \pmod{m_2} \\ \dots \\ x \equiv x_0 \pmod{m_k} \end{cases}$$

Тогда $m_i \mid (x - x_0)$ при $1 \leqslant i \leqslant k$. Так как все m_i попарно взаимно просты, то эти сравнения будут верны только для тех x, что $M \mid (x - x_0)$, что равносильно $x \equiv x_0 \pmod M$. ■

Теорема. *Пусть числа $m_1, m_2, \dots, m_k$ попарно взаимно просты. Рассмотрим следующие системы сравнений:*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases} \qquad \begin{cases} x' \equiv a'_1 \pmod{m_1} \\ x' \equiv a'_2 \pmod{m_2} \\ \dots \\ x' \equiv a'_k \pmod{m_k} \end{cases},$$

тогда $x = x' \iff \forall i : a_i = a'_i$.

Доказательство. Собственно, если бы это было не так, то для одинакового набора a существовало бы два различных решения x и x' (по модулю).

Но это бы означало, что $x - x'$ сравнимо с 0 по каждому модулю, а значит и сравнимо с 0 по произведению модулей. Но это означает, что $x = x'$. ■

Последняя теорема говорит о том, что для набора модулей можно подобрать такин наборы a, что каждый остаток по произведению модулей может являться решением системы сравнений.

7. **Мультипликативность функции Эйлера. Формула для функции Эйлера.**

Теорема (Мультипликативность функции Эйлера) Если a и b взаимно просты, то $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Доказательство. Пусть $z \leqslant ab$. Докажем, что число z является взаимно простым с ab тогда и только тогда, когда z является взаимно простым с a и b одновременно.

Обозначим x как остаток при делении z на a и y как остаток при делении z на b.

- $\Rightarrow$: Пусть z является взаимно простым с ab. Следовательно, НОД$(z, ab) = 1$. В этом случае, если НОД$(z, a) = d > 1$, то $z = z'd$ и $a = a'd$, а в этом случае НОД$(z'd, a'db) \geqslant d > 1$.
  А значит, НОД$(z, a) = 1$. Аналогично, НОД$(z, b) = 1$.
- $\Leftarrow$: Пусть z является взаимно простым с a и взаимно простым с b. Тогда $z \equiv x \pmod a$ и $z \equiv y \pmod b$. Применяя китайскую теорему об остатках, получаем, что существует $z \leqslant ab$, что

  $$\begin{aligned} z &\equiv x \pmod a, \\ z &\equiv y \pmod b. \end{aligned}$$

  Следовательно, всякой паре x, y ($x < a$, $y < b$) однозначно соответствует число $z < ab$, причем x — взаимно простое с a, и y — взаимно простое с b, а z — взаимно простое с ab.
  Всего чисел, взаимно простых с ab ровно столько, сколько существует пар x, y ($x < a$, $y < b$), таких что НОД$(x, a) = 1$ и НОД$(y, b) = 1$. Следовательно, $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

■

Лемма. *Если число p — простое, то $\varphi(p^n) = p^{n-1} \cdot (p-1)$.*

Доказательство. Функция Эйлера от числа n — это количество чисел, взаимно простых с n, меньших n. Посчитаем количество чисел от 1 до p^n, которые не взаимно просты с p^n.

Все такие числа кратны p. То есть имеют вид $p, 2p, \dots, (p^{n-1}-1) \cdot p$. Всего таких чисел $p^{n-1}-1$. Поэтому, количество чисел, взаимно простых с p^n равно $(p^n - 1) - (p^{n-1} - 1) = p^n - p^{n-1} = p^{n-1} \cdot (p-1)$. ■

Теорема (Формула для функции Эйлера) Если n — произвольное натуральное число, то $\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$, где $p_1, \dots, p_k$ — все возможные простые множители числа n.

