

# Элементы теории чисел

Лектор: Королев Максим Александрович

14 ноября 2024 г.



Конспект: Кирилл Яковлев, 108 группа

tg: @fourkenz

# Содержание

1	Делимость целых чисел	3
2	Наименьшее общее кратное и наибольший общий делитель (НОК и НОД)	4
3	Алгоритм Евклида	6
4	Решение в целых числах линейного уравнения с двумя неизвестными	6
5	Простые числа	7
6	Мультипликативные функции	11
7	Непрерывные дроби	18
8	Теория сравнений	27
9	Сравнения с одним неизвестным	34

**Введение.** Следующие понятия считаются интуитивно ясными:

1. Понятие натурального ряда  $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$ .
2. У каждого натурального числа  $n$  существует единственное натуральное число  $m = n + 1$  следующее за ним.
3. Понятие отрицательных чисел и нуля.
4. Понятие суммы, разности и произведения двух целых чисел.

**Аксиома.** Если  $M \subset \mathbb{N}$  обладает следующими свойствами:  $(1 \in M)$  и  $(\forall n \in M \text{ выполнено } n + 1 \in M)$ , то  $M = \mathbb{N}$ .

**Следствие 1.** Всякое непустое подмножество натурального ряда содержит минимальный элемент.

**Следствие 2.** Всякое непустое конечное подмножество натурального ряда содержит максимальный элемент.

**Следствие 3.** (Принцип математической индукции)

Если известно, что некоторое утверждение о натуральных числах выполнено для натурального числа  $a$ , а также из предположения о том, что утверждение верно при некотором  $n$  следует справедливость этого утверждения и для числа  $n+1$ , то это утверждение верно для всех натуральных чисел, больше или равных  $a$ .

## 1 Делимость целых чисел

**Определение 1.1.** Пусть  $a, b \in \mathbb{N}, b \neq 0$ . Говорят что  $a$  делится на  $b$ , если существует  $c \in \mathbb{Z}$ , такое, что  $a = bc$ .

**Замечание.**  $a$  называется делимым, а  $b$  называется делителем числа  $a$ . Запись  $b \mid a$  означает, что  $b$  делит  $a$ . Если  $b$  не делит  $a$ , то пишут  $b \nmid a$ .

**Лемма 1.1.** Пусть  $a, b, c \in \mathbb{Z}$ , тогда:

1.  $1 \mid a$ .
2.  $a \neq 0 \Rightarrow a \mid a$ .
3.  $a \mid b \Rightarrow a \mid bc$ .
4.  $a \mid b$  и  $b \mid c \Rightarrow a \mid c$ .

$$5. a \mid b \text{ и } a \mid c \Rightarrow a \mid (b + c).$$

$$6. a \mid b \text{ и } b \neq 0 \Rightarrow |a| \leq |b|.$$

**Теорема 1.1.** Если  $a \in \mathbb{Z}, b \in \mathbb{N}$ , то существует единственная пара целых чисел  $q$  и  $r$ , такие, что  $a = bq + r$ , где  $0 \leq r \leq b - 1$ .

*Доказательство.* Докажем существование: Если  $a$  делится на  $b$ , то  $a = bc$ . В таком случае возьмем  $q = c, r = 0$ . Теперь пусть  $a$  не делится на  $b$ . Рассмотрим непустое множество  $M$  натуральных чисел, представимых в виде  $a - kb, k \in \mathbb{Z}$ , возьмем  $k = -(|a| + 1)$ , тогда  $a - kb = b(|a| + 1) + a \geq b(|a| + 1) - |a| \geq 1 \cdot (|a| + 1) - |a| = 1 \Rightarrow a - kb$  - натуральное. Значит, у  $M$  есть минимальный элемент  $a - kb$ . Возьмем  $q = k, r = a - kb = a - bq > 1$ . Осталось показать, что  $0 \leq r \leq b - 1$ . Предположим, что  $r \geq b$ . Если  $r = b$ , то  $a = bq + b = b(q + 1)$  получаем противоречие, так как  $a$  не делится на  $b$ . Значит,  $r = b + m, m \geq 1$ . Получаем  $1 \leq m = r - b < r$ , при этом  $a = bq + r = bq + b + m = b(q + 1) + m \Rightarrow m = a - b(q + 1) \Rightarrow m \in M$  и  $m < r$ , получаем противоречие, так как  $a$  не делится на  $b$ . Доказано, что  $r < b \Rightarrow$  представление  $a = bq + r$  - искомое. Докажем единственность: предположим, что для некоторого  $a$  и  $b$  имеются пары чисел с указанным свойством:  $q, r$  и  $q_1, r_1$ , причем  $0 \leq r \leq r_1 \leq b - 1$ . Тогда  $a = bq + r = bq_1 + r_1 \Rightarrow 0 \leq b(q - q_1) = r_1 - r$ . Значит,  $b$  делит разность  $r_1 - r$ . Допустим, что  $q \neq q_1$ , тогда по пункту 6 леммы 1.1 получаем  $b \leq r_1 - r$  и в то же время  $r_1 - r \leq b - 1 < b$ . Получаем противоречие, поэтому  $q = q_1$ , следовательно, и  $r = r_1$ .  $\square$

## 2 Наименьшее общее кратное и наибольший общий делитель (НОК и НОД)

**Определение 2.0.**  $n \geq 2, a_1, \dots, a_n \in \mathbb{N}$  пусть натуральное число  $k$  делится на каждое из этих чисел. Тогда  $k$  - общее кратное чисел  $a_1, \dots, a_n$ .

Пусть  $a_1, \dots, a_n$  - целые числа не все равные нулю. Натуральное число  $d$  называется общим делителем  $a_1, \dots, a_n$ , если  $d$  делит каждое из этих чисел.

**Замечание.** Множество таких  $k$  непусто, в нем лежит, например, произведение всех этих чисел.

Множество таких  $d$  конечно: если  $a_i \neq 0$ , то  $d$  находится среди делителей числа  $a_i$ , (по пункту 6 леммы 1.1)  $d \leq |a_i|$ , значит числа  $d$  образуют конечное множество, оно непусто, так как содержит единицу.

**Определение 2.1.** Наименьшее натуральное число, делящееся на каждое из чисел  $a_1, \dots, a_n$ , называют их наименьшим общим кратным, его обозначают  $[a_1, \dots, a_n]$ .

**Теорема 2.1.** Каждое общее кратное натуральных чисел  $a_1, \dots, a_n$  делится на их НОК.

*Доказательство.* Пусть  $M$  - общее кратное  $a_1, \dots, a_n$ ,  $K = [a_1, \dots, a_n]$ . Поделим  $M$  на  $K$  с остатком:  $M = kq + r$ ,  $0 \leq r \leq k - 1 \leq k$ . Допустим, что  $K \neq 0$ . По определению, всякое число  $a_i$  делит оба числа  $M$  и  $K \Rightarrow a_i$  делит разность  $k = M - qK$ , значит  $k$  является общим кратным для  $a_1, \dots, a_n$ , но  $k < K$ , получаем противоречие, так как какое-то кратное оказалось меньше минимального. Значит,  $k = 0$  и  $M = qK$ .  $\square$

**Определение 2.2.** Наибольшее из натуральных чисел  $d$ , делящих каждое из чисел  $a_1, \dots, a_n$ , называют наибольшим общим делителем  $a_1, \dots, a_n$ , его обозначают  $(a_1, \dots, a_n)$ .

**Определение 2.3.** Числа  $a$  и  $b$  называется взаимно простыми, если  $(a, b) = 1$ . Числа  $a_1, \dots, a_n$  называются взаимно простыми в совокупности, если  $(a_1, \dots, a_n) = 1$ . Числа  $a_1, \dots, a_n$  попарно взаимно просты, если  $(a_i, a_j) = 1 \forall i, j : 1 \leq i < j \leq n$ .

**Теорема 2.2.**  $[a, b] \cdot (a, b) = ab, \forall a, b \in \mathbb{N}$ .

*Доказательство.*  $ab$  - общее кратное  $a$  и  $b$ . По теореме 2.1  $ab$  делится на  $[a, b]$ , то есть  $ab = c[a, b]$ , где  $c \geq 1$  - натуральное число. Покажем, что  $a$  и  $b$  делятся на  $c$ . Действительно,  $a = \frac{ab}{[a, b]} \cdot \frac{[a, b]}{b} = c \cdot \frac{[a, b]}{b}$ ,  $b = \frac{ab}{[a, b]} \cdot \frac{[a, b]}{a} = c \cdot \frac{[a, b]}{a}$ , но оба числа  $\frac{[a, b]}{a}$  и  $\frac{[a, b]}{b}$  - натуральные, значит  $c$  - общий делитель  $a$  и  $b$ . Пусть теперь  $d$  - произвольный общий делитель  $a$  и  $b$ , тогда  $\frac{ab}{d} = a \cdot \frac{b}{d}$ , то есть число  $\frac{ab}{d}$  делится нацело на каждое из чисел  $a$  и  $b$ . По теореме 2.1, оно делится на  $[a, b]$ , то есть  $\frac{ab}{d} = [a, b]m$ , где  $m \geq 1$  - натуральное число, но тогда  $\frac{ab}{[a, b]} = c = dm$ , то есть  $d$  делит  $c$ . В силу пункта 6 леммы 1.1  $d \leq c$ , значит  $c = (a, b)$ .  $\square$

**Теорема 2.3.** Пусть  $a, b, c \in \mathbb{N}$ , причем  $a \mid bc$  и  $(a, b) = 1$ , тогда  $a \mid c$ .

*Доказательство.*  $(a, b) = 1 \Rightarrow$  (по теореме 2.2)  $bc$  делится нацело на  $[a, b] = ab$ , то есть  $bc = abm$ , где  $m \geq 1$  - натуральное число. Сократим обе части на  $b$ , получим  $c = am$ .  $\square$

**Теорема 2.4.** Пусть  $\Delta = (a, b) \geq 1 \Rightarrow (\frac{a}{\Delta}, \frac{b}{\Delta}) = 1$ .

*Доказательство.* Пусть  $m \in \mathbb{N}$  и  $m \mid \frac{a}{\Delta}, m \mid \frac{b}{\Delta}$  предположим, что  $m > 1 \Rightarrow cm = \frac{a}{\Delta}, dm = \frac{b}{\Delta} \Rightarrow \Delta cm = a, \Delta dm = b \Rightarrow \Delta m \mid a$  и  $\Delta m \mid b \Rightarrow \Delta m$  - общий делитель  $a$  и  $b$ . Но т.к.  $m > 1$ , то  $\Delta m > \Delta \Rightarrow \Delta = (a, b) \leq \Delta m$  - противоречие, поскольку  $\Delta$  - НОД  $\Rightarrow m = 1 \Rightarrow (\frac{a}{\Delta}, \frac{b}{\Delta}) = 1$ .  $\square$

### 3 Алгоритм Евклида

**Лемма 3.1.** Пусть  $a \in \mathbb{Z}, b \in \mathbb{N}$  и  $b \mid a$ . Тогда  $(a, b) = b$ .

*Доказательство.* Пусть  $(a, b) = c \Rightarrow c \mid b \Rightarrow$  (по лемме 1.1)  $c \leq b$ , но  $b \mid a, b \mid b \Rightarrow b$  - общий делитель  $a$  и  $b \Rightarrow b \leq c \Rightarrow b = c = (a, b)$ .  $\square$

**Лемма 3.2.** Пусть  $a \in \mathbb{Z}, b \in \mathbb{N}, a = bq + r : r, q \in \mathbb{Z}, r \geq 0$ . Тогда  $(a, b) = (b, r)$ .

*Доказательство.* Пусть  $\Delta = (a, b), \delta = (b, r)$ . Имеем  $\delta \mid b \Rightarrow \delta \mid bq, \delta \mid r \Rightarrow$  (лемма 1.1)  $\delta \mid bq + r = a \Rightarrow \delta \mid a, \delta \mid b \Rightarrow \delta$  - общий делитель  $a$  и  $b \Rightarrow \delta \leq \Delta$ .  $\Delta \mid b, \Delta \mid bq, \Delta \mid a \Rightarrow$  (лемма 1.1)  $\Delta \mid a - bq = r \Rightarrow \Delta$  - общий делитель  $b$  и  $r \Rightarrow \Delta \leq \delta \Rightarrow \Delta = \delta$ .  $\square$

**Алгоритм.** Получаем, что при поиске НОД  $a$  и  $b, (a, b)$  можно заменять любой парой  $(b, r) = (b, a - bq), q \in \mathbb{Z}$ . Положим  $r_0 = a, r_1 = b$ .

