

Элементарная алгебра

Виды выражений

Одночлен (моном) — произведение переменных и коэффициентов; *многочлен (полином)* — сумма одночленов.

Двучлен (бином) — многочлен из двух одночленов; *трёхчлен (трином)* — многочлен из трёх одночленов.

Многочлен P от одной переменной x можно представить так:

$$P = \sum_{k=0}^n a_k x^{n-k}$$

Малая теорема Безу

Для многочлена $P =: P(x)$ справедливо:

$$P(x) = f(x)(x - r) + P(r)$$

Это следует из деления многочлена с остатком. Значит,

$$(x - r) \mid P(x) \iff P(r) = 0.$$

Свойства неравенств

Отношение сравнения *транзитивно*; неравенства можно *складывать (не вычитать)*, а также *перемножать* и возводить в натуральную степень k (*без смены знака*):

$$\begin{cases} a < b \\ c \leq d \end{cases} \implies \begin{cases} a + c < b + d \\ ac < bd \\ a^k < b^k \end{cases}$$

При умножении на отрицательное число знак неравенства *инвертируется*:

$$a < b \iff am > bm, \quad m \in \mathbb{R}^-$$

Неравенство Коши

Пусть $a, b \in \mathbb{R}^+$. Тогда верно (*О.Л. Коши*):

$$\frac{a+b}{2} \geq \sqrt{ab}$$

Доказательство.

$$\frac{a+b}{2} \geq \sqrt{ab} \iff a+b \geq 2\sqrt{ab} \iff a-2\sqrt{ab}+b \geq 0 \iff (\sqrt{a}-\sqrt{b})^2 \geq 0 \blacksquare$$

Неравенство Бернулли

Пусть $n \geq 2$, $x > 0$. Тогда верно (*Я. Бернулли*):

$$(1+x)^n > 1+nx$$

Доказательство. Проверим базис индукции $n = 2$:

$$(1+x)^2 > 1+2x \iff 1+2x+x^2 > 1+2x \quad \square$$

Проверим индукционный шаг $n + 1$. Пусть утверждение верно для некоторого $n > 2$, тогда:

$$(1+x)^n > 1+nx \iff (1+x)^{n+1} > (1+nx)(1+x) \iff (1+x)^{n+1} > 1+(n+1)x+nx^2 \iff (1+x)^{n+1} > 1+(n+1)x \blacksquare$$

Свойства функций

Функция f *возрастает*, когда

$$\forall x_1, x_2 \in D_f, x_1 < x_2 \implies f(x_1) < f(x_2).$$

Максимумом функции f называется такая точка x_0 , что

$$\forall \varepsilon > 0 \exists U_\varepsilon(x_0) : \forall x \in U f(x) < f(x_0).$$

Функция f *убывает*, когда

$$\forall x_1, x_2 \in D_f, x_1 < x_2 \implies f(x_1) > f(x_2).$$

Минимумом функции f называется такая точка x_0 , что

$$\forall \varepsilon > 0 \exists U_\varepsilon(x_0) : \forall x \in U f(x) > f(x_0).$$

Функция f *чётна*, когда

$$\forall x \in D_f \implies f(-x) = f(x).$$

Функция f *нечётна*, когда

$$\forall x \in D_f \implies f(-x) = -f(x).$$

Функция f *периодична*, когда

$$\forall x \in D_f \exists T \neq 0 : f(x) = f(x \pm T),$$

где T — **период** функции; наименьший положительный период называется *основным*.

Функция модуля

Абсолютная величина (*модуль*) — чётная функция $f: \mathbb{R} \rightarrow \mathbb{R}_0^+$, которая задаётся формулой:

$$f(x) = |x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$$

Она *дистрибутивна* относительно умножения, отчасти — относительно сложения: $|a + b| \leq |a| + |b|$.

Степенная функция

Возведение в чётную степень — чётная функция; график — *парабола*:

$$f: \mathbb{R} \xrightarrow{x \mapsto x^n} \mathbb{R}_0^+, \quad n \in \mathbb{N}$$

Обратная функция к $f|_{\mathbb{R}_0^+}$ — **арифметический корень**:

$$f^{-1}: \mathbb{R}_0^+ \xrightarrow{x \mapsto \sqrt[n]{x}} \mathbb{R}_0^+$$

Возведение в нечётную степень — нечётная функция; график — *кубическая парабола*:

$$g: \mathbb{R} \xrightarrow{x \mapsto x^n} \mathbb{R}, \quad n \in \mathbb{N}$$

Обратная функция к g — **арифметический корень**:

$$g^{-1}: \mathbb{R} \xrightarrow{x \mapsto \sqrt[n]{x}} \mathbb{R}$$

Функция знака

Функция знака (*сигнум-функция*) — нечётная функция $\operatorname{sgn}: \mathbb{R} \rightarrow \{-1; 0; 1\}$, которая определяет знак аргумента:

$$\operatorname{sgn} x = \begin{cases} 1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases}$$

Условия выпуклости функции

Функция f *выпукла вверх* на отрезке $[a; b]$, когда для отрезка g с концами в точках $\langle a; f(a) \rangle, \langle b; f(b) \rangle$ справедливо:

$$\forall x \in [a; b] \quad f(x) \geq g(x)$$

Функция f *выпукла вниз* на отрезке $[a; b]$, когда для отрезка g с концами в точках $\langle a; f(a) \rangle, \langle b; f(b) \rangle$ справедливо:

$$\forall x \in [a; b] \quad f(x) \leq g(x)$$

Функция f выпукла вверх \iff функция $-f$ выпукла вниз.

Функция f выпукла вверх на $[a; b]$, если для $a \leq x \leq b$ верно:

$$\operatorname{tg} \alpha_{bx} \leq \operatorname{tg} \alpha_{ab} \leq \operatorname{tg} \alpha_{ax} \quad \operatorname{tg} \alpha_{mn} := \operatorname{tg}(\overrightarrow{oX}; \overrightarrow{mn})$$

Функция натурального логарифма

Функция натурального логарифма — значение интеграла:

$$\ln x = \int_1^x \frac{dt}{t}, \quad \ln: \mathbb{R}^+ \rightarrow \mathbb{R}$$

Свойства:

$$\ln ax = \ln a + \ln x$$

$$\ln x^{\frac{m}{n}} = \frac{m}{n} \ln x$$

Логарифмическая функция

Логарифмическая функция по основанию a — отношение:

$$\log_a x = \frac{\ln x}{\ln a}, \quad \log_a: \mathbb{R}^+ \rightarrow \mathbb{R}, \quad a \neq 1$$

Свойства:

$$\log_a a^{\frac{m}{n}} = \frac{m}{n}$$

$$\log_a b = \frac{\log_c b}{\log_c a}, \quad c \neq 1$$

$$\log_a a^x = x$$

$$a^{\log_a b} = b$$

$$\log_a b = \frac{1}{\log_b a}, \quad a, b \neq 1$$

Элементарная теория чисел

Делимость

Пусть $a, b \in \mathbb{Z}$. Тогда a — **делитель** b , когда

$$ax = b, x \in \mathbb{Z} \iff a \mid b \iff |a| \leq |b|$$

Отношение делимости *транзитивно*, такое выражение можно *перемножить* с другим:

$$\times \begin{cases} a \mid b \\ c \mid d \end{cases} \implies ac \mid bd$$

Общий делитель чисел делит их *линейную комбинацию*:

$$a \mid b, c \implies a \mid bx + cy, \quad x, y \in \mathbb{Z}$$

Заметим, что $a = bx + cy^*$, когда $(b, c) \mid a$.

Доказательство. Пусть $d := (b, c)$, тогда:

$$d \mid b, c \implies d \mid (bx + cy) \implies d \mid a \quad \blacksquare$$

Коэффициенты Безу (x, y) *неуникальны* и легко выражаются (*доказывается подстановкой в соотношение*):

$$(x + mk, y - ak), \quad k \in \mathbb{Z}$$

* Такое уравнение называют *соотношением Безу*, а x и y — *коэффициентами Безу* (*Э. Безу*).

Наибольший общий делитель

*Наибольший общий делитель** для $\{a_k\}_{k \in \mathbb{N}}$ — такое $\gcd(\{a_k\})$, что

$$\exists d: d \mid \gcd(\{a_k\}) \mid \{a_k\}.$$

Упрощённая запись $\gcd(\{a_k\}) = (\{a_k\})$.

Этот бинарный оператор *коммутативен, ассоциативен и дистрибутивен*.

Наименьшее общее кратное

*Наименьшее общее кратное*** для $\{a_k\}_{k \in \mathbb{N}}$ — такое $\text{lcm}(\{a_k\})$, что

$$\exists m: \{a_k\} \mid \text{lcm}(\{a_k\}) \mid m.$$

Упрощённая запись $\text{lcm}(\{a_k\}) = [\{a_k\}]$.

Этот бинарный оператор *коммутативен и ассоциативен, однако не дистрибутивен*.

Двойственность

НОД и НОК двойственны друг другу:

$$(a, b) \cdot [a, b] = ab$$

Доказательство. Пусть $m := [a, b]$, тогда:

$$a, b \mid m \iff ab \mid am, bm \iff ab \mid (am, bm) \iff ab \mid (a, b)m$$

Так как $(a, b) \mid [a, b] \mid ab$, то $ab/(a, b) \mid [a, b]$.

Значит, $ab/(a, b) \leq [a, b]$. Но $[a, b]$ — *наименьшее* общее кратное a, b . Следовательно, $ab/(a, b) \nless [a, b]$, поэтому:

$$ab/(a, b) = [a, b] \iff ab = (a, b) \cdot [a, b] \blacksquare$$

* Сокращённо *НОД*, или *Greatest Common Divisor (GCD)*.

** Сокращённо *НОК*, или *Least Common Multiple (LCM)*.

Модульная арифметика

Конгруэнтность

Два целых числа **конгруэнтны** (*сравнимы*) по модулю m , когда их разность кратна m (*К.Ф. Гаусс*):

$$a \equiv b \pmod{m} \iff m \mid (a - b) \iff a = b + mk, k \in \mathbb{Z}$$

Отношение конгруэнтности *транзитивно*, поэтому числа образуют *систему остаточных классов* \mathbf{Z}_m по модулю m . Например, \mathbf{Z}_3 :

$$\{\dots, -6, -3, \mathbf{0}, 3, 6, \dots\} \text{ класс } r_0$$

$$\{\dots, -5, -2, \mathbf{1}, 4, 7, \dots\} \text{ класс } r_1$$

$$\{\dots, -4, -1, \mathbf{2}, 5, 8, \dots\} \text{ класс } r_2$$

Свойства сравнения

Конгруэнтные числа можно *складывать*, *перемножать* и передавать *многочлену* $f \in \mathbb{Z}[x]$:

$$\begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod{m} \\ ac \equiv bd \pmod{m} \\ f(a) \equiv f(b) \pmod{m} \end{cases}$$

Конгруэнтные числа можно *умножать* (*делить*) на одно число с *увеличением* (*сокращением*) модуля:

$$a \equiv b \pmod{m} \iff ad \equiv bd \pmod{md}$$

$$ad \equiv bd \pmod{m} \iff a \equiv b \pmod{\frac{m}{(m,d)}}$$

Из транзитивности делимости следует:

$$a \equiv b \pmod{m}, n \mid m \implies a \equiv b \pmod{n}$$

Признаки делимости

Для вывода признаков делимости лучше использовать *десятичное представление* числа $\overline{a_1 a_2 \dots a_n}$:

$$\overline{a_1 a_2 \dots a_n} = \sum_{i=0}^{n-1} a_{n-i} 10^i$$

- При модуле $m = 2^k; 5^k; 10^k$ одночлены $a_{n-i}10^i \equiv a_{n-i}0 = 0$ ($i \geq k$). Значит, число $\overline{a_1 a_2 \dots a_n}$ кратно m , когда последние k цифры кратны m :

$$\overline{a_1 a_2 \dots a_n} \equiv 0 \iff \overline{a_{n-k+1} \dots a_{n-1} a_n} \equiv 0$$

- При модуле $m = 3; 9$ одночлены $a_{n-i}10^i \equiv a_{n-i}1^i = a_{n-i}$. Значит, число $\overline{a_1 a_2 \dots a_n}$ кратно m , когда сумма цифр кратна m :

$$\overline{a_1 a_2 \dots a_n} \equiv 0 \iff a_1 + a_2 + \dots + a_n \equiv 0$$

- При модуле $m = 11$ одночлены $a_{n-i}10^i \equiv a_{n-i}(-1)^i$. Значит, число $\overline{a_1 a_2 \dots a_n}$ кратно 11, когда знакопеременная сумма цифр кратна 11:

$$\overline{a_1 a_2 \dots a_n} \equiv 0 \iff a_1 - a_2 + \dots - a_n \equiv 0$$

- При модуле $m = 7$ вычтем из числа n последнюю цифру; останется $\lfloor n/10 \rfloor$. Последняя цифра равна $n - 10\lfloor n/10 \rfloor$. Вычтем из числа удвоенную последнюю цифру:

$$\left\lfloor \frac{n}{10} \right\rfloor - 2(n - 10 \left\lfloor \frac{n}{10} \right\rfloor) \equiv 0 \iff 21 \left\lfloor \frac{n}{10} \right\rfloor - 2n \equiv 0$$

Одночлен $21\lfloor n/10 \rfloor \equiv 0$. Значит, число $\overline{a_1 a_2 \dots a_n}$ кратно 7, когда удвоенная разность последней цифры числа и самого числа без этой цифры кратна 7:

$$\overline{a_1 a_2 \dots a_n} \equiv 0 \iff \overline{a_1 a_2 \dots a_{n-1}} - 2a_n \equiv 0$$

Функция Эйлера

Функция $\phi(m)$ считает количество положительных целых чисел, меньших m и взаимно простых с ним (для малых и простых m целесообразно перебрать вручную):

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

p — простой делитель m ;

$1/p$ — часть чисел, кратных p ;

$1 - 1/p$ — часть чисел, взаимно простых с p .

