Элементарная алгебра

Виды выражений

Одночлен *(моном)* — произведение переменных и коэффициентов.

Многочлен *(полином)* — сумма одночленов.

Двучлен *(бином)* — многочлен из двух одночленов.

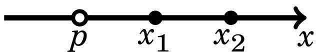
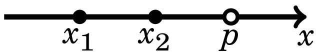
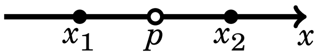
Трёхчлен *(трином)* — многочлен из трёх одночленов.

Многочлен P от одной переменной x можно представить так:

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

Квадратный трёхчлен

Расположение корней относительно числа p:

Расположение корней	Равносильно
	$\begin{cases} D > 0 \\ af(p) > 0 \\ p < x_0 \end{cases}$
	$\begin{cases} D > 0 \\ af(p) > 0 \\ x_0 < p \end{cases}$
	$af(p) < 0$

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 m знак неравенства *инвертируется*:

$$a < b \iff am > bm$$

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 $n = 2$:

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

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 $f : \mathbb{R} \to \mathbb{R}_0^+$, 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*:

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

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

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

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

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

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

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

Функция знака

Функция знака *(сигнум-функция)* — нечётная функция $\operatorname{sgn}\colon \mathbb{R} \to \{-1; 0; 1\}$, 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:

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

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:

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

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

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

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

Функция натурального логарифма

Функция натурального логарифма — значение интеграла:

$$\ln x = \int_1^x \frac{\mathrm{d}t}{t}, \quad \ln\colon \mathbb{R}^+ \to \mathbb{R}$$

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:

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

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:

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

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

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

---

* 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

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

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 $lcm(\{a_k\})$, что

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

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

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, $ab/(a,b) \le [a,b]$. 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:

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

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

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 знакочередующаяся 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.

Допустим, это не так. Тогда:

$$ar_k \equiv ar_l \implies r_k \equiv r_l$$

Но $r_k \not\equiv r_l \implies ar_k \not\equiv ar_l$ $\square$

Φ и Φ_a конгруэнтны.

Пусть $ar_k \equiv r_l,\ r_l \in \mathbf{Z}_m$.

Так как $m \nmid ar_k$, то:

$$r_l \in \Phi \implies \Phi \equiv \Phi_a \ \square$$

Перемножим элементы множеств Φ и Φ_a:

$$r_0 r_1 \dots r_{\phi(m)} \equiv ar_0 ar_1 \dots ar_{\phi(m)} \implies$$
$$r_0 r_1 \dots r_{\phi(m)} \equiv a^{\phi(m)} r_0 r_1 \dots r_{\phi(m)} \implies a^{\phi(m)} \equiv 1 \ \blacksquare$$

> **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 $a^b \equiv a^{b \bmod \phi(m)}$. $\blacksquare$

Алгоритм Евклида

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

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

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

$$+\begin{cases} a - b \equiv 0 \pmod{m} \\ b \equiv 0 \pmod{m} \end{cases} \implies \begin{cases} a \equiv 0 \pmod{m} \\ b \equiv 0 \pmod{m} \end{cases}$$

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:

$$\begin{cases} \dfrac{a}{b} + \dfrac{c}{d} \equiv \dfrac{ad + bc}{cd} \pmod{m} \\ \dfrac{a}{b} \times \dfrac{c}{d} \equiv \dfrac{ac}{bd} \pmod{m} \\ \dfrac{eg}{fg} \equiv \dfrac{e}{f} \pmod{m} \end{cases}$$

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:

$$\begin{aligned} 4x &\equiv 4 \pmod 6 \ \mid \cdot 1/2 \\ 2x &\equiv 2 \pmod 3 \end{aligned}$$

Применим *алгоритм Евклида* в алгебраическом виде:

«Прямой» алгоритм:

$$\begin{aligned} 3 &= 2 \cdot 1 + 1 \\ 2 &= \mathbf{1} \cdot 2 + 0 \end{aligned}$$

«Обратный» алгоритм:

$$\begin{aligned} 1 &= 3 \cdot \mathbf{1} + 2 \cdot (\mathbf{-1}) \mid \cdot 2 \\ 2 &= 3 \cdot \mathbf{2} + 2 \cdot (\mathbf{-2}) \end{aligned}$$

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

Ответ: $x = -2$.

Китайская теорема об остатках

Сравнения можно объединять в *систему*:

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

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 $(m_1, m_2) \mid (a_1 - a_2)$. □

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, $m_i \mid x - y \implies [m_1, \dots, m_n] \mid x - y \iff x \equiv y \pmod{[m_1, \dots, m_n]}$. ■

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:

$$\begin{cases} x \equiv 2 & \pmod{3} \\ x \equiv 2 & \pmod{4} \\ 2x \equiv -3 & \pmod{5} \end{cases}$$

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:

$$\forall i_1, i_2 \in [1; r],\ i_1 \neq i_2\ (p_{i1}^{\alpha_{i1}}, p_{i2}^{\alpha_{i2}}) = 1 \implies$$

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

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:

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

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

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

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*:

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

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

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

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

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

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

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

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

$$\mathrm{tg}\colon \mathbb{R}\backslash\{\pi/2 + \pi n \mid n \in \mathbb{Z}\} \xrightarrow{\alpha \mapsto y/x} \mathbb{R}$$

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

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

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

$$\mathrm{ctg}\colon \mathbb{R}\backslash\{\pi n \mid n \in \mathbb{Z}\} \xrightarrow{\alpha \mapsto x/y} \mathbb{R}$$

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

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

Основные тождества

Из определений тригонометрических функций следует:

$$\sin^2\alpha + \cos^2\alpha = 1 \qquad \arccos x = \arcsin(\sqrt{1-x^2})$$

$$1+\operatorname{tg}^2\alpha = 1/\cos^2\alpha \qquad \arccos x = (\sqrt{1-x^2}/x)$$

$$1+\operatorname{ctg}^2\alpha = 1/\sin^2\alpha \qquad \arcsin y = \operatorname{arcctg}(\sqrt{1-y^2}/y)$$

Сумма и разность двух углов

Из скалярного произведения векторов следует:

$$\cos(\alpha\pm\beta) = \cos\alpha\cos\beta \mp \sin\alpha\sin\beta$$

$$\sin(\alpha\pm\beta) = \sin\alpha\cos\beta \pm \sin\beta\cos\alpha$$

$$\operatorname{tg}(\alpha\pm\beta) = \frac{\operatorname{tg}\alpha \pm \operatorname{tg}\beta}{1\mp\operatorname{tg}\alpha\operatorname{tg}\beta} \qquad \operatorname{ctg}(\alpha\pm\beta) = \frac{\operatorname{ctg}\alpha\operatorname{ctg}\beta \mp 1}{\operatorname{ctg}\alpha \pm \operatorname{ctg}\beta}$$

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

Рассмотрим их скалярное произведение:

$$+\begin{cases}\vec{A}\cdot\vec{B} = \cos\alpha\cos\beta + \sin\alpha\sin\beta\\ \vec{A}\cdot\vec{B} = \|\vec{A}\|\,\|\vec{B}\|\cos(\alpha-\beta) = \cos(\alpha-\beta)\end{cases} \implies$$

$$\cos(\alpha-\beta) = \cos\alpha\cos\beta + \sin\alpha\sin\beta \;\square$$

Затем полезно применить эти четыре формулы:

$$\alpha+\beta = \alpha-(-\beta)$$

$$\sin(\alpha-\beta) = \cos((\pi/2-\alpha)+\beta)$$

$$\operatorname{tg}\alpha = \sin\alpha/\cos\alpha \qquad \operatorname{ctg}\alpha = \cos\alpha/\sin\alpha \;\blacksquare$$

Двойной угол

Из формул суммы и разности двух углов следует:

$$\cos 2\alpha = \cos^2\alpha - \sin^2\alpha \qquad \sin 2\alpha = 2\sin\alpha\cos\alpha$$

$$\operatorname{tg}2\alpha = \frac{2\operatorname{tg}\alpha}{1-\operatorname{tg}^2\alpha} \qquad \operatorname{ctg}2\alpha = \frac{\operatorname{ctg}^2\alpha - 1}{2\operatorname{ctg}\alpha}$$

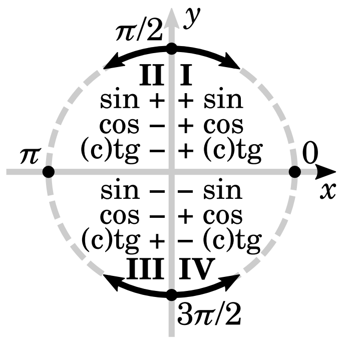
$$(\sin\alpha \pm \cos\alpha)^2 = 1 \pm \sin 2\alpha$$

Формулы приведения

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

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

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



Следствие. Для обратных функций верно:

$$\arcsin x + \arccos x = \pi/2 \qquad \arccos x + \arccos(-x) = \pi$$

$$\operatorname{arctg} x + \operatorname{arcctg} x = \pi/2 \qquad \operatorname{arcctg} x + \operatorname{arcctg}(-x) = \pi$$

Формулы понижения степени

Из формул двойного угла и основного тригонометрического тождества следует:

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

$$\sin^2\frac{\alpha}{2} = \frac{1-\cos\alpha}{2} \qquad \operatorname{ctg}^2\frac{\alpha}{2} = \frac{1-\cos\alpha}{\cos\alpha + 1}$$

Из них легко выводятся формулы *половинного угла*.