Выполняем деление с остатком:

$$r_0 = r_1 q_1 + r_2, 0 < r_2 < r_1 \Rightarrow (r_0, r_1) = (r_1, r_2)$$

$$r_1 = r_2 q_2 + r_3, 0 < r_3 < r_2 \Rightarrow (r_1, r_2) = (r_2, r_3)$$

$$r_2 = r_3 q_3 + r_4, 0 < r_4 < r_3 \Rightarrow (r_2, r_3) = (r_3, r_4)$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n, 0 < r_n < r_{n-1} \Rightarrow (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n)$$

$$r_{n-1} = r_n q_n$$

$$\Rightarrow (\text{лемма 3.1}) (r_{n-1}, r_n) = r_n \Rightarrow (a, b) = r_n$$

### 4 Решение в целых числах линейного уравнения с двумя неизвестными

Рассмотрим уравнение  $(*) ax + by = c$ , такое, что  $a, b, c \in \mathbb{Z}, a$  и  $b$  не равняются нулю одновременно.  $x, y \in \mathbb{Z}$  - неизвестные.

**Теорема 4.1.** (1) Уравнение  $(*)$  разрешимо  $\Leftrightarrow \Delta = (a, b) \mid c$ .

(2) В случае разрешимости, множество решений этого уравнения бесконечно, все решения имеют вид  $x = x_0 + \frac{b}{\Delta}t, y = y_0 - \frac{a}{\Delta}t$ , где  $x_0, y_0$  - произвольное решение, а  $t \in \mathbb{Z}$ .

*Доказательство.* Докажем первый пункт:

$(\Rightarrow)$  Если  $x, y$  - решение, то  $\Delta \mid ax, \Delta \mid by \Rightarrow$  (лемма 1.1)  $\Delta \mid ax + by \Rightarrow \Delta \mid c$ .

$(\Leftarrow)$  Не теряя общности, можем считать, что  $a \geq b \geq 0$ . Доказываем индукцией по сумме  $a + b$ .

База:  $a + b = 1 \Rightarrow b = 0$  и  $a = 1 \Rightarrow$  уравнение имеет вид  $ax = c \Rightarrow x = c$ .

Можем предъявить решение  $x = c, y = 0$ . В этом случае  $\Delta = (1, 0) \mid 1$ .

Шаг:  $n \geq 1$ , считаем, что утверждение доказано для всех уравнений с условием  $a \geq b \geq 0, 1 \leq a + b \leq n$ . Пусть  $ax + by = c$ , где  $a \geq b \geq 0$ ,

$a + b = n + 1$  и  $\Delta = (a, b) \mid c \Rightarrow$  докажем, что есть хотя бы одно решение.

Пусть  $b = 0, ax = c, \Delta = (a, 0) = a, a \mid c \Rightarrow c = at \Rightarrow x = t, y = 0$  -

решение. Пусть  $b \geq 1$ . Рассмотрим уравнение  $(a - b)X + bY = c$ ,

$a - b \geq 0, b \geq 1 > 0. (a - b) + b = (a + b) - b = n + 1 - b \leq n. (a - b, b) = (a, b) \mid c$

$\Rightarrow$  по предположению индукции есть целочисленное решение  $X_0, Y_0$ .

$(a - b)X_0 + bY_0 = c \Rightarrow aX_0 - b(Y_0 - X_0) = c \Rightarrow x = X_0, y = Y_0 - X_0$  - решение.

Докажем второй пункт (проверим, что  $x_0, y_0$  - решение):

$a(x_0 + \frac{b}{\Delta}t) + b(y_0 - \frac{a}{\Delta}t) = ax_0 + \frac{ab}{\Delta}t + ay_0 - \frac{ab}{\Delta}t = ax_0 + by_0 = c$ . Обратно: пусть  $x_0, y_0$  и  $x, y$  - различные решения.  $ax_0 + by_0 = c, ax + by = c$

$\Rightarrow a(x - x_0) + b(y - y_0) = 0 \Rightarrow a(x - x_0) = b(y_0 - y). \Delta = (a, b)$

$\Rightarrow a = \alpha\Delta, b = \beta\Delta \Rightarrow$  (теорема 2.4)  $(\alpha, \beta) = 1$

$\Rightarrow \alpha\Delta(x - x_0) = \beta\Delta(y_0 - y) \Rightarrow \alpha(x - x_0) = \beta(y_0 - y)$

$\Rightarrow \alpha \mid \beta(y_0 - y) \Rightarrow \alpha \mid (y_0 - y) \Rightarrow y_0 - y = \alpha t \Rightarrow \alpha(x - x_0) = \beta\alpha t$

$\Rightarrow x - x_0 = \beta t.$

□

## 5 Простые числа

**Определение 5.1.** Натуральное число  $n > 1$  называется простым, если оно имеет ровно два делителя: 1 и  $n$ . В противном случае это число называется составным.

**Замечание.** Единица не причисляется ни к простым, ни к составным.

**Лемма 5.1.** Наименьший делитель натурального числа  $n > 1$ , отличный от единицы - простое число.

*Доказательство.* Пусть  $d \mid n, 1 < d \leq n$ , и  $d$  - наименьший с этими свойствами. Пусть  $d$  - составное. Тогда  $\exists k : k \mid d$  и  $1 < k < d$ . По лемме 1.1  $k \mid n$ , но  $1 < k < d$  - противоречие с тем, что  $d$  - минимальный.  $\square$

**Теорема 5.1.** Множество простых чисел бесконечно.

*Доказательство.* Пусть множество простых конечно:  $p_1 < p_2 < \dots < p_n$  - все простые числа. Рассмотрим число  $N = p_1 p_2 \dots p_n + 1$ . По лемме 5.1 наименьший делитель  $p > 1$  числа  $N$  - простое число. Но  $p$  отлично от  $p_1 \dots p_n$ ,  $p$  делит  $N$  нацело, а  $N$  при делении на каждое из  $p_1 \dots p_n$  дает остаток 1 - противоречие.  $\square$

Пусть  $x > 0$ , через  $\pi(x)$  обозначим количество простых чисел на отрезке  $[0, x]$  ( $\pi(x)$  - количество простых чисел не превосходящих  $x$ ).

$$\pi(x) = \sum_{p \leq x} 1$$

(Теорема 5.1)  $\Leftrightarrow \pi(x)$  - не ограничена сверху  $\Leftrightarrow \pi(x) \rightarrow +\infty$  при  $x \rightarrow +\infty$ .

Гипотеза Лежандра:  $\pi(x) = \frac{x}{\ln x - C}$ , где  $C = 1,08366$ . Позднее Гаусс выдвинет более сложное и более точное предположение. Из доказательства теоремы Чебышева:  $\forall \varepsilon > 0 \exists x_0 = x_0(\varepsilon)$ , т.ч.  $\forall x \geq x_0$  выполнено неравенство:

$$(A - \varepsilon) \frac{x}{\ln x} < \pi(x) < (B + \varepsilon) \frac{x}{\ln x}$$

$$A = \ln\left(\frac{2^{\frac{1}{2}} 3^{\frac{1}{3}} 5^{\frac{1}{5}}}{30^{\frac{1}{30}}}\right), B = \frac{6}{5}A$$

Асимптотический закон распределения простых чисел:

$$\lim_{x \rightarrow +\infty} \left( \frac{\pi(x)}{\frac{x}{\ln x}} \right) = 1 \Leftrightarrow A = B = 1 \Leftrightarrow \pi(x) = (1 + \bar{o}(1)) \frac{x}{\ln x}$$

**Лемма 5.2.** Пусть  $N$  - составное число,  $p$  - наименьший простой делитель. Тогда  $p \leq \sqrt{N}$ .

*Доказательство.*  $N$  - составное  $\Rightarrow \exists a, b : 1 < a < N, 1 < b < N$  и  $ab = N$ . Значит  $a \mid N, b \mid N, p$  - наименьший  $\Rightarrow p \leq a, p \leq b \Rightarrow p^2 \leq ab = N \Rightarrow p \leq \sqrt{N}$ .  $\square$



**Решето Эратосфена.** Выписываем все числа от 2 до  $N$ , первое число в таблице - простое, это 2. Вычеркиваем все числа кратные 2, кроме нее самой. Первое невычеркнутое число после 2 - это 3 - значит оно простое. Вычеркиваем все числа, кратные 3, кроме самой 3. Первое невычеркнутое число после 3 - простое и т.д. После того как найдено наибольшее простое  $p$  не превосходящее  $\sqrt{N}$  и вычеркнуты все числа кратные  $p$ , в таблице останутся лишь простые числа, не превосходящие  $N$  и только они.

**Теорема 5.2.** (Основная теорема арифметики)

Каждое целое число, большее 1, раскладывается в произведение простых чисел, притом единственным способом (с точностью до порядка сомножителей).

*Доказательство.* Существование:

Индукция по  $n > 1$ . Числа  $n = 2, n = 3$  - простые, для них это утверждение справедливо. Пусть  $n > 3$ , и допустим, что справедливость утверждения проверена для всех  $m < n$ . Если  $n$  - простое, то утверждение очевидно. Пусть  $n$  - составное. По лемме 5.1 его наименьший делитель - простое число  $\Rightarrow n = p_1 k$ , но  $k = \frac{n}{p_1} \leq \frac{n}{2} < n$ . По предположению индукции  $k = p_2 \dots p_r$ , где  $p_2, \dots, p_r$  - простые.  $\Rightarrow n = p_1 k = p_1 p_2 \dots p_r$  - искомое разложение.

Единственность:

Пусть  $n = p_1 \dots p_r = q_1 \dots q_s$ , где  $p_i, q_i$  - простые числа и  $r \leq s$ . Тогда

$p_1 \dots p_r = q_1 a_1$ , где  $a_1 = q_2 \dots q_s \Rightarrow p_1 \mid q_1 a_1$ . Возможно два случая:

1)  $(p, q) > 1 \Rightarrow p_1 = q_1$ .

2)  $(p, q) = 1 \Rightarrow$  (теорема 2.3)  $p_1 \mid a_1 = q_2 \dots q_s, a_1 = q_2 a_2, a_2 = q_3 \dots q_s$ ,

$p_1 \mid q_2 a_2 \Rightarrow$  либо  $p_1 = q_2$ , либо  $p_1 \mid a_2$  и т.д. Но  $a_1 > a_2 > \dots \geq 1 \Rightarrow$  на одном из шагов обязательно будет иметь место равенство  $p_1 = q_k, k \leq s$  (иначе оказалось бы, что  $p_1 \mid 1$ , а это невозможно). Итак,  $p_1$  совпадает с одним из чисел  $q_1, \dots, q_s$ .

Будем считать, что  $p_1 = q_1 \Rightarrow p_2 \dots p_r = q_2 \dots q_s$  продолжаем рассуждение и получаем, что  $p_2$  совпадает с одним из  $q_2, \dots, q_s$ , пусть  $p_2 = q_2$  и т.д. Если  $r < s$  после  $r$  шагов получили бы противоречивое равенство:  $1 = q_{r+1} \dots q_s \Rightarrow r = s$  и множества  $\{p_1, \dots, p_r\}$  и  $\{q_1, \dots, q_s\}$  совпадают.  $\square$

**Замечание.**  $n > 1, n = q_1 \dots q_s \Rightarrow n$  можно записать в виде  $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ ,  $p_1 < p_2 < \dots < p_k$  - каноническое разложение  $n$  на простые сомножители.

**Определение 5.2.** Пусть  $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, p$  - простое. Тогда

$$\nu_p(n) = \begin{cases} 0, & \text{если } p \nmid n, \\ \alpha, & \text{если } p = p_i. \end{cases}$$

**Лемма 5.3.** (Свойства  $\nu_p(n)$ )

1. Для любых целых чисел  $a, b > 1$  и любого простого  $p$  справедливо равенство:  $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ .
2. Пусть  $m, n > 1$  - целые числа, тогда  $m \mid n \Leftrightarrow \nu_p(m) \leq \nu_p(n)$  для любого простого  $p$ .