Функция Эйлера мультипликативна (только для взаимно простых натуральных чисел).

Теорема Эйлера

Теорема. Пусть $a \in \mathbb{Z}$, $(a, m) = 1$. Тогда верно (Л. Эйлер):

$$a^{\phi(m)} \equiv 1 \pmod{m}, \quad a \not\equiv 0 \pmod{m}$$

Доказательство. Введём систему остаточных классов \mathbf{Z}_m . В ней есть m классов: r_0, r_1, \dots, r_{m-1} .

Пусть множество Φ содержит в себе $\phi(m)$ остатков, взаимно простых с m . Домножим каждый элемент на a и образуем новое множество Φ_a . Заметим, что:

Элементы Φ_a из разных классов. Φ и Φ_a конгруэнтны.

Допустим, это не так. Тогда: Пусть $ar_k \equiv r_l, r_l \in \mathbf{Z}_m$.

$$ar_k \equiv ar_l \Rightarrow r_k \equiv r_l$$

Так как $m \nmid ar_k$, то:

Но $r_k \not\equiv r_l \Rightarrow ar_k \not\equiv ar_l \quad \square$

$$r_l \in \Phi \Rightarrow \Phi \equiv \Phi_a \quad \square$$

Перемножим элементы множеств Φ и Φ_a :

$$r_0 r_1 \dots r_{\phi(m)} \equiv ar_0 ar_1 \dots ar_{\phi(m)} \Rightarrow$$

$$r_0 r_1 \dots r_{\phi(m)} \equiv a^{\phi(m)} r_0 r_1 \dots r_{\phi(m)} \Rightarrow a^{\phi(m)} \equiv 1 \quad \blacksquare$$

Следствие. Пусть $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $(m, a) = 1$. Тогда:

$$a^b \equiv a^{b \bmod \phi(m)} \pmod{m}, \quad a \not\equiv 0 \pmod{m}$$

Доказательство. Представим b в арифметическом виде:

$$b = \phi(m) \left\lfloor \frac{b}{\phi(m)} \right\rfloor + b \bmod \phi(m)$$

$\phi(m)$ — модуль деления.

$\lfloor b/\phi(m) \rfloor$ — целое частное.

$b \bmod \phi(m)$ — остаток.

Подставим полученное выражение:

$$a^{\phi(m) \lfloor b/\phi(m) \rfloor + b \bmod \phi(m)} = (a^{\phi(m)})^{\lfloor b/\phi(m) \rfloor} a^{b \bmod \phi(m)}$$

Так как $a^{\phi(m)} \equiv 1$, получается $a^b \equiv a^{b \bmod \phi(m)} \quad \blacksquare$

Алгоритм Евклида

Пусть $a, b \in \mathbb{N}^0$ ($a > b$), тогда:

$$(a, b) = (a \bmod b, b)$$

Доказательство. Допустим, $m \mid (a - b)$, b :

$$+ \begin{cases} a - b \equiv 0 & (\bmod m) \\ b \equiv 0 & (\bmod m) \end{cases} \Rightarrow \begin{cases} a \equiv 0 & (\bmod m) \\ b \equiv 0 & (\bmod m) \end{cases}$$

Получаем, что любой общий делитель m у $a - b$, b есть у a , b . Следовательно, $(a, b) = (a - b, b)$.

При повторе вычитания получится остаток от деления на b :

$$(a, b) = (a \bmod b, b) \blacksquare$$

Мультипликативная инверсия

Пусть $ab \equiv 1 \pmod{m}$ — линейное сравнение, где b — **мультипликативная инверсия** числа a по модулю m :

$$b \equiv a^{-1} \equiv \frac{1}{a} \pmod{m}, \quad (a, m) = 1$$

«Дробные» числа можно *складывать, перемножать и сокращать* как рациональные:

$$\begin{cases} \frac{a}{b} + \frac{c}{d} \equiv \frac{ad + bc}{cd} & (\bmod m) \\ \frac{a}{b} \times \frac{c}{d} \equiv \frac{ac}{bd} & (\bmod m) \\ \frac{eg}{fg} \equiv \frac{e}{f} & (\bmod m) \end{cases}$$

Линейное сравнение

Линейное сравнение вида $ax \equiv b \pmod{m}$ разрешимо относительно x , когда $(m, a) \mid b$. (по соотношению Безу)

План решения:

- упростить линейное сравнение;
- рассчитать (m, a) по алгоритму Евклида;
- выразить (m, a) через полученные остатки;
- домножить соотношение Безу на b .

Пример. Решить линейное сравнение: $4x \equiv 4 \pmod{6}$.

Упростим сравнение:

$$4x \equiv 4 \pmod{6} \mid : 1/2$$

$$2x \equiv 2 \pmod{3}$$

Применим *алгоритм Евклида* в алгебраическом виде:

«Прямой» алгоритм:

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

«Обратный» алгоритм:

$$1 = 3 \cdot 1 + 2 \cdot (-1) \mid : 2$$

$$2 = 3 \cdot 2 + 2 \cdot (-2)$$

Итак, коэффициенты Безу найдены: $x = -2$, $y = 2$.

Ответ: $x = -2$.

Китайская теорема об остатках

Сравнения можно объединять в *систему*:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Она разрешима относительно x по модулю $[m_1, \dots, m_n]$, когда разрешима каждая пара сравнений, в частности $(m_1, m_2) \mid a_1 - a_2$.

Доказательство. Рассмотрим пару сравнений из системы:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \iff \begin{cases} x = a_1 + m_1 j, & j \in \mathbb{Z} \\ x = a_2 - m_2 k, & k \in \mathbb{Z} \end{cases} \iff m_1 j + m_2 k = a_2 - a_1$$

Данное соотношение Безу имеет целые коэффициенты j, k , когда $(m_1, m_2) \mid (a_1 - a_2)$. \square

По индукции, система будет разрешима относительно x , когда будет разрешима каждая пара сравнений.

Допустим, $x \equiv y \equiv a_i \pmod{m_i}$, $i \in \{i\}_{i=1}^n$ — решение всей системы. Значит, $m_i \mid x - y \implies [m_1, \dots, m_n] \mid x - y \iff x \equiv y \pmod{[m_1, \dots, m_n]}$. \blacksquare

План решения каждой пары сравнений:

- упростить линейные сравнения;
- преобразовать их в соотношения Безу, приравнять их;
- решить полученное выражение как линейное сравнение.

Пример. Решить систему сравнений:

$$\begin{cases} x \equiv 2 & (\text{mod } 3) \\ x \equiv 2 & (\text{mod } 4) \\ 2x \equiv -3 & (\text{mod } 5) \end{cases}$$

Упростим последнее сравнение:

$$2x \equiv -3 \pmod{5} \iff x \equiv 1 \pmod{5}$$

Преобразуем первую пару сравнений в соотношения Безу:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{4} \end{cases} \iff \begin{cases} x = 2 + 3j, & j \in \mathbb{Z} \\ x = 2 + 4k, & k \in \mathbb{Z} \end{cases}$$

Приравняем их и решим как сравнение:

$$2 + 3j = 2 + 4k \iff 2 \equiv 2 + k \pmod{3} \iff k \equiv 0 \pmod{3}$$

Значит, $x = 2 + 4k \equiv 2 \pmod{12}$ — решение первой пары.

Аналогично решив следующую (*и последнюю*) пару, получим решение всей системы: $x \equiv 26 \pmod{60}$.

Ответ: $x \equiv 26 \pmod{60}$.

Сравнение по составному модулю

Пусть $f \in \mathbb{Z}[x]$. Тогда для $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ разрешимо

$$f(x) \equiv 0 \pmod{m},$$

если разрешимы $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}, i \in [1; r] \cap \mathbb{Z}$.

Доказательство \implies . Пусть $x \in \mathbb{Z}$ — решение

$$f(x) \equiv 0 \pmod{m}, p_i^{\alpha_i} \mid m \implies f(x) \equiv 0 \pmod{p_i^{\alpha_i}}. \blacksquare$$

Доказательство \impliedby . Пусть x_i — решение

$$f(x_i) \equiv 0 \pmod{p_i^{\alpha_i}}$$

По китайской теореме об остатках:

$$\forall i_1, i_2 \in [1; r], i_1 \neq i_2 (p_{i_1}^{\alpha_{i_1}}, p_{i_2}^{\alpha_{i_2}}) = 1 \implies$$

$$\exists x: x \equiv x_i \pmod{p_i^{\alpha_i}} \implies f(x) \equiv 0 \pmod{[p_1^{\alpha_1}, \dots, p_r^{\alpha_r}]} \implies f(x) \equiv 0 \pmod{m} \blacksquare$$

Сравнение по степени простого модуля

Пусть $f \in \mathbb{Z}[x]$. Тогда для простого p разрешимо

$$f(x) \equiv 0 \pmod{p^\alpha},$$

если разрешимы $f(x) \equiv 0 \pmod{p^i}$, $i \in [1; \alpha] \cap \mathbb{Z}$.

Доказательство. Аналогично прошлому пункту.

Лемма Гензеля

Пусть для $f \in \mathbb{Z}[x]$ верно (*К. Гензель*):

$$f(a) \equiv 0 \pmod{p^\alpha}, \quad f'(a) \not\equiv 0 \pmod{p}$$

Тогда существует такое уникальное t , что:

$$f(a + tp^\alpha) \equiv 0 \pmod{p^{\alpha+1}}$$

Доказательство. Пусть a — решение $f(x) \equiv 0 \pmod{p^\alpha}$, которое можно представить в виде $x = a + tp^\alpha$.

По теореме Тейлора:

$$\begin{aligned} f(a + tp^\alpha) &= f(a) + tp^\alpha f'(a) + t^2 p^{2\alpha} f''(a)/2! + \dots \\ &+ t^n p^{n\alpha} f^{(n)}(a)/n! \equiv f(a) + tp^\alpha f'(a) \pmod{p^{\alpha+1}} \blacksquare \end{aligned}$$

Следствие. Пусть для $f \in \mathbb{Z}[x]$ верно

$$f(x_\alpha) \equiv 0 \pmod{p^\alpha}, \quad f'(x_\alpha) \not\equiv 0 \pmod{p}.$$

Тогда решение сравнения по модулю $p^{\alpha+1}$ имеет вид:

$$x_{\alpha+1} \equiv x_\alpha - \frac{f(x_\alpha)}{f'(x_\alpha)} \pmod{p^{\alpha+1}}$$

Доказательство. По лемме Гензеля:

$$f(x_\alpha) + tp^\alpha f'(x_\alpha) \equiv 0 \pmod{p^{\alpha+1}} \iff$$

$$tp^\alpha \equiv -\frac{f(x_\alpha)}{f'(x_\alpha)} \pmod{p^{\alpha+1}} \iff$$

$$x_\alpha + tp^\alpha \equiv x_{\alpha+1} \equiv x_\alpha - \frac{f(x_\alpha)}{f'(x_\alpha)} \pmod{p^{\alpha+1}} \blacksquare$$

Тригонометрия

Основные функции

Единичной называется окружность, которая задаётся уравнением $x^2 + y^2 = 1$.

Тригонометрические функции соотносят *координаты* точки единичной окружности и *градусную меру дуги*, образуемой ей с начальным радиусом.

Синус — нечётная функция с периодом 2π ; график — *синусоида*:

$$\sin: \mathbb{R} \xrightarrow{\alpha \mapsto y} [-1; 1]$$

Обратная нечётная функция к $\sin|_{[-\pi/2; \pi/2]}$ — **арксинус**:

$$\sin^{-1} = \arcsin: [-1; 1] \xrightarrow{\alpha \mapsto y} [-\pi/2; \pi/2]$$

Косинус — чётная функция с периодом 2π ; график — *синусоида* со смещением влево на $\pi/2$ («*косинусоида*»):

$$\cos: \mathbb{R} \xrightarrow{\alpha \mapsto x} [-1; 1]$$

Обратная функция к $\cos|_{[0; \pi]}$ — **арккосинус**:

$$\cos^{-1} = \arccos: [-1; 1] \xrightarrow{\alpha \mapsto x} [0; \pi]$$

Тангенс — нечётная функция с периодом π ; график — *тангенсоида*:

$$\operatorname{tg}: \mathbb{R} \setminus \{\pi/2 + \pi n \mid n \in \mathbb{Z}\} \xrightarrow{\alpha \mapsto y/x} \mathbb{R}$$

Обратная нечётная функция к $\operatorname{tg}|_{(-\pi/2; \pi/2)}$ — **арктангенс**:

$$\operatorname{tg}^{-1} = \operatorname{arctg}: \mathbb{R} \xrightarrow{y/x \mapsto \alpha} (-\pi/2; \pi/2)$$

Котангенс — нечётная функция с периодом π ; график — *тангенсоида* с симметрией относительно оси Ox и смещением вправо на $\pi/2$ («*котангенсоида*»):

$$\operatorname{ctg}: \mathbb{R} \setminus \{\pi n \mid n \in \mathbb{Z}\} \xrightarrow{\alpha \mapsto x/y} \mathbb{R}$$

Обратная функция к $\operatorname{ctg}|_{(0; \pi)}$ — **арккотангенс**:

$$\operatorname{ctg}^{-1} = \operatorname{arcctg}: \mathbb{R} \xrightarrow{x/y \mapsto \alpha} (0; \pi)$$

Основные тождества

Из определений тригонометрических функций следует:

$$\begin{array}{ll} \sin^2 \alpha + \cos^2 \alpha = 1 & \arccos x = \arcsin(\sqrt{1-x^2}) \\ 1 + \operatorname{tg}^2 \alpha = 1/\cos^2 \alpha & \arccos x = \operatorname{arctg}(\sqrt{1-x^2}/x) \\ 1 + \operatorname{ctg}^2 \alpha = 1/\sin^2 \alpha & \arcsin y = \operatorname{arcctg}(\sqrt{1-y^2}/y) \end{array}$$

Сумма и разность двух углов

Из скалярного произведения векторов следует:

$$\begin{array}{l} \cos(\alpha \pm \beta) = \cos \alpha \cos \beta \mp \sin \alpha \sin \beta \\ \sin(\alpha \pm \beta) = \sin \alpha \cos \beta \pm \sin \beta \cos \alpha \\ \operatorname{tg}(\alpha \pm \beta) = \frac{\operatorname{tg} \alpha \pm \operatorname{tg} \beta}{1 \mp \operatorname{tg} \alpha \operatorname{tg} \beta} \quad \operatorname{ctg}(\alpha \pm \beta) = \frac{\operatorname{ctg} \alpha \operatorname{ctg} \beta \mp 1}{\operatorname{ctg} \alpha \pm \operatorname{ctg} \beta} \end{array}$$

Доказательство. Пусть $\vec{A} = \langle \cos \alpha; \sin \alpha \rangle$, $\vec{B} = \langle \cos \beta; \sin \beta \rangle$.