Доказательство. Из основной теоремы арифметики следует, что всякое натуральное число $n > 1$ единственным образом представляется в виде:

$$n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k},$$

где $p_1, \dots, p_k$ — простые числа, а $a_1, \dots, a_k$ — натуральные числа. Из мультипликативности функции Эйлера и леммы следует:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{a_1}) \cdot \dots \cdot \varphi(p_k^{a_k}) \\ &= p_1^{a_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot p_k^{a_k} \cdot \left(1 - \frac{1}{p_k}\right) \\ &= p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

■

8. **Формула Байеса. Формула полной вероятности.**

Теорема (Формула Байеса) Если вероятность событий A и B полжительна (> 0), то

$$\Pr[A \mid B] = \frac{\Pr[A] \cdot \Pr[B \mid A]}{\Pr[B]}$$

Доказательство. Запишем вероятность события $A \cap B$ через условные вероятности двумя способами:

$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B \mid A],$$
$$\Pr[A \cap B] = \Pr[B] \cdot \Pr[A \mid B].$$

Отсюда:

$$\Pr[A] \cdot \Pr[B \mid A] = \Pr[B] \cdot \Pr[A \mid B].$$

Разделим обе части на $\Pr[B]$ и получим формулу Байеса:

$$\Pr[A \mid B] = \frac{\Pr[A] \cdot \Pr[B \mid A]}{\Pr[B]}.$$

■

Теорема (Формула полной вероятности) Пусть $B_1, \dots, B_n$ — разбиение вероятностного пространства U. То есть $U = B_1 \cup \dots \cup B_n$ и $B_i \cap B_j = \varnothing$ при $i \neq j$. Пусть также $\Pr[B_i] > 0$ для всякого i. Тогда для всякого события A:

$$\Pr[A] = \sum_{i=1}^{n} \Pr[A \mid B_i] \cdot \Pr[B_i].$$

Доказательство.

$$\Pr[A] = \sum_{i=1}^{n} \Pr[A \cap B_i] = \sum_{i=1}^{n} \Pr[A \mid B_i] \cdot \Pr[B_i].$$

Первое равенство получается по формуле сложения вероятностей непересекающихся событий. Второе равенство — по определению условной вероятности. ■

9. Парадокс дней рождения (математическое ожидание числа людей с совпавшими днями рождения)

Рассмотрим n случайных людей и посмотрим на количество совпадений дней рождения у них, то есть на количество пар людей, имеющих день рождения в один день. Каким в среднем будет это число?

Сформулируем вопрос точно. Вероятностное пространство: всюду определённая функция из n-элементного множества людей $\{x_1, \dots, x_n\}$ в 365-элементное множество дней в году. Все исходы равновозможные.

Обозначим случайную величину, равную количеству пар людей с совпадающими днями рождения, через ξ. Нам требуется посчитать математическое ожидание случайной величины ξ. Но при этом случайная величина довольно сложная, и подсчитывать математическое ожидание непосредственно из определения трудно.

Идея состоит в следующем: давайте разобьём сложную случайную величину ξ в сумму нескольких простых случайных величин. Тогда мы сможем подсчитать отдельно математические ожидания всех простых величин, а затем, пользуясь линейностью математического ожидания, просто сложить результаты.

Обозначим через I_{ij} случайную величину, равную 1, если у людей x_i и x_j дни рождения совпадают, и равную 0 в противном случае. Тогда можно заметить, что

$$\xi = \sum_{i<j} I_{ij}.$$

Подсчитаем математическое ожидание случайной величины I_{ij}. Нетрудно увидеть, что вероятность того, что у двух случайных людей дни рождения совпадают, равна $\frac{1}{365}$, так что с вероятностью $\frac{1}{365}$ случайная величина равна 1, и с вероятностью $1 - \frac{1}{365}$ равна 0.

Получаем, что $\mathrm{E}[I_{ij}] = \frac{1}{365}$ (для всякой пары i, j). Для математического ожидания ξ из линейности получаем

$$\mathrm{E}[\xi] = \mathrm{E}\left[\sum_{i<j} I_{ij}\right] = \sum_{i<j} 1 \cdot \frac{1}{365} = \frac{n \cdot (n-1)}{2 \cdot 365}.$$

Например, если число людей n больше 27, то $E[\xi] > 1$, то есть естественно ожидать, что будет не меньше одного совпадения дней рождения.

10. Неравенство Маркова.