*Доказательство.*

1. При перемножении степеней с одинаковыми основаниями, их показатели складываются.
2. ( $\Rightarrow$ ) Пусть  $n = km \Rightarrow \nu_p(n) = \nu_p(k) + \nu_p(m) \geq \nu_p(m)$ .  
 ( $\Leftarrow$ ) Все разности  $\nu_p(n) - \nu_p(m)$  - целые неотрицательные. Рассмотрим число:

$$k = \prod_p p^{\nu_p(n) - \nu_p(m)}$$

Если  $k = 1$ , то  $\nu_p(n) = \nu_p(m)$  для всех  $p$  и  $m = n$ . В силу основной теоремы арифметики, в этом случае  $m \mid n$ . Пусть  $k > 1$ , тогда в силу пункта 1:

$$km = \prod_p p^{\nu_p(n) - \nu_p(m)} \cdot \prod_p p^{\nu_p(m)} = \prod_p p^{\nu_p(n)} = n$$

то есть  $m \mid n$ .

□

**Лемма 5.4.** Для любых  $a, b \in \mathbb{N}$  справедливы равенства:

$$[a, b] = \prod_p p^{\max(\nu_p(a), \nu_p(b))}$$

$$(a, b) = \prod_p p^{\min(\nu_p(a), \nu_p(b))}$$

*Доказательство.* Обозначим  $K = [a, b]$ ,  $N = \prod_p p^{\max(\nu_p(a), \nu_p(b))}$  поскольку

$\nu_p(a) \leq \nu_p(N)$ ,  $\nu_p(b) \leq \nu_p(N)$ , то  $a$  и  $b$  делят  $N$  в силу леммы 5.3. Значит  $N$  - общее кратное чисел  $a$  и  $b$ . С другой стороны, поскольку  $a$  и  $b$  делят  $K$ , то по лемме 5.3 имеем  $\nu_p(a) \leq \nu_p(K)$ ,  $\nu_p(b) \leq \nu_p(K)$ , так что  $\nu_p(K) \geq \max(\nu_p(a), \nu_p(b)) = \nu_p(N)$  для любого простого  $p$ . Значит,  $N \mid K$ , но  $N \leq K \Rightarrow N = K$ . Вторая часть утверждения следует из первой, если воспользоваться равенством

$$(a, b) = \frac{ab}{[a, b]}$$

и тем, что  $x + y = \max(x, y) + \min(x, y) \forall x, y \in \mathbb{R}$ .

□

## 6 Мультипликативные функции

Обозначения и пояснения:

1. Обозначение  $\sum_{d|n} f(d)$  - сумма значений функции  $f$  по всем делителям  $d$  числа  $n$ .
2. Двойная сумма вычисляется следующим образом:

$$\sum_{m=1}^M \sum_{n=1}^N g(mn) = \sum_{n=1}^N g(1, n) + \sum_{n=1}^N g(2, n) + \dots + \sum_{n=1}^N g(M, n)$$

**Определение 6.1.** Функция  $f$ , определенная на множестве  $\mathbb{N}$  называется мультипликативной, если для любых взаимно простых  $a, b \in \mathbb{N}$  выполнено равенство:

$$f(ab) = f(a)f(b)$$

**Теорема 6.1.** (Простейшие свойства мультипликативных функций)

Пусть  $f, g$  - мультипликативные функции. Тогда:

1. Если  $f \not\equiv 0$ , то  $f(1) = 1$ .
2. Если  $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$  - каноническое разложение  $n$ , то  $f(n) = f(p_1^{\alpha_1}) \dots f(p_r^{\alpha_r})$ .
3. Функция  $h$ , определенная для любого  $n \in \mathbb{N}$  равенством  $h(n) = f(n)g(n)$  - мультипликативна.

*Доказательство.* 1. Так как  $f \not\equiv 0$ , то  $\exists a \in \mathbb{N} : f(a) \neq 0$ . Тогда  $f(a) = f(a \cdot 1) = f(a)f(1) \Rightarrow f(1) = 1$ .

2. 3. Напрямую следует из определения.

□

Для исследования дальнейших свойств мультипликативных функций потребуются несколько вспомогательных лемм

**Лемма 6.1.** Пусть  $p$  - простое число,  $r \geq 2$  и пусть целые числа  $a_1, \dots, a_r$  попарно взаимно просты, причем  $p \mid a_1 \dots a_r$ . Тогда найдется номер  $1 \leq s \leq r$  такой, что  $p \mid a_s$ .

*Доказательство.* Индукция по  $r$ . Если  $r = 2$ , то это есть очевидно следствие теоремы 2.3. Пусть  $m \geq 3$  и утверждение доказано для всех  $r \leq m - 1$ . Пусть  $a_1, \dots, a_m$  попарно взаимно просты и  $p \mid a_1 \dots a_m$ . Полагая  $a = a_1 \dots a_{m-1}$

будем иметь:  $p \mid aa_m$ . Если  $(p, a) = 1$ , то  $p \mid a_m$  по теореме 2.3. Пусть  $(p, a) > 1$ . Так как  $p$  - простое, то  $(p, a) = p$  и  $p$  делит некоторый сомножитель  $a_s$  :  
 $1 \leq s \leq m - 1$ . □

**Лемма 6.2.** Пусть  $b \mid a$  и  $c \mid a$ , причем  $(b, c) = 1$ . Тогда  $bc \mid a$ .

*Доказательство.* Из условия следует, что  $a$  - общее кратное  $b$  и  $c$ . По теореме 2.1  $a$  делится на  $[b, c]$ , по теореме 2.2  $[b, c] = bc$ . □

**Следствие.** Пусть  $r \geq 2$ , и пусть целые числа  $b_1 \dots b_r$  попарно взаимно просты, причем  $b_1 \mid a, \dots, b_r \mid a$ . Тогда  $b_1 \dots b_r \mid a$ .

*Доказательство.* Индукция по  $r$ . Если  $r = 2$ , получаем утверждение леммы. Пусть  $m \geq 3$  и утверждение доказано для всех  $r \leq m - 1$ . Пусть  $b_1, \dots, b_m$  попарно взаимно просты и каждое из них делит  $a$ . В силу предложения индукции,  $a$  делится на произведение  $b = b_1 \dots b_{m-1}$ . Заметим, что  $(b, b_m) = 1$ . Действительно, в противном случае найдется простое число  $p$ , делящееся как на  $b_m$  так и на  $b$ . По лемме 6.1  $p$  будет делить и некоторые  $b_\xi : 1 \leq \xi \leq m - 1$ . Следовательно  $(b_m, b_\xi) \geq p > 1$ , что противоречит условию. Так как  $a$  делится на  $b$  и  $b_m$ , и  $(b, b_m) = 1$ , то в силу леммы 6.2  $a$  делится на  $bb_m = b_1 \dots b_m$ . □

**Лемма 6.3.** Пусть числа  $a$  и  $b$  взаимно просты, и пусть  $d_1$  и  $d_2$  пробегают соответственно множества всех делителей  $a$  и  $b$ . Тогда величина  $d = d_1 d_2$  пробегает без повторений всё множество делителей числа  $ab$ .

*Доказательство.*

1. Если  $d_1 \mid a$ ,  $d_2 \mid b$ , то  $a = kd_1$ ,  $b = md_2$  при некоторых  $k, m \in \mathbb{Z}$ , так что  $ab = kmd_1 d_2$ , то есть  $d_1 d_2$  - делитель  $ab$ .
2. Допустим, что  $d_1 d_2 = \delta_1 \delta_2$  для некоторых чисел  $d_1, \delta_1$  делящих  $a$  и некоторых чисел  $d_2, \delta_2$ , делящих  $b$ . Очевидно, что  $(d_1, \delta_2) = 1$ , так как в противном случае нашлось бы простое  $p$ , делящееся одновременно и  $a$  и  $b$ , что невозможно. Но  $d_1 \mid \delta_1 \delta_2$  по теореме 2.3  $d_1 \mid \delta_1$  и, следовательно  $d_1 \leq \delta_1$ . Аналогично доказывается, что  $\delta_1 \mid d_1$  и  $\delta_1 \leq d_1$ . Значит  $d_1 = \delta_1, d_2 = \delta_2$ , то есть все произведения  $d_1$  и  $d_2$  различны.
3. Докажем, наконец, что всякий делитель  $d$  числа  $ab$  встретится среди произведений  $d_1 d_2$ . Если  $d = 1$ , то это очевидно. Пусть  $d \geq 2$  и  $p_1^{\alpha_1} \dots p_r^{\alpha_r}$  - каноническое разложение  $d$ . Число  $q_1 = p_1^{\alpha_1} \mid ab$ . Из теоремы 2.3 следует, что  $q_1$  делит либо  $a$ , либо  $b$  (но не оба сразу). То же верно и для чисел  $q_\xi = p_\xi^{\alpha_\xi}, \xi = 2, 3, \dots, r$ . Пусть, для определенности,  $q_1, \dots, q_t$  - все

сомножители, делящие  $a$ , и  $q_{t+1}, \dots, q_r$  - все сомножители, делящие  $b$ . По следствию леммы 6.2 произведение  $d_1 = q_1 \dots q_t$  делит  $a$ , произведение  $d_2 = q_{t+1}, \dots, q_r$  делит  $b$ , но  $d_1 d_2 = d$ .

□

**Теорема 6.2.** Пусть функция  $f$  мультипликативна. Тогда функция  $F$ , определенная при любом  $n \in \mathbb{N}$  равенством:

$$F(n) = \sum_{d|n} f(d)$$

мультипликативна.

*Доказательство.* Пусть  $(a, b) = 1$ . По лемме 6.3, все делители  $ab$  получим без повторений, рассмотрев все произведения  $d = d_1 d_2$ , где  $d_1 \mid a$ ,  $d_2 \mid b$ . Значит

$$\begin{aligned} F(ab) &= \sum_{d|ab} f(d) = \sum_{d_1|a} \sum_{d_2|b} f(d_1 d_2) = \sum_{d_1|a} \sum_{d_2|b} f(d_1) f(d_2) = \\ &= \left( \sum_{d_1|a} f(d_1) \right) \left( \sum_{d_2|b} f(d_2) \right) = F(a) F(b). \end{aligned}$$

Взаимная простота  $d_1$  и  $d_2$  очевидна.

□

**Следствие.** Если  $p_1^{\alpha_1} \dots p_r^{\alpha_r}$  - каноническое разложение  $n$ , а  $F$  - функция из условия теоремы, то

$$F(n) = \prod_{i=1}^r (1 + f(p_i) + f(p_i^2) + \dots + f(p_i^{\alpha_i}))$$

(при условии что  $f \not\equiv 0$ ).

**Определение 6.2.** Функция Мебиуса  $\mu(n)$  определяется равенствами:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ делится на квадрат простого числа,} \\ (-1)^k, & \text{если } n = p_1 \dots p_k \text{ - различные простые числа.} \end{cases}$$

Примеры:  $\mu(2) = (-1)^1 = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = -1, \mu(6) = (-1)^2 = 1, \mu(7) = -1, \mu(8) = \mu(9) = 0, \mu(10) = (-1)^2 = 1$   $n = p_1 \dots p_k$ ,  $m = q_1 \dots q_r$ ,  $(m, n) = 1 \Rightarrow mn = p_1 \dots p_k q_1 \dots q_r \Rightarrow \mu(mn) = (-1)^{k+r} = (-1)^k (-1)^r = \mu(m) \mu(n)$ .  $p$  - простое  $\Rightarrow \mu(p) = -1, \mu(p^2) = 0, \mu(p^3) = 0, \dots$

**Теорема 6.3.** (Основное свойство функции Мебиуса)

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{во всех остальных случаях.} \end{cases}$$

*Доказательство.* Пусть  $F(n) = \sum_{d|n} \mu(d) \Rightarrow$  (По теореме 6.2)  $F$  - мультипликативна. Пусть  $p$  - простое,  $n = p^\alpha, \alpha \geq 1 \Rightarrow F(p^\alpha) = \sum_{d|p^\alpha} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^\alpha) = 1 - 1 = 0$ .  $\square$

**Определение 6.3.** Функция Эйлера  $\varphi(n)$  определяется для натурального  $n$  как количество чисел  $m$  с условиями  $1 \leq m \leq n$ , таких, что  $(m, n) = 1$

**Примеры.**  $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 1 + 1 + 0 = 2, \varphi(4) = 1 + 0 + 1 + 0 = 2, \varphi(5) = 1 + 1 + 1 + 1 + 0 = 4, \varphi(6) = 1 + 0 + 0 + 0 + 1 + 0 = 2$

**Теорема 6.4.** Функция Эйлера  $\varphi$  мультипликативна. Кроме того, если  $p_1, \dots, p_k$  - все различные делители  $n$ , тогда:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

*Доказательство.* Надо подсчитать число тех  $m$ , для которых  $(m, n) = 1$ . По теореме 6.3

$$\begin{aligned} \sum_{d|(m,n)} \mu(d) &= \begin{cases} 1, & \text{если } (m, n) = 1, \\ 0, & \text{иначе.} \end{cases} \\ \Rightarrow \varphi(n) &= \sum_{1 \leq m \leq n} \sum_{d|(m,n)} \mu(d) = \sum_{d|n} \mu(d) \sum_{d \leq m \leq n, d|m} 1 \\ 1 \leq m = kd &\leq n \Rightarrow 1 \leq k \leq \frac{n}{d} \\ \Rightarrow \sum_{d|n} \mu(d) \sum_{d \leq m \leq n, d|m} 1 &= \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d} \end{aligned}$$

Функции  $\mu(d)$  и  $\frac{1}{d}$  - мультипликативные  $\Rightarrow \frac{\mu(d)}{d}$  - мультипликативна  $\Rightarrow$  по теореме 6.2  $\Rightarrow \sum_{d|n} \frac{\mu(d)}{d}$  - мультипликативна  $\Rightarrow \varphi(n)$  - мультипликативна.