Сумма и разность двух функций

Из формул суммы и разности двух углов следует:

$$\sin\alpha \pm \sin\beta = 2\sin\frac{\alpha\pm\beta}{2}\cos\frac{\alpha\mp\beta}{2}$$

$$\cos\alpha + \cos\beta = 2\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2}$$

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

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

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,

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

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:

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

Случай с косинусом доказывается аналогично. $\blacksquare$

Подстановка Вейерштрасса

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

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

Доказательство. Распишем каждую функцию:

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

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

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:

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

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

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

Ограниченное множество

Множество M ограничено *сверху*, если

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

Точной *(минимальной*, англ. *supretumit)* 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 $n \to \infty$, $(b_n - a_n) \to 0$, то ξ единственна:

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

Доказательство. По теореме Вейерштрасса:

$$\lim_{n\to\infty} a_n = \sup\{a_n\} \qquad \lim_{n\to\infty} b_n = \inf\{b_n\}$$

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:

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

Локальный экстремум

Локальный **максимум** функции f — такая точка x_0, что

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

Локальный **минимум** функции f — такая точка x_0, что

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

Их объединяют в точки *локального* **экстремума**.

Критической называется такая точка x_0, что

$$\left[\begin{array}{l} f'(x_0) = 0 \ \textit{(стационарна)} \\ f'(x_0) = \text{undefined} \end{array}\right.$$

Алгебра логики

Определение

Алгебра логики — алгебраическая структура, которая образована двухэлементным множеством $\{0; 1\}$.

Высказывание — повествовательное предложение, о котором можно сказать в данный момент, что оно *истинно* или *ложно*.

Логическая связка — операция алгебры логики:

1) *Инверсия* «$\neg$» — логическое *«не»*.
2) *Конъюнкция* «$\wedge$» — логическое *«и»*.
3) *Дизъюнкция* «$\vee$» — логическое *«или»*.
4) *Строгая дизъюнкция* «$\dot{\vee}$» — логическое *«искл. или»*.
5) *Импликация* «$\rightarrow$» — логическое « $\Longrightarrow$ ».
6) *Эквиваленция* «$\equiv$» — логическое « $\Longleftrightarrow$ ».

Свойства

Конъюнкция и дизъюнкция *коммутативны*, *ассоциативны* и *дистрибутивны* относительно друг друга.

> **Идемпотентность.**
>
> $$A \wedge A = A \qquad A \vee A = A$$

> **Закон противоречия** и **исключённого третьего.**
>
> $$A \wedge \overline{A} = 0 \qquad A \vee \overline{A} = 1$$

> **Закон поглощения.**
>
> $$A \wedge 1 = A \qquad A \wedge 0 = 0$$
> $$A \vee 1 = 1 \qquad A \vee 0 = A$$

> **Закон де Мо́ргана.**
>
> $$\overline{A \wedge B} = \overline{A} \vee \overline{B} \qquad \overline{A \vee B} = \overline{A} \wedge \overline{B}$$

Нормальная форма

Терм — компонент логической функции:

— **макстерм** — переменные прямой и инверсной форм связаны *дизъюнкцией*;
— **минтерм** — переменные прямой и инверсной форм связаны *конъюнкцией*;

Ранг *терма* — число переменных, которые в него входят.

Нормальная дизъюнктивная форма *(DNF)* — дизъюнкция минтермов любого ранга.

Нормальная конъюнктивная форма *(CNF)* — конъюнкция макстермов любого ранга:

$$A \dot{\vee} B = (A \vee B) \wedge (\overline{A} \vee \overline{B})$$
$$A \equiv B = (\overline{A} \vee B) \wedge (A \vee \overline{B})$$

$$A \to B = \overline{A} \vee B$$

Нормальная импликативная форма *(INF)* — конъюнкция макстермов любого ранга, которые заменены импликацией:

$$A \vee B = (\overline{A} \to B) \wedge (\overline{B} \to A)$$

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 $f: X \to Y$, $g: Y \to Z$ существует $h: X \to Z$, 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 $f: X \to Y$ на $S \subseteq D_f$ называется такое $f|_S: S \to Y$, 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 $d: M \times M \to R_0^+$, 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*;
— $d(x,y) \le d(x,z) + d(y,z)$ — *«неравенство треугольника»*.

Алгебраическая операция

Отображение $*: X^n \to X$ 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 $y\colon X \to Y$ и $x\colon Y \to X$ — отображения, то y *инъективно*, а x *сюръективно*.

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

Так как g функционально, то

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

то есть f *инъективно*. □

Когда X накладывается на себя, то

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

то есть g *сюръективно*. ■

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 $\widehat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$:

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

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

Комплексные числа

Система комплéксных 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 $(a \equiv \Re e\ z)$;
Ob — мнимая ось $(b \equiv \Im m\ z)$.

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 $z \in \mathbb{C}$ —

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

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

Сопряжение — операция смены знака мнимой части z:

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

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 $|z_1z_2|=||z_1|\cdot|z_2||$ и аргументом $\arg(z_1z_2)=\arg z_1+\arg z_2$.

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

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

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 $z=r(\cos\phi+i\sin\phi)$:

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

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:

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

Значит,

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

Длина отрезка

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

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

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 $A\langle a\rangle$, $B=\langle b\rangle$, $a=x_1+y_1i$, $b=x_2+y_2i$. Тогда:

$$a\bar{b}+\bar{a}b = (x_1+y_1i)(x_2-y_2i)+(x_1-y_1i)(x_2+y_2i) =$$

$$2(x_1x_2+y_1y_2) = 2\overrightarrow{OA}\cdot\overrightarrow{OB} \;\blacksquare$$

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:

$$2\overrightarrow{AB}\cdot\overrightarrow{CD} = 2(\overrightarrow{OB}-\overrightarrow{OA})(\overrightarrow{OD}-\overrightarrow{OC}) =$$

$$2(\overrightarrow{OB}\cdot\overrightarrow{OD}-\overrightarrow{OB}\cdot\overrightarrow{OC}-\overrightarrow{OA}\cdot\overrightarrow{OD}+\overrightarrow{OA}\cdot\overrightarrow{OC}) =$$

$$\cancel{2}\cdot\frac{1}{\cancel{2}}(b\bar{d}+\bar{b}d-b\bar{c}-\bar{b}c-a\bar{d}-\bar{a}d+a\bar{c}+\bar{a}c) =$$

$$(a-b)(\bar{c}-\bar{d})+(\bar{a}-\bar{b})(c-d) \;\blacksquare$$

Коллинеарность

Коллинеарными называются:

— *точки*, которые лежат на одной прямой;

— *векторы*, которые лежат на одной прямой или на параллельных прямых.

> *Критерий коллинеарности* точек A, B с O:
> $$\frac{a}{b} = \overline{\left(\frac{a}{b}\right)} \quad \text{или} \quad \left[\begin{aligned} a &= 0 \\ b &= 0 \end{aligned}\right.$$

Доказательство. Очевидно, что:

$$\left[\begin{aligned} \arg a - \arg b &= 0 \\ \arg a - \arg b &= \pm\pi \end{aligned}\right. \implies \arg\frac{a}{b} = 0; \pm\pi$$

По определению аргумента комплексного числа:

$$\frac{a}{b} \text{ — действительное число} \implies \frac{a}{b} = \overline{\left(\frac{a}{b}\right)} \blacksquare$$

> *Критерий коллинеарности* векторов $\overrightarrow{AB}$, $\overrightarrow{CD}$:
> $$\frac{b-a}{d-c} = \overline{\left(\frac{b-a}{d-c}\right)} \quad \text{или} \quad \left[\begin{aligned} \overrightarrow{AB} &= \vec{0} \\ \overrightarrow{CD} &= \vec{0} \end{aligned}\right.$$

Доказательство. По определению комплексных чисел:

$$\overrightarrow{AB} \sim b - a, \; \overrightarrow{CD} \sim d - c$$

По критерию коллинеарности двух точек с O:

$$\frac{b-a}{d-c} = \overline{\left(\frac{b-a}{d-c}\right)} \blacksquare$$

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

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

> *Критерий коллинеарности* трёх точек:
> $$\frac{b-a}{c-a} = \overline{\left(\frac{b-a}{c-a}\right)} \quad \text{или} \quad \left[\begin{aligned} \overrightarrow{AB} &= \vec{0} \\ \overrightarrow{AC} &= \vec{0} \end{aligned}\right.$$

Доказательство. Очевидно, что:

$$\overrightarrow{AB} \parallel \overrightarrow{AC} \iff A, B, C \text{ коллинеарны}$$

По критерию коллинеарности векторов:

$$\frac{b-a}{c-a} = \overline{\left(\frac{b-a}{c-a}\right)} \blacksquare$$

> *Уравнение секущей AB*:
> $$(\bar{a}-\bar{b})z + (b-a)\bar{z} + a\bar{b} - b\bar{a} = 0$$

Доказательство. Нет и не будет: раздел будет снесён.

Вычислительная геометрия

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 $\lambda \in \mathbb{R}$. Тогда координаты точки C равны:
>
> $$x_C = \frac{x_A + \lambda x_B}{1 + \lambda} \qquad y_C = \frac{y_A + \lambda y_B}{1 + \lambda}$$

Доказательство. По условию:

$$\overrightarrow{AC} = \lambda \overrightarrow{CB} \iff \overrightarrow{OC} - \overrightarrow{OA} = \lambda \left(\overrightarrow{OB} - \overrightarrow{OC} \right)$$

По теореме Фалеса:

$$\begin{cases} x_C - x_A = \lambda \left(x_B - x_C \right) \\ y_C - y_A = \lambda \left(y_B - y_C \right) \end{cases} \iff \begin{cases} x_C = \dfrac{x_A + \lambda x_B}{1 + \lambda} \\ y_C = \dfrac{y_A + \lambda y_B}{1 + \lambda} \end{cases} \blacksquare$$

Коллинеарность

Коллинеарными называются:

— *точки*, которые лежат на одной прямой;

— *векторы*, которые лежат на одной прямой или на параллельных прямых.