Рассмотрим их скалярное произведение:

$$\begin{aligned} + \left\{ \begin{array}{l} \vec{A} \cdot \vec{B} = \cos \alpha \cos \beta + \sin \alpha \sin \beta \\ \vec{A} \cdot \vec{B} = \|\vec{A}\| \|\vec{B}\| \cos(\alpha - \beta) = \cos(\alpha - \beta) \end{array} \right. & \Rightarrow \\ \cos(\alpha - \beta) = \cos \alpha \cos \beta + \sin \alpha \sin \beta & \square \end{aligned}$$

Затем полезно применить эти четыре формулы:

$$\begin{array}{l} \alpha + \beta = \alpha - (-\beta) \\ \sin(\alpha - \beta) = \cos((\pi/2 - \alpha) + \beta) \\ \operatorname{tg} \alpha = \sin \alpha / \cos \alpha \quad \operatorname{ctg} \alpha = \cos \alpha / \sin \alpha \blacksquare \end{array}$$

Двойной угол

Из формул суммы и разности двух углов следует:

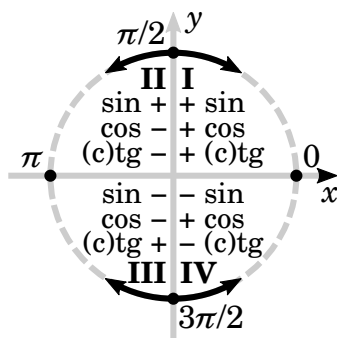
$$\begin{array}{ll} \cos 2\alpha = \cos^2 \alpha - \sin^2 \alpha & \sin 2\alpha = 2 \sin \alpha \cos \alpha \\ \operatorname{tg} 2\alpha = \frac{2 \operatorname{tg} \alpha}{1 - \operatorname{tg}^2 \alpha} & \operatorname{ctg} 2\alpha = \frac{\operatorname{ctg}^2 \alpha - 1}{2 \operatorname{ctg} \alpha} \\ (\sin \alpha \pm \cos \alpha)^2 = 1 \pm \sin 2\alpha \end{array}$$

Формулы приведения

Из формул суммы и разности двух углов следуют *формулы приведения*, которые имеют вид:

$$f(\pi n/2 \pm \alpha) = \pm \text{cof}(\alpha), \quad n \in \mathbb{Z}$$

Конечная функция и её знак определяются по графику; стрелками обозначены места смены функции на *кофункцию*.



Следствие. Для обратных функций верно:

$$\begin{aligned} \arcsin x + \arccos x &= \pi/2 & \arccos x + \arccos(-x) &= \pi \\ \arctg x + \text{arcctg} x &= \pi/2 & \text{arcctg} x + \text{arcctg}(-x) &= \pi \end{aligned}$$

Формулы понижения степени

Из формул двойного угла и основного тригонометрического тождества следует:

$$\begin{aligned} \cos^2 \frac{\alpha}{2} &= \frac{\cos \alpha + 1}{2} & \text{tg}^2 \frac{\alpha}{2} &= \frac{1 - \cos \alpha}{\cos \alpha + 1} \\ \sin^2 \frac{\alpha}{2} &= \frac{1 - \cos \alpha}{2} & \text{ctg}^2 \frac{\alpha}{2} &= \frac{1 - \cos \alpha}{\cos \alpha + 1} \end{aligned}$$

Из них легко выводятся формулы *половинного угла*.

Сумма и разность двух функций

Из формул суммы и разности двух углов следует:

$$\begin{aligned} \sin \alpha \pm \sin \beta &= 2 \sin \frac{\alpha \pm \beta}{2} \cos \frac{\alpha \mp \beta}{2} \\ \cos \alpha + \cos \beta &= 2 \cos \frac{\alpha + \beta}{2} \cos \frac{\alpha - \beta}{2} \\ \cos \alpha - \cos \beta &= -2 \sin \frac{\alpha + \beta}{2} \sin \frac{\alpha - \beta}{2} \end{aligned}$$

$$a \sin \alpha + b \cos \alpha = c \sin(\alpha + \phi) = c \cos(\alpha - \phi), \quad c = \sqrt{a^2 + b^2}$$

Из них можно вывести формулы *произведения двух функций*.

Доказательство. Рассмотрим сумму синусов:

$$\sin(x+y) + \sin(x-y) =$$

$$\sin x \cos y + \sin y \cos x + \sin x \cos y - \sin y \cos x = 2 \sin x \cos y$$

Введём обозначения:

$$\begin{cases} x+y = \alpha \\ x-y = \beta \end{cases} \iff \begin{cases} 2x = \alpha + \beta \\ 2y = \alpha - \beta \end{cases} \iff \begin{cases} x = \frac{\alpha+\beta}{2} \\ y = \frac{\alpha-\beta}{2} \end{cases}$$

Таким образом,

$$\sin \alpha + \sin \beta = 2 \sin \frac{\alpha + \beta}{2} \cos \frac{\alpha - \beta}{2}. \quad \square$$

Похожие формулы доказываются аналогично. \square

Рассмотрим синус суммы двух углов:

$$c \sin(\alpha + \phi) = c \sin \alpha \cos \phi + c \sin \phi \cos \alpha$$

Обозначим $a = c \cos \phi$, $b = c \sin \phi$ и найдём сумму квадратов:

$$a^2 + b^2 = c^2 (\sin^2 \phi + \cos^2 \phi) = c^2 \iff c = \sqrt{(a^2 + b^2)} \quad \square$$

Случай с косинусом доказывается аналогично. \blacksquare

Подстановка Вейерштрасса

Тригонометрические функции от α можно выразить через тангенс от $\alpha/2$ (*К. Вейерштрасс*):

$$\sin \alpha = \frac{2 \operatorname{tg} \frac{\alpha}{2}}{1 + \operatorname{tg}^2 \frac{\alpha}{2}} \quad \cos \alpha = \frac{1 - \operatorname{tg}^2 \frac{\alpha}{2}}{1 + \operatorname{tg}^2 \frac{\alpha}{2}}$$

Доказательство. Распишем каждую функцию:

$$\sin \alpha = \frac{2 \sin \frac{\alpha}{2} \cos \frac{\alpha}{2}}{\sin^2 \frac{\alpha}{2} + \cos^2 \frac{\alpha}{2}} = \frac{2 \operatorname{tg} \frac{\alpha}{2}}{1 + \operatorname{tg}^2 \frac{\alpha}{2}} \quad \square$$

$$\cos \alpha = \frac{\cos^2 \frac{\alpha}{2} - \sin^2 \frac{\alpha}{2}}{\sin^2 \frac{\alpha}{2} + \cos^2 \frac{\alpha}{2}} = \frac{1 - \operatorname{tg}^2 \frac{\alpha}{2}}{1 + \operatorname{tg}^2 \frac{\alpha}{2}} \quad \blacksquare$$

Общая алгебра

Соответствие

Соответствие (бинарное отношение) между множествами X и Y — произвольное множество $\rho \subseteq X \times Y$.

Упрощённая запись $x \in X, y \in Y, \langle x, y \rangle \in \rho =: x \rho y$.

$X \supseteq D_\rho$ — область определения (прообраз) соответствия;

$Y \supseteq E_\rho$ — область значений (образ) соответствия.

Соответствие ρ инъективно, когда

$$\forall x_1, x_2 \in D_\rho \exists y \in E_\rho: x_1 \rho y, x_2 \rho y \iff x_1 = x_2.$$

Соответствие ρ функционально, когда

$$\forall x \in D_\rho \exists! y \in E_\rho: x \rho y.$$

Такое соответствие называется **отображением** (функцией) и обозначается:

$$\rho: X \xrightarrow{x \mapsto y} Y$$

Соответствие ρ сюръективно, когда

$$\forall y \in Y \exists x \in D_\rho: x \mapsto y.$$

Соответствие ρ всюду определено, когда

$$\forall x \in X \exists y \in E_\rho: x \mapsto y.$$

Свойства соответствий

Пусть $* \subseteq X \times X, \circ \subseteq X \times X$ — произвольные соответствия.

Соответствие $*$ ассоциативно, когда

$$\forall x, y, z \in X \implies (x * y) * z = x * (y * z).$$

Соответствие $*$ коммутативно, когда

$$\forall x, y \in X \implies x * y = y * x.$$

Соответствие $*$ дистрибутивно относительно \circ , когда

$$\forall x, y, z \in X \implies \begin{cases} x * (y \circ z) = x * y \circ x * z \\ (y \circ z) * x = y * x \circ z * x \end{cases}.$$

Композиция отображений

Для отображений $f: X \rightarrow Y$, $g: Y \rightarrow Z$ существует $h: X \rightarrow Z$, которое называется их **композицией**.

Упрощённая запись $\forall x \in X \ h(x) = g(f(x)) = (g \circ f)(x)$.

Композиция *ассоциативна*, однако *не коммутативна*.

Ограничение и продолжение

Ограничением отображения $f: X \rightarrow Y$ на $S \subseteq D_f$ называется такое $f|_S: S \rightarrow Y$, что

$$\forall s \in S: f|_S(s) = f(s).$$

В свою очередь, f является *продолжением* отображения $f|_S$.

Метрическое пространство

Метрическое пространство — алгебраическая структура $\langle M; d \rangle$, где d — метрика.

Метрика d множества M — функция $d: M \times M \rightarrow R_0^+$, которая определяет *расстояние* между его двумя элементами.

Например, *евклидова метрика* использует теорему Пифагора в n -мерном пространстве:

$$d(x, y) = \sqrt{\sum_{k=1}^n (x_k - y_k)^2}$$

Для метрического пространства $\langle M; d \rangle$, $x, y, z \in M$ выполняются следующие *аксиомы*:

- $d(x, y) = 0 \iff x = y$ — *тождество*;
- $d(x, y) = d(y, x)$ — *симметрия*;
- $d(x, y) \leq d(x, z) + d(y, z)$ — «*неравенство треугольника*».

Алгебраическая операция

Отображение $*$: $X^n \rightarrow X$ называется n -местной *алгебраической операцией* на X .

Нейтральным называется такой элемент $e \in X$, что

$$\forall x \in X \implies e * x = x \text{ и } x * e = x.$$

Левым или **правым** *нейтральным* называется такой элемент $e \in X$, что

$$\forall x \in X \implies e * x = x \text{ или } x * e = x.$$

Если $x * y = e$, то x — **левый** *обратный* элемент к y , а y — **правый** *обратный* к x .

Стоит отметить, что если $y: X \rightarrow Y$ и $x: Y \rightarrow X$ — отображения, то y *инъективно*, а x *сюръективно*.

Доказательство. По условию, множество X накладывается на себя. Значит, f *всюду определено*.

Так как g функционально, то

$$\forall x_1, x_2 \in X \exists y \in E_f: x_1 f y, x_2 f y \iff x_1 = x_2,$$

то есть f *инъективно*. \square

Когда X накладывается на себя, то

$$\forall x \in E_g \exists y \in D_g: x \mapsto y,$$

то есть g *сюръективно*. \blacksquare

Элементы x и y **взаимно** *обратны*, когда $x * y = y * x = e$.

Алгебраическая структура

Алгебраическая структура (система) — множество X с введёнными на нём алгебраическими операциями:

$$\langle X; *_1, *_2, \dots, *_n \rangle$$

Полугруппа — алгебраическая структура $\langle X; * \rangle$ с двухместной ассоциативной операцией $*$.

Группа — полугруппа, для которой существуют нейтральный и обратный элементы.

Кольцо — коммутативная аддитивная группа, мультипликативная полугруппа, где \times дистрибутивно относительно $+$.

Поле — коммутативное кольцо с обратным элементом для \times .

Числовые системы

Система натуральных чисел — коммутативная аддитивная и мультипликативная полугруппа $\langle \mathbb{N}; +, \times \rangle$.

Система целых чисел — коммутативное кольцо $\langle \mathbb{Z}; +, \times \rangle$.

Система рациональных чисел — упорядоченное поле $\langle \mathbb{Q}; +, \times \rangle$.

Система действительных чисел — непрерывное упорядоченное поле $\langle \mathbb{R}; +, \times \rangle$.