$n = p^\alpha, p$  - простое,  $\alpha \geq 1$

$$\begin{aligned} \Rightarrow \varphi(p^\alpha) &= p^\alpha \sum_{d|p^\alpha} \frac{\mu(d)}{d} = p^\alpha \left( \frac{\mu(1)}{1} + \frac{\mu(p)}{p} + \frac{\mu(p^2)}{p^2} + \dots + \frac{\mu(p^\alpha)}{p^\alpha} \right) = \\ &= p^\alpha \left( 1 + \frac{\mu(p)}{p} \right) = p^\alpha \left( 1 + \frac{1}{p} \right) \end{aligned}$$

$$\begin{aligned}
n = p_1^{\alpha_1} \dots p_k^{\alpha_k} &\Rightarrow \varphi(n) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) = \\
&= p_1^{\alpha_1} \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

□

**Теорема 6.5.** (Формула обращения Мебиуса) Пусть  $\forall n \geq 1$  функции  $f$  и  $g$  связаны соотношением

$$f(n) = \sum_{d|n} g(d) \quad (1)$$

Тогда  $\forall n \geq 1$  выполнено равенство

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \quad (2)$$

Обратно, если  $\forall n \geq 1$   $f$  и  $g$  связаны соотношением (2), то  $\forall n \geq 1$  верно (1).

*Доказательство.* ( $\Rightarrow$ ) Пусть выполнено (1), преобразуем величину

$$\begin{aligned}
\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{\delta|\frac{n}{d}} g(\delta) = \sum_{d\delta|n} \mu(d) g(\delta) = \sum_{\delta|n} g(\delta) \sum_{d|\frac{n}{\delta}} \mu(d) = \\
&= (\text{по теореме 6.3}) g(n).
\end{aligned}$$

Пояснение:

$$\sum_{d|\frac{n}{\delta}} \mu(d) = \begin{cases} 1, & \text{если } \frac{n}{\delta} = 1, \\ 0, & \text{если } \frac{n}{\delta} > 1. \end{cases} \Leftrightarrow \begin{cases} 1, & \text{если } n = \delta, \\ 0, & \text{если } n > \delta. \end{cases}$$

( $\Leftarrow$ ) Пусть есть (2), преобразуем

$$\begin{aligned}
\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \sum_{\delta|\frac{n}{d}} \mu(d) f\left(\frac{d}{\delta}\right) = \\
&= \sum_{\Delta\delta|n} \mu(\delta) f(\Delta) = \sum_{\Delta|n} f(\Delta) \sum_{\delta|\frac{n}{\Delta}} \mu(\delta) = (\text{по теореме 6.3}) f(n)
\end{aligned}$$

□

**Следствие.**

$$\sum_{d|n} \varphi(d) = n$$

*Доказательство.* Выше доказали, что

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

это равенство (2), где  $g(n) = \varphi(n)$ ,  $f(k) = k$ . По формуле обращения Мебиуса, для этих функций выполнено (1):  $f(n) = n = \sum_{d|n} g(n) = \sum_{d|n} \varphi(n)$   $\square$

**Определение 6.4.** Функция делителей  $\tau(n)$  определяется, как число делителей натурального  $n \geq 1$ .

$$\tau(n) = \sum_{d|n} 1.$$

**Замечание.**  $f(1) \equiv 1$  - мультипликативна  $\Rightarrow$  (по теореме 6.2)  $\tau(n)$  - мультипликативна.

**Утверждение 6.1.**  $n = p^\alpha$ ,  $p$  - простое.

$$\tau(p^\alpha) = \sum_{d|p^\alpha} 1 = \alpha + 1$$

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \Rightarrow \tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1).$$

**Определение 6.5.**  $\sigma(n)$  - сумма делителей числа  $n \geq 1$

$$\sigma(n) = \sum_{d|n} d$$

**Примеры.**  $\sigma(6) = 1 + 2 + 3 + 6 = 12$ ,  $p$  - простое  $\Rightarrow \sigma(p) = p + 1$ .

Из теоремы 6.2 следует мультипликативность  $\sigma(n)$ .

$$n = p^\alpha \Rightarrow \sigma = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

$$\text{Если } n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \Rightarrow \sigma(n) = \sigma(p_1^{\alpha_1}) \dots \sigma(p_k^{\alpha_k}) = \prod_{s=1}^r \frac{p_1^{\alpha_s+1} - 1}{p_s - 1} = \prod_{p^\alpha || n} \frac{p^{\alpha+1} - 1}{p - 1}$$

**Замечание.** Функции  $\tau(n)$  и  $\sigma(n)$  - частный случай функции  $\sigma_\beta(n)$ ,  $\beta$  - любое вещественное число.  $\sigma_\beta(n) \sum_{d|n} 1 = \tau(n)$ ,  $\sigma_1(n) = \sigma(n)$ .

Упражнение: Доказать, что  $\sigma(n) + \varphi(n) = n\tau(n)$  имеет место  $\Leftrightarrow n$  - простое.

**Определение 6.6.** Делитель  $d$  числа  $n$  называется собственным, если  $d < n$ .

**Определение 6.7.** Число  $n$  называется совершенным, если оно равно сумме своих собственных делителей:  $n = \sigma(n) - n \Leftrightarrow \sigma(n) = 2n$



**Примеры.**  $\sigma(6) = 12 = 6 \cdot 2$ ,  $\sigma(28) = 56 = 2 \cdot 28$ .

**Теорема 6.6.** (Эйлер)

Четное число является совершенным  $\Leftrightarrow$  когда оно имеет вид  $2^{p-1}(2^p - 1)$ , где  $p$  и  $2^p - 1$  - простые числа. (без доказательства)

Простые числа вида  $M_p = 2^p - 1$ , где  $p$  - простое, называются простыми Мерсена. Сейчас известно 51 простое число Мерсена. Самое большое из них отвечает простому  $p = 82589933$ . В записи  $M_p$  - 24862048 цифр. (результат получен 21.12.2018) Неизвестно, конечно или нет множество простых Мерсена. Гипотеза: если  $\pi_M(x)$  - число простых Мерсена не превосходящих  $x$ , то  $\pi_M(x) \approx \ln \ln x$ . Неизвестно, существуют или нет нечетные совершенные числа. Если  $N$  - нечетное совершенное число, то

(1)  $N > 10^{1500}$  (2012г.)

(2) Наибольший простой делитель  $N$  превосходит  $10^8$  (2008г.)

(3) Второй по величине простой делитель  $N$  превосходит  $10^4$  (1999г.)

(4) Пусть  $k \geq 1$ . Тогда имеется не более чем  $2^{4^k}$  несчетных совершенных чисел, имеющих ровно  $k$  различных простых делителей. (2003г.)

**Определение 6.8.** Числа  $a$  и  $b$  ( $1 < a < b$ ) называются дружественными, если (a)  $a$  есть сумма собственных делителей  $b$ , (b) число  $b$  - сумма собственных

делителей  $a$ : 
$$\begin{cases} \sigma(b) - b = a, \\ \sigma(a) - a = b. \end{cases} \Leftrightarrow \sigma(a) = \sigma(b) = a + b.$$

**Примеры.** (ЕЩЕ НЕ ГОТОВО)

Неизвестно, конечно или нет множество дружественных пар чисел. Сейчас известно 1229319267 таких пар. Пусть  $A(x)$  - число дружественных пар с  $a \leq x$ .  $\frac{A(x)}{x} \rightarrow 0$  при  $x \rightarrow \infty$  (П. Эрдеш 1955г.)

## 7 Непрерывные дроби

**Пример.** Заметим, что  $43 = 19 \cdot 2 + 5$ ,  $19 = 5 \cdot 3 + 4$ . Рассмотрим дробь:

$$\begin{aligned} \frac{a}{b} = \frac{19}{43} &= \frac{1}{\frac{43}{19}} = \frac{1}{2 \cdot 19 + 5} = \frac{1}{2 + \frac{5}{19}} = \frac{1}{2 + \frac{1}{\frac{19}{5}}} = \frac{1}{2 + \frac{1}{5 \cdot 3 + 4}} = \\ &= \frac{1}{2 + \frac{1}{3 + \frac{1}{\frac{5}{4}}}} = \frac{1}{2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}} \end{aligned}$$

**Определение 7.1.** Непрерывной (цепной) дробью будем называть выражение вида:

$$[q_0; q_1, q_2, \dots, q_n] = q_0 = \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_n}}}} \quad (*)$$

**Теорема 7.1.** Пусть  $a$  - целое,  $b$  - натуральное и пусть  $(a, b) = 1$ . Пусть кроме того,  $q_0, q_1, \dots, q_n$  - все неполные частные, возникающие при отыскании  $(a, b)$  с помощью алгоритма Евклида. Тогда число  $\alpha = \frac{a}{b}$  разлагается в непрерывную дробь вида  $(*)$ .

*Доказательство.* Доказательство следует из цепочки равенств:

$$\begin{aligned} a &= bq_0 + r_1, \\ b &= r_1q_1 + r_2, \\ r_1 &= r_2q_2 + r_3, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n \end{aligned}$$

Получаем:

$$\frac{a}{b} = q_0 + \frac{r_1}{b} = q_0 + \frac{1}{\frac{b}{r_1}} = q_0 + \frac{1}{q_1 + \frac{r_2}{r_1}} = q_0 + \frac{1}{q_1 + \frac{1}{\frac{r_1}{r_2}}} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}}} = \dots$$

Собирая полученные равенства вместе приходим к (\*). □

**Пример.**

$$a = 37, \quad b = 8,$$

$$37 = 8 \cdot 4 + 5,$$

$$8 = 5 \cdot 1 + 3,$$

$$5 = 3 \cdot 1 + 2, \quad \Rightarrow \alpha = \frac{37}{8} = [4; 1, 1, 1, 2].$$

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

$$2 = 1 \cdot 2.$$

**Определение 7.2.** Величины  $q_0, q_1, \dots, q_n$  в разложении числа  $\alpha = \frac{a}{b}$  из теоремы 7.1 называется неполным частным  $b$  в разложении  $\alpha$  в непрерывную дробь.

Дроби

$$\begin{aligned} \delta_0 &= q_0 \\ \delta_1 &= q_0 + \frac{1}{q_1} \\ \delta_2 &= q_0 + \frac{1}{q_1 + \frac{1}{q_2}} \\ &\vdots \end{aligned}$$

называются подходящими дробями.

**Пример.**

$$q_0 = 4, \quad q_1 = 1, \quad q_2 = 1, \quad q_3 = 1, \quad q_4 = 2.$$

Тогда

$$\begin{aligned} \delta_0 &= 4 \\ \delta_1 &= 4 + \frac{1}{1} = 5 \\ \delta_2 &= 4 + \frac{1}{1 + \frac{1}{1}} = 4 + \frac{1}{2} = \frac{9}{2} \end{aligned}$$

$$\delta_3 = 4 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = 4 + \frac{2}{3} = \frac{14}{3}$$

Пусть  $\alpha$  - число, не являющееся рациональным (такие числа будем называть иррациональными). Тогда для  $\alpha$  тоже можно построить разложение в непрерывную дробь. Это разложение будет бесконечным (в отличие от рационального  $\alpha = \frac{a}{b}$ ), поэтому такое построение требует определенной аккуратности и проводится в несколько шагов. На первом шаге строятся подходящие дроби, отвечающие числу  $\alpha$ , затем исследуются их свойства. В итоге доказывается сходимость последовательности подходящих дробей к числу  $\alpha$ , что и завершает построение.