> **Критерий коллинеарности** двух векторов:
>
> $$\vec{a} = \lambda \vec{b},\ \lambda \in \mathbb{R} \iff \begin{cases} x_a = \lambda x_b \\ y_a = \lambda y_b \end{cases}$$

В частности, нулевой вектор коллинеарен *любому* вектору:

$$\vec{0} = 0\vec{a}$$

Уравнение секущей по двум известным точкам:

$$A\langle x_a, y_a\rangle,\ B\langle x_b, y_b\rangle \implies \frac{x - x_a}{x_b - x_a} = \frac{y - y_a}{y_b - y_a}$$

Доказательство. Пусть $\overrightarrow{AX}$, $\overrightarrow{AB}$ — коллинеарные векторы.

По критерию коллинеарности двух векторов:

$$\begin{cases} x - x_a = \lambda\,(x_b - x_a) \\ y - y_a = \lambda\,(y_b - y_a) \end{cases} \iff \lambda = \frac{x - x_a}{x_b - x_a} = \frac{y - y_a}{y_b - y_a} \ \blacksquare$$

Скалярное произведение

Теорема. Косинус угла α между векторами $\vec{a}$ и $\vec{b}$ равен:

$$\cos\alpha = \frac{x_a x_b + y_a y_b}{|\vec{a}|\,|\vec{b}|}$$

Доказательство. Отложим векторы $\overrightarrow{AB} = \vec{a}, \overrightarrow{AC} = \vec{b}$ от начала координат.

По теореме косинусов:

$$BC^2 = AB^2 + AC^2 - 2\left|\overrightarrow{AB}\right|\left|\overrightarrow{AC}\right|\cos\alpha \implies$$

$$\cos\alpha = \frac{AB^2 + AC^2 - BC^2}{2\left|\overrightarrow{AB}\right|\left|\overrightarrow{AC}\right|}$$

По теореме Пифагора:

$$\begin{cases} AB^2 = x_a^2 + y_a^2 \\ AC^2 = x_b^2 + y_b^2 \\ BC^2 = (x_a - x_b)^2 + (y_a - y_b)^2 \end{cases} \implies$$

$$AB^2 + AC^2 - BC^2 = 2(x_a x_b + y_a y_b) \implies$$

$$\cos\alpha = \frac{x_a x_b + y_a y_b}{|\vec{a}|\,|\vec{b}|} \ \blacksquare$$

Скалярное произведение *векторов* $\vec{a}, \vec{b}$ — величина:

$$x_a x_b + y_a y_b =: \vec{a} \cdot \vec{b}$$

Теорема. Скалярное произведение двух векторов равно:

$$\vec{a} \cdot \vec{b} = |\vec{a}| \left|\vec{b}\right| \cos \alpha,$$

α — угол между векторами.

Теорема. Если вектора $\vec{a}$ и $\vec{b}$ коллинеарны, то:
— $\vec{a} \cdot \vec{b} > 0 \implies$ вектора *сонаправлены*;
— $\vec{a} \cdot \vec{b} < 0 \implies$ вектора *несонаправлены*;
— $\vec{a} \cdot \vec{b} = 0 \implies$ один из векторов *нулевой*.

Ориентированный угол

Ориентированным называется угол α между $\vec{a}$ и $\vec{b}$, на который нужно повернуть $\vec{a}$, чтобы он был сонаправлен с $\vec{b}$:

$$\angle(\vec{a}, \vec{b}) \text{ — обозначение, } \alpha \in (-\pi; \pi]$$

Знак ориентированного угла:

— **положжительный**, если поворот происходит в *положительном* направлении системы координат;
— **отрицательный**, если поворот происходит в *отрицательном* направлении системы координат;
— **нуль**, если вектора *сонаправлены*.

Косое произведение

Косое произведение *векторов* $\vec{a}, \vec{b}$ — величина:

$$x_a x_b - y_a y_b =: \vec{a} \wedge \vec{b}$$

Теорема. Косое произведение двух векторов равно:

$$\vec{a} \wedge \vec{b} = |\vec{a}| \left|\vec{b}\right| \sin \alpha,$$

α — угол между векторами.

Теорема. Знак косого произведения векторов *совпадает* со знаком ориентированного угла.

Доказательство вытекает из *чётности* синуса угла между векторами.

Взаимное расположение объектов

Расположение *точки* A относительно *прямой, луча или отрезка* BC:

- $\angle(\overrightarrow{BA}, \overrightarrow{BC}) > 0 \implies A$ лежит в **левой** полуплоскости;
- $\angle(\overrightarrow{BA}, \overrightarrow{BC}) < 0 \implies A$ лежит в **правой** полуплоскости;
- $\angle(\overrightarrow{BA}, \overrightarrow{BC}) = 0 \implies A$ **коллинеарна** прямой BC.

Взаимное расположение *двух отрезков или лучей* AB и CD:

- концы обоих отрезков лежат в *разных* полуплоскостях относительно друг друга $\implies$ отрезки **пересекаются**;
- концы одного отрезка лежат в *одной* полуплоскости относительно другого $\implies$ отрезки **не пересекаются**;
- концы одного отрезка лежат *на* прямой другого отрезка:
  - конец одного отрезка лежит *на* другом $\implies$ отрезки имеют **общий подотрезок**;
  - концы одного отрезка *не* лежат на другом $\implies$ отрезки **не пересекаются**.

Ориентированная площадь

Ориентированной называется площадь многоугольника, которая обладает знаком его ориентированных углов.

> **Теорема.** Ориентированная площадь треугольника равна половине *косого произведения* векторов ориентированного угла.

Ориентированная площадь — *аддитивная* величина, к основным методам её расчёта относят:

- метод трапеций;
- метод треугольников.

Метод трассировки луча

> **Задача.** На плоскости даны многоугольник и точка. Решить вопрос о принадлежности точки многоугольнику.

Алгоритм трассировки луча:

1) Проверить принадлежность точки стороне многоугольника: если *истина*, остановить алгоритм.
2) Выпустить из точки в случайном направлении луч.
3) Посчитать число n пересечений луча со сторонами многоугольника:

$$\begin{cases} n \equiv 0 \pmod 2 \implies \text{точка снаружи} \\ n \equiv 1 \pmod 2 \implies \text{точка внутри} \end{cases}$$

Метод заметающей прямой

Да.

Предел последовательности

Определение

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

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

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

Этот оператор *«дистрибутивен»* относительно *сложения*, *умножения* и *деления* *(предел знаменателя не равен нулю)*.

Частичным называется предел подпоследовательности.

Свойства

> Сходимость $\implies$ ограниченность.

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

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

По «дистрибуции» модуля относительно сложения:

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

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

> **Предельный переход.** Пусть $n \to \infty$, $x_n \to a$, $y_n \to b$. Тогда справедливо следствие:
>
> $$x_n \le y_n \text{ или } x_n < y_n \implies a \le b$$

Доказательство. По определению предела:

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

Следовательно,

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

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

При $x_n < y_n$ доказательство аналогично. ■

Теорема о промежуточной функции. Пусть $n \to \infty$, $x_n, y_n \to a$. Тогда справедливо следствие:

$$\forall \{z_n\} \colon x_n \le z_n \le y_n \implies z_n \to a$$

Доказательство. По определению предела:

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

Следовательно,

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

Условие Коши

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

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

Фундаментальность $\implies$ ограниченность.

Доказательство. По условию Коши:

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

По «дистрибуции» модуля относительно сложения:

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

$$|x_n| < \varepsilon + |x_m|$$

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

Принцип компактности отрезка

Ограниченность $\implies$ частичная сходимость:

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

Доказательство. По принципу Кантора:

$$\forall k \in \mathbb{N} \; \exists! \xi \in [a_k; b_k] \subset [a_{k-1}; b_{k-1}] \iff$$

$$\lim_{k\to\infty} a_k = \lim_{k\to\infty} b_n = \xi$$

Образуем подпоследовательность:

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

По теореме о промежуточной функции:

$$a_k \le x_{n_k} \le b_k \implies \lim_{k\to\infty} x_{n_k} = \xi \ \blacksquare$$

> Частичный предел фундаментальной последовательности является её пределом.

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

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

По условию Коши:

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

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

$$|x_n - a| \le \varepsilon/2 < \varepsilon \iff \lim_{k\to\infty} x_n = a \ \blacksquare$$

Критерий Коши

> Сходимость $\iff$ фундаментальность.

Доказательство $\implies$. По определению предела:

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

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

По «дистрибуции» модуля относительно сложения:

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

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

Теорема Вейерштрасса

> Монотонность $\implies$ сходимость:
> $$\left[\begin{array}{l}\forall\{x_n\}\nearrow \lim_{n\to\infty} x_n = \sup\{x_n\}\\ \forall\{y_n\}\searrow \lim_{n\to\infty} y_n = \inf\{y_n\}\end{array}\right.$$

Доказательство. По определению точной верхней границы:

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

Так как последовательность неубывает, то

$$\forall \epsilon > 0\ \exists N\colon\ \forall n > N\ x_n \in U_\epsilon(\sup\{x_n\}) \implies$$
$$\lim_{n\to\infty} x_n = \sup\{x_n\}.\ \square$$

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

Предел функции

Определение

Предел функции f в точке x_0 — такое a, что *(О.Л. Коши)*

$$\forall \varepsilon > 0\ \exists \delta > 0\colon\ \underbrace{\forall x \in \mathring{U}_{\delta}(x_0)}_{\mathrm{I}},\ \underbrace{f(x) \in U_{\varepsilon}(a)}_{\mathrm{II}}.$$

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 в точке x_0 — такое a, что *(Э. Гейне)*

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

Упрощённая запись $\lim_{x\to x_0} f(x) = a$ или $x \to x_0, f(x) \to a$.