Теорема (Неравенство Маркова) Пусть ξ — случайная величина, принимающая только **неотрицательные** значения. Тогда для всякого $x > 0$ верно

$$\Pr[\xi \geqslant x] \leqslant \frac{\mathrm{E}[\xi]}{x}.$$

Требуется доказать, что $\mathrm{E}[\xi] \geqslant x \cdot \Pr[\xi \geqslant x]$.

Пусть случайная величина ξ принимает значения $a_1, \ldots, a_k$ с вероятностями $p_1, \ldots, p_k$. Запишем, чему равно её математическое ожидание по определению:

$$\mathrm{E}[\xi] = a_1 p_1 + a_2 p_2 + \cdots + a_k p_k.$$

Посмотрим отдельно на те a_i, которые меньше x, и отдельно на те a_i, которые не меньше x. Если первое заменить на нуль, то сумма может только уменьшиться.

Если вторые заменить на x, то сумма также не может стать больше. После таких замен, у нас остаётся сумма нескольких слагаемых, каждое из которых есть $x \cdot p_i$, где p_i — вероятность некоторого значения случайной величины, не меньшего x. Нетрудно увидеть, что такая сумма как раз равна $x \cdot \Pr[\xi \geqslant x]$.

11. Нижняя оценка на максимальное количество ребер в разрезе.

Разрезом графа $G(V, E)$ называется назбиение множества V вершин графа на два непересекающихся подмножества V_1 и V_2, таких что $V = V_1 \cup V_2$ и $V_1 \cap V_2 = \varnothing$.

Размером разреза называется число рёбер, попадающих в разрез. То есть рёбер (u, v), таких что $u \in V_1, v \in V_2$.

Теорема. *Всякий граф $G(V, E)$ имеет разрез размера не меньше* $\frac{|E|}{2}$.

Доказательство. Рассмотрим случайный разрез графа G. Более точно, мы берём равномерное распределение на множестве всех разрезов графа G. Разрез задается подмножеством $S \subseteq V$: такому подмножеству ставится в соответствие разрез $(S, V \setminus S)$.

Всего подмножеств (а значит, и разрезов) 2^n, так что вероятность каждого разреза есть $\frac{1}{2^n}$. Вероятность того, что вершина окажется в случайном разрезе равна $\frac{1}{2}$, следовательно, для каждой пары вершин $x \neq y$ все четыре события «$x \in S, y \in S$», «$x \notin S, y \in S$», «$x \in S, y \notin S$», «$x \notin S, y \notin S$» имеют вероятность $\frac{1}{4}$.

Итак, рассмотрим случайный разрез и рассмотрим случайную величину ξ, равную размеру разреза. Посчитаем её математическое ожидание. Для этого, как и раньше, стоит разбить случайную величину в сумму более простых случайных величин. Для всякого $e \in E$ рассмотрим случайную величину ξ_e, равную 1, если ребро e входит в разрез, и равную 0 в противном случае.

Тогда нетрудно видеть, что $\xi = \sum\limits_{e \in E} \xi_e$, а значит:

$$\mathrm{E}[\xi] = \sum_{e \in E} \mathrm{E}[\xi_e].$$

Однако, для случайной величины ξ_e математическое ожидание уже нетрудно посчитать. Действительно, для всякого фиксированного ребра e вероятность, что оно попадёт в разрез равна $\frac{1}{2}$. А значит, $\mathrm{E}[\xi_e] = \frac{1}{2}$ для всякого $e \in E$, откуда

$$\mathrm{E}[\xi] = \sum_{e \in E} \frac{1}{2} = \frac{|E|}{2}.$$

Из этого следует, что есть конкретный разрез, содержащий не меньше $\frac{|E|}{2}$ рёбер. ∎

12. Любое бесконечное множество содержит счётное подмножество. Любое подмножество счётного множества конечно или счётно.

Теорема. *Любое бесконечное множество содержит счётное подмножество.*

Доказательство. Рассмотрим прозвольное бесконечное множество A. Нам надо выписать последовательность из некоторых его элементов, не обязательно всех. Будем действовать самым простым образом.

Первый элемент a_0 возьмем произвольно. Поскольку A бесконечно, в нем есть ещё элементы (кроме a_0). В качестве a_1 возьмем любой из них. И так далее.