Проективно расширенная числовая прямая — расширение множества действительных чисел $\widehat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$:

$$a \pm \infty = \infty \pm a = \infty, \quad a \neq \infty$$

$$b \cdot \infty = \infty \cdot b = \infty, \quad b \neq 0$$

$$\frac{a}{\infty} = 0 \quad \frac{b}{0} = \infty$$

Комплексные числа

Система комплексных чисел — непрерывное поле $\langle \mathbb{C}; +, \times \rangle$, в котором есть *мнимая единица* i :

$$i^2 = -1$$

Плоскость комплексных чисел — декартова система координат Oab с биективным соответствием вида:

$$z = a + bi \leftrightarrow M\langle a, b \rangle \equiv M\langle z \rangle$$

Oa — действительная ось ($a \equiv \Re z$);

Ob — мнимая ось ($b \equiv \Im z$).

Модуль $z \in \mathbb{C}$ — расстояние от O до $M(z)$:

$$|z| = r = |OM| = \sqrt{a^2 + b^2} = \sqrt{z\bar{z}}$$

Тригонометрическая форма $z \in \mathbb{C}$ —

$$z = r(\cos \varphi + i \sin \varphi), \quad \varphi \in (-\pi; \pi]$$

$\varphi \equiv \arg z$ — *аргумент комплексного числа*, или угол, образованный \overrightarrow{OM} с действительной осью.

Сопряжение — операция смены знака мнимой части $z \in \mathbb{C}$:

$$z = a + bi \rightarrow \bar{z} = a - bi$$

Она *дистрибутивна* относительно $+$, \times .

Извлечение квадратного корня из $z = a + bi$:

$$\sqrt{z} = \pm \left(\sqrt{\frac{|z| + a}{2}} + \operatorname{sgn}(b) i \sqrt{\frac{|z| - a}{2}} \right)$$

Доказательство. По определению нужно найти такое v , что

$$v^2 = (x + yi)^2 = x^2 + 2xyi - y^2 = a + bi = z.$$

Получаем систему уравнений:

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases} \iff + \begin{cases} (x^2 - y^2)^2 = a^2 \\ 4x^2y^2 = b^2 \end{cases} \iff (x^2 + y^2)^2 = |z|^2$$

Извлечём корень из обеих частей уравнения:

$$\pm \begin{cases} x^2 + y^2 = |z| \\ x^2 - y^2 = a \end{cases} \iff \begin{cases} 2x^2 = |z| + a \\ 2y^2 = |z| - a \end{cases} \iff$$

$$x = \pm \sqrt{\frac{|z| + a}{2}}, \quad y = \pm \sqrt{\frac{|z| - a}{2}}$$

Так как $xy = b/2$, то при $b \geq 0 \implies \operatorname{sgn} x = \operatorname{sgn} y$, иначе $\operatorname{sgn} x = -\operatorname{sgn} y$. В общем виде это записывается так:

$$v = \pm \left(\sqrt{\frac{|z| + a}{2}} + \operatorname{sgn}(b) i \sqrt{\frac{|z| - a}{2}} \right) \blacksquare$$

Произведение чисел $z_1, z_2 \in \mathbb{C}$ — число с модулем $|z_1 z_2| = |z_1| \cdot |z_2|$ и аргументом $\arg(z_1 z_2) = \arg z_1 + \arg z_2$.

Следствие. Возведение в степень числа $z = r(\cos \phi + i \sin \phi)$:

$$z^n = r^n (\cos n\phi + i \sin n\phi), \quad n \in \mathbb{Z}$$

Частное чисел $z_1, z_2 \in \mathbb{C}$ — число с модулем $|z_1/z_2| = |z_1|/|z_2|$ и аргументом $\arg(z_1/z_2) = \arg z_1 - \arg z_2$.

Извлечение корня n степени из $z = r(\cos \phi + i \sin \phi)$:

$$\sqrt[n]{z} = \sqrt[n]{r} \left(\cos \frac{\phi + 2\pi k}{n} + i \sin \frac{\phi + 2\pi k}{n} \right), \quad k \in \{m\}_{m=0}^{n-1}$$

Доказательство. По определению нужно найти такое v , что

$$v^n = \rho^n (\cos n\alpha + i \sin n\alpha) = r(\cos \phi + i \sin \phi) = z$$

Получаем систему уравнений:

$$\begin{cases} \rho^n = r \\ n\alpha = \phi + 2\pi k \end{cases} \iff \begin{cases} \rho = \sqrt[n]{r} \\ \alpha = (\phi + 2\pi k)/n, \quad k \in \mathbb{Z} \end{cases}$$

Значит,

$$v = \sqrt[n]{r} \left(\cos \frac{\phi + 2\pi k}{n} + i \sin \frac{\phi + 2\pi k}{n} \right). \blacksquare$$

Деление отрезка в отношении

Точка C делит отрезок AB в отношении $\lambda \in \mathbb{R}$, если:

$$\begin{cases} C \in AB \\ \overrightarrow{AC} = \lambda \overrightarrow{CB} \\ \lambda \neq -1 \end{cases}$$

Теорема. Пусть C делит AB в отношении $\lambda \in \mathbb{R}$; $A = A\langle a \rangle$, $B = B\langle b \rangle$. Тогда комплексная координата точки C равна:

$$c = \frac{a + \lambda b}{1 + \lambda}$$

Также формула является достаточным критерием принадлежности трёх точек одной прямой.

Доказательство. По условию:

$$\begin{aligned} \overrightarrow{AC} = \lambda \overrightarrow{CB} &\iff \overrightarrow{OC} - \overrightarrow{OA} = \lambda (\overrightarrow{OB} - \overrightarrow{OC}) \iff \\ c - a &= \lambda (b - c) \iff c = \frac{a + \lambda b}{1 + \lambda} \blacksquare \end{aligned}$$

Причём если C — середина AB , то:

$$\lambda = 1 \implies c = \frac{a + b}{2}$$

Длина отрезка

Расстояние между точками $A\langle a \rangle$ и $B\langle b \rangle$ —

$$|\overrightarrow{AB}| = |a - b| \implies AB^2 = (a - b)(\bar{a} - \bar{b})$$

Уравнение окружности с центром $A\langle a \rangle$ радиуса r —

$$(z - a)(\bar{z} - \bar{a}) = r^2$$

Скалярное произведение векторов

Скалярное произведение радиус-векторов —

$$2\overrightarrow{OA} \cdot \overrightarrow{OB} = a\bar{b} + \bar{a}b$$

Доказательство. Пусть $A\langle a \rangle$, $B = \langle b \rangle$, $a = x_1 + y_1 i$,

$b = x_2 + y_2 i$. Тогда:

$$\begin{aligned} a\bar{b} + \bar{a}b &= (x_1 + y_1 i)(x_2 - y_2 i) + (x_1 - y_1 i)(x_2 + y_2 i) = \\ &= 2(x_1 x_2 + y_1 y_2) = 2\overrightarrow{OA} \cdot \overrightarrow{OB} \blacksquare \end{aligned}$$

Пусть $A\langle a \rangle$, $B\langle b \rangle$, $C\langle c \rangle$, $D\langle d \rangle$ — четыре различные точки. Тогда скалярное произведение произвольных векторов —

$$2\overrightarrow{AB} \cdot \overrightarrow{CD} = (b - a)(\bar{d} - \bar{c}) + (\bar{b} - \bar{a})(d - c)$$

Доказательство. По условию:

$$\begin{aligned} 2\overrightarrow{AB} \cdot \overrightarrow{CD} &= 2(\overrightarrow{OB} - \overrightarrow{OA})(\overrightarrow{OD} - \overrightarrow{OC}) = \\ &= 2(\overrightarrow{OB} \cdot \overrightarrow{OD} - \overrightarrow{OB} \cdot \overrightarrow{OC} - \overrightarrow{OA} \cdot \overrightarrow{OD} + \overrightarrow{OA} \cdot \overrightarrow{OC}) = \\ &= 2 \cdot \frac{1}{2}(b\bar{d} + \bar{b}d - b\bar{c} - \bar{b}c - a\bar{d} - \bar{a}d + a\bar{c} + \bar{a}c) = \\ &= (a - b)(\bar{c} - \bar{d}) + (\bar{a} - \bar{b})(c - d) \blacksquare \end{aligned}$$

Коллинеарность векторов

Критерий коллинеарности точек O, A, B —

$$\frac{a}{b} = \frac{\bar{a}}{\bar{b}} \quad \text{или} \quad \begin{cases} a = 0 \\ b = 0 \end{cases}$$

Критерий параллельности векторов $\overrightarrow{AB}, \overrightarrow{CD}$ —

$$\overrightarrow{AB} \parallel \overrightarrow{CD} \iff \frac{b - a}{d - c} = \frac{\bar{b} - \bar{a}}{\bar{d} - \bar{c}}$$

Если A, B, C, D лежат на одной окружности, то:

$$\overrightarrow{AB} \parallel \overrightarrow{CD} \iff \frac{b}{d} = \frac{a}{c}$$

Критерий принадлежности трёх точек одной прямой —

$$\frac{b - a}{c - a} = \frac{\bar{b} - \bar{a}}{\bar{c} - \bar{a}}$$

Уравнение прямой, проходящей через точки $A\langle a \rangle$, $B\langle b \rangle$ —

$$(\bar{a} - \bar{b})z + (b - a)\bar{z} + a\bar{b} - b\bar{a} = 0$$

Предел последовательности

Предел

Предел последовательности $\{x_n\}$ — такое a , что

$$\forall \varepsilon > 0 \exists N: \forall n > N \ x_n \in U_\varepsilon(a).$$

Упрощённая запись $\lim_{n \rightarrow \infty} x_n = a$ или $n \rightarrow \infty, x_n \rightarrow a$.

Этот оператор *дистрибутивен* относительно сложения, умножения.

Частичным называется предел подпоследовательности.

Свойства предела

Сходимость \Rightarrow ограниченность.

Доказательство. Пусть $\lim_{n \rightarrow \infty} x_n = a$. По определению:

$$\forall \varepsilon > 0 \exists N: \forall n > N \ x_n \in U_\varepsilon(a)$$

По «дистрибуции» модуля относительно сложения:

$$|x_n| = |x_n - a + a| \leq |x_n - a| + |a| < \varepsilon + |a|$$

Положим, что $\forall m \leq N \ L = \max(|\{x_m\}|, \varepsilon + |a|) \Rightarrow |x_n| \leq L$. ■

Пусть $n \rightarrow \infty, x_n \rightarrow a, y_n \rightarrow b$. Выполняя *предельный переход*, при $x_n \leq y_n$ или $x_n < y_n$ сохраняется неравенство $a \leq b$.

Доказательство. По определению предела:

$$\forall \varepsilon > 0 \exists N: \forall n > N \ x_n \in U_\varepsilon(a), y_n \in U_\varepsilon(b)$$

Следовательно,

$$+ \begin{cases} x_n \leq y_n \\ a - x_n < \varepsilon \\ y_n - b < \varepsilon \end{cases} \iff \begin{cases} y_n - x_n \geq 0 \\ y_n - x_n < 2\varepsilon + b - a \end{cases} \iff \frac{a - b}{2} < \varepsilon$$

Так как ε — сколь угодно малое положительное число, то $a - b \leq 0 \iff a \leq b$. □

При $x_n < y_n$ доказательство аналогично. ■

Пусть $n \rightarrow \infty, x_n, y_n \rightarrow a$. Тогда при $\forall \{z_n\}: x_n \leq z_n \leq y_n$ справедливо $z_n \rightarrow a$. (*теорема о промежуточной функции*)

Доказательство. По определению предела:

$$\forall \varepsilon > 0 \exists N: \forall n > N \ x_n, y_n \in U_\varepsilon(a)$$

Следовательно,

$$a - \varepsilon < x_n \leq z_n \leq y_n < a + \varepsilon \implies z_n \in U_\varepsilon(a) \implies \lim_{n \rightarrow \infty} z_n = a. \blacksquare$$

Условие Коши

Последовательность $\{x_n\}$ удовлетворяет условию Коши (является фундаментальной), если

$$\forall \varepsilon > 0 \exists N: \forall n, m > N \ |x_n - x_m| < \varepsilon.$$

Фундаментальность \implies ограниченность.

Доказательство. По условию Коши:

$$\forall \varepsilon > 0 \exists N: \forall n, m > N \ |x_n - x_m| < \varepsilon$$

По «дистрибуции» модуля относительно сложения:

$$\begin{aligned} \begin{cases} |x_n - x_m| < \varepsilon \\ |x_n| = |x_n - x_m + x_m| \end{cases} &\iff \begin{cases} |x_n - x_m| < \varepsilon \\ |x_n| \leq |x_n - x_m| + |x_m| \end{cases} \iff \\ &|x_n| < \varepsilon + |x_m| \end{aligned}$$

Положим, что $\forall k \leq N \ L = \max(|\{x_k\}|, \varepsilon + |x_m|) \implies |x_n| \leq L. \blacksquare$

Принцип компактности отрезка

Ограниченность \implies частичная сходимость:

$$\forall \{x_n\} \in [a; b] \exists \{n_k\} \uparrow: \lim_{k \rightarrow \infty} x_{n_k} = \xi$$

Доказательство. По принципу Кантора:

$$\begin{aligned} \forall k \in \mathbb{N} \exists! \xi \in [a_k; b_k] \subset [a_{k-1}; b_{k-1}] &\iff \\ \lim_{k \rightarrow \infty} a_k = \lim_{k \rightarrow \infty} b_k = \xi & \end{aligned}$$

Образуем подпоследовательность:

$$\{x_{n_k} \mid \{n_k\} \uparrow, x_{n_k} \in [a_k; b_k]\}$$

По теореме о промежуточной функции:

$$a_k \leq x_{n_k} \leq b_k \implies \lim_{k \rightarrow \infty} x_{n_k} = \xi \blacksquare$$

Частичный предел фундаментальной последовательности является её пределом.