Бесконечно малая и большая

Бесконечно малой *(б.м.)* называется такая функция $\alpha(x)$ при $x \to x_0$, что:

$$\lim_{x\to x_0} \alpha(x) = 0$$

> **Связь предела и б.м.** Если функция f имеет предел $\lim_{x\to x_0} f(x) = a$, то справедливо:
>
> $$f(x) = a + \underset{x\to x_0}{\alpha(x)},\ \ \alpha \text{ — б.м.}$$

Бесконечно большой *(б.б.)* называется такая функция $y(x)$ при $x \to x_0$, что:

$$\lim_{x\to x_0} y(x) = \infty$$

> **Связь бесконечно малой и большой.** Верен факт:
>
> $$\underset{x\to x_0}{\alpha(x)} \text{ — б.м.},\ \forall x \in \mathring{U}_{x_0}\ \alpha(x) \neq 0 \iff \frac{1}{\alpha} \text{ — б.б.}$$

Композиция функций

> Пусть f, g — функции. Тогда:
> $$\begin{cases} \lim_{x \to x_0} f(x) = y_0 \\ \lim_{y \to y_0} g(x) = z_0 \end{cases} \implies \begin{cases} \lim_{x \to x_0} (g \circ f)(x) = z_0 \\ f(x) \neq y_0 \end{cases}$$

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

$$\begin{cases} \forall \varepsilon > 0\ \exists \delta > 0 \colon \forall y \in \mathring{U}_\delta(y_0) \subseteq D_g,\ f(x) \in U_\varepsilon(z_0) \\ \forall \delta > 0\ \exists \sigma > 0 \colon \forall x \in \mathring{U}_\sigma(x_0) \subseteq D_f,\ g(x) \in U_\delta(y_0) \end{cases}$$

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

$$\begin{cases} \forall \varepsilon > 0\ \exists \sigma > 0 \colon \forall x \in \mathring{U}_\sigma(x_0) \subseteq D_f,\ \varphi(x) \in U_\varepsilon(z_0) \\ y \neq y_0 \implies f(x) \neq y_0 \end{cases} \iff$$

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

Односторонний предел

Односторонним *(правым или левым)* называется предел функции, который определён в терминах односторонних окрестностей *(монотонных последовательностей)*:

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

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

Сущестование предела равносильно существованию *равных* односторонних пределов:

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

Асимптота

Асимптота — прямая, к которой *неограниченно* приближается кривая, но не сливается с ней.

Горизонтальная асимптота для графика функции f задаётся уравнением:

$$y = \lim_{x \to \infty} f(x)$$

Наклонная асимптота для графика функции f задаётся уравнением $y = kx + b$, где

$$k = \lim_{x\to\infty} \frac{f(x)}{x},$$
$$b = \lim_{x\to\infty} (f(x) - kx).$$

Вертикальная асимптота для графика функции f задаётся уравнением $x = a$, где

$$\lim_{x\to a+0} f(x) = \infty \text{ или } \lim_{x\to a-0} f(x) = \infty.$$

Непрерывность

Пусть $f : X \to Y$ — функция. 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

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

Односторонняя непрерывность в точке x_0 определяется через односторонние пределы.

Непрерывными в точке x_0 являются *сумма*, *произведение*, *частное* *(предел знаменателя не равен нулю)* и *композиция* непрерывных в ней функций.

Функция f **непрерывна** *на промежутке* $[a; b]$, если она непрерывна в каждой точке этого промежутка:

$$f \in \mathbb{C}[a; b] \text{ — нотация}$$

> **Предел под непрерывной функцией.** Пусть f, g — функции, g непрерывна в точке x_0. Тогда:
>
> $$\lim_{x\to x_0} f(x) = a \implies \lim_{x\to x_0} (g \circ f)(x) = g(\lim_{x\to x_0} f(x))$$

Доказательство схоже с теоремой о пределе *композиции функций*.

Замечательные пределы

Когда-нибудь это будет пояснено *(я надеюсь)*:

$$\lim_{x\to 0}\frac{\sin x}{x}=1 \qquad \lim_{x\to\infty}\left(1-\frac{1}{x}\right)^x=e$$

Теорема о промежуточном значении

> Пусть $f\in\mathbb{C}[a;b]$. Тогда справедливо:
>
> $$\forall c\in[f(a);f(b)]\ \exists\xi\in[a;b]: c=f(\xi)$$

Доказательство. По принципу Кантора:

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

$$n\to\infty,\ a_n,b_n\to\xi$$

По определению непрерывности функции на промежутке:

$$n\to\infty,\ f(a_n),f(b_n)\to f(\xi)$$

По теореме о промежуточной функции:

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

> **Метод бисекции.** Пусть $f\in\mathbb{C}[a;b]$. Тогда справедливо:
>
> $$\operatorname{sgn} f(a)\neq\operatorname{sgn} f(b) \implies \exists c\in[a;b]: f(c)=0$$

Используется, если нужно найти *примерный* нуль функции.

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:

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

Доказательство $\Longleftarrow$. По условию Коши:

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

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

По фундаментальности и сходимости к одной точке x_0:

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

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:

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

По принципу компактности отрезка:

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

По определению непрерывности:

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

Дифференциальное исчисление

Дифференцируемость

Дифференцируемой *(«линейной в малом») в точке* x_0 называется такая функция f, для которой справедливо:

$$\Delta f = (k + \underset{\Delta x \to 0}{\alpha(x)})\,\Delta x,\ \alpha \text{ — б.м.}$$

Односторонняя дифференцируемость в точке x_0 определяется через односторонние пределы.

Дифференциал *функции* f — линейная часть Δf:

$$k\,\Delta x =: \mathrm{d}f$$

Производная *в точке* x_0 — предел вида: *(Ж.Л. Лагранж)*

$$k = \lim_{\Delta x \to 0} \frac{\Delta f}{\Delta x} =: f'(x_0)$$

Свойства

Таблица *«дистрибуции»* производной:

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

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

$$(f \circ g)' = (f' \circ g)g' \qquad (kf)' = kf',\ k = \mathrm{const}$$

> Дифференцируемость $\implies$ непрерывность.

Доказательство. По определению производной:

$$\lim_{\Delta x \to 0} \frac{\Delta f}{\Delta x} = f'(x_0) \iff \frac{\Delta f}{\Delta x} = f'(x_0) + \underset{\Delta x \to 0}{\alpha(x)}\,\Delta x \iff$$

$$\Delta f = \Delta x(f'(x_0) + \alpha(x)\,\Delta x) \implies \Delta x \to 0,\ \Delta f \to 0\ \blacksquare$$

> **Производная обратной функции.** Пусть $y = f(x)$ — дифференцируемая функция. Тогда справедливо:
>
> $$f^{-1'}(y) = \frac{1}{f'(x)},\ f'(x) \neq 0$$

Доказательство. По условию запишем тождество:

$$\frac{\Delta f}{\Delta x} = 1 \colon \frac{\Delta x}{\Delta f}$$

По предельному переходу и непрерывности функций:

$$\lim_{\Delta x \to 0} \frac{\Delta f}{\Delta x} = 1 \colon \lim_{\Delta f \to 0} \frac{\Delta x}{\Delta f} \overset{\text{опр}}{\iff} f'(x) = 1 \colon f^{-1'}(y) \iff$$

$$\iff f^{-1'}(y) = \frac{1}{f'(x)},\, f'(x) \neq 0 \ \blacksquare$$

Элементарные производные

Таблица производных элементарных функций:

$$C' = 0 \qquad (x^n)' = nx^{n-1},\ n \neq 0 \qquad \ln' x = 1/x$$

$$\sin' \alpha = \cos \alpha \qquad \cos' \alpha = -\sin \alpha$$

$$\operatorname{tg}' \alpha = 1/\cos^2 \alpha \qquad \operatorname{ctg}' \alpha = -1/\sin^2 \alpha$$

$$\arcsin' x = 1/\sqrt{1-x^2} \qquad \arccos' x = -1/\sqrt{1-x^2}$$

$$\operatorname{arctg}' x = 1/(1+x^2) \qquad \operatorname{arcctg}' x = -1/(1+x^2)$$

Касательная

Касательная — прямая, которая проходит через точку x_0 кривой и представляет *предельное* положение секущей при $x \to x_0$, или $\Delta x \to 0$.

> **Геометрический смысл производной.** Угловой коэффициент *(тангенс)* касательной к графику функции f равен *производной* в этой точке:
>
> $$k = \operatorname{tg} \alpha = f'(x_0)$$

Доказательство. По определению касательной:

$$\lim_{x \to x_0} \frac{\Delta f}{\Delta x} = \operatorname{tg} \alpha = k$$

По определению производной:

$$f'(x_0) = \operatorname{tg} \alpha = k \ \blacksquare$$

> **Уравнение касательной** к графику функции f в точке x_0 имеет вид:
>
> $$y - f(x_0) = f'(x_0)(x - x_0)$$

Доказательство. По уравнению секущей графика f:

$$\frac{x - x_0}{x_1 - x_0} = \frac{y - f(x_0)}{f(x_1) - f(x_0)} \implies y - f(x_0) = \frac{f(x_1) - f(x_0)}{x_1 - x_0}(x - x_0)$$

По определению касательной:

$$y - f(x_0) = \lim_{x_1 \to x_0} \frac{f(x_1) - f(x_0)}{x_1 - x_0}(x - x_0) = f'(x_0)(x - x_0) \blacksquare$$

Промежутки монотонности

> Если функция f дифференцируема в точке x_0, то
>
> $$\begin{cases} f'(x_0) > 0 \implies f\uparrow \text{ около } x_0 \\ f'(x_0) < 0 \implies f\downarrow \text{ около } x_0 \end{cases}.$$

Доказательство. По определению производной:

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

При достаточно малом Δx верно:

$$\frac{\Delta f}{\Delta x} > 0 \iff \left[\begin{array}{l} \Delta f, \Delta x > 0 \\ \Delta f, \Delta x < 0 \end{array}\right. \iff f\uparrow \text{ около } x_0 \ \square$$

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

Условие существования экстремума

> Точка локального экстремума $\implies$ критическая точка.

