

# Дискретная математика, Коллоквиум 2

Балюк Игорь  
@lodthe, [GitHub](#)

2019 — 2020

Материалы взяты из учебника Александра Рубцова.

## Содержание

<b>1</b>	<b>Определения</b>	<b>3</b>
1.1	Деление целых чисел с остатком.	3
1.2	Сравнения по модулю. Основные свойства.	3
1.3	Арифметика остатков (вычетов). Обратимые остатки (вычеты).	3
1.4	Малая теорема Ферма.	3
1.5	Функция Эйлера. Теорема Эйлера.	3
1.6	Наибольший общий делитель. Алгоритм Евклида.	3
1.7	Расширенный алгоритм Евклида нахождения решения линейного диофантова уравнения.	4
1.8	Простые числа, формулировка основной теоремы арифметики.	4
1.9	Равномощные множества.	5
1.10	Счётные множества.	5
1.11	Множества мощности континуум.	5
1.12	Основные определения элементарной теории вероятностей: исходы, события, вероятность события.	5
1.13	Формулировка формулы включений и исключений для вероятностей.	5
1.14	Условная вероятность.	5
1.15	Независимые события. Основные свойства независимых событий.	5
1.16	Формула полной вероятности.	5
1.17	Случайная величина и математическое ожидание. Линейность математического ожидания.	6
1.18	Формулировка неравенства Маркова.	6
1.19	Определение схемы в некотором функциональном базисе. Представление схем графами.	6
1.20	Полный базис. Примеры полных и неполных базисов.	6
1.21	Полином Жегалкина (в стандартном виде).	7
1.22	Схемная сложность функции (размер схемы).	7
<b>2</b>	<b>Вопросы на знание доказательств</b>	<b>7</b>
2.1	Сравнение $ax \equiv 1 \pmod{N}$ имеет решение тогда и только тогда, когда $\text{НОД}(a, N) = 1$ .	7
2.2	Малая теорема Ферма.	7
2.3	Теорема Эйлера.	8
2.4	Корректность алгоритма Евклида и расширенного алгоритма Евклида.	8
2.5	Основная теорема арифметики.	8
2.6	Китайская теорема об остатках.	8
2.7	Мультипликативность функции Эйлера. Формула для функции Эйлера.	8
2.8	Формула Байеса. Формула полной вероятности.	8
2.9	Парадокс дней рождения (математическое ожидание числа людей с совпавшими днями рождения)	9
2.10	Неравенство Маркова.	9
2.11	Нижняя оценка на максимальное количество ребер в разрезе.	9
2.12	Любое бесконечное множество содержит счётное подмножество. Любое подмножество счётного множества конечно или счётно.	9
2.13	Конечное или счётное объединение конечных или счётных множеств конечно или счётно	9

2.14	Счётность декартова произведения счетных множеств. Счётность множества рациональных чисел. . . . .	9
2.15	Равномощность отрезков, интервалов, лучей и прямых (явные биекции). . . . .	9
2.16	Несчетность множества бесконечных двоичных последовательностей. . . . .	9
2.17	Теорема Кантора-Бернштейна. . . . .	9
2.18	Нижняя оценка на число монотонных булевых функций: монотонных булевых функций от $2n$ переменных не меньше $2^{\frac{2^n}{2n+1}}$ . . . . .	9
2.19	Существование и единственность полинома Жегалкина (в стандартном виде) для любой булевой функции. . . . .	9
2.20	Разложение в ДНФ и КНФ булевой функции. . . . .	9
2.21	Верхняя оценка $O(n2^n)$ схемной сложности булевой функции от $n$ переменных. . . . .	9
2.22	Булевы схемы для сложения и умножения $n$ -битовых чисел. Оценка размера. . . . .	9
2.23	Булева схема для задачи о связности графа. Оценка размера. . . . .	10
2.24	Задача об угадывании числа. Верхняя и нижняя оценки. . . . .	10
2.25	Задача о сортировке нижняя оценка. . . . .	10
2.26	Задача о нахождении самой тяжелой монеты. Верхние и нижние оценки. . . . .	10