Этап первый:

Определим целое  $q_0$  так, чтобы выполнялись неравенства:

$$q_0 < \alpha < q_0 + 1$$

и положим  $\alpha_0 = \alpha$ , так что

$$q_0 < \alpha_0 < q_0 + 1$$

но тогда  $\alpha_0 = q_0 + \beta_0$ , где  $0 < \beta_0 < 1$  и, следовательно,

$$\alpha_1 = \frac{1}{\beta_0} > 1$$

и

$$\alpha_0 = q_0 + \frac{1}{\alpha_1}$$

Число  $\alpha_1$ , очевидно, иррационально, определим по нему целое число  $q_1$  так, чтобы выполнялись неравенства:

$$q_1 < \alpha_1 < q_1 + 1$$

но  $\alpha_1 > 1$ , так что  $q_1 \geq 1$ , т.е.  $q_1$  - натуральное. Далее

$$\alpha_1 = q_1 + \beta_1$$

где  $0 < \beta_1 < 1$  и следовательно

$$\alpha_2 = \frac{1}{\beta_1} > 1, \quad \alpha_1 = q_1 + \frac{1}{\alpha_2}, \quad \alpha_0 = q_0 + \frac{1}{q_1 + \frac{1}{\alpha_2}}$$

Число  $\alpha_2$  также иррационально. Повторяя это процесс далее, получим бесконечные последовательности иррациональных чисел  $\alpha_1, \alpha_2, \dots, \alpha_\xi, \dots$  (причем  $\alpha_\xi > 1$  для всех  $\xi$ ) и натуральных чисел  $q_1, \dots, q_\xi$  таких, что

$$q_\xi = [\alpha_\xi] \text{ и } \alpha_\xi = q_\xi + \frac{1}{\alpha_\xi + 1}$$

Величины  $q_0, q_1, q_2, \dots$  станем называть неполными частными разложения  $\alpha$  в непрерывную дробь. Несложно видеть, что при любом  $\xi$  справедливо равенство

$$\alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_{\xi-1} + \frac{1}{\alpha_\xi}}}}}$$

Определим по этим числам последовательность подходящих дробей  $\delta_\xi$ ,  $\xi = 0, 1, \dots$  равенствами

$$\delta_0 = q_0, \quad \delta_1 = q_0 + \frac{1}{q_1}, \quad \delta_2 = q_0 + \frac{1}{q_1 + \frac{1}{q_2}}, \quad \dots$$

$$\delta_\xi = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_{\xi-1} + \frac{1}{\alpha_\xi}}}}}$$

Выпишем первые три такие дроби:

$$\delta_0 = q_0, \quad \delta_1 = \frac{q_0 q_1 + 1}{q_1}, \quad \delta_2 = \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1}$$

обозначим их еще так:

$$\delta_0 = \frac{P_0}{Q_0}, \text{ где } P_0 = q_0, \quad Q_0 = 1$$

$$\delta_1 = \frac{P_1}{Q_1}, \text{ где } P_1 = q_0 q_1 + 1, \quad Q_1 = q_1$$

$$\delta_2 = \frac{P_2}{Q_2}, \text{ где } P_2 = q_0 q_1 q_2 + 1, \quad Q_2 = q_1 q_2 + 1$$

посмотрим как эти величины связаны между собой:

$$P_1 = q_1 P_0 + 1, \quad Q_1 = q_1 Q_0 + 0$$

$$P_2 = q_2(q_0 q_1 + 1) + q_0 = q_2 P_1 + P_0, \quad Q_2 = q_2 Q_1 + Q_0$$

Введем (формально) величины  $P_{(-1)} = 1, Q_{(-1)} = 0$  (к подходящим дробям они не имеют отношения: выражение  $\frac{P_{(-1)}}{Q_{(-1)}} = \frac{1}{0}$  не определено)

Тогда равенства для  $P_1, Q_1, P_2, Q_2$  запишутся единообразно:

$$P_\xi = q_\xi P_{\xi-1} + P_{\xi-2}, \quad Q_\xi = q_\xi Q_{\xi-1} + Q_{\xi-2} \quad (\xi = 1, 2)$$

Оказывается, эти соотношения верны и для всех  $\xi \geq 3$ . Чтобы аккуратно доказать их поступим следующим образом. Этап второй:

Пусть даны переменные  $x_0, x_1, x_2, \dots, x_\xi, \dots$  произвольной природы (не обязательно целые числа). Рассмотрим величины  $P_\xi$  и  $Q_\xi$ , определенные рекуррентными соотношениями

$$\begin{cases} P_\xi = x_\xi P_{\xi-1} + P_{\xi-2} \\ Q_\xi = x_\xi Q_{\xi-1} + Q_{\xi-2} \end{cases} \quad (3)$$

ясно, что  $P_\xi$  и  $Q_\xi$  - некоторые многочлены от переменных  $x_1, \dots, x_\xi, \dots$ , например:  $P_3 - x_3 P_2 + P_1 = x_3(x_0 x_1 x_2 + x_0 + x_2) + x_0 x_1 + 1 = x_0 x_1 x_2 x_3 + x_0 x_1 + x_0 x_3 + x_2 x_3 + 1$ , положим также  $h_\xi = P_\xi Q_{\xi-1} - P_{\xi-1} Q_\xi$ .

**Лемма 7.1.** При любом  $\xi \geq 0$  справедливо равенство:  $h_\xi = (-1)^{\xi-1}$

*Доказательство.* Индукция по  $\xi$ . В случае  $\xi = 0$  имеем:

$$h_0 = P_0 Q_{(-1)} - P_{(-1)} Q_0 = -P_{(-1)} Q_0 = -1 = (-1)^{0-1}$$

Пусть соотношение доказано для всех  $\xi \leq m$ . Тогда

$$\begin{aligned} h_{m+1} &= P_{m+1} Q_m - P_m Q_{m+1} = (x_{m+1} P_m + P_{m-1}) Q_m - P_m (x_{m+1} Q_m + Q_{m-1}) = \\ &= x_{m+1} (P_m Q_m - P_m Q_m) + P_{m-1} Q_m - P_m Q_{m-1} = -h_m = -(-1)^{m-1} = (-1)^m \end{aligned}$$

□

**Лемма 7.2.** Если  $x_0 = q_0, x_1 = q_1, x_\xi = q_\xi$  - целые числа, а величины  $P_\xi$  и  $Q_\xi$  определены в (3) то справедливы равенства

$$(P_\xi, Q_\xi) = (P_\xi, P_{\xi-1}) = (Q_\xi, Q_{\xi-1}) = 1$$

*Доказательство.* Сразу следует из леммы 7.1. □

**Лемма 7.3.** Пусть  $x_1, \dots, x_\xi, \dots$  - произвольные переменные, и пусть выражения  $\Delta_0, \dots, \Delta_\xi, \dots$  зависящие от  $x_1, \dots, x_\xi, \dots$  определяются следующим образом:  $\Delta_0 = x_0$ , а при  $\xi \geq 1$  выражение для  $\Delta_\xi$  получим заменив в выражении для  $\Delta_{\xi-1}$   $x_{\xi-1}$  на  $x_{\xi-1} + \frac{1}{x_\xi}$ , так что, например,

$$\Delta_1 = x_0 + \frac{1}{x_1}, \quad \Delta_2 = x_0 + \frac{1}{x_1 + \frac{1}{x_2}}, \quad \Delta_3 = x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3}}}$$

тогда при любом  $\xi \geq 0$  справедливо равенство  $\Delta_\xi = \frac{P_\xi}{Q_\xi}$ , где  $P$  и  $Q$  определены соотношениями (3)

*Доказательство.* Индукция по  $\xi$ . В случае  $\xi = 0, 1$  эти соотношения фактически были проверены ранее. Пусть они верны для всех  $\xi \leq m$ . Тогда

$$\Delta_\xi = \frac{P_m}{Q_m} = \frac{x_m P_{m-1} + P_{m-2}}{x_m Q_{m-1} + Q_{m-2}}$$

по определению,  $\Delta_{m+1}$  получим из  $\Delta_m$  заменой  $x_m$  на  $x_m + \frac{1}{x_{m+1}}$  переменная  $x_m$ , очевидно не входит в выражения для  $P_{m-1}, P_{m-2}, Q_{m-1}, Q_{m-2}$ . Следовательно

$$\begin{aligned} \Delta_{m+1} &= \frac{(x_m + \frac{1}{x_{m+1}})P_{m-1} + P_{m-2}}{(x_m + \frac{1}{x_{m+1}})Q_{m-1} + Q_{m-2}} = \frac{(x_{m+1}x_m + 1)P_{m-1} + x_{m-1}P_{m-2}}{(x_{m+1}x_m + 1)Q_{m-1} + x_{m-1}Q_{m-2}} = \\ &= \frac{x_{m+1}(x_m P_{m-1} + P_{m-2}) + P_{m-1}}{x_{m+1}(x_m Q_{m-1} + Q_{m-2}) + Q_{m-1}} = \frac{x_{m+1}P_m + P_{m-1}}{x_{m+1}Q_m + Q_{m-1}} \end{aligned}$$

но числитель и знаменатель последней дроби совпадают в силу (3) с  $P_{m+1}$  и  $Q_{m+1}$  □

**Теорема 7.2.** Пусть  $\alpha$  - произвольное вещественное число, и пусть  $q_0, q_1, \dots$  - конечная или бесконечная последовательность неполных частных разложения  $\alpha$  в непрерывную дробь. Тогда подходящие дроби  $\delta_\xi$ ,  $\xi = 0, 1, \dots$ , отвечающие такому разложению, вычисляются по формулам

$$\delta_\xi = \frac{P_\xi}{Q_\xi} \tag{4}$$

где величины  $P_\xi$  и  $Q_\xi$  определяются следующими рекуррентными соотношениями:  $P_\xi = q_\xi P_{\xi-1} + P_{\xi-2}$ ,  $Q_\xi = q_\xi Q_{\xi-1} + Q_{\xi-2}$  с начальными условиями  $P_{(-1)} = 1$ ,  $Q_{(-1)} = 0$ ,  $P_0 = q_0$ ,  $Q_0 = 1$ . Все дроби (4) при этом несократимы.

*Доказательство.* Равенство (4) есть прямое следствие леммы 7.1 □

Если  $\alpha \notin \mathbb{Q} \Rightarrow q_0, q_1, q_2, \dots, \delta_\xi = \frac{P_\xi}{Q_\xi}$ . Осталось непонятным какое отношение имеют дроби  $\delta_\xi$  к числу  $\alpha$ .

Этап третий:

**Лемма 7.4.** При любом  $\xi \geq 1$  верны неравенства:  $\delta_{2\xi} > \delta_{2\xi-2}$  ( $\delta_{2\xi+1} < \delta_{2\xi-1}$ ) то есть подходящие дроби с четными (нечетными) номерами образуют монотонно возрастающую (убывающую последовательность).

*Доказательство.*

$$\begin{aligned} \delta_k - \delta_{k-1} &= \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k Q_{k-1} - P_{k-1} Q_k}{Q_k Q_{k-1}} = (\text{по лемме 7.1}) \\ &= \frac{h_k}{Q_k Q_{k-1}} = \frac{(-1)^{k-1}}{Q_k Q_{k-1}} \end{aligned}$$

тогда

$$\begin{aligned} \delta_{2\xi} - \delta_{2\xi-2} &= (\delta_{2\xi} - \delta_{2\xi-1}) + (\delta_{2\xi-1} - \delta_{2\xi-2}) = \frac{(-1)^{2\xi-1}}{Q_{2\xi} Q_{2\xi-1}} + \frac{(-1)^{2\xi-2}}{Q_{2\xi-1} Q_{2\xi-2}} = \\ &= \frac{1}{Q_{2\xi-1}} \left( \frac{1}{Q_{2\xi-2}} - \frac{1}{Q_{2\xi}} \right) = \frac{Q_{2\xi} - Q_{2\xi-2}}{Q_{2\xi} Q_{2\xi-1} Q_{2\xi-2}} = (Q_{2\xi} = q_{2\xi} Q_{2\xi-1} + Q_{2\xi-2}) \\ &= \frac{q_{2\xi} Q_{2\xi-1}}{Q_{2\xi} Q_{2\xi-1} Q_{2\xi-2}} = \frac{q_{2\xi}}{Q_{2\xi} Q_{2\xi-2}} > 0 \end{aligned}$$

Неравенство  $\delta_{2\xi+1} - \delta_{2\xi-1} < 0$  доказывается аналогично. □

**Лемма 7.5.** В условиях леммы 7.4 справедливы неравенства:  $\delta_\xi < \alpha$ ,  $\xi$  - четное и  $\delta_\xi > \alpha$ ,  $\xi$  - нечетное.