Доказательство. По определению локального максимума:

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

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

Допустим, она существует; по определению производной:

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

По предельному переходу:

$$\left[\begin{array}{l} \Delta x > 0 \implies \Delta f / \Delta x < 0 \implies f'(x_0) \leq 0 \\ \Delta x < 0 \implies \Delta f / \Delta x > 0 \implies f'(x_0) \geq 0 \end{array}\right. \iff$$

$$0 \leq f'(x_0) \leq 0 \iff f'(x_0) = 0 \ \square$$

Для локального минимума доказательство аналогично. ■

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

Доказательство. По определению критической точки:

$$\left[\begin{array}{l} f'(x_0) = 0 \\ f'(x_0) = \text{undefined} \end{array}\right.$$

Допустим для определённости:

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

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 $[a; b]$. Тогда:
>
> $$f(a) = f(b) \implies \exists \xi \in (a; b) : f'(\xi) = 0$$

Доказательство. По теореме Вейерштрасса:

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

По условию существования экстремума:

$$f(a) = f(b) = f(m) \implies f'(M) = 0 \ \square$$

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

Теорема Лагранжа

> Пусть f дифференцируема на $[a;b]$. Тогда верно:
> $$\exists \xi \in (a;b) : f'(\xi) = \frac{\Delta f}{\Delta x}$$

Доказательство. Пусть $\varphi(x) := f(x) - \lambda x$.

Подберём λ так, чтобы $\varphi(a) = \varphi(b)$:

$$f(a) - \lambda a = f(b) - \lambda b \iff (b-a)\lambda = f(b) - f(a) \iff$$
$$\iff \lambda = \frac{f(b) - f(a)}{b-a}$$

По теореме Ролля:

$$\exists \xi \in (a;b) : \varphi'(\xi) = 0 \iff f'(\xi) - \lambda = 0 \iff$$
$$\iff \lambda = f'(\xi) \implies f'(\xi) = \frac{f(b) - f(a)}{b-a} = \frac{\Delta f}{\Delta x} \ ■$$

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:

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

Пусть $f, g \in \mathbb{C}[a;b]$ и $f' = g'$. Тогда:

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

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

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

По условию постоянства функции:

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

Интегральное исчисление

Неопределённый интеграл

Первообразная для функции f на множестве X — такая функция F, что:

$$\forall x \in X \; F'(x) = f(x)$$

> Если у функции f есть первообразная F, то для любой константы C функция $F + C$ тоже первообразная, причём других нет.

Доказательство. По определению первообразной:

$$F' = f$$

По дистрибуции производной:

$$(F + C)' = f \implies F + C \text{ — первообразная для } f \; \square$$

Пусть Φ — другая первообразная для f:

$$\begin{cases} \Phi' = f \\ F' = f \end{cases} \implies \Phi' - F' = (\Phi - F)' = f - f = 0$$

По условию постоянства функции:

$$\Phi - F = C \iff \Phi = F + C \; \blacksquare$$

Неопределённый интеграл — множество всех первообразных функции f:

$$F(x) + C =: \int f(x)\,\mathrm{d}x$$

f — подынтегральная функция;
$f(x)\,\mathrm{d}x$ — подынтегральное выражение;
x — переменная интегрирования;
C — постоянная интегрирования.

Свойства

Операция интегрирования *дистрибутивна* относительно *сложения*, а также:

$$\int F'(x)\,\mathrm{d}x = F(x) + C \quad \mathrm{d}\left(\int F(x)\,\mathrm{d}x\right) = F(x)\,\mathrm{d}x$$

$$\left(\int F(x)\,\mathrm{d}x\right)' = F(x) + C \quad \int kF(x)\,\mathrm{d}x = k\int F(x)\,\mathrm{d}x, \; k \neq 0$$

Интегрирование по частям. Пусть $u\mathrm{d}v$ — подынтегральная функция. Тогда справедливо:

$$\int u\mathrm{d}v = uv - \int v\mathrm{d}u$$

Доказательство. По «дистрибуции» производной:

$$(uv)' = u'v + uv'$$

По определению интеграла:

$$\int (u'v + uv')\mathrm{d}x = uv + C \iff \int u'v\mathrm{d}x + \int uv'\mathrm{d}x = uv + C$$

По определению дифференциала:

$$\begin{cases} \mathrm{d}u = u'\mathrm{d}x \\ \mathrm{d}v = v'\mathrm{d}x \end{cases} \implies \int v\mathrm{d}u + \int u\mathrm{d}v = uv + C \iff$$

$$\iff \int u\mathrm{d}v = uv - \int v\mathrm{d}u \ \blacksquare$$

Инвариантность. Смена переменной интегрирования на другую дифференцируемую функцию является *равносильным* переходом:

$$\int f(x)\mathrm{d}x = F(x) + C \iff \int f(\varphi(x))\mathrm{d}\varphi(x) = F(\varphi(x)) + C$$

Дифференциальное уравнение

Дифференциальным называется уравнение с неизвестной функцией под знаком *производной* или *дифференциала*.

Метод Фурье. Решение дифференциального уравнения $y' = \varphi(x)\psi(y)$ удовлетворяет условию: *(Ж. Фурье)*

$$\left[\begin{array}{ll} \displaystyle\int \frac{\mathrm{d}y}{\psi(y)} = \int \varphi(x)\mathrm{d}x, & \psi(y) \neq 0 \\ y = y_0, & \psi(y_0) = 0 \end{array}\right.$$

Доказательство. По условию:

$$y' = \varphi(x)\psi(y) \iff \frac{y'}{\psi(y)} = \varphi(x),\ \psi \neq 0$$

Возьмём интеграл от обеих частей уравнения:

$$\frac{y'\mathrm{d}x}{\psi(y)} = \varphi(x)\mathrm{d}x \implies \int \frac{\mathrm{d}y}{\psi(y)} = \int \varphi(x)\mathrm{d}x \ \square$$

По условию:

$$\psi(y_0) = 0 \implies (y_0)' = 0 \implies 0 = 0 \ \blacksquare$$

Площадь плоской фигуры

Вложеннной *в фигуру F* называется такая фигура P, которая целиком лежит внути F:

$$S_*(F) \text{ — } \textit{внутренняя площадь } F$$

Объемлющей *фигуру F* называется такая фигура Q, которая целиком содержит F:

$$S^*(F) \text{ — } \textit{внешняя площадь } F$$

Квадрируемой называется такая фигура F, у которой множества $S_*(F)$ и $S^*(F)$ имеют единую точную границу:

$$\sup S_*(F) = \inf S^*(F) = S(F) \text{ — } \textit{площадь } F$$

Спрямляемой называется кривая с *конечной* длиной.

Свойства квадрируемости

> **Критерий квадрируемости.** Фигура F квадрируема тогда и только тогда, когда:
>
> $$\forall \varepsilon > 0 \ \exists \ P \subseteq F \subseteq Q \colon S(Q) - S(P) < \varepsilon$$

Доказательство $\implies$. Зафиксируем $\varepsilon > 0$.

По определению точных границ множеств $S(P)$, $S(Q)$:

$$\begin{cases} \forall \varepsilon/2 > 0 \ \exists \ P \subseteq F \colon S(F) - S(P) < \varepsilon/2 \\ \forall \varepsilon/2 > 0 \ \exists \ Q \supseteq F \colon S(Q) - S(F) < \varepsilon/2 \end{cases} \implies$$
$$\implies S(Q) - S(P) < \varepsilon \ \blacksquare$$

Доказательство $\impliedby$. По определению точных верхних границ множеств $S(P)$, $S(Q)$:

$$S(Q) - S(P) < \varepsilon \implies 0 \leq \inf_{Q \supseteq F} S(Q) - \sup_{P \subseteq F} S(P) < \epsilon$$

По определению квадрируемой фигуры:

$$\inf S^*(F) - \sup(S_*(F)) = 0 \iff \inf S^*(F) = \sup S_*(F) \implies$$
$$\implies F \text{ квадрируема } \blacksquare$$

> **Признак квадрируемости.** Если граница фигуры F — спрямляемая кривая, то F квадрируема.

Доказательство. По условию:

$$S^*(F) - S_*(F) \text{ — S фигуры, объемлющей границу } F$$

По определению точных границ множеств $S^*(F),\ S_*(F)$:

$$\inf S^*(F) - \sup S_*(F) = S_{\text{гр}} = 0 \implies F \text{ квадрируема } \blacksquare$$

> **Аддитивность.** Пусть F_1 и F_2 квадрируемы, причём $F_1 \cup F_2 = F,\ F_1 \cap F_2 = \emptyset$. Тогда F *тоже* квадрируема.

Доказательство. По условию:

$$F = F_1 \cup F_2 \implies S_{\text{гр}} \le S_{\text{гр}1} + S_{\text{гр}2}$$

По критерию квадрируемости:

$$S_{\text{гр}1} + S_{\text{гр}2} = 0 \implies S_{\text{гр}} = 0 \implies F \text{ квадрируема } \blacksquare$$

> Пересечение квадрируемых фигур *квадрируемо*.

Доказательство *аналогично* предыдущему свойству.

Определённый интеграл

Разбиение отрезка $[a;b]$ — конечное упорядоченное множество $X \subseteq [a;b]$, причём $a, b \in X$.

Частичным называется отрезок, составленный из *соседних* элементов разбиения:

$$\Delta x_k = x_k - x_{k-1} \text{ — } \textit{длина} \text{ частичного отрезка } [x_{k-1}; x_k]$$

Интегральная сумма функции f на $[a;b]$ имеет вид:

$$\sum_{k=1}^{n} f(\xi_k)\,\Delta x_k,\ \xi_k \in [x_{k-1}; x_k]$$

Нижней (верхней) называется такая интегральная сумма, в которой ξ_k *минимизирует (максимизирует)* значение f на частичном отрезке.