# 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 с 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

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

## 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.  $a \equiv d \pmod{c} \iff (a_x) \equiv (b - x) \pmod{c}$
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.  $a \equiv b \pmod{d}, b \equiv c \pmod{c} \iff a \equiv c \pmod{d}$

Например, можно найти  $2^{100} \pmod{7}$  (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  $0, 1, \dots, N-1$ , взаимно простых с  $N$ . Пусть  $a$  — один из этих остатков. Тогда

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

Функцию  $\varphi$  называют **функцией Эйлера** и традиционно обозначают буквой  $\varphi$ . 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  $c$  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:

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

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

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

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

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  $Pr : U \rightarrow [0; 1]$ , такая что  $\sum_{x \in U} Pr[x] = 1$ . Функция

$Pr$  называется **вероятностным распределением**, а число  $Pr[x]$  называется **вероятностью исхода**  $x \in U$ . Вероятностью события  $A$  называется число  $Pr[A] = \sum_{x \in A} Pr[x]$ .

## 13. Формулировка формулы включений и исключений для вероятностей.

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

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

## 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  $\frac{|A \cap B|}{|B|}$ , 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

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

## 15. Независимые события. Основные свойства независимых событий.

События  $A$  и  $B$  называются независимыми, если

$$Pr[A] = Pr[A | B].$$

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  $B_i \cap B_j = \emptyset$  при  $i \neq j$ . Пусть также  $Pr[B_i] > 0$  для всякого  $i$ . Тогда для всякого события  $A$

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

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

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

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

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

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

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

### 18. Формулировка неравенства Маркова.

**Лемма.** Пусть  $\xi$  — случайная величина, принимающая только **неотрицательные** значения. Тогда для всякого  $x > 0$  верно

$$Pr[\xi \geq x] \leq \frac{E[\xi]}{x}.$$

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

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

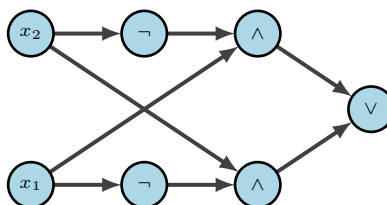
В булевой схеме задано некое число  $m \geq 1$  и члены последовательности  $g_{s-m+1}, \dots, g_s$  называются **выходами схемы**. Число  $m$  называют числом выходов схемы.

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

**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  $\neg x = x | x$  и  $x_1 \wedge x_2 = \neg(x_1 | x_2) = (x_1 | x_2) | (x_1 | x_2)$ .
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:

$$1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus x_1 x_2 x_3;$$

## 22. Схемная сложность функции (размер схемы).

**Схемная сложность** булева отображения  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$  (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 $\text{НОД}(a, N) = 1$ .

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

*Доказательство.* Докажем теорему в обе стороны.

- $\Leftarrow$ : Пусть  $\text{НОД}(a, N) = 1$ . 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  $\text{НОД}(a, N) = 1$ . Докажем от противного.

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

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

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

■

### 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.

### 4. Корректность алгоритма Евклида и расширенного алгоритма Евклида.

### 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.

### 7. Мультипликативность функции Эйлера. Формула для функции Эйлера.

### 8. Формула Байеса. Формула полной 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  $\xi$ . Нам требуется посчитать математическое ожидание случайной величины  $\xi$ . Но при этом случайная величина довольно сложная, и подсчитывать математическое ожидание непосредственно из определения трудно.

Идея состоит в следующем: давайте разобьём сложную случайную величину  $\xi$  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  $E[I_{ij}] = \frac{1}{365}$  (для всякой пары  $i, j$ ). Для математического ожидания  $\xi$  из линейности получаем

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

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.**

**11. Нижняя оценка на максимальное количество ребер в разрезе.**

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

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

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

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

**16. Несчетность множества бесконечных двоичных последовательностей.**

**17. Теорема Кантора-Бернштейна.**

**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.**

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