В общем случае, когда нам нужно выбрать очередной элемент a_n, мы рассматриваем подмножество $\{a_0, \ldots, a_{n-1}\}$. Оно конечно, а значит, не совпадает со всем множеством A (которое по предположению бесконечно). Значит, в A есть элементы, не лежащие в этом подмножестве — и мы можем взять любой из них в качестве a_n.

Получили бесконечную последовательность из элементов A, и множество элементов этой последовательности образует искомое счётное подмножество множества A. ■

Теорема. *Любое подмножество счётного множества конечно или счётно.*

Доказательство. Рассмотрим счётное множество A и его подмножество A'. Выпишем элементы A в последовательность:

$$a_0, a_1, a_2, \ldots, a_n, \ldots.$$

Вычеркнем из этой последовательности те элементы, которые не лежат в A'. В результате останется последовательность элементов A' — конечная или бесконечная.

В первом случае множество будет конечным, во втором — счётным. Формально говоря, для бесконечного подмножества $A' \subset A$ искомая биекция $f : \mathbb{N} \to A'$ ставит в соответствие числу n элемент множества A', который стоит n-м по счёту в последовательности (если считать только элементы A'). ■

13. Конечное или счётное объединение конечных или счётных множеств конечно или счётно

Теорема. *Конечное или счётное объединение конечных или счётных множеств конечно или счётно.*

Доказательство. Пусть есть счётное количество счётных множеств $A_0, A_1, A_2, \ldots$. Расположим их элементы в виде таблицы:

$$\begin{array}{lllll} A_0: & a_{00} & a_{01} & a_{02} & \ldots \\ A_1: & a_{10} & a_{11} & a_{12} & \ldots \\ A_2: & a_{20} & a_{21} & a_{22} & \ldots \\ A_3: & a_{30} & a_{31} & a_{32} & \ldots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Здесь в первой строке мы последовательно выписали элементы A_0, во второй — элементы A_1 и так далее. Теперь соединяем эти последовательности в одну, идя по диагоналям:

$$a_{00}, a_{01}, a_{10}, a_{02}, a_{11}, a_{20}, a_{03}, a_{12}, a_{21}, a_{30}, \ldots.$$

При этом нужно следить, чтобы члены последовательности не повторялись: когда мы рассматриваем очередной элемент таблицы, нужно проверить, не встретился ли он раньше. Если он уже был, его нужно пропустить.

Мы предполагали, что все A_i счётны и что их счётное число. Если самих множеств лишь конечное число, или если какие-то из множеств конечны, то в таблице часть ячеек окажется пустой. Соответственно, мы будем их пропускать при составлении последовательности. В результате либо получится бесконечная последовательность, и тогда объединение счётно, либо получится только конечная последовательность — и тогда объединение конечно. ■

14. Счётность декартова произведения счетных множеств. Счётность множества рациональных чисел.

Теорема. *Декартово произведение двух счётных множеств $A \times B$ счётно.*

Доказательство. По определению декартово произведение есть множество всех упорядоченных пар вида (a, b), в которых $a \in A$ и $b \in B$. Разделим пары на группы, объединив пары с одинаковой первой компонентой (каждая группа имеет вид $\{a\} \times B$ для какого-то $a \in A$). Тогда каждая группа счётна, поскольку находится во взаимно однозначном соответствии с B (пара определяется своим вторым элементом), и групп столько же, сколько элементов в A, то есть счётное число. Так как счетное объединение счетных множеств счетно, то такое множество тоже счетно. ■

Теорема. *Множество рациональных чисел счётно.*

Доказательство. Это следует из доказанной теоремы. Всякое рациональное число можно представить в виде упорядоченной пары (a, b), где $a \in \mathbb{Z}$, $b \in \mathbb{N} \setminus \{0\}$. Всякая такая пара лежит во множестве $\mathbb{Z} \times \mathbb{N}$. Множества $\mathbb{N}$ и $\mathbb{Z}$ счетны $\implies$ их декартово произведение счетно $\implies$ множество рациональных чисел счетно, т.к. является подмножеством $\mathbb{Z} \times \mathbb{N}$ и бесконечно. ■

15. Равномощность отрезков, интервалов, лучей и прямых (явные биекции).