Доказательство. Пусть $\{x_n\}$ фундаментальна \Rightarrow она ограничена.

По принципу компактности отрезка $\lim_{k \rightarrow \infty} x_{n_k} = a$.

По условию Коши:

$$\forall \varepsilon/2 > 0 \exists N: \forall n, m > N |x_n - x_m| < \varepsilon/2$$

Зафиксируем n . При $x_m = x_{n_k} > N$ перейдём к пределу:

$$|x_n - a| \leq \varepsilon/2 < \varepsilon \iff \lim_{k \rightarrow \infty} x_{n_k} = a \blacksquare$$

Критерий Коши

Сходимость \iff фундаментальность.

Доказательство \Rightarrow . По определению предела:

$$\forall \varepsilon > 0 \exists N: \forall n > N x_n \in U_{\varepsilon/2}(a)$$

Значит, $\forall n, m > N |x_n - x_m| = |(x_n - a) + (a - x_m)|$.

По «дистрибуции» модуля относительно сложения:

$$|x_n - x_m| \leq |x_n - a| + |x_m - a| < \varepsilon/2 + \varepsilon/2 = \varepsilon \blacksquare$$

Доказательство \Leftarrow . Пусть $\{x_n\}$ фундаментальна \Rightarrow она ограничена \Rightarrow по принципу компактности отрезка она частично сходится к $c \Rightarrow$ по условию Коши и принципу компактности отрезка она сходится к c . \blacksquare

Теорема Вейерштрасса

Монотонность \Rightarrow сходимость:

$$\left[\begin{array}{l} \forall \{x_n\} \nearrow \lim_{n \rightarrow \infty} x_n = \sup\{x_n\} \\ \forall \{y_n\} \searrow \lim_{n \rightarrow \infty} y_n = \inf\{y_n\} \end{array} \right.$$

Доказательство. По определению точной верхней границы:

$$\forall n \in \mathbb{N} x_n \leq \sup\{x_n\}$$

Так как последовательность неубывает, то

$$\forall \varepsilon > 0 \exists N: \forall n > N x_n \in U_\varepsilon(\sup\{x_n\}) \Rightarrow$$

$$\lim_{n \rightarrow \infty} x_n = \sup\{x_n\}. \quad \square$$

Для $\{y_n\} \searrow$ доказательство аналогично. ■

Предел функции

Предел

Предел функции $f: X \rightarrow Y$ в точке $x_0 \in X$ по Коши — такое $a \in Y$, что (О.Л. Коши)

$$\forall \varepsilon > 0 \exists \delta > 0: \underbrace{\forall x \in \mathring{U}_\delta(x_0) \subseteq D_f}_I, \underbrace{f(x) \in U_\varepsilon(a)}_{II}.$$

I — функция f определена в какой-либо проколотой δ -окрестности точки x_0 ;

II — функция f имеет образ в какой-либо проколотой ε -окрестности точки a .

Предел функции $f: X \rightarrow Y$ в точке $x_0 \in X$ по Гейне — такое $a \in Y$, что (Э. Гейне)

$$\forall \{x_n\} \in D_f: \lim_{n \rightarrow \infty} x_n = x_0 \ (x_n \neq x_0) \implies \lim_{n \rightarrow \infty} f(x_n) = a.$$

Упрощённая запись $\forall x \in X \lim_{x \rightarrow x_0} f(x) = a$ или $x \rightarrow x_0, f(x) \rightarrow a$.

Критерий Коши

Сходимость \iff выполнение условия Коши:

$$\forall \varepsilon > 0 \exists \delta > 0: \forall x', x'' \in \mathring{U}_\delta(x_0) |f(x') - f(x'')| < \varepsilon$$

Доказательство \implies . По определению предела:

$$\forall \varepsilon > 0 \exists \delta > 0: \mathring{U}_\delta(x_0) \subseteq D_f, U_{\varepsilon/2}(a) \cap E_f \neq \emptyset$$

Пусть $x', x'' \in \mathring{U}_\delta(x_0)$; по неравенству треугольника:

$$|f(x') - f(x'')| \leq |f(x') - a| + |f(x'') - a| < \varepsilon/2 + \varepsilon/2 = \varepsilon \blacksquare$$

Доказательство \Leftarrow . По условию Коши:

$$\exists \{x_n\} \in D_f: \lim_{n \rightarrow \infty} x_n = x_0, x_n \neq x_0$$

Последовательности $\{f(x_n)\}$ фундаментальны \implies сходятся.

По фундаментальности и сходимости к одной точке x_0 :

$$\lim_{x \rightarrow x_0} f(x) = a \blacksquare$$

Предел композиции функций

Пусть $f: X \rightarrow Y, g: Y \rightarrow Z$. Тогда:

$$\begin{cases} \lim_{x \rightarrow x_0} f(x) = y_0 \\ \lim_{x \rightarrow x_0} g(x) = z_0 \end{cases} \iff \begin{cases} \lim_{x \rightarrow x_0} (g \circ f)(x) = z_0 \\ f(x) \neq y_0 \end{cases}$$

Доказательство. Пусть $g \circ f = \varphi$; по определению предела:

$$\begin{cases} \forall \varepsilon > 0 \exists \delta > 0: \dot{U}_\delta(y_0) \subseteq D_g, U_\varepsilon(z_0) \cap E_g \neq \emptyset \\ \forall \delta > 0 \exists \sigma > 0: \dot{U}_\sigma(x_0) \subseteq D_f, U_\delta(y_0) \cap E_f \neq \emptyset \end{cases}$$

Из $\dot{U}_\delta(y_0) \cap U_\delta(y_0) = \dot{U}_\delta(y_0)$ следует:

$$\begin{cases} \forall \varepsilon > 0 \exists \sigma > 0: \dot{U}_\sigma(x_0) \subseteq D_f, U_\varepsilon(\varphi(x)) \cap E_g \neq \emptyset \\ y \neq y_0 \iff f(x) \neq y_0 \end{cases} \iff$$

$$\lim_{x \rightarrow x_0} \varphi(x) = z_0, f(x) \neq y_0. \blacksquare$$

Бесконечно малая функция

Функция g *бесконечно мала* относительно f при $x \rightarrow x_0$, если

$$g(x) = \varepsilon(x)f(x) := o(f), \quad \lim_{x \rightarrow x_0} \varepsilon(x) = 0.$$

Верно следующее утверждение:

$$\lim_{x \rightarrow x_0} f(x) = a \iff f(x) = a + o(x)$$

Доказательство \Rightarrow . По определению предела:

$$\forall \varepsilon > 0 \exists \delta > 0: 0 < |x - x_0| < \delta, |f(x) - a| < \varepsilon$$

По теореме о промежуточной функции:

$$0 \leq |f(x) - a| < \varepsilon \implies \lim_{x \rightarrow x_0} (f(x) - a) = 0 \iff$$

$$f(x) - a = o(x) \iff f(x) = a + o(x) \blacksquare$$

Доказательство \Leftarrow . По условию:

$$f(x) = a + o(x) \iff |f(x) - a| = |o(x)|$$

По определению бесконечно малой функции:

$$\forall \varepsilon > 0 \exists \delta > 0: 0 < |x - x_0| < \delta, |o(x)| < \varepsilon$$

По определению предела:

$$|f(x) - a| < \varepsilon \iff \lim_{x \rightarrow x_0} f(x) = a \blacksquare$$

Односторонний предел

Правосторонним называется предел функции, который определён в терминах правосторонних ε -окрестностей (*неубывающих последовательностей*):

$$\lim_{x \rightarrow x_0 + 0} f(x) = a \quad \text{или} \quad x \rightarrow x_0 + 0, f(x) \rightarrow a$$

Левосторонним называется предел функции, который определён в терминах левосторонних ε -окрестностей (*возрастающих последовательностей*).

$$\lim_{x \rightarrow x_0 - 0} f(x) = a \quad \text{или} \quad x \rightarrow x_0 - 0, f(x) \rightarrow a$$

Существование предела равносильно существованию *равных* односторонних пределов:

$$\lim_{x \rightarrow x_0} f(x) \iff \lim_{x \rightarrow x_0 + 0} f(x) = \lim_{x \rightarrow x_0 - 0} f(x)$$

Непрерывность

Пусть $\forall \varepsilon > 0 \ U_\varepsilon(x_0) \subseteq D_f$. Тогда:

$x - x_0 =: \Delta x$ — *приращение аргумента* в точке x_0 ;
 $f(x) - f(x_0) =: \Delta f$ — *приращение функции* в точке x_0 .

Функция f *непрерывна* в точке x_0 , если

$$\lim_{x \rightarrow x_0} f(x) = f(x_0) \quad \text{или} \quad \Delta x \rightarrow 0, \Delta f \rightarrow 0.$$

Определения *непрерывности справа* и *слева* точки x_0 связаны с правосторонними и левосторонними пределами.

Непрерывными в точке x_0 являются *сумма*, *произведение* и *композиция* непрерывных в ней функций.

Теорема Вейерштрасса

Пусть $f \in C[a; b]$. Тогда в некоторых точках отрезка функция достигает своих точных верхней и нижней границ на $[a; b]$.

Доказательство. Пусть $\sup f([a; b]) =: M$, $\inf f([a; b]) =: m$.

По определению точных верхней и нижней границ:

$$\forall x \in [a; b] \quad f(x) \in [m; M]$$

По принципу компактности отрезка:

$$\lim_{n \rightarrow \infty} f(x_n) = M \quad \lim_{k \rightarrow \infty} x_{n_k} = \xi$$

По определению непрерывности:

$$\lim_{k \rightarrow \infty} f(x_{n_k}) = f(\xi) \implies f(\xi) = M \blacksquare$$

Теорема о промежуточном значении

Пусть f непрерывна на промежутке $X \ni a, b$. Тогда:

$$\forall c \in [f(a); f(b)] \quad \exists \xi \in [a; b] : c = f(\xi)$$

Доказательство. По принципу Кантора:

$$\begin{aligned} \forall n \in \mathbb{N} \quad \exists \xi \in [a_n; b_n] \subset [a_{n-1}; b_{n-1}] \subseteq X \implies \\ n \rightarrow \infty, \quad a_n, b_n \rightarrow \xi \end{aligned}$$

По определению непрерывности функции на промежутке:

$$n \rightarrow \infty, \quad f(a_n), f(b_n) \rightarrow f(\xi)$$

По теореме о промежуточной функции:

$$f(a_n) \leq c \leq f(b_n) \implies c = f(\xi) \blacksquare$$

Дифференциальное исчисление

Производная

Функция f имеет в точке x_0 производную (дифференцируема в ней), если (Ж.Л. Лагранж)

$$\forall \epsilon > 0 \ U_\epsilon(x_0) \cap D_f \neq \emptyset, \quad \lim_{\Delta x \rightarrow 0} \frac{\Delta f}{\Delta x} =: f'(x_0).$$

Этот оператор дистрибутивен относительно сложения:

$$(f \cdot g)' = f'g + fg'$$

$$\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$$

$$(f \circ g)' = (f' \circ g)g'$$

Свойства производной

Дифференцируемость \Rightarrow непрерывность.

Доказательство. По определению производной:

$$\lim_{\Delta x \rightarrow 0} \frac{\Delta f}{\Delta x} = f'(x_0) \iff \frac{\Delta f}{\Delta x} = f'(x_0) + o(\Delta x) \iff$$

$$\Delta f = \Delta x(f'(x_0) + o(\Delta x)) \implies \Delta x \rightarrow 0, \Delta f \rightarrow 0 \blacksquare$$

Приращение дифференцируемой функции легко представить в виде:

$$\Delta f = f'(x_0) \Delta x + o(\Delta x) \Delta x$$

Дифференциал функции — линейная часть её приращения:

$$dy := f'(x_0) \Delta x$$

Значит, формула производной имеет вид:

$$f'(x_0) = \frac{dy}{\Delta x} = \frac{dy}{dx} \quad (\Delta x = dx)$$

Производные элементарных функций

Таблица производных элементарных функций:

$C' = 0$	$(x^n)' = nx^{n-1}$
$\sin' \alpha = \cos \alpha$	$\cos' \alpha = -\sin \alpha$
$\operatorname{tg}' \alpha = \frac{1}{\cos^2 \alpha}$	$\operatorname{ctg}' \alpha = -\frac{1}{\sin^2 \alpha}$
$\arcsin' x = \frac{1}{\sqrt{1-x^2}}$	$\arccos' x = -\frac{1}{\sqrt{1-x^2}}$
$\operatorname{arctg}' x = \frac{1}{1+x^2}$	$\operatorname{arcctg}' x = -\frac{1}{1+x^2}$

Промежутки монотонности

Если функция f дифференцируема в точке x_0 , то

$$\begin{cases} f'(x_0) > 0 \Rightarrow f \uparrow \text{ около } x_0 \\ f'(x_0) < 0 \Rightarrow f \downarrow \text{ около } x_0 \end{cases}.$$

Доказательство. По определению производной:

$$f'(x_0) > 0 \Leftrightarrow \lim_{\Delta x \rightarrow 0} \frac{\Delta f}{\Delta x} > 0 \Leftrightarrow \frac{\Delta f}{\Delta x} > o(\Delta x)$$

При достаточно малом Δx верно:

$$\frac{\Delta f}{\Delta x} > 0 \Leftrightarrow \begin{cases} \Delta f, \Delta x > 0 \\ \Delta f, \Delta x < 0 \end{cases} \Leftrightarrow f \uparrow \text{ около } x_0 \quad \square$$

Для $f'(x_0) < 0$ доказательство аналогично. ■

Условие существования экстремума

Точка локального экстремума \Rightarrow критическая точка.