Определённый интеграл — предел интегральной суммы:

$$\lim_{n\to+\infty}\sum_{k=1}^{n} f(\xi_k)\,\Delta x_k =: \int_a^b f(x)\,\mathrm{d}x$$

Криволинейная трапеция — подграфик неотрицательной и непрерывной функции на $[a;b]$.

> **Геометрический смысл.** Пусть f задаёт криволинейную трапецию T на $[a;b]$. Тогда её площадь равна:
>
> $$S(T) = \int_a^b f(x)\,\mathrm{d}x$$

Доказательство. По признаку квадрируемости:

$$f \in \mathbb{C}[a;b] \implies T \text{ квадрируема}$$

По определению интегральных сумм:

$$S^*(T) \text{ — \textit{верхняя} сумма}; \quad S_*(T) \text{ — \textit{нижняя} сумма}$$

По определению квадрируемости:

$$S^*(T) - S_*(T) < \varepsilon \implies \inf S^*(T) = \sup S_*(T) = S(T) \implies$$
$$\implies \lim_{n\to+\infty}\sum_{k=1}^{n} f(\xi_k)\,\Delta x_k = S(T)$$

По определению определённого интеграла:

$$S(T) = \int_a^b f(x)\,\mathrm{d}x \ \blacksquare$$

> Непрерывность $\implies$ интегрируемость.

Доказательство. Когда-нибудь...

> **Оценка определённого интеграла.** Пусть функция f на отрезке $[a;b]$ принимает значения из $[m;M]$. Тогда:
>
> $$m(b-a) \le \int_a^b f(x)\,\mathrm{d}x \le M(b-a)$$

Очевидным является *геометрическое* доказательство через площади фигур.

Свойства

Операция интегрирования *дистрибутивна* относительно *сложения*, а также:

$$\int_a^a F(x)\,\mathrm{d}x = 0 \quad \int_a^b F(x)\,\mathrm{d}x = -\int_b^a F(x)\,\mathrm{d}x$$

$$\int_a^b kF(x)\,\mathrm{d}x = k\int_a^b F(x)\,\mathrm{d}x,\ k \neq 0$$

> **Аддитивность.** Пусть $f \in [a;b],\ c \in [a;b]$. Тогда верно:
>
> $$\int_a^b F(x)\,\mathrm{d}x = \int_a^c F(x)\,\mathrm{d}x + \int_c^b F(x)\,\mathrm{d}x$$

Интегрировать можно *неравенства*, если они непрерывны на области интегрирования:

$$\begin{cases} f, g \in \mathbb{C}[a;b] \\ f(x) \leq g(x) \end{cases} \implies \int_a^b f(x)\,\mathrm{d}x \leq \int_a^b g(x)\,\mathrm{d}x$$

Интеграл с переменным пределом

> **Теорема о среднем.** Пусть $f \in \mathbb{C}[a;b]$. Тогда верно:
>
> $$\exists \xi \in [a;b]\colon\ \int_a^b f(x)\,\mathrm{d}x = f(\xi)(b-a)$$

Доказательство. По оценке определённого интеграла:

$$m \leq f(x) \leq M \implies m(b-a) \leq \int_a^b f(x)\,\mathrm{d}x \leq M(b-a) \implies$$

$$\implies m \leq \frac{\int_a^b f(x)\,\mathrm{d}x}{b-a} \leq M,\ a \neq b$$

По теореме о промежуточном значении:

$$\exists \xi \in [a;b] : f(\xi) = \frac{\int_a^b f(x)\,\mathrm{d}x}{b-a} \implies \int_a^b f(x)\,\mathrm{d}x = f(\xi)(b-a)\ \blacksquare$$

Интеграл с переменным верхним пределом — функция вида:

$$S(x) = \int_a^x f(t)\,\mathrm{d}t,\ x \in [a;b]$$

> Пусть функция f непрерывна в окрестности точки $t = x$. Тогда в x функция $S(x)$ дифференцируема, причём
>
> $$S'(x) = \left(\int_a^x f(t)\,\mathrm{d}t\right)' = f(x).$$

Доказательство. По геометрическому смыслу определённого интеграла:

$$\Delta S = S(x+\Delta x) - S(x) = \int_a^{x+\Delta x} f(t)\,\mathrm{d}t - \int_a^x f(t)\,\mathrm{d}t =$$
$$= \int_a^x f(t)\,\mathrm{d}t + \int_x^{x+\Delta x} f(t)\,\mathrm{d}t - \int_a^x f(t)\,\mathrm{d}t = \int_x^{x+\Delta x} f(t)\,\mathrm{d}t$$

По теореме о среднем:

$$\exists \xi \in [x;x+\Delta x]\colon\ \int_x^{x+\Delta x} f(t)\,\mathrm{d}t = f(\xi)(x+\Delta x - x) = f(\xi)\Delta x$$

По предельному переходу:

$$\Delta S = f(\xi)\Delta x \iff \frac{\Delta S}{\Delta x} = f(\xi) \implies \lim_{\Delta x\to 0}\frac{\Delta S}{\Delta x} = \lim_{\Delta x\to 0} f(\xi) \implies$$
$$\implies S'(x) = f(x)\ \blacksquare$$

Формула Ньютона—Лейбница

> Пусть F — первообразная для функции f. Тогда верно:
>
> $$\int_a^b f(x)\,\mathrm{d}x = F(x)\big|_a^b = F(b) - F(a)$$

Доказательство. По свойству интеграла с переменным верхним пределом:

$$S'(x) = f(x) \implies S(x) = F(x) + C \text{ — первообразные}$$

По определению определённого интеграла:

$$S(a) = \int_a^a f(t)\,\mathrm{d}t = 0 \implies C = -F(a) \implies S(x) = F(x) - F(a)$$

По условию:

$$x = b \implies S(b) = F(b) - F(a) \iff \int_a^b f(t)\,\mathrm{d}t = F(b) - F(a) \blacksquare$$

Длина кривой

> Пусть график функции f — кривая. Тогда её длина на промежутке $[a;b]$ равна:
>
> $$L = \int_a^b \sqrt{1 - f'^2(x)}\,\mathrm{d}x$$

Доказательство. Пусть задано *разбиение* $X \subseteq [a;b]$.

Тогда длина хорды в точках $x_k,\ x_{k-1}$ равна:

$$l_k = \sqrt{(\Delta f_k)^2 + (\Delta x_k)^2} = \Delta x_k \sqrt{1 - \left(\frac{\Delta f_k}{\Delta x_k}\right)^2}$$

По теореме Лагранжа:

$$\exists \xi \in [x_{k-1}; x_k] : l_k = \Delta x_k \sqrt{1 - f'^2(\xi)}$$

По предельному переходу:

$$L \geq \sum_{k=0}^{n} \Delta x_k \sqrt{1 - f'^2(\xi)} \implies L = \lim_{n \to \infty} \sum_{k=0}^{n} \Delta x_k \sqrt{1 - f'^2(\xi)}$$

По определению определённого интеграла:

$$\lim_{n \to \infty} \sum_{k=0}^{n} \Delta x_k \sqrt{1 - f'^2(\xi)} = \int_a^b \sqrt{1 - f'^2(x)}\,\mathrm{d}x \implies$$

$$\implies L = \int_a^b \sqrt{1 - f'^2(x)}\,\mathrm{d}x \blacksquare$$

Объём тела

Гладкой называется такая поверхность...

Скоро...

Поиск с возвратом

Поиск с возвратом — метод нахождения решений задачи полным перебором 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:

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

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:

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

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, $A_1 = T_{1W_1}$, $A_2 = T_{2W_2}$, $B_1 = T_1 \backslash A_1$, $B_2 = T_2 \backslash A_2$ — их поддеревья:

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

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

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

Шаг рекурсивного построения решения M:

$$\begin{cases} v_i = v_j, \ w_k = w_l \implies v_i \mapsto w_k, \text{комбинировать} \\ v_i \neq v_j, \ w_k = w_l \implies A_1 \to T_2 \ (B_1 \to \lambda) \\ v_i = v_j, \ w_k \neq w_l \implies T_1 \to A_2 \ (\lambda \to B_2) \\ v_i \neq v_j, \ w_k \neq w_l \implies \left[\begin{array}{l} A_1 \to A_2 \text{ или } A_1 \to T_2 \\ B_1 \to B_2 \text{ или } T_1 \to A_2 \end{array} \right. \end{cases}$$

Динамика

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)*:

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

$$\begin{cases} v \in V_1,\ w \in V_2 \\ \mathrm{depth}_v = \mathrm{depth}_w \\ \{v_i, \dots, v_j\} = \mathrm{children}_v \\ \{w_k, \dots, w_l\} = \mathrm{children}_w \\ \langle v_i \dots v_j, w_k \dots w_l \rangle \sim \gamma_{\min}(G_1 \to G_2) \\ G_1 = T_{1W_i} \cup \dots \cup T_{1W_j} \\ G_2 = T_{2W_k} \cup \dots \cup T_{2W_l} \\ \forall s \in \{i, \dots, j\}\ \mathrm{root}_{T_{1Ws}} = v_s \\ \forall t \in \{k, \dots, l\}\ \mathrm{root}_{T_{2Wt}} = w_t \end{cases}$$

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

Уравнение Беллмана

Введём задачу на оптимизацию вида:

$$\underset{d \in \Delta}{\mathrm{opt}}\{H(d)\} \qquad \begin{aligned} d &\text{ — выбор;} \\ \Delta &\text{ — допустимое множество;} \\ H &\text{ — целевая функция одной переменной.} \end{aligned}$$

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

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

Пусть H — целевая функция нескольких переменных.