*Доказательство.* Рассмотрим выражения

$$\alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_\xi + \frac{1}{\alpha_{\xi+1}}}}}}$$



$$\delta_{\xi+1} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_\xi + \frac{1}{q_{\xi+1}}}}}}, \quad \delta_\xi = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_\xi}}}}$$

выражения для  $\alpha$  и  $\delta_{\xi+1}$  получаются из выражения для  $\delta_\xi$  формальной заменой  $q_\xi$  на  $q_\xi + \frac{1}{\alpha_{\xi+1}}$  и на  $q_\xi + \frac{1}{q_{\xi+1}}$  соответственно.

$$\delta_\xi = \frac{P_\xi}{Q_\xi} = \frac{q_\xi P_{\xi-1} + P_{\xi-2}}{q_\xi Q_{\xi-1} + Q_{\xi-2}} \Rightarrow \alpha = \frac{(q_\xi + \frac{1}{\alpha_{\xi+1}})P_{\xi-1} + P_{\xi-2}}{(q_\xi + \frac{1}{\alpha_{\xi+1}})Q_{\xi-1} + Q_{\xi-2}} = \frac{A_\xi}{B_\xi}$$

$$\delta_{\xi+1} = \frac{(q_\xi + \frac{1}{q_{\xi+1}})P_{\xi-1} + P_{\xi-2}}{(q_\xi + \frac{1}{q_{\xi+1}})Q_{\xi-1} + Q_{\xi-2}} = \frac{P_{\xi+1}}{Q_{\xi+1}}$$

ВЫЧИСЛИМ:

$$\alpha - \delta_{\xi+1} = \frac{A_\xi}{B_\xi} - \frac{P_{\xi+1}}{Q_{\xi+1}} = \frac{A_\xi Q_{\xi+1} - B_\xi P_{\xi+1}}{B_\xi Q_{\xi+1}}$$

ЧИСЛИТЕЛЬ:

$$\begin{aligned} * &= (q_\xi + \frac{1}{q_{\xi+1}})(q_\xi + \frac{1}{\alpha_{\xi+1}})(P_{\xi-1}Q_{\xi-1} - P_{\xi-1}Q_{\xi-1}) + (P_{\xi-2}Q_{\xi-2} - P_{\xi-2}Q_{\xi-2}) + \\ &+ (q_\xi + \frac{1}{q_{\xi+1}}) + (P_{\xi-2}Q_{\xi-1} - P_{\xi-1}Q_{\xi-2}) + (q_\xi + \frac{1}{\alpha_{\xi+1}}) + (P_{\xi-1}Q_{\xi-2} - P_{\xi-2}Q_{\xi-1}) \end{aligned}$$

итак, числитель разности  $\alpha - \delta_{\xi+1}$  равен

$$\begin{aligned} (P_{\xi-1}Q_{\xi-2} - P_{\xi-2}Q_{\xi-1})(q_\xi + \frac{1}{\alpha_{\xi+1}} - q_\xi - \frac{1}{q_{\xi+1}}) &= h_{\xi-1}(\frac{1}{\alpha_{\xi+1}} - \frac{1}{q_{\xi+1}}) = \\ &= (-1)^{\xi-2} \frac{q_{\xi+1} - \alpha_{\xi+1}}{\alpha_{\xi+1}q_{\xi+1}} = \frac{(-1)^{\xi+1}\alpha_{\xi+1}}{\alpha_{\xi+1}q_{\xi+1}} \end{aligned}$$

$\Rightarrow$  знак разности  $\alpha - \delta_r$  совпадает с  $(-1)^r$  □

**Теорема 7.3.** Последовательность подходящих дробей, отвечающих разложению иррационального числа  $\alpha$  в непрерывную дробь, сходится к числу  $\alpha$ .

*Доказательство.* По лемме 7.4 последовательность  $\delta_{2\xi}$ ,  $\xi = 0, 1, 2, \dots$  монотонно возрастает. По лемме 7.5 она ограничена сверху числом  $\alpha$ . Аналогично, последовательность  $\delta_{2\xi+1}$  монотонно убывает и ограничена снизу числом  $\alpha$ . По известной теореме из математического анализа, эти последовательности имеют пределы. По лемме 7.5 :  $\delta_{2\xi} < \alpha < \delta_{2\xi+1}$  при любом  $\xi \geq 0$ . Значит,

$$0 < \alpha - \delta_{2\xi} < \delta_{2\xi+1} - \delta_{w\xi} = \frac{1}{Q_{2\xi}Q_{2\xi+1}}, \quad 0 < \delta_{2\xi+1} - \alpha < \delta_{2\xi+1} - \delta_{w\xi} = \frac{1}{Q_{2\xi}Q_{2\xi+1}}$$

Пусть  $\tau = \frac{1+\sqrt{5}}{2} > 1,6$ . Докажем, что  $Q_\xi \geq \tau^{\xi-1}$

Индукция по  $\xi$ . База:  $Q_1 = 1 = \tau^{1-1}$ . Пусть доказано для всех  $\xi : q \leq \xi \leq m$ .  
 $\tau^2 = \tau + 1 \Rightarrow \tau^{k+2} = \tau^{k+1} + \tau^k$  для всех  $k \geq 0$ .

Тогда

$$Q_{m+1} = q_{m+1}Q_m + Q_{m-1} \geq Q_m + Q_{m-1} \geq \tau^{m-1} + \tau^{m-2} = \tau^m$$

$$\begin{aligned} Q_{2\xi}Q_{2\xi-1} &\geq \tau^{2\xi-1}\tau^{2\xi-2} = \tau^{4\xi-3} = \frac{\tau^{4\xi}}{\tau^3}, \quad 0 < \alpha - \delta_{2\xi}, \quad \delta_{2\xi+1} - \alpha < \frac{\tau^3}{\tau^{4\xi}} = \\ &= \frac{2 + \sqrt{5}}{\left(\frac{7+3\sqrt{5}}{2}\right)^\xi} < \frac{5}{6^\xi} \rightarrow 0 \quad (\xi \rightarrow +\infty) \end{aligned}$$

□

**Замечание.** Последовательность неполных частных  $q_0, q_1, q_2, \dots$  (бесконечная) периодична (начиная с некоторого номера)  $\Leftrightarrow \alpha$  - квадратичная иррациональность, то есть  $\alpha = \frac{A+B\sqrt{D}}{C}$ ,  $A, B, C, D \in \mathbb{Z}$ ,  $D \geq 1$  - бесквадратное. Например:

$$\sqrt{2} = [1; 2, 2, \dots] = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots}}}$$

**Замечание.** Лишь для немногих  $\alpha \notin \mathbb{Q}$ , не являющихся квадратичной иррациональностью, известны разложения в цепную дробь.

Число  $e = 2,718281828459045\dots$

$$\alpha = \frac{e-1}{e+1} = [0; 2, 6, 10, 14, 18, 22, \dots]$$

$$\alpha = \frac{e^{\frac{2}{k}} - 1}{e^{\frac{2}{k}} + 1} = \text{th}\left(e^{\frac{1}{k}}\right) = [0; 1k, 3k, 5k, 7k, \dots] \quad (\text{Л. Эйлер, 1737г.})$$

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \dots] \quad (\text{Л. Эйлер, 1737г.})$$

$$\alpha = \sqrt[3]{2} = [1; 3, 1, 5, 1, 1, 4, 1, 1, 8, \dots]$$

$$\alpha = \sqrt[3]{6} = [1; 1, 4, 2, 7, 3, 508, 1, 5, 5, \dots]$$

$$\pi = [3; 7, 5, 1, 292, 1, 1, 1, 2, 1, \dots]$$

**Замечание.** Рассмотрим  $N \geq 3$  и дроби  $\frac{a}{N}$ ,  $1 \leq a \leq N-1$ ,  $(a, N) = 1$  (таких дробей  $\varphi(N)$  штук). Разложим каждую в непрерывную дробь:

$$\frac{a}{N} = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_n}}}}$$

где  $n = n(a)$  - длина разложения. Вопрос: Каково среднее значение  $n(a)$  при изменении  $a$ ?

$$\frac{1}{\varphi(N)} \sum_{a=1}^N n(a) \approx \frac{12}{\pi^2} (\ln 2) + A, \quad A - \text{некоторая константа} \quad (\text{Х. Хейльбрин, 1969г.})$$

## 8 Теория сравнений

Пусть  $m \geq 2$  - целое.

**Определение 8.1.** Целые числа  $a$  и  $b$  называются сравнимыми по модулю  $m$ , если  $a - b$  делится на  $m$ . Или, что то же, когда  $a$  и  $b$  при делении на  $m$  дают одинаковые остатки. Число  $m$  при этом называется модулем сравнения. Пишут  $a \equiv b \pmod{m}$ .

**Примеры.**  $8 \equiv 2 \pmod{3}$ ,  $15 \equiv 1 \pmod{7}$ ,  $24 \equiv 0 \pmod{6}$

**Теорема 8.1.** (Простейшие свойства сравнений)

1.  $a \equiv a \pmod{m}$ ,  $\forall a$
2. если  $a \equiv b \pmod{m}$ , то и  $b \equiv a \pmod{m}$
3. если  $a \equiv b \pmod{m}$ ,  $b \equiv c \pmod{m}$ , то  $a \equiv c \pmod{m}$
4. если  $a \equiv b \pmod{m}$ ,  $c \equiv d \pmod{m}$ , то  $a + c \equiv b + d \pmod{m}$  и  $ac \equiv bd \pmod{m}$

*Доказательство.* 1-3 очевидно. Докажем 4:

$$\begin{aligned} a &= b + km, \quad c = d + lm \Rightarrow a + c = (b + d) + (k + l)m \equiv b + d \pmod{m} \\ ac &= (b + km)(d + lm) = bd + blm + dkm + klm^2 = bd + m(bl + dk + lkm) \equiv \\ &\equiv bd \pmod{m} \quad \square \end{aligned}$$

**Следствие.**  $a \equiv b \pmod{m}$ ,  $c, n$  - целые числа,  $n \geq 1$ , то  $ca^n \equiv cb^n \pmod{m}$

**Следствие.**  $a \equiv b \pmod{m}$ ,  $P(x)$  - многочлен с целыми коэффициентами  
 $\Rightarrow P(a) \equiv P(b) \pmod{m}$ .

**Теорема 8.2.** Пусть  $m \geq 2$ . Тогда

1. Если  $ab \equiv ac \pmod{m}$  и  $(a, m) = 1$ , то  $b \equiv c \pmod{m}$ .
2. Если  $a \equiv b \pmod{m}$ ,  $d \geq 1$  - целое, то  $ad \equiv bd \pmod{md}$ .
3. Если  $a \equiv b \pmod{m}$ , то  $(a, m) = (b, m)$ .
4. Если  $a \equiv b \pmod{m}$  и  $d \mid m$ ,  $d \geq 2$ , то  $a \equiv b \pmod{d}$ .

*Доказательство.*

1.  $ab \equiv ac + km \Rightarrow a(b - c) = km$ , если  $b = c$ , то утверждение очевидно. Пусть  $b \neq c \Rightarrow b - c \neq 0$  и из равенства  $a(b - c) = km$  следует, что  $a \mid km$ . Но  $(a, m) = 1 \Rightarrow$  по теореме 2.3  $a \mid k$ , то есть  $k = an \Rightarrow a(b - c) = anm \Rightarrow b - c = nm \Rightarrow b \equiv c \pmod{m}$ .
2.  $a = b + km \Rightarrow ad = bd + kmd \Rightarrow ad \equiv bd \pmod{md}$ .
3. По лемме 3.2 если  $\alpha = bq + r$ , то  $(\alpha, \beta) = (\beta, r)$ . Тогда  $a \equiv b \pmod{m} \Rightarrow a = b + km \Rightarrow (\alpha = a, \beta = m, r = b) \Rightarrow (\alpha, \beta) = (a, m) = (\beta, r) = (m, b)$ .
4.  $a = b + km$ ,  $m = nd$ ,  $d \geq 2 \Rightarrow a = b + knd \Rightarrow a \equiv b \pmod{d}$ .