Доказательство. По определению локального максимума:

$$\exists \delta > 0: \forall x \in \mathring{U}_\delta(x_0) \quad f(x_0) > f(x)$$

Производная в точке x_0 либо существует, либо нет. \square

Допустим, она существует; по определению производной:

$$\lim_{x \rightarrow x_0} \frac{\Delta f}{\Delta x} = f'(x_0)$$

По предельному переходу:

$$\begin{cases} \Delta x > 0 \Rightarrow \Delta f / \Delta x < 0 \Rightarrow f'(x_0) \leq 0 \\ \Delta x < 0 \Rightarrow \Delta f / \Delta x > 0 \Rightarrow f'(x_0) \geq 0 \end{cases} \iff 0 \leq f'(x_0) \leq 0 \iff f'(x_0) = 0 \quad \square$$

Для локального минимума доказательство аналогично. ■

Если в критической точке производная меняет знак, она является локальным экстремумом.

Доказательство. По определению критической точки:

$$\begin{cases} f'(x_0) = 0 \\ f'(x_0) = \text{undefined} \end{cases}$$

Допустим для определённости:

$$\begin{cases} \exists \delta > 0: \forall x \in \overset{\circ}{U}_{\delta-}(x_0) \ f'(x) > 0 \\ \exists \delta > 0: \forall x \in \overset{\circ}{U}_{\delta+}(x_0) \ f'(x) < 0 \end{cases}$$

По промежуткам монотонности:

$$\begin{cases} f \uparrow \text{ на } U_{\delta-}(x_0) \\ f \downarrow \text{ на } U_{\delta+}(x_0) \end{cases} \iff x_0 \text{ — локальный максимум } \square$$

Для локального минимума доказательство аналогично. ■

Теорема Ролля

Пусть f дифференцируема на $(a; b)$, непрерывна на $f[a; b]$, и $f(a) = f(b)$. Тогда: (*М. Ролль*)

$$\exists \xi \in (a; b): f'(\xi) = 0$$

Доказательство. По теореме Вейерштрасса:

$$f(m) = \inf f([a; b]) \quad f(M) = \sup f([a; b])$$

При $f(a) = f(b) = f(m)$ по условию существования экстремума:

$$f'(M) = 0 \quad \square$$

При $f(m) = f(M)$ функция — константа на $[a; b]$, производная которой равна нулю. ■

Теорема Лагранжа

Пусть f дифференцируема на $(a; b)$ и непрерывна на $f[a; b]$. Тогда: (*Ж.Л. Лагранж*)

$$\exists \xi \in (a; b) : f'(\xi) = \frac{f(b) - f(a)}{b - a}$$

Доказательство. Пусть $\varphi(x) := f(x) - \lambda x$; подберём λ так, чтобы $\varphi(a) = \varphi(b)$:

$$\begin{aligned} f(a) - \lambda a = f(b) - \lambda b &\iff (b - a)\lambda = f(b) - f(a) \iff \\ \lambda &= \frac{f(b) - f(a)}{b - a} \end{aligned}$$

По теореме Ролля:

$$\begin{aligned} \exists \xi \in (a; b) : \varphi'(\xi) = 0 &\iff f'(\xi) - \lambda = 0 \iff \\ \lambda = f'(\xi) &\implies f'(\xi) = \frac{f(b) - f(a)}{b - a} \quad \blacksquare \end{aligned}$$

Условие постоянства функции

Пусть f непрерывна на $[a; b]$ и состоит из стационарных точек на $(a; b)$. Тогда $f([a; b]) = C$.

Доказательство. По теореме Лагранжа:

$$\forall x', x'' \in [a; b] \exists \xi \in (x'; x'') : f'(\xi) = \frac{f(x'') - f(x')}{x'' - x'}$$

По определению стационарной точки:

$$f'(\xi) = 0 \implies \frac{f(x'') - f(x')}{x'' - x'} = 0 \iff f(x'') = f(x') \quad \blacksquare$$

Пусть f, g непрерывны на $[a; b]$ и $f' = g'$. Тогда:

$$\forall x \in [a; b] f(x) - g(x) = C$$

Доказательство. Пусть $\varphi := f - g$; по условию:

$$\forall x \in (a; b) \quad \varphi'(x) = f'(x) - g'(x) = 0$$

По условию постоянства функции:

$$\varphi'(x) = 0 \iff \varphi(x) = C \iff f(x) - g(x) = C \blacksquare$$

Теория графов

Ориентированный граф

Граф (*ориентированный граф или орграф*) — упорядоченная пара $G = \langle V, E \rangle$, где

V — непустое множество *вершин (узлов)*;

E — конечное множество *рёбер*, $E \subseteq V \times V$.

Порядок графа G — число его вершин $n = |V|$.

Размер графа G — число его рёбер $m = |E|$.

Ребро $e = \langle v, w \rangle$ задаётся вершинами v, w , где v — начало ребра, а w — его конец; вершины v, w являются *соседними*.

Входящая валентность вершины v графа G — число рёбер, чей конец в v :

$$\text{indeg}(v) = |\{\langle u, v \rangle \mid \langle u, v \rangle \in E\}|$$

Исходящая валентность вершины v графа G — число рёбер, чьё начало в v :

$$\text{outdeg}(v) = |\{\langle v, u \rangle \mid \langle v, u \rangle \in E\}|$$

Валентность вершины v графа G — сумма входящей и исходящей валентностей вершины:

$$\text{deg}(v) = \text{indeg}(v) + \text{outdeg}(v)$$

Свойство. Пусть $G = \langle V, E \rangle$ — граф с n вершинами и m рёбрами, причём $V = \{v_1, \dots, v_n\}$. Тогда:

$$\sum_{i=1}^n \text{indeg}(v_i) = \sum_{i=1}^n \text{outdeg}(v_i) = m$$

Подграф $G = \langle V, E \rangle$, *порождённый* на $W \subset V$, — граф вида

$$G_W = \langle W, E \cap W \times W \rangle.$$

Последовательность вершин

Маршрут от вершины v_i до вершины v_j графа G — последовательность вершин или рёбер:

$$\left\{ \begin{array}{l} [v_i, v_{i+1}, \dots, v_{j-1}, v_j] \text{ вершины} \\ [e_i, e_{i+1}, \dots, e_{j-1}, e_j] \text{ рёбра} \\ e_k = \langle v_{k-1}, v_k \rangle, k \in \{i+1, \dots, j\} \end{array} \right.$$

Закрытым называется такой маршрут, где начальная и конечная вершины совпадают.

Цепь — маршрут без повтора рёбер; *простая цепь* — маршрут без повтора рёбер и вершин (*кроме, возможно, первой и последней вершины*); *цикл* — закрытая простая цепь.

Ациклическим (лесом) называется граф без циклов.

Неориентированный граф

Неорграф (*неориентированный граф*) — такой граф $G = \langle V, E \rangle$, что $\forall v, w \in V \langle v, w \rangle \in E \Rightarrow \langle w, v \rangle \in E$.

Валентность вершины v неорграфа — число рёбер, которые связаны с v .

Связным называется такой неорграф, между любыми вершинами которого есть маршрут.

Компонент связности неорграфа — связный подграф, который не входит в состав такого же подграфа.

Связность графа

Связным называется такой орграф, у которого аналогичный неорграф связный.

Орграф $G = \langle V, E \rangle$ называется *сильно связным*, если

$$\forall v, w \in V \exists \begin{cases} \text{маршрут от } v \text{ до } w \\ \text{маршрут от } w \text{ до } v \end{cases}$$

Компонент сильной связности графа — сильно связный подграф, который не входит в состав такого же подграфа.

Виды неориентированных графов

Неориентированный граф $G = \langle V, E \rangle =: K_n$, $n = |V|$ называется *полным*, если $\forall v, w \in V, v \neq w \langle v, w \rangle \in E$.

Неориентированный граф $G = \langle V, E \rangle$ называется *однородным*, если $\forall v, w \in V \deg(v) = \deg(w)$.

Свободное дерево

Дерево (*свободное*) — компонент связности леса $T = \langle V, E \rangle$.

Свойство. Пусть $T = \langle V, E \rangle$. Тогда $|E| = |V| - 1$.

Поддерево $T = \langle V, E \rangle$, порождённое на $W \subset V$, — дерево вида:

$$T_W = \langle W, E \cap W \times W \rangle$$

Корневое дерево

Корневое дерево (*ориентированное дерево или одерево*) — такой орграф, у которого:

- аналогичный неорграф есть свободное дерево;
- есть единственная вершина с нулевой входящей валентностью, или *корень*.

Пусть $T = \langle V, E \rangle$ — дерево, $\langle v, w \rangle \in E$:

$v =: \text{parent}_w$ — *родитель*
вершины w .

$w \in \text{children}_v$ — *ребёнок*
вершины v .

Корневым называется узел
без родителей.

Листовым называется узел
без детей.

Родственными называются вершины с общими родителями.

Первый в памяти ребёнок узла v — first_v , *последний* — last_v ;
следующий в памяти родственник узла v — next_v .

Уровень вершины v дерева T — длина простой цепи от root_T до v ; обозначается depth_v .

Способы представления графа

Матрица смежности для $G = \langle V, E \rangle$ — булева матрица V^2 , элементы которой равны логическому значению выражения:

$$\langle v, w \rangle \in E \mid v, w \in V$$

Матрица занимает $\mathcal{O}(V^2)$ места; проверка смежности проходит за $\mathcal{O}(1)$.

Список смежности для $G = \langle V, E \rangle$ — множество вершин $v \in V$, которым соответствует другое множество вершин:

$$\{w \in V \mid \langle v, w \rangle \in E\}$$

Список занимает $\mathcal{O}(|V| + |E|)$ места; проверка смежности проходит за $\mathcal{O}(\text{outdeg}(v))$.

Способы представления дерева

Массив родителей для $T = \langle V, E \rangle$ — массив вершин $v \in V$, которым соответствует их родитель.

Массив занимает $\mathcal{O}(|V|)$ места; вывод родителя и порядка дерева проходят за $\mathcal{O}(1)$.

«*Первый ребёнок, следующий родственник*» для $T = \langle V, E \rangle$ — такая упорядоченная пара массивов вершин $\langle F, N \rangle$, что

F — массив из первых детей для всех вершин;

N — массив из следующих родственников для всех вершин.

Массив занимает $\mathcal{O}(|V|)$ места; вывод первого ребёнка, следующего родственника и порядка дерева проходят за $\mathcal{O}(1)$.

Редактирование дерева

К **элементарным операциям** редактирования дерева относятся:

- *удаление* листового узла v с ребром $\langle \text{parent}_v, v \rangle$: $v \mapsto \lambda$;
- *вставка* листового узла v с ребром $\langle \text{parent}_v, v \rangle$: $\lambda \mapsto v$;
- *замещение* вершины v другой вершиной w : $v \mapsto w$.

Пусть $T_1 = \langle V_1, E_1 \rangle$, $T_2 = \langle V_2, E_2 \rangle$ — корневые деревья.

Трансформация T_1 в T_2 — упорядоченное биективное отображение $E \subseteq V_1 \cup \{\lambda\} \times V_2 \cup \{\lambda\}$.

Биективное *отображение* T_1 в T_2 — такое $M \subseteq W_1 \times W_2$

для $W_1 \subseteq V_1$, $W_2 \subseteq V_2$, что:

$$\begin{cases} \langle \text{root}_{T_1}, \text{root}_{T_2} \rangle \in M \neq \emptyset \\ \langle \text{parent}_v, \text{parent}_w \rangle \in M \iff \langle v, w \rangle \in M \\ v_2 = \text{next}_{v_1}, w_2 = \text{next}_{w_1} \iff \langle v_1, w_1 \rangle, \langle v_2, w_2 \rangle \in M \end{cases}$$

Лемма. Пусть M — отображение T_1 в T_2 . Тогда:

$$\forall \langle v, w \rangle \in M \text{ depth}_v = \text{depth}_w$$

Стоимость элементарной операции над T_1 и T_2 задаётся метрикой $\gamma: V_1 \cup V_2 \cup \{\lambda\} \times V_1 \cup V_2 \cup \{\lambda\} \rightarrow \mathbb{R}_0^+$.

Стоимость трансформации T_1 в T_2 (E) задаётся метрикой:

$$\gamma(E) = \sum_{\langle v, w \rangle \in E} \gamma(v, w)$$

Редакционная дистанция между T_1 и T_2 — функция:

$$\gamma_{\min} = \min(\{\gamma(E) \mid \forall E\})$$

Редакционный граф для T_1 и T_2 — неорграф $G = \langle V, E \rangle$ с вершинами вида vw , $v \in V_1 \cup \{v_0\}$, $w \in V_2 \cup \{w_0\}$ (v_0, w_0 — *мнимые узлы*), рёбра которого определяются по правилу:

$$\begin{cases} \text{depth}_{v_{i+1}} \geq \text{depth}_{w_{j+1}} \iff \langle v_i w_j, v_{i+1} w_j \rangle \in E \ (v_{i+1} \mapsto \lambda) \\ \text{depth}_{v_{i+1}} = \text{depth}_{w_{j+1}} \iff \langle v_i w_j, v_{i+1} w_{j+1} \rangle \in E \ (v_{i+1} \mapsto w_{j+1}) \\ \text{depth}_{v_{i+1}} \leq \text{depth}_{w_{j+1}} \iff \langle v_i w_j, v_i w_{j+1} \rangle \in E \ (\lambda \mapsto w_{j+1}) \end{cases}$$

Лемма. Пусть G — редакционный граф для T_1 и T_2 . Тогда маршрут P от $v_0 w_0$ до $v_{n_1} w_{n_2}$ задаёт трансформацию:

$$\begin{aligned} E = & \{ \langle v_{i+1}, \lambda \rangle \mid \langle v_i w_j, v_{i+1} w_j \rangle \in P \} \cup \dots \\ & \dots \{ \langle v_{i+1} w_{j+1} \rangle \mid \langle v_i w_j, v_{i+1} w_{j+1} \rangle \in P \} \cup \dots \\ & \dots \{ \langle \lambda, w_{j+1} \rangle \mid \langle v_i w_j, v_i w_{j+1} \rangle \in P \} \end{aligned}$$

Алгоритм редактирования дерева занимает $\mathcal{O}(n_1 n_2)$ места, используя $\mathcal{O}(n_1 n_2)$ времени.