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

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

$\Delta = D_1 \times \dots \times D_n$ — 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:

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

Модель динамики

Целевой называется функция, у которой нужно найти *экстремум* *(оптимальное значение)*.

Состояние системы зависит от конечного числа *параметров* *(часто от одного или двух)*.

> **Принцип оптимальности**. Оптимальное решение зависит лишь от текущего состояния и цели, а не от предыстории. *(Р. Беллман)*

Сертификат *решения* — последовательность управляющих шагов, которые оптимизируют целевую функцию.

Типы задач на динамику:

— оптимизация целевой функции;
— подсчёт количества вариантов решения;
— составление сертификата решения.

Подходы динамики

Мемоизация — *рекурсивный* подход динамики, при котором подсчитанные результаты *кешируются* и используются повторно *(вычисления отложены)*.

Табуляция — *итеративный* подход динамики, при котором кеш заполняется сразу, на основе тривиальных подзадач.

Также пояснить про одномерный и двумерный кеш, определение кеша?

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 — число его вершин.

Размер графа — число его рёбер.

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:

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

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

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

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

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

> **Свойство.** Пусть $G = \langle V, E \rangle$ — граф с n вершинами и m рёбрами. Тогда:
>
> $$\sum_{i=1}^{n} \operatorname{indeg}(v_i) = \sum_{i=1}^{n} \operatorname{outdeg}(v_i) = m$$

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

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

Неориентированный граф

Неорграф *(неориентированный граф)* — такой граф $G = \langle V, E \rangle$, что:

$$\forall v, w \in V \ \langle v, w \rangle \in E \implies \langle w, v \rangle \in E$$

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

Кратными называются два и более рёбер, которые образованы *одинаковыми* вершинами.

Последовательность вершин

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

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

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

Цепь — путь без повтора рёбер.

Простая цепь — путь без повтора рёбер и вершин *(кроме, возможно, первой и последней вершины)*.

Цикл — закрытая простая цепь.

Паросочетание — множество попарно несмежных рёбер.

Эйлеровой называется такая последовательность вершин, которая проходит по всем *рёбрам* графа.

> **Критерий эйлеровости.** Связный неорграф *эйлеров*, если валентность всех его вершин чётна.

> **Критерий полуэйлеровости.** Связный неорграф *полуэйлеров*, если:
> — валентность всеъ вершин *чётна*;
> — ноль или две вершины имеют *нечётную* валентность.

Ациклическим *(лесом)* называется граф без циклов.

Виды графов

Полным называется такой неорграф $G = \langle V, E \rangle$, что:

$$E = V \times V$$

Однородным называется такой неорграф, у которого *валентности* всех вершин равны.

Транспонированным называется такой граф G^T по отношению к G, у которого все рёбра *инвертированы*.

Взвешенным называется такой граф, в котором каждому ребру сопоставляется число — *вес, длина, стоимость*.

Связность

Связный:

— *неорграф*, между любыми вершинами которого есть маршрут;
— *орграф*, у которого аналогичный неорграф *связный*.

Сильно связным называется такой *орграф* $G = \langle V, E \rangle$, что:

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

Точка сочленения — вершина, удаление которой делает граф *несвязным*.

Мост — ребро, удаление которого делает граф *несвязным*.

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

Компонента сильной связности *орграфа* — сильно связный подграф, который не входит в состав такого же подграфа.

Дерево

Свободное дерево T — компонента связности леса.

> **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 *(ориентированное дерево или ордерево)* — такой орграф, у которого:

— аналогичный неорграф есть свободное дерево;
— есть **корень** — единственная вершина с нулевой входящей валентностью.

Остовное дерево — ациклический связный подграф неорграфа, в который входят все его вершины.

Минимальным называется такое *остовное дерево*, которое обладает минимальным суммарным весом всех рёбер.

Вершины дерева

Пусть T — корневое дерево, причём $\langle v, w \rangle \in E_T$:

— **родитель** вершины w — это $v =: \mathrm{parent}_w$;
— **ребёнок** вершины v — это $w \in \mathrm{children}_v$.

Корневым называется узел без родителей *(с нулевой входящей валентностью)*.

Листовым называется узел без детей *(с нулевой исходящей валентностью)*.

Сиблинги — вершины с общими родителями.

Уровень вершины v — длина простой цепи от root_T до v:

$$\mathrm{depth}_v \text{ — обозначение}$$

Рёбра леса

Пусть $G = \langle V, E \rangle$ — лес:

— **обратное** ребро соединяет вершину с её *предком*;
— **прямое** ребро соединяет вершину с её *потомком*;
— **перекрёстное** ребро принадлежит множеству $V \times V \backslash E$.

Безопасным называется ребро, которое принадлежит *минимальному остовному дереву*.

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 — хеш-таблица вида:

$$\text{вершина} \ \mapsto \ \text{смежные узлы}$$

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

Способы представления дерева

Массив родителей — хеш-таблица вида:

$$v \mapsto \mathrm{children}_v$$

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

«**Первый ребёнок, следующий сиблинг**» — хеш-таблица вида:

$$v \mapsto \langle \mathrm{first}_v, \mathrm{next}_v \rangle$$

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

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 $\langle \mathrm{parent}_v, v \rangle$: $v \mapsto \lambda$;
— *вставка* листового узла v с ребром $\langle \mathrm{parent}_v, v \rangle$: $\lambda \mapsto v$;
— *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:

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

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

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

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

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:

$$\left[\begin{array}{l} \mathrm{depth}_{v_{i+1}} \geq \mathrm{depth}_{w_{j+1}} \iff \langle v_i w_j, v_{i+1} w_j \rangle \in E \ (v_{i+1} \mapsto \lambda) \\ \mathrm{depth}_{v_{i+1}} = \mathrm{depth}_{w_{j+1}} \iff \langle v_i w_j, v_{i+1} w_{j+1} \rangle \in E \ (v_{i+1} \mapsto w_{j+1}) \\ \mathrm{depth}_{v_{i+1}} \leq \mathrm{depth}_{w_{j+1}} \iff \langle v_i w_j, v_i w_{j+1} \rangle \in E \ (\lambda \mapsto w_{j+1}) \end{array}\right.$$

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:

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

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:

$$\mathrm{order}\colon V \to \{1, \dots, |V|\}$$

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

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

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

Алгоритмы на графах

Обход графа

Обход в глубину *(Depth-First Search, DFS)* — метод, при котором граф обходят сначала по детям, потом по сиблингам.

> **Алгоритмы:**
> — поиск эйлерового пути, цикла;
> — тест ацикличности;
> — поиск мостов, точек сочленения;
> — топологическая сортировка;
> — построение компонент связности:
>   > обыкновенных *(грядки, водостоки)*;
>   > сильных *(алгоритм Косараджу, конденсация)*.
> — 2-SAT;
> — алгоритм Куна.

Обход в ширину *(Breadth-First Search, BFS)* — метод, при котором граф обходят сначала по сиблингам, потом по детям.

> **Алгоритмы:**
> — алгоритм Кана;
> — проверка графа на двудольность;
> — поиск кратчайших рёберных путей.

Нет циклов $\implies$ не требуется массив *visited*.

Также были задачи на потоки. Рассмотреть их!

Поиск эйлерового пути

Алгоритм поиска эйлерового *цикла*:

```
if is_eulerian(graph): #1
  ecirc = graph.get_ecirc(v) #2
else:
  ecirc = -1

def get_ecirc(v): # DFS
  ecirc = list()
  for n in edges[v]:
```

```
    if edges[v][n] > 0:
      edges[v][n] -= 1
      ecirc += get_ecirc(n)
  return ecirc + [v] #3
```

1) Проверить граф на *эйлеровость*.
2) Начать с любой вершины v.
3) Если дан орграф, ответ нужно *инвертировать*.

Алгоритм поиска эйлерового *пути*:

```
if is_semi_eulerian(graph): #1
  epath = graph.get_epath(v) #2
else:
  epath = -1

def get_epath(v): # DFS
  epath = list()
  for n in edges[v]:
    if edges[v][n] > 0:
      edges[v][n] -= 1
      epath += get_epath(n)
  return epath + [v] #3
```

1) Проверить граф на *полуэйлеровость*.
2) Начать с вершины нечётной степени v.

   НО: если дан орграф, выбрать вершину большей *исходящей* валентности.
3) Если дан орграф, ответ нужно *инвертировать*.

Применяется в **задачах**:

— китайский почтальон;
— домино, восстановление строки.

Топологическая сортировка

Алгоритм топологической сортировки через *DFS*:

```
def topo_sort(v): # DFS
  vertices[v].visited = 1
  stack = list()
  for n in vertices[v].adjacent:
```

```
    if not vertices[v].visited:
      stack += topo_sort(n)
  return stack + [v]
```

Алгоритм Кана

Алгоритм топологической сортировки через *BFS*:

```
def topo_sort(queue=deque()):
  for v in vertices: #1
    if vertices[v].indegree == 0:
      queue.append(v)
  order = list()
  while queue:
    q = queue.popleft()
    order.append(q)
    for n in vertices[q].adjacent_out:
      vertices[n].indegree -= 1
      if vertices[n].indegree == 0: #2
        queue.append(n)
  return order
```

1) Найти *корни* графа, добавить их в очередь.
2) Если какая либо из соседних вершин стала *корнем*.

Применяется в **задачах**:

— лексикографическая сортировка;
— топологическое маркирование;
— тест ацикличности.