Теорема. *Отрезок* $[0; 1]$ *равномощен интервалу* $(0; 1)$.

Доказательство. Построим биекцию.

1. Заметим, что $[0; 1] = \{0\} \cup (0; 1) \cup \{1\}$.
2. Выделим на отрезке и интервале счётное подмножество, например $\left\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \quad \right\}$.
3. Сопоставим точке 0 отрезка точку $\frac{1}{2}$ интервала. Точке 1 отрезке — точке $\frac{1}{3}$ интервала. После сопоставим всем точкам $\frac{1}{a}$ счётного подмножества отрезка точку $\frac{1}{a+1}$ интервала.
4. Всем оставшимся точкам отрезка сопоставим их же на интервале.

■

Теорема. *Интервал* $(0; 1)$ *и луч* $(0; +\infty)$ *равномощны.*

Доказательство. Существует биекция: $f : x \in (0; 1) \to \left(\frac{1}{x} - 1\right) \in (0; +\infty)$. ■

Теорема. *Луч* $(0; +\infty)$ *и прямая* $(-\infty; +\infty)$ *равномощны.*

Доказательство. Найдем биекцию.

1. Заметим, что $(0; +\infty) = (0; 1) \cup \{1\} \cup (1; +\infty)$.
2. Сопоставим интервалу $(0; 1)$ луч $(-\infty; 0)$ по формуле
$$f : x \in (0; 1) \to -\left(\frac{1}{x} - 1\right) \in (-\infty; 0).$$
3. Сопоставим точке 1 луча точку 0 прямой.
4. Сопоставим лучу $(1; +\infty)$ луч $(0; +\infty)$:
$$f : x \in (1; +\infty) \to (x - 1) \in (0; +\infty).$$

■

Теорема. *Прямая* $(-\infty; +\infty)$ *и отрезок* $[0; 1]$ *равномощны.*

Доказательство.

1. Прямая $(-\infty; +\infty)$ равномощна интервалу $\left(-\frac{\pi}{2}; \frac{\pi}{2}\right)$:
$$f : x \in (-\infty; +\infty) \to \operatorname{arctg}(x) \in \left(-\frac{\pi}{2}; \frac{\pi}{2}\right).$$

2. Интервал $\left(-\frac{\pi}{2}; \frac{\pi}{2}\right)$ равномощен интервалу $(0;1)$, достаточно поделить каждую точку первого на π и прибавить $\frac{1}{2}$.
3. Мы уже доказали, что $(0;1)$ равномощно $[0;1]$. Следовательно, прямая $(-\infty;+\infty)$ равномощна отрезку $[0;1]$.

■

16. Несчетность множества бесконечных двоичных последовательностей.

Теорема. *Множество бесконечных последовательностей нулей и единиц несчётно.*

Доказательство. Предположим, что это множество счётно, то есть что последова тельности нулей и единиц можно пронумеровать. Обозначим последовательность с номером i через a_i, а её члены обозначим $a_{i0}, ai1, \ldots$.

Удобно члены последовательностей писать слева направо, а саму последовательность последовательностей писать сверху вниз.

Получится нечто вроде бесконечной таблицы:

$$\begin{array}{ccccc} a_0: & a_{00} & a_{01} & a_{02} & \cdots \\ a_1: & a_{10} & a_{11} & a_{12} & \cdots \\ a_2: & a_{20} & a_{21} & a_{22} & \cdots \\ a_3: & a_{30} & a_{31} & a_{32} & \cdots \\ \vdots: & \vdots & \vdots & \vdots & \ddots \end{array}$$

Теперь рассмотрим «диагональную» последовательность в этой таблице, то есть последовательность:

$$a_{00}, a_{11}, a_{22}, a_{33}, \ldots$$

и заменим в ней все биты на противоположные. Другими словами, положим $b_i = 1 - a_{ii}$ и рассмотрим последовательность $b = (b_0, b_1, b_2, \ldots)$.

Последовательность b отличается от любой последовательности a_i в i-ой позиции, поскольку $b_i = 1 - a_{ii} \neq a_{ii}$, так что последовательности b нет в нашей нумерации всех последовательностей, а там по предположению были все. Мы пришли к противоречию, а значит, множество всех бесконечных последовательностей нулей и единиц несчетно. ■

17. Теорема Кантора-Бернштейна.