Обход дерева

Обход дерева $T = \langle V, E \rangle$ — биективное отображение:

$$\text{order}: V \rightarrow \{1, \dots, |V|\}$$

Прямой называется такой обход дерева $T = \langle V, E \rangle$, что:

$$\begin{cases} \text{order}(\text{root}_T) = 1 \\ \text{order}(\text{first}_v) = \text{order}(v) + 1, \text{first}_v \neq \emptyset \\ \text{order}(\text{next}_v) = \text{order}(v) + \text{size}(v), \text{next}_v \neq \emptyset \end{cases}$$

Алгоритм прямого обхода дерева занимает линейное место, используя линейное время.

Поиск с возвратом

Поиск с возвратом — метод нахождения решений задачи полным перебором всех допустимых расстановок элементов конечного множества:

- в качестве *частичного решения* используется пустое упорядоченное множество M , которое расширяется до полного по одному элементу за операцию;
- если решение *полное* или *не удовлетворяет условию*, алгоритм приступает к другому частичному решению.

Пусть $T_1 = \langle V_1, E_1 \rangle$, $T_2 = \langle V_2, E_2 \rangle$ — корневые деревья.

Кандидат для $v \in V_1$ — элемент множества

$$C_v := \{w \mid w \in V_2, \text{depth}_v = \text{depth}_w\} \cup \{\lambda\}.$$

Возвратное дерево для T_1 и T_2 — такое дерево $T = \langle V, E \rangle$ с мнимым корнем, что:

$$\left\{ \begin{array}{l} M \subseteq V_1 \times W \text{ (упорядочено, биективно)} \\ W = [\text{root}_T, \dots, w] \setminus \{\text{root}_T\} \subseteq V_2 \cup \{\lambda\} \subseteq V \\ \text{children}_w = \emptyset \\ \forall \langle w_1, w_2 \rangle \subseteq W \text{ order}(w_1) < \text{order}(w_2) \\ w_1, w_2 \neq \lambda \\ \forall \langle v_i, w_j \rangle \in M \ w_j \in C_{v_i} \end{array} \right\} \begin{array}{l} \text{I} \\ \text{II} \\ \text{III} \end{array}$$

- I — всякая простая цепь возвратного дерева от корня до листа без корня соответствует *уникальному* отображению T_1 в T_2 ;
- II — индекс узлов одной простой цепи от корня до листа без корня *строго возрастает*;
- III — всякий узел простой цепи от корня до листа без корня является *кандидатом* для соответствующего узла T_1 .

Итерация построения полного решения M для условия P :

$$\begin{cases} \forall c \in C_{W.\text{last}()} \quad W := W \cup \{c\} \\ T(M) := M \text{ — частичное решение} \\ M \wedge P(M) \wedge T(M) \neq \emptyset \implies \text{расширить } M \\ M \wedge P(M) \wedge T(M) = \emptyset \implies \text{следующее } M \end{cases}$$

Дерево ветвей и границ для T_1 и T_2 — такое возвратное дерево для T_1 и T_2 , что $P := P \wedge R$, где:

$$R(M_i) = \begin{cases} \alpha_{\min} = \emptyset \implies \alpha_{\min} := \max \\ \alpha_{\min} \geq \gamma(M_i) \implies \text{True}, \alpha_{\min} := \gamma(M_i) \\ \alpha_{\min} < \gamma(M_i) \implies \text{False} \end{cases}$$

«Разделяй и властвуй»

«Разделяй и властвуй» — метод рекурсивного нахождения решений задачи:

- задача делится на меньшие, *независимые* друг от друга подзадачи, пока они не будут сведены к *тривиальным*;
- решения тривиальных подзадач *комбинируются* в единое к исходной задаче.

Пусть $T_1 = \langle V_1, E_1 \rangle$, $T_2 = \langle V_2, E_2 \rangle$ — корневые деревья, $A_1 = T_{1W_1}$, $A_2 = T_{2W_2}$, $B_1 = T_1 \setminus A_1$, $B_2 = T_2 \setminus A_2$ — их поддеревья:

$$\begin{cases} W_1 = \{v_m \in V_1 \mid \text{order}(v_m) < \text{order}(v)\} \\ W_2 = \{w_n \in V_2 \mid \text{order}(w_p) < \text{order}(w)\} \\ v := \text{last}_{v_i}, \quad w := \text{last}_{w_k} \end{cases}$$

Дерево «разделяй и властвуй» для T_1 и T_2 — такое ордерено $T = \langle V, E \rangle$ с вершинами вида $v_i v_j w_k w_l$, что:

$$\begin{cases} v_i, v_j \in V_1, \quad w_k, w_l \in V_2 \\ \text{root}_T = v_1 v_{n_1} w_1 w_{n_2} \quad (T_1 \rightarrow T_2) \end{cases}$$

Шаг рекурсивного построения решения M :

$$\begin{cases} v_i = v_j, \quad w_k = w_l \implies v_i \mapsto w_k, \text{ комбинировать} \\ v_i \neq v_j, \quad w_k = w_l \implies A_1 \rightarrow T_2 \quad (B_1 \rightarrow \lambda) \\ v_i = v_j, \quad w_k \neq w_l \implies T_1 \rightarrow A_2 \quad (\lambda \rightarrow B_2) \\ v_i \neq v_j, \quad w_k \neq w_l \implies \begin{cases} A_1 \rightarrow A_2 \text{ или } A_1 \rightarrow T_2 \\ B_1 \rightarrow B_2 \text{ или } T_1 \rightarrow A_2 \end{cases} \end{cases}$$

Динамическое программирование

Динамическое программирование — метод рекурсивного нахождения решений задачи:

- задача делится на меньшие, *зависимые* друг от друга подзадачи, пока они не будут сведены к *тривиальным*;
- решения тривиальных подзадач *комбинируются* в единое к исходной задаче.

Мемоизация («сверху вниз») — кеширование и повторное использование ранее подсчитанных результатов.

Табуляция («снизу вверх») — заполнение кеша на основе тривиальных подзадач.

Лучшее решение выбирается из матрицы лучших решений его подграфов (*у них по рекурсии есть свои матрицы*):

$$\begin{array}{cccc} \langle v_i, w_k \rangle & \langle v_i, w_k w_{k+1} \rangle & \cdots & \langle v_i, w_k \dots w_l \rangle \\ \langle v_i v_{i+1}, w_k \rangle & \langle v_i v_{i+1}, w_k w_{k+1} \rangle & \cdots & \langle v_i v_{i+1}, w_k \dots w_l \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle v_i \dots v_j, w_k \rangle & \langle v_i \dots v_j, w_k w_{k+1} \rangle & \cdots & \langle v_i \dots v_j, w_k \dots w_l \rangle \end{array}$$

$$\left\{ \begin{array}{l} v \in V_1, w \in V_2 \\ \text{depth}_v = \text{depth}_w \\ \{v_i, \dots, v_j\} = \text{children}_v \\ \{w_k, \dots, w_l\} = \text{children}_w \\ \langle v_i \dots v_j, w_k \dots w_l \rangle \sim \gamma_{\min}(G_1 \rightarrow G_2) \\ G_1 = T_{1w_i} \cup \dots \cup T_{1w_j} \\ G_2 = T_{2w_k} \cup \dots \cup T_{2w_l} \\ \forall s \in \{i, \dots, j\} \text{ root}_{T_{1w_s}} = v_s \\ \forall t \in \{k, \dots, l\} \text{ root}_{T_{2w_t}} = w_t \end{array} \right.$$

Алгоритм табуляции занимает $\mathcal{O}(n_1 n_2)$ места, используя $\mathcal{O}(n_1 n_2)$ времени.

Теория алгоритмов

Динамическое программирование

Динамическое программирование — метод решения задач на оптимизацию *по принципу оптимальности*:

«оптимальная структура имеет оптимальные подструктуры» (*Р. Беллман*)

Уравнение Беллмана

Введём задачу на оптимизацию вида:

d — выбор;
 $\text{opt}_{d \in \Delta} \{H(d)\}$ Δ — допустимое множество;
 H — целевая функция одной переменной.

Оптимум — оптимальное значение целевой функции
(выбор d^* оптимизирует H):

$$H^* := H(d^*) \quad d^* := \arg \text{opt}_{d \in \Delta} \{H(d)\}$$

Пусть H — целевая функция нескольких переменных.

Оптимум такой задачи можно найти либо *полным перебором*, либо *последовательным принятием решений*:

$$\begin{aligned} H^* &= \text{opt}_{\langle d_1, \dots, d_n \rangle \in \Delta} \{H(d_1, \dots, d_n)\} \\ &= \text{opt}_{d_1 \in D_1} \{ \text{opt}_{d_2 \in D_2} \{ \dots \{ \text{opt}_{d_n \in D_n} \{h(d_1, \dots, d_n)\} \} \dots \} \} \\ &= \text{opt}_{d_1 \in D_1} \{H(d_1, d_2^*(d_1), \dots, d_n^*(d_1))\} \end{aligned}$$

$\Delta = D_1 \times \dots \times D_n$ — пространство решений;

$D_n(d_1, \dots, d_{n-1})$ — множество решений, которое зависит от предыдущих $\langle d_1, \dots, d_{n-1} \rangle$ решений;

$d_i^*(d_1, \dots, d_{i-1})$ — локальный выбор d , оптимизирующий H .

Распределение ресурсов

В задаче на *оптимальное распределение ресурсов* требуется разделить ограниченное число ресурсов на множество их

потребителей, у которых есть стоимость.

Общая формула:

$$f(k, m) = \min_{d \in \{0, \dots, m\}} \{C(k, d) + f(k + 1, m - d)\}$$

Теория множеств

Открытое множество

ε -окрестность точки $x_0 \in X$ метрического пространства $\langle X, d \rangle$ — такое множество точек $x \in X$, что $d(x_0, x) < \varepsilon$.

Упрощённая запись $\{x \mid d(x_0, x) < \varepsilon\} =: U_\varepsilon(x_0)$.

Особые случаи:

$$U_\varepsilon(+\infty) := (1/\varepsilon; +\infty)$$

$$U_\varepsilon(-\infty) := (-\infty; -1/\varepsilon)$$

Проколотой называется ε -окрестность точки x_0 без неё:

$$\overset{\circ}{U}_\varepsilon(x_0) := U_\varepsilon(x_0) \setminus \{x_0\}$$

Правосторонней (левосторонней) называется ε -окрестность точки x_0 без левой (правой) половины:

$$U_{\varepsilon+}(x_0) := [x_0; \varepsilon) \quad U_{\varepsilon-}(x_0) := (\varepsilon; x_0]$$

Ограниченное множество

Множество M ограничено *сверху*, если

$$\forall m \in M \exists C \in \mathbb{R} : m \leq C.$$

Точной (минимальной, англ. *supremum*) называется такая *верхняя* граница множества M — $\sup M$, что

$$\forall \varepsilon > 0 \exists m \in M : m \in U_{\varepsilon-}(\sup M).$$

Множество M ограничено *снизу*, если

$$\forall m \in M \exists C \in \mathbb{R} : m \geq C.$$

Точной (максимальной, англ. *infimum*) называется такая *нижняя* граница множества M — $\inf M$, что

$$\forall \varepsilon > 0 \exists m \in M : m \in U_{\varepsilon+}(\inf M).$$

Принцип Кантора

Последовательность вложенных отрезков содержит точки ξ , которые принадлежат им всем:

$$\forall n \in \mathbb{N} \exists \xi \in [a_n; b_n] \subset [a_{n-1}; b_{n-1}]$$

Если $n \rightarrow \infty$, $(b_n - a_n) \rightarrow 0$, то ξ единственна:

$$\lim_{n \rightarrow \infty} a_n = \sup\{a_n\} = \lim_{n \rightarrow \infty} b_n = \inf\{b_n\} = \xi$$

Доказательство. По теореме Вейерштрасса:

$$\lim_{n \rightarrow \infty} a_n = \sup\{a_n\} \quad \lim_{n \rightarrow \infty} b_n = \inf\{b_n\}$$

Значит, $\forall (n \in \mathbb{N}, \xi \in [\sup\{a_n\}; \inf\{b_n\}]) \xi \in [a_n; b_n]$. \square

Если $\inf\{b_n\} = \sup\{a_n\}$, то ξ единственна:

$$0 = \inf\{b_n\} - \sup\{a_n\} = \lim_{n \rightarrow \infty} b_n - \lim_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} (b_n - a_n) \blacksquare$$

Локальный экстремум

Локальный максимум функции f — такая точка x_0 , что

$$\exists \delta > 0: \sup U_\delta(x_0) = f(x_0).$$

Локальный минимум функции f — такая точка x_0 , что

$$\exists \delta > 0: \inf U_\delta(x_0) = f(x_0).$$

Их объединяют в точки *локального экстремума*.