□

**Примеры.**

1.  $27 \equiv 3 \pmod{4} \Rightarrow 3 \equiv 1 \pmod{4}$ .
2.  $26 \equiv 4 \pmod{22} \Rightarrow 13 \equiv 2 \pmod{11}$ .
3.  $48 \equiv 28 \pmod{10}$ , но  $12 \not\equiv 7 \pmod{10}$ .

**Пример.** Найти остаток от деления  $11^6$  на 9.

$$\begin{aligned} 11 &\equiv 2 \pmod{9} \Rightarrow 11^6 \equiv 2^6 \pmod{9} \Rightarrow 11^6 \equiv (2^3)^2 \pmod{9} \\ &\Rightarrow 11^6 \equiv (-1)^2 \pmod{9} \Rightarrow 11^6 \equiv 1 \pmod{9}. \end{aligned}$$

**Пример.** Натуральное число  $n = 8k + 7$  не представимо суммой трех квадратов целых чисел.

$x$  - четное  $\Rightarrow x = 4y$  либо  $x = 4y + 2$ ,  $x^2 = (4y)^2 = 16y^2 \equiv 0 \pmod{8}$ .

$x^2 = (4y + 2)^2 = 16y^2 + 16y + 4 \equiv 4 \pmod{8}$ .

$x$  - нечетное  $\Rightarrow x = 4y \pm 1 \Rightarrow 16y^2 \pm 8y + 1 \equiv 1 \pmod{8}$ . Следовательно,  $x^2 \equiv 0, 1, 4 \pmod{8}$ , но число 7 нельзя представить суммой трех величин, принимающих значения 0, 1 и 4.

**Теорема.** (Теорема Лагранжа)

Если  $n \neq 4^a(8k + 7)$ , то  $n$  представимо суммой трех квадратов целых чисел.

Сколько может быть чисел  $n : 1 \leq n \leq x$ ,  $x \rightarrow +\infty$ ,  $n = a^2 + b^2$  ?

Таких чисел примерно  $\frac{Bx}{\sqrt{\ln x}}$ , где  $B = 0,7\dots$  - постоянная Рамануджана-Ландау.

**Теорема 8.3.** (8.4???) Если числа  $a$  и  $b$  сравнимы по модулям  $m_1, \dots, m_k$ , то они сравнимы по модулю  $m = \text{НОК}(m_1, \dots, m_k)$ .

*Доказательство.* Если  $a = b$ , то утверждение очевидно. Пусть  $a \neq b$ , не теряя общности будем считать, что  $a > b$ . Так как  $a \equiv b \pmod{m_i}$ ,  $i \in \overline{1, k} \Rightarrow$  натуральное число  $a - b \equiv 0 \pmod{m}$ , то есть число  $a - b$  делится на каждое из чисел  $m_1, \dots, m_k \Rightarrow a - b$  - их общее кратное. По теореме 2.1 получаем, что  $[m_1, \dots, m_k] \mid (a - b)$  □

Пусть задан модуль  $m \geq 2$ . Все множество  $\mathbb{Z}$  разобьем на непересекающиеся подмножества, относя к одному и тому же подмножеству те числа, что при делении на  $m$  дают одинаковые остатки. Именно,  $a = q_1m + r_1$ ,  $b = q_2m + r_2$ ,  $0 \leq r_1, r_2 \leq m - 1$  относятся к одному и тому же подмножеству  $\Leftrightarrow r_1 = r_2$ . Так получим ровно  $m$  подмножеств, которые отвечают остаткам  $r = 0, 1, \dots, m - 1$  (все они непусты).

**Определение 8.2.** Построенные таким образом подмножества  $\mathbb{N}$  называются классами вычетов по модулю  $m$ . Элементы каждого из этих подмножеств называются вычетами этого класса. Класс вычетов по модулю  $m$ , содержащий число  $a$ , иногда обозначают через  $\bar{a}$  или  $[a]$  или  $[a]_m$ .

Очевидно, что равенство классов  $\bar{a}$  и  $\bar{b}$  имеет место  $\Leftrightarrow a \equiv b \pmod{m}$ . Множество всех классов вычетов по модулю  $m$  будем обозначать символом  $\mathbb{Z}_m$

**Пример.** Пусть  $m = 4 \Rightarrow$  остатки: 0, 1, 2, 3  $\Rightarrow \mathbb{Z}_4$  состоит из классов:

1)  $a = 4n$ ,    2)  $a = 4n + 1$ ,    3)  $a = 4n + 2$ ,    4)  $a = 4n + 3$ .

**Определение 8.3.** Пусть  $m \geq 2$  и пусть  $a_1, \dots, a_m$  - произвольные представители различных классов вычетов по модулю  $m$ . Тогда совокупность  $a_1, \dots, a_m$  называется полной системой вычетов по модулю  $m$ .

**Примеры.**

1.  $m = 4$ , числа  $a_1 = 13, a_2 = 7, a_3 = 6, a_4 = 8$ .

$$a_4 \equiv 0 \pmod{4}, a_1 \equiv 1 \pmod{4}, a_2 \equiv 2 \pmod{4}, a_3 \equiv 3 \pmod{4}$$

$\Rightarrow 13, 7, 6, 8$  - полная система вычетов по модулю 4.

2.  $m = 5, a_1 = 2, a_2 = 6, a_3 = 16, a_4 = 8, a_5 = 9$ .

$$a_1 \equiv 2 \pmod{5}, a_2 \equiv 1 \pmod{5}, a_3 \equiv 1 \pmod{5}, a_4 \equiv 3 \pmod{5},$$

$a_5 \equiv 4 \pmod{5} \Rightarrow$  числа  $2, 6, 16, 8, 9$  не образуют полную систему вычетов по модулю 5.

Обычно в качестве полной системы вычетов по модулю  $m$  берут совокупность  $0, 1, \dots, m-1$ , состоящую из наименьших неотрицательных представителей всех классов вычетов.

Иногда удобно работать с системой вычетов, составленной из наименьших по абсолютной величине представителей классов вычетов.

**Пример.** Пусть  $m = 7$ :

$\dots, -21, -14, -7, 0, 7, 14, 21, \dots \equiv 0 \pmod{7}$  - берем 0

$\dots, -20, -13, -6, 1, 8, 15, 22, \dots \equiv 1 \pmod{7}$  - берем 1

$\dots, -19, -12, -5, 2, 9, 16, 23, \dots \equiv 2 \pmod{7}$  - берем 2

$\dots, -18, -11, -4, 3, 10, 17, 24, \dots \equiv 3 \pmod{7}$  - берем 3

$\dots, -17, -10, -3, 4, 11, 18, 25, \dots \equiv 4 \pmod{7}$  - берем -3

$\dots, -16, -9, -2, 5, 12, 19, 26, \dots \equiv 5 \pmod{7}$  - берем -2

$\dots, -15, -8, -1, 6, 13, 20, 27, \dots \equiv 6 \pmod{7}$  - берем -1

Итак, полная наименьшая по абсолютной величине система вычетов по модулю 7 :  $\{-3, -2, -1, 1, 2, 3, 0\}$

**Пример.** Общий случай:

Для нечетного  $n$  получаем  $-\frac{m-1}{2}, -\frac{m-3}{2}, \dots, -1, 0, 1, \dots, \frac{m-3}{2}, \frac{m-1}{2}$ .

Для четного  $n$  получаем  $-\frac{m}{2} + 1, \dots, -1, 0, 1, \dots, \frac{m}{2} - 1, \frac{m}{2}$ .

**Теорема 8.4.** Пусть  $m \geq 2, a, b \in \mathbb{Z}$ , причем  $(a, m) = 1$ . Если величина  $x$  пробегает полную систему вычетов по модулю  $m$ , то и величина  $ax + b$  пробегает полную систему вычетов по модулю  $m$ .

*Доказательство.* Достаточно доказать, что если  $x_1 \not\equiv x_2 \pmod{m}$ , то сравнение  $ax_1 \equiv ax_2 \pmod{m}$  невозможно. По теореме 8.2 п.1 на  $a$  можно сократить: получим  $x_1 \equiv x_2 \pmod{m}$  - противоречие.  $\square$

**Следствие.** Пусть  $m \geq 2$ ,  $a \in \mathbb{Z}$ ,  $(a, m) = 1$ . Тогда существует единственный класс вычетов  $c \pmod{m}$  такой, что  $ac \equiv 1 \pmod{m}$ .

*Доказательство.* Для  $ax - 1$  при некотором  $x = c$  будет выполнено:  $ac - 1 \equiv 0 \pmod{m}$ ,  $ac \equiv 1 \pmod{m}$ . Пусть  $ac_1 \equiv 1 \pmod{m}$  и  $ac_2 \equiv 1 \pmod{m} \Rightarrow a(c_1 - c_2) \equiv 0 \pmod{m} \Rightarrow m \mid a(c_1 - c_2) \Rightarrow m \mid (c_1 - c_2)$ , то есть это возможно лишь при  $c_1 \equiv c_2 \pmod{m}$ .  $\square$

**Замечание.** Такой вычет  $c$  (класс вычетов  $\bar{c}$ ) называют обратным к  $a$  (соответственно обратным к классу  $\bar{a}$ ). Обозначим его как  $a^*$  (соответственно  $\bar{a}^*$ ).

**Пример.**  $m = 5$ ,  $a = 3$ ,  $b = 4$

$x$	$3x + 4$	$3x + 4 \pmod{5}$
0	4	4
1	7	2
2	10	0
3	13	3
4	16	1

**Замечание.** Условие  $(a, m) = 1$  опустить нельзя.

**Пример.** (Почему условие выше опустить нельзя)  $m = 6$ ,  $a = 2$ ,  $b = 1$

$x$	$2x + 1$	$2x + 1 \pmod{6}$
0	1	1
1	3	3
2	5	5
3	7	1
4	9	3
5	11	5

**Пример.**  $m = 7$

$$\begin{aligned}
 1 \cdot 1 &\equiv 1 \pmod{7} \Rightarrow 1^* \equiv 1 \pmod{7} \\
 2 \cdot 4 &\equiv 1 \pmod{7} \Rightarrow 2^* \equiv 4 \pmod{7} \\
 3 \cdot 5 &\equiv 1 \pmod{7} \Rightarrow 3^* \equiv 5 \pmod{7} \\
 4 \cdot 2 &\equiv 1 \pmod{7} \Rightarrow 4^* \equiv 2 \pmod{7} \\
 5 \cdot 3 &\equiv 1 \pmod{7} \Rightarrow 5^* \equiv 3 \pmod{7} \\
 6 \cdot 6 &\equiv 1 \pmod{7} \Rightarrow 6^* \equiv 6 \pmod{7}
 \end{aligned}$$

Согласно теореме 8.2 (пункт 3), числа, принадлежащие одному классу вычетов по модулю  $m$ , имеют с модулем один и тот же НОД.  $(a \equiv b \pmod{m}) \Rightarrow (a, m) = (a, b)$

Поэтому особый интерес представляют классы, для которых этот НОД равен 1. Взяв от каждого такого класса по одному вычету, получим приведенную систему вычетов по модулю  $m$ . Возьмем в качестве такой полной системы вычетов числа  $0, 1, \dots, m-1$ . Так как среди этих чисел количество взаимно простых с модулем  $m$  равно  $\varphi(m)$ , то и любая приведенная система вычетов содержит  $\varphi(m)$  элементов. Обозначение:  $\mathbb{Z}_m^*$ .

**Пример.**  $m = 6$ ;  $0, 1, 2, 3, 4, 5 \Rightarrow 1, 5$  - приведенная система вычетов.

$m = 7$ ;  $0, 1, 2, 3, 4, 5, 6 \Rightarrow 1, 2, 3, 4, 5, 6$  - приведенная система вычетов.

$m = 10$ ;  $0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \Rightarrow 1, 3, 7, 9$  - приведенная система вычетов.

$m$  - простое  $\Rightarrow \mathbb{Z}_m^* = \{1, 2, \dots, p-1\}$ .

**Теорема 8.5.** (8.6??) Пусть  $m \geq 2$ ,  $a$  - целое число,  $(a, m) = 1$ , и пусть  $x$  пробегает приведенную систему вычетов по модулю  $m$ . Тогда и величина  $ax$  будет пробегать приведенную систему вычетов по модулю  $m$ .