Теорема (Кантора-Бернштейна) Если для множеств A и B существует инъекция из A в B и инъекция из B в A, то существует и биекция между A и B.

Доказательство. Пусть $f : A \to B$ и $g : B \to A$ — инъекции. Рассмотрим (возможно, бесконечный) ориентированный граф с вершинами $A \cup B$ (для простоты обозначений предположим, что A и B не пересекаются).

Для точек $x \in A$ и $y \in B$ мы проводим ребро из x в y, если $f(x) = y$, и ребро из y в x, если $g(y) = x$.

Если нарисовать множество A слева, а множество B справа, то можно сказать, что мы проводим рёбра слева направо согласно функции f и справа налево согласно функции g.

По построению из каждой точки выходит ровно одно ребро. А сколько рёбер входит? Поскольку функции инъективны, то не больше одного (но может не входить ни одного).

Разобьем граф на компоненты связности (забыв для этого об ориентации рёбер) и рассмотрим каждую компоненту отдельно. Как устроены эти компоненты? Есть три возможности. Связная компонента может быть

- Циклом из стрелок.
- Бесконечной цепочкой стрелок, начинающейся в некоторой вершине (в которую ничего не входит).
- Бесконечной в обе стороны цепочкой стрелок (то есть, мы якобы посмотрели в «центр» цепочки из предыдущего пункта).

В самом деле, вперёд всегда можно идти по единственной стрелке, а назад либо можно пойти единственным образом, либо нельзя пойти вовсе. Если, идя вперёд, мы дважды попадём в одну вершину, то образуется цикл (и это возможно, лишь если мы вернёмся в начальную вершину). Если нет, то образуется бесконечная цепочка вперёд; её можно однозначно продолжать назад, при этом либо мы упрёмся в вершину, где назад не пройти, либо получим двустороннюю цепочку.

Это верно для любого ориентированного графа, в котором из каждой вершины выходит ровно одна стрелка и в каждую вершину входит не больше одной стрелки. В нашем конкретном случае есть дополнительная структура: вершины бывают левые и правые (из A и из B). Они чередуются, поэтому цикл может быть только чётной длины и содержит поровну вершин из A и из B.

Любое из отображений f и g может быть использовано, чтобы построить биекцию между A- и B-вершинами цикла (так что есть минимум два варианта биекции). То же самое верно для бесконечной в обе стороны цепочки (два варианта). Если же цепочка бесконечна только в одну сторону, то для построения биекции годится только одно из отображений.

Скажем, если она начинается с элемента $a \in A$, то годится только функция f (при которой a соответствует $f(a)$, затем $g(f(a))$ соответствует $f(g(f(a)))$ и так далее). Но в любом случае одна из функций f и g годится, так что внутри каждой связной компоненты у нас есть биекция, и остаётся их объединить для всех связных компонент. ■

18. Нижняя оценка на число монотонных булевых функций: монотонных булевых функций от $2n$ переменных не меньше $2^{\frac{2^n}{2n+1}}$

19. Существование и единственность полинома Жегалкина (в стандартном виде) для любой булевой функции.

Теорема. *Каждая булева функция единственным образом представляется в виде полинома Жегалкина.*

Доказательство. Заметим, что различных булевых функций от n переменных 2^{2^n} штук. При этом конъюнкций вида $x_{i_1}, \ldots, x_{i_k}$ существует ровно 2^n, так как из n возможных сомножителей каждый или входит в конъюнкцию, или нет. В полиноме у каждой такой конъюнкции стоит 0 или 1, то есть существует 2^{2^n} различных полиномов Жегалкина от n переменных.

Теперь достаточно доказать, что различные полиномы реализуют различные функции.

Предположим противное. Тогда приравняв два различных полинома и перенеся один из них в другую часть равенства, получим полином, тождественно равный нулю и имеющий ненулевые коэффициенты. Тогда рассмотрим слагаемое с единичным коэффициентом наименьшей длины, то есть с наименьшим числом переменных, входящих в него (любой один, если таких несколько). Подставив единицы на места этих переменных, и нули на места остальных, получим, что на этом наборе только одно это слагаемое принимает единичное значение, то есть нулевая функция на одном из наборов принимает значение 1. Противоречие.