Критической называется такая точка x_0 , что

$$\begin{cases} f'(x_0) = 0 \text{ (стационарна)} \\ f'(x_0) = \text{undefined} \end{cases}$$

Комбинаторика

Принципы подсчёта

Правило сложения. Пусть S — конечное множество, образованное объединением подмножеств S_1, \dots, S_k . Тогда:

$$|S| = |S_1| + \dots + |S_k|$$

Правило умножения. Пусть S — конечное множество, которое есть декартово произведение $S_1 \times \dots \times S_k$. Тогда:

$$|S| = |S_1| \times \dots \times |S_k|$$

Правило вычитания. Пусть S — подмножество конечного множества T , \bar{S} — его комплемент. Тогда:

$$|S| = |T| - |\bar{S}|$$

Принцип Дирихле. Пусть S_1, \dots, S_m — конечные непересекающиеся множества, причём:

$$|S_1| + \dots + |S_m| = n$$

Тогда существуют такие $i, j \in [1; m] \cap \mathbb{N}$, что:

$$|S_i| \geq \left\lceil \frac{n}{m} \right\rceil \quad |S_j| \leq \left\lfloor \frac{n}{m} \right\rfloor$$

Основные понятия

Пусть X — конечное множество, $n := |X|$, $[m] := [1; m] \cap \mathbb{N}$.

Упорядоченное разбиение m элементов из X — соответствие

$$s: [m] \rightarrow X.$$

Неупорядоченное разбиение m элементов из X — множество S мощностью m с элементами из X .

Перестановка — упорядоченное биективное разбиение:

$$P_n: [n] \rightarrow X, \quad P_n = n!$$

k-Размещение — упорядоченное инъективное разбиение:

$$A_n^k: [k] \rightarrow X, \quad A_n^k = \frac{P_n}{P_{n-k}}$$

k -Сочетание — неупорядоченное инъективное разбиение:

$$C_n^k: [k] \rightarrow X, \quad C_n^k = \frac{A_n^k}{P_k}, \quad C_n^k \equiv \binom{n}{k}$$

Полиномиальная теорема

Полиномиальными называются коэффициенты $\binom{n}{k_1, \dots, k_r}$ многочлена при $k_1, \dots, k_r \in \mathbb{N}_0$:

$$(x_1 + \dots + x_r)^n = \sum_{\substack{k_1, \dots, k_r \geq 0 \\ k_1 + \dots + k_r = n}} \binom{n}{k_1, \dots, k_r} x_1^{k_1} \dots x_r^{k_r}$$

Теорема. Для $k_1, \dots, k_r \geq 0$ с $k_1 + \dots + k_r = n$ справедливо:

$$\begin{aligned} \binom{n}{k_1, \dots, k_r} &= \binom{n}{k_1} \binom{n - k_1}{k_2} \dots \binom{n - k_1 - \dots - k_{r-1}}{k_r} \\ &= \frac{n!}{k_1! \cdot \dots \cdot k_r!} \end{aligned}$$

Доказательство. Раскроем скобки:

$$(x_1 + \dots + x_r)^n = \sum_{i_1=1}^r \dots \sum_{i_n=1}^r x_{i_1} \dots x_{i_n}$$

Одночлен $x_1 \dots x_r$ равен $x_1^{k_1} \dots x_r^{k_r}$, если среди индексов i_1, \dots, i_n ровно k_j равны $j \in [1; r] \cap \mathbb{Z}$.

Выбор k_j индексов происходит среди $n - k_1 - \dots - k_{j-1}$ оставшихся. Поэтому таких упорядоченных выборов $\binom{n - k_1 - \dots - k_{j-1}}{k_j}$:

$$\binom{n}{k_1, \dots, k_r} = \binom{n}{k_1} \binom{n - k_1}{k_2} \dots \binom{n - k_1 - \dots - k_{r-1}}{k_r} \quad \square$$

По формуле сочетаний:

$$\begin{aligned} & \frac{n!}{k_1! \cancel{(n - k_1)!}} \cdot \frac{\cancel{(n - k_1)!}}{k_2! \cancel{(n - k_1 - k_2)!}} \cdot \dots \cdot \frac{\cancel{(n - k_1 - \dots - k_{r-1})!}}{k_r! (n - k_1 - \dots - k_r)} \\ &= \frac{n!}{k_1! \cdot \dots \cdot k_r! \cdot 0!} = \frac{n!}{k_1! \cdot \dots \cdot k_r!} \quad \blacksquare \end{aligned}$$

Формула Паскаля

Для $n \geq 1$ и $0 \leq k \leq n$ справедливо:

$$\binom{n}{k_1, \dots, k_r} = \sum_{i=1}^r \binom{n-1}{k_1, \dots, k_i-1, \dots, k_r}$$

Доказательство. Раскроем скобки:

$$(x_1 + \dots + x_r)^n = \sum_{\substack{k_1, \dots, k_r \\ k_1 + \dots + k_r = n}} \binom{n}{k_1, \dots, k_r} x_1^{k_1} \dots x_r^{k_r}$$

Раскроем скобки иначе:

$$\begin{aligned} (x_1 + \dots + x_r)^n &= (x_1 + \dots + x_r) (x_1 + \dots + x_r)^{n-1} \\ &= (x_1 + \dots + x_r) \cdot \sum_{\substack{k'_1, \dots, k'_r \\ k'_1 + \dots + k'_r = n-1}} \binom{n-1}{k'_1, \dots, k'_r} x_1^{k'_1} \dots x_r^{k'_r} \\ &= \sum_{i=1}^r \sum_{\substack{k'_1, \dots, k'_r \\ k'_1 + \dots + k'_r = n-1}} \binom{n-1}{k'_1, \dots, k'_r} x_1^{k'_1} \dots x_i^{k'_i+1} \dots x_r^{k'_r} \end{aligned}$$

Произведём замену индексов $k_i := k'_i + 1$, $k_j := k'_j$ ($i \neq j$):

$$\begin{aligned} (x_1 + \dots + x_r)^n &= \\ \sum_{\substack{k_1, \dots, k_r \\ k_1 + \dots + k_r = n}} \sum_{i=1}^r \binom{n-1}{k_1, \dots, k_i-1, \dots, k_r} x_1^{k_1} \dots x_r^{k_r} \blacksquare \end{aligned}$$

Принцип включения-исключения

Пусть A_1, \dots, A_n — конечные множества. Тогда верно:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k+1} \left| \bigcap_{j=1}^k A_j \right|$$

Доказательство. Пусть $x \in \bigcup_i^n A_i$, причём x содержится в k множествах A_1, \dots, A_k .

Левая часть формулы — 1. Докажем, что правая часть тоже:

$\binom{k}{1}$ раз x встречается во множествах мощностью 1;

...

$\binom{k}{k}$ раз x встречается во множествах мощностью k .

Подставляем биномиальные коэффициенты в формулу:

$$\binom{k}{1} - \binom{k}{2} + \dots + (-1)^{k+1} \binom{k}{k} = \sum_{i=1}^k \binom{k}{i} (-1)^{i+1}$$

По определению биномиальных коэффициентов:

$$\sum_{i=1}^k \binom{k}{i} (-1)^{i+1} = \binom{k}{0} - \sum_{i=0}^k (-1)^i 1^{k-i} = \binom{k}{0} - (1-1)^k = 1 \blacksquare$$

Правило биекции

Пусть $f: X \rightarrow Y$ — биективное соответствие, где X, Y — конечные множества. Тогда:

$$|X| = |Y|$$

Задача. Сколько подмножеств имеет n -множество?

Решение. Пусть Y — n -множество.

Пусть $\overline{x_1 \dots x_n}$ — бинарная n -строка, где x_i указывает на наличие i -го элемента в произвольном множестве $\mathcal{P}(Y)$.

Пусть $f: X \rightarrow \mathcal{P}(Y)$ — соответствие, где X — множество всех возможных бинарных n -строк. Очевидно, что:

$$f \text{ — биекция} \implies |Y| = |X|$$

По правилу умножения:

$$|X| = 2^n \implies |\mathcal{P}(Y)| = 2^n$$

Ответ: $|\mathcal{P}(Y)| = 2^n$.

Биномиальные коэффициенты

Свойство 1. Для $n \in \mathbb{N}$ и $r \in [0; n] \cap \mathbb{Z}$ верно:

$$\binom{n}{r} = \binom{n}{n-r}$$

Доказательство. Пусть A — n -множество, из которого нужно выбрать B — r -подмножество.

По определению биномиальных коэффициентов:

$$\text{число неупорядоченных} \\ \text{выборок } B = \binom{n}{r}$$

С другой стороны, рассмотрим комплемент $A \setminus B$:

$$\text{число неупорядоченных} \\ \text{выборок } A \setminus B = \binom{n}{n-r}$$

Пусть $f: A_1 \rightarrow A_2$ — биективное соответствие, $A_1 = A_2 = A$.

Любой элемент $x \in B \subset A_1$ можно сопоставить $x \in A \setminus B \subset A_2$.
Значит, числа таких сопоставлений равны:

$$\binom{n}{r} = \binom{n}{n-r} \blacksquare$$

Свойство 2. Для $n \in \mathbb{N}$ верно:

$$\sum_{r=0}^n \binom{n}{r} = 2^n$$

Доказательство. Пусть A — n -множество, для которого посчитаем $|\mathcal{P}(A)|$.

С одной стороны, $|\mathcal{P}(A)| = 2^n$ по доказанному.

С другой стороны, посчитаем $|\mathcal{P}(A)|$ через биномиальные коэффициенты: есть $\binom{n}{r}$ способов выбрать r -подмножество.

По правилу сложения:

$$|\mathcal{P}(A)| = \sum_{r=0}^n \binom{n}{r} \Rightarrow \sum_{r=0}^n \binom{n}{r} = 2^n \blacksquare$$

Метод шаров и перегородок

Число способов составить r -мультимножество из n -множества равно:

$$\left(\left(\begin{matrix} n \\ r \end{matrix}\right)\right) := \binom{n+r-1}{r} = \left(\left(\begin{matrix} n \\ k-1 \end{matrix}\right)\right) + \left(\left(\begin{matrix} n-1 \\ k \end{matrix}\right)\right)$$

Доказательство. Для подсчёта числа всех возможных r -мультимножеств введём $n-1$ *перегородок* — считается, что элементы между двумя соседними перегородками равны.

Таким образом, число способов заполнить $n+r-1$ позиций с выбором r шаров (или *вставкой $n-1$ перегородок*) равно:

$$\binom{n+r-1}{r} \square$$

По формуле Паскаля:

$$\begin{aligned} \left(\left(\begin{matrix} n \\ k-1 \end{matrix}\right)\right) + \left(\left(\begin{matrix} n-1 \\ k \end{matrix}\right)\right) &= \binom{n+k-2}{k-1} + \binom{n+k-2}{k} \\ &= \binom{n+k-1}{k} \blacksquare \end{aligned}$$

Задача. Посчитать число неотрицательных целых решений

$$3x_1 + 3x_2 + 3x_3 + 7x_4 = 22.$$

Решение. Методом полного перебора, $x_4 \in \{0, 1, 2, 3\}$.

По методу шаров и перегородок:

$$\begin{aligned} \left[\begin{array}{l} x_4 = 0 \Rightarrow 3(x_1 + x_2 + x_3) = 22 \Leftrightarrow \text{решений нет} \\ x_4 = 1 \Rightarrow 3(x_1 + x_2 + x_3) = 15 \Leftrightarrow x_1 + x_2 + x_3 = 5 \\ x_4 = 2 \Rightarrow 3(x_1 + x_2 + x_3) = 8 \Leftrightarrow \text{решений нет} \\ x_4 = 3 \Rightarrow 3(x_1 + x_2 + x_3) = 1 \Leftrightarrow \text{решений нет} \end{array} \right. \\ \Leftrightarrow \left(\left(\begin{matrix} 3 \\ 5 \end{matrix}\right)\right) = \binom{7}{5} = 21 \end{aligned}$$

Ответ: 21 решение.

Правило деления

Пусть $f: X \rightarrow Y$ — отображение k -к-одному, где X, Y — конечные множества. Тогда:

$$|X| = k |Y|$$

Задача. Сколько существует рассадок 4 рыцарей вокруг стола? Две рассадки эквивалентны, если одну можно получить из другой поворотом.

Решение. Пусть $A = \{x_1, x_2, x_3, x_4\}$ — множество рыцарей, X — множество 4-строк вида $x_j \dots x_k$, $1 \leq j, k \leq 4$, $i \neq j$.

Пусть $f: X \rightarrow Y$ — соответствие, где Y — множество всех возможных рассадок для A . Очевидно, что:

$$f \text{ — } n\text{-к-одному} \implies k |Y| = |X| \iff |Y| = |X| / k$$

По правилу умножения:

$$|X| = 4 \cdot 3 \cdot 2 \cdot 1 = P_4 = 24 \implies |Y| = 24/4 = 6$$

Ответ: $|Y| = 6$.

Число Стирлинга

Число Стирлинга второго порядка — количество способов разбить n -множество на k подмножеств:

$$C(n, k) \equiv \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = k \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\} + \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\}$$

Частные случаи:

$$\left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} = 0 \quad \left\{ \begin{matrix} n \\ 1 \end{matrix} \right\} = 1 \quad \left\{ \begin{matrix} n \\ n \end{matrix} \right\} = 1 \quad \left\{ \begin{matrix} n \\ n-1 \end{matrix} \right\} = \binom{n}{2}$$

Доказательство. Скоро... наверное.