Алгоритм Косараджу

Алгоритм поиска компонент сильной связности:

```
reverse = graph.transpose() #1
order = reverse.topo_sort() #2
mark = 0
for v in order[::-1]: #3
  if not graph.vertices[v].visited:
    mark_component(v, mark)
    mark += 1
```

```python
def mark_component(v, mark): # DFS
  vertices[v].visited = 1
  vertices[v].mark = mark
  for n in vertices[v].adjacent:
    if not vertices[n].visited:
      mark_component(n, mark)
```

1) Построить *транспонированный* граф *reverse*.
2) Применить *топологическую сортировку* к *reverse*.
3) Применить *DFS* на *graph* в обратном порядке топологической сортировки:

   цикл поиска в глубину ≡ сильная компонента связности

2-SAT

Алгоритм решения:

1) Перевести CNF в INF.
2) Построить граф импликаций.
3) Найти компоненты сильной связности в графе.
4) Проверить, что для любой вершины x графа справедливо:

$$c[x] \neq c[\neg x]$$

5) Если требуется вывести ответ, то воспользоваться формулой:

$$x = \begin{cases} \text{true}, & c[x] < c[\neg x] \\ \text{false}, & c[x] > c[\neg x] \end{cases}$$

Поиск мостов

Алгоритм поиска мостов на неорграфе:

```python
def get_bridges(v, parent=-1): # DFS
  vertices[v].visited = 1
  time += 1
  vertices[v].ord = time #1
  vertices[v].min = time
  bridges = set()
  for n in vertices.adjacent:
    if n == parent: #2
      continue
    if vertices[n].visited: #3
```

```
      vertices[v].min = min(vertices[v].min, \
                            vertices[n].ord)
    else: #4
      bridges |= get_bridges(n, v) #5
      vertices[v].min = min(vertices[v].min, \
                            vertices[n].min)
      if vertices[n].min > vertices[v].ord and \
         parent != -1: #6
           bridges.add((v, n))
  return bridges
```

1) Запись текущего порядка захода в вершину.
2) Если $\langle v, n \rangle$ — ребро в *обратную сторону*.
3) Если $\langle v, n \rangle$ — *обратное ребро*.
4) Если $\langle v, n \rangle$ — *ребро дерева*.
5) Мост может быть отмечен *несколько раз* за алгоритм.
6) Критерий моста:

$$[\langle v, neigh \rangle \text{ — мост}] = \begin{cases} \text{true}, & \min[neigh] > \text{ord}[v] \\ \text{false}, & \min[neigh] \leq \text{ord}[v] \end{cases}$$

Поиск точек сочленения

Алгоритм поиска точек сочленения на неорграфе:

```
def get_cuts(v, parent=-1): # DFS
  vertices[v].visited = 1
  time += 1
  vertices[v].ord = time #1
  vertices[v].min = time
  children, cuts = 0, set()
  for n in vertices.adjacent:
    if n == parent: #2
      continue
    if vertices[n].visited: #3
      vertices[v].min = min(vertices[v].min, \
                            vertices[n].ord)
    else: #4
      children += 1
      cuts |= get_cuts(n, v) #5
      vertices[v].min = min(vertices[v].min, \
                            vertices[n].min)
```

```
    if vertices[n].min >= vertices[v].ord and \
       parent != -1: #6
         cuts.add(v)
  if children > 1 and parent == -1:
    cuts.add(v)
  return cuts
```

1) Запись текущего порядка захода в вершину.
2) Если $\langle v, n \rangle$ — ребро в *обратную сторону*.
3) Если $\langle v, n \rangle$ — *обратное ребро*.
4) Если $\langle v, n \rangle$ — *ребро дерева*.
5) Вершина может быть отмечена *несколько раз* за алгоритм.
6) Критерий точки сочленения:

$$[v \text{ — т. сочленения}] = \begin{cases} \text{true}, & \min[neigh] \geq \text{ord}[v] \\ \text{false}, & \min[neigh] < \text{ord}[v] \end{cases}$$

Алгоритм Куна

Алгоритм поиска максимального паросочетания на двудольном графе:

```
for v in vertices.part: #1
  if has_ichain(v):
    null_all_visited(vertices)

matching = dict() # empty == None
def has_ichain(v): # DFS
  if vertices[v].visited:
    return False
  vertices[v].visited = 1
  for n in vertices[v].adjacent:
    if matching[n] == None or \
       has_ichain(matching[n]): #2
         matching[n] = v
         return True
  return False
```

1) Рассматриваются все вершины *одной доли* двудольного графа.
2) Если пары нет или если есть *увеличивающаяся цепь*.

Кратчайший путь

Волновой алгоритм — да.

Алгоритм Дейкстры ищёт кратчайшие пути из заданной вершины до всех остальных вершин взвешенного графа *(вес рёбер неотрицательный)*:

```
def dijkstra(): # tabulation
  vertices[1].cost = 0 #1
  for _ in vertices:
    v = (None, inf)
    for i in vertices:
      if not vertices[i].visited and \
         vertices[i].min < v[1]:
           v = (i, vertices[i].min)
    if v[0] == None: #2
      break
    vertices[v[0]].visited = 1
    for n in vertices[v[0]].adjacent:
      curr_cost = vertices[v[0]].min + \
                  edges[n][v[0]].cost
      if curr_cost < vertices[n].min:
        vertices[n].min = curr_cost
        vertices[n].parent = v[0] #3
```

1) База динамики; по умолчанию вес рёбер — ∞.
2) Если добраться до вершины невозможно.
3) Параметр для составления сертификата решения.

Алгоритм Беллмана-Форда — да.

Алгоритм Прима

Алгоритм поиска минимального остовного дерева *(по структуре идентичен алгоритму Дейкстры)*:

```
def prim(): # greedy
  vertices[1].min = 0 #1
  for _ in vertices:
    v = (None, inf)
    for i in vertices:
      if not vertices[i].visited and \
```

```
        vertices[i].min < v[1]:
          v = (i, vertices[i].min)
    if v[0] == None: #2
      break
    vertices[v[0]].visited = 1
    if vertices[v[0]].parent != None: #3
      add_safe_edge(v[0], vertices[v[0]].parent)
    for n in vertices[v[0]].adjacent:
      curr_cost = edges[v[0]][n]
      if curr_cost < vertices[n].min:
        vertices[n].min = curr_cost
        vertices[n].parent = v[0]
```

1) База динамики; по умолчанию вес рёбер — ∞.
2) Если добраться до вершины невозможно.
3) Вывести *безопасное ребро*, если обработано хотя бы две вершины.

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, кото-рое 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

$$s\colon [m] \to X.$$

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

Перестановка — упорядоченное биективное разбиение:

$$P_n\colon [n] \to X, \quad P_n = n!$$

k-Размещение — упорядоченное инъективное разбиение:

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

k-Сочетание — неупорядоченное инъективное разбиение:

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

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:

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

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 выборок $\binom{n - k_1 - \dots - k_{j-1}}{k_j}$:

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

По формуле сочетаний:

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

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:

$$(x_1 + \dots + x_r)^n = (x_1 + \dots + x_r)(x_1 + \dots + x_r)^{n-1}$$

$$= (x_1 + \dots + x_r) \cdot \sum_{\substack{k'_1, \dots, k'_r \\ k'_1 + \dots + k'_r = n-1}} \binom{n-1}{k'_1, \dots, k'_r} x_1^{k'_1} \dots x_r^{k'_r}$$

$$= \sum_{i=1}^{r} \sum_{\substack{k'_1, \dots, k'_r \\ k'_1 + \dots + k'_r = n-1}} \binom{n-1}{k'_1, \dots, k'_r} x_1^{k'_1} \dots x_i^{k'_i + 1} \dots x_r^{k'_r}$$

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

$$(x_1 + \dots + x_r)^n =$$

$$\sum_{\substack{k_1, \dots, k_r \\ k_1 + \dots + k_r = n-1}} \sum_{i=1}^{r} \binom{n-1}{k_1, \dots, k_i - 1, \dots, k_r} x_1^{k_1} \dots x_r^{k_r} \ \blacksquare$$

Принцип включения-исключения

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

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

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 множестввх 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 $f : X \to Y$ — 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 $f : X \to \mathcal{P}(Y)$ — 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:

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

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

$$\begin{matrix}\text{число неупорядоченных} \\ \text{выборок } A \backslash B\end{matrix} = \binom{n}{n-r}$$

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

Любой элемент $x \in B \subset A_1$ можно сопоставить $x \in A \backslash B \subset A_2$. 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:

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

Метод шаров и перегородок

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

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

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:

$$\left(\!\!\binom{n}{k-1}\!\!\right) + \left(\!\!\binom{n-1}{k}\!\!\right) = \binom{n+k-2}{k-1} + \binom{n+k-2}{k} = \binom{n+k-1}{k} \blacksquare$$

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:

$$\left[\begin{array}{llll} x_4 = 0 & \implies 3(x_1+x_2+x_3) = 22 & \iff & \text{решений нет} \\ x_4 = 1 & \implies 3(x_1+x_2+x_3) = 15 & \iff & x_1+x_2+x_3 = 5 \\ x_4 = 2 & \implies 3(x_1+x_2+x_3) = 8 & \iff & \text{решений нет} \\ x_4 = 3 & \implies 3(x_1+x_2+x_3) = 1 & \iff & \text{решений нет} \end{array}\right.$$

$$\iff \left(\!\!\binom{3}{5}\!\!\right) = \binom{7}{5} = 21$$

Ответ: 21 решение.

Правило деления

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

$$|X| = 4\,|Y|$$

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 $\overline{x_j \ldots x_k},\ 1 \le j, k \le 4,\ i \ne j$.

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

$$f \text{ — } n\text{-к-одному} \implies 4\,|Y| = |X| \iff |Y| = |X|\,/4$$

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:

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

Частные случаи:

$$\left\{ {n \atop 0} \right\} = 0 \qquad \left\{ {n \atop 1} \right\} = 1 \qquad \left\{ {n \atop n} \right\} = 1 \qquad \left\{ {n \atop n-1} \right\} = \binom{n}{2}$$

Доказательство. Скоро... наверное.