Значит, каждая булева функция реализуется полиномом Жегалкина единственным образом. Имеем 2^{2^n} полиномов Жегалкина, каждые два из которых реализуют различные булевы функции. Следовательно, по принципу Дирихле, для всякой булевой функции существует ее представление в виде полинома Жегалкина, причем только одно. ■

20. Разложение в ДНФ и КНФ булевой функции.

21. Верхняя оценка $O(n2^n)$ схемной сложности булевой функции от n переменных.

22. Булевы схемы для сложения и умножения n-битовых чисел. Оценка размера.

23. Булева схема для задачи о связности графа. Оценка размера.

24. Задача об угадывании числа. Верхняя и нижняя оценки.

25. Задача о сортировке нижняя оценка.

Дано n объектов, все разного веса. За один шаг разрешается сравнить веса двух объектов (мы узнаем, какой из этих объектов тяжелее). Требуется расположить эти объекты в порядке возрастания веса.

Теорема. *Сложность задачи о сортировке n объектов не меньше* $\sum\limits_{k=1}^{n} \lceil \log_2 k \rceil$.

Доказательство. Доказательство будем вести индукцией по n.

Для $n = 1$ оценка верна — никаких сравнений не требуется.

Пусть утверждение доказано для n, докажем его для $n+1$. Сначала возьмем первые n объектов и упорядочим их, пользуясь предположением индукции. После этого у нас остается $\lceil \log_2(n+1) \rceil$ сравнений, и нам нужно один оставшийся объект поместить в уже упорядоченный список из n объектов. То есть, для $(n+1)$го объекта есть $n+1$ место среди упорядоченного списка из n объектов и нам нужно его найти. Пользуясь тем же рассуждением, что и в задаче про угадывание числа, это можно сделать как раз за $\lceil \log_2(n+1) \rceil$ сравнение (сравниваем со средним объектом и сокращаем количество возможных позиций почти в два раза). ■

26. Задача о нахождении самой тяжелой монеты. Верхние и нижние оценки.

Теорема. *Для нахождения самого тяжелого из n объектов необходимо и достаточно $n-1$ взвешивания.*

Доказательство.

- Сначала докажем, что $n-1$ взвешивания достаточно. Проще всего вести рассуждение по индукции.

  Если $n = 1$, то ничего взвешивать не нужно.

  Пусть мы доказали утверждение для $n-1$. Рассмотрим n объектов. Возьмем любые два и сравним их. Заметим, что более легкий из них не может быть самым тяжелым, так что его можно выбросить из рассмотрения. Таким образом у нас остается $n-1$ объект и по предположению индукции мы можем найти самый тяжелый из них за $n-2$ оставшихся взвешивания.

- Теперь докажем, что меньше чем за $n-1$ взвешивание найти самый тяжелый объект нельзя. Пусть мы сделали $n-2$ взвешивания. Рассмотрим следующий граф.

  Его вершинами будут наши объекты, и мы соединяем ребрами те из них, которые мы сравнили в одном из взвешиваний. Тогда в этом графе n вершин и $n-2$ ребра. Значит этот граф не связен.

  Рассмотрим множество V_1 объектов в одной из его компонент связности и множество V_2 всех остальных объектов. Предположим, для определен ности, что самый тяжелый объект находится в V_1. Увеличим вес всех объектов в V_2 на одно и то же очень большое число, такое чтобы все объекты в V_2 стали тяжелее всех объектов в V_1. При этом результаты всех взвешиваний не изменятся, поскольку все сравнения были либо внутри V_1, либо внутри V_2, а самая тяжелая монета станет другой (теперь она будет в V_2).

  Таким образом, все взвешивания дадут один и тот же результат в обеих ситуациях, а самый тяжелый объект будет разным. Значит в одной из двух ситуаций наш протокол выдает неправильный ответ. Мы пришли к противоречию, а значит для нахождения самого тяжелого объекта требуется не меньше $n-1$ сравнения.

■