*Доказательство.* Что нужно проверить.

1.  $ax_1 \equiv ax_2$  невозможно, если  $x_1 \not\equiv x_2 \pmod{m}$ .

2.  $(ax, m) = 1$  для всех  $x \in \mathbb{Z}_m^*$ .

1. был проверен при доказательстве теоремы 8.4.

2. пусть  $(ax, m) = \delta > 1 \Rightarrow$  для некоторого  $x : (x, m) = 1 \Rightarrow \delta \mid ax$ , причем  $a \neq 0$  и  $x \neq 0$  (следует из взаимной простоты с  $m$ )  $\Rightarrow$  (по теореме 2.3)  $\delta \mid a$ . Но  $\delta \mid m$ . Значит  $\delta \mid (a, m) \Rightarrow (a, m) \geq \delta > 1$  противоречие.  $\square$

**Теорема 8.6.** (Теорема Эйлера)

Пусть  $m \geq 2$ ,  $a$  - целое,  $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$ .

*Доказательство.* Пусть  $1 = r_1 < r_2 < \dots < r_c < \dots < r_{m-1}$ ,  $c = \varphi(m)$  - приведенная система вычетов. Пусть  $ar_k \equiv \rho_k \pmod{m}$ , где  $0 < \rho < m$ . Из теоремы 8.5 следует, что  $\rho_1, \dots, \rho_k$  образуют перестановку чисел  $r_1, \dots, r_k$ . Перемножим сравнения почленно:  $a^c r_1, \dots, r_c \equiv \rho_1 \dots \rho_c \pmod{m}$ . Но  $r_1, \dots, r_c = \rho_1 \dots \rho_c = R$  и число  $R$  взаимно просто с  $m$  (следует из теоремы 2.3). По теореме 8.2 (пункт 1), обе части сравнения  $a^c R \equiv R \pmod{m} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$ .  $\square$

**Следствие.** (Малая теорема Ферма)

Пусть  $p$  - простое число. Тогда при любом целом  $a$  выполняется сравнение:  $a^p \equiv a \pmod{p}$ .



*Доказательство.* Если  $p \mid a$ , то очевидно. Если  $(a, p) = 1$ , то  $a^{\varphi(p)} \equiv 1 \pmod{p}$   
 $\Rightarrow a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$ . □

## 9 Сравнения с одним неизвестным

Пусть  $f(x) = a_n x^n + \dots + a_1 x + a_0$  - многочлен с целыми коэффициентами. Будем изучать сравнения вида (1)  $f(x) \equiv 0 \pmod{m}$ . Если  $a_n \not\equiv 0 \pmod{m}$ , то число  $m$  называется степенью сравнения. Решить сравнение (1) - значит найти все целые числа  $x$ , ему удовлетворяющие. По следствию 2 из 8.1,  $a \equiv b \pmod{m} \Rightarrow f(a) \equiv f(b) \pmod{m}$ . Значит, если (1) удовлетворяет некоторое число  $x$ , и  $x \equiv a \pmod{m}$ , то (1) удовлетворяют все числа сравнимые с  $a$  по модулю  $m$ . По этой причине весь класс вычетов  $a \pmod{m}$  удобно считать за одно решение.

### Сравнения первой степени

Всякое сравнение первой степени можно переписать в виде:  $ax \equiv b \pmod{m}$ . Рассмотрим сперва случай, когда  $(a, m) = 1$ . По теореме 8.4 получаем, что такое сравнение имеет единственное решение.

1. Способ 1. По теореме Эйлера получим  $x_0 \equiv ba^{\varphi(m)-1} \pmod{m}$ .

Тогда  $ax_0 \equiv aba^{\varphi(m)-1} \equiv ba^{\varphi(m)} \pmod{m} \equiv b \cdot 1 \pmod{m} \equiv b \pmod{m}$ .

2. Способ 2. (Разложение в непрерывную дробь)  $\alpha = \frac{m}{a}$  подходящие дроби:  $\delta_0, \delta_1, \dots, \delta_{s-1} = \frac{P_{s-1}}{Q_{s-1}}, \delta_s = \frac{P_s}{Q_s} = \frac{m}{a}$ . Известно по лемме 7.1  $P_s Q_{s-1} - P_{s-1} Q_s = (-1)^{s-1} \Rightarrow m Q_{s-1} - a P_{s-1} = (-1)^{s-1}$ .  $a P_{s-1} = (-1)^s + m Q_{s-1} \Rightarrow a(-1)^s P_{s-1} = 1 + m Q_{s-1}(-1)^s \Rightarrow a(-1)^s P_{s-1} b = b + m b Q_{s-1}(-1)^s$ . Переходя к сравнению по модулю  $m$ , получим:  $a(-1)^s P_{s-1} b \equiv b \pmod{m} \Rightarrow (-1)^s P_{s-1} b \pmod{m}$  - решение.

**Пример.**

$$\frac{13}{7} = 1 + \frac{6}{7} = 1 + \frac{1}{\frac{7}{6}} = 1 + \frac{1}{1 + \frac{1}{6}}$$

Значит  $x \equiv (-1)^2 \cdot 2 \cdot 3 \pmod{13} \equiv 6 \pmod{13}$ .

Пусть  $(a, m) = d > 1$ ,  $ax \equiv b \pmod{m}$ . Необходимое условие разрешимости - делимость  $b$  на  $d$ . (т.к. если сравнение разрешимо, то  $ax = b + km$  для некоторого целого  $k$ ). Покажем что это условие достаточное. Пусть  $a = a_1 d$ ,  $b = b_1 d$ ,  $m = m_1 d$ ,  $(a_1, m_1) = 1$ . Значит  $a_1 d x \equiv b_1 d \pmod{m_1 d}$ . По теореме 8.2, можно все сократить на  $d$ :  $a_1 x \equiv b_1 \pmod{m_1}$ . По доказанному выше, это сравнение имеет единственное решение по модулю  $m_1$ :  $x \equiv x_1 \pmod{m_1}$ . Все числа вида (2)  $x_1, x_1 \pm m_1, x_1 \pm 2m_1, \dots, x_1 \pm tm_1, \dots$  - решения исходного сравнения. Так как

$x_1$  - решение, то  $a_1x_1 = b_1 + km_1$ ,  $k$  - некоторое целое число  $\Rightarrow a(x_1 \pm tm_1) = ax_1 \pm tam_1 = \alpha a_1x_1 \pm ta_1\alpha m_1 \equiv \alpha a_1m_1 \pmod{m} \equiv \alpha(b_1 + km_1) \pmod{m} \equiv b + km \pmod{m} \equiv b \pmod{m} \Rightarrow$  из ряда (2) нужно отобрать числа, различные по модулю  $m$ .  $x_1, x_1 + m_1, x_1 + 2m_1, \dots, x_1 + (\alpha - 1)m_1$  все они различны по модулю  $m$ .

**Теорема 9.1.** Пусть  $m \geq 2, a, b$  - целые числа, причем  $(a, m) = d$ . Сравнение  $ax \equiv b \pmod{m}$  разрешимо  $\Leftrightarrow d \mid b$ . В случае разрешимости сравнение имеет  $d$  решений.

**Пример.** ПРИМЕР 9.2

## Китайская теорема об остатках

Рассмотрим систему линейных сравнений, где  $m_1, \dots, m_k$  - попарно взаимно простые:

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \vdots \\ x \equiv a_k \pmod{m_k}. \end{cases} \quad (5)$$

**Теорема 9.2.** Пусть  $M = m_1 \dots m_k$ , а числа  $M_s, N_s, s = 1, \dots, k$  определены соотношением:  $M = m_s M_s, M_s N_s \equiv 1 \pmod{m_s}$ . Пусть  $x_0 = M_1 N_1 a_1 + \dots + M_k N_k a_k$ . Тогда решение системы (5) имеет вид:  $x \equiv x_0 \pmod{M}$ .

*Доказательство.*

( $\Rightarrow$ ) Пусть  $x \equiv x_0 \pmod{M} \equiv x_0 \pmod{m_1, \dots, m_k} \Rightarrow$  по теореме 8.3

$x \equiv x_0 \pmod{m_1}, M_2 = m_1 m_3 \dots m_k, M_3 = m_1 m_2 m_4, \dots, m_k$  и так далее  $\Rightarrow$  все числа  $M_2, M_3, \dots, M_k$  кратны  $m_1 \Rightarrow x \equiv M_1 N_1 a_1 \pmod{m_1} \equiv 1 \cdot a_1 \pmod{m_1} \equiv a_1 \pmod{m_1}$ . Аналогично проверяется, что  $x \equiv a_s \pmod{m_s}, s = 2, \dots, k$ .

( $\Leftarrow$ ) Пусть  $x$  - решение (5),  $y = x - x_0 \Rightarrow y \equiv a_1 - a_1 \pmod{m_1} \equiv 0 \pmod{m_1}$ . Аналогично проверяется, что  $y$  кратно и  $m_2, \dots, m_k \Rightarrow y$  - общее кратное чисел  $m_1, \dots, m_k \Rightarrow$  по теореме 2.1  $y$  делится на  $\text{НОК}(m_1, \dots, m_k) = m_1 \dots m_k = M \Rightarrow$  по теореме 2.2  $y \equiv x - x_0 \equiv 0 \pmod{M}$ .

□

**Пример.**  $x \equiv 1 \pmod{2}$ ,  $x \equiv 2 \pmod{3}$ ,  $x \equiv 4 \pmod{5}$ .

Тогда  $m_1 = 2$ ,  $m_2 = 3$ ,  $m_3 = 5 \Rightarrow M = 30$ ,  $M_1 = 15$ ,  $M_2 = 10$ ,  $M_3 = 6$

$\Rightarrow 15N_1 \equiv 1 \pmod{2} \Leftrightarrow N_1 \equiv 1 \pmod{2} \Rightarrow N_1 = 1$ .

$\Rightarrow 10N_2 \equiv 1 \pmod{3} \Leftrightarrow N_2 \equiv 1 \pmod{3} \Rightarrow N_2 = 1$ ,

$\Rightarrow 6N_3 \equiv 1 \pmod{5} \Leftrightarrow N_3 \equiv 1 \pmod{5} \Rightarrow N_3 = 1$ .

Тогда  $x_0 = 15 \cdot 1 \cdot 1 + 10 \cdot 1 \cdot 2 + 6 \cdot 1 \cdot 4 \pmod{30} \equiv 15 + 20 + 24 \equiv 29 \pmod{30}$ .

**Теорема 9.3.** Пусть  $f(x)$  - произвольная целозначная функция,  $m > 2$  - целое, причем  $m = km$ , где  $k, n > 1$ ,  $(k, n) = 1$ . Пусть далее

$$\begin{cases} x \equiv a_1 \pmod{k}, \\ \vdots \\ x \equiv a_r \pmod{k}. \end{cases}$$

- все решения сравнения  $f(x) \equiv 0 \pmod{k}$

$$\begin{cases} x \equiv b_1 \pmod{n}, \\ \vdots \\ x \equiv b_r \pmod{n}. \end{cases}$$

- все решения сравнения  $f(x) \equiv 0 \pmod{n}$ . Тогда все решения сравнения  $f(x) \equiv 0 \pmod{m}$  задаются следующими формулами:

(\*)  $x \equiv a_i n n^* + b_j k k^* \pmod{m}$ , где  $1 \leq i \leq r$ ,  $1 \leq j \leq s$ ,

$n n^* \equiv 1 \pmod{k}$ ,  $k k^* \equiv 1 \pmod{n}$ .

*Доказательство.*

( $\Rightarrow$ ) (\*) - дает решения: фиксируем  $i$  и  $j$

$\Rightarrow x \equiv a_i n n^* \pmod{k} \equiv a_i \cdot 1 \pmod{k} \equiv a_i \pmod{k} \Rightarrow f(x) \equiv 0 \pmod{k}$ ,

$x \equiv b_j k k^* \pmod{n} \equiv b_j \cdot 1 \pmod{n} \equiv b_j \pmod{n} \Rightarrow f(x) \equiv 0 \pmod{n}$

$\Rightarrow$  по теореме 2.2  $f(x) \equiv 0 \pmod{kn} \equiv 0 \pmod{m}$ .

( $\Leftarrow$ ) Обратное очевидно. Надо заметить: все  $x \pmod{m}$  в (\*) различны. Если

$a_i n n^* + b_j k k^* \equiv a'_i n n^* + b'_j k k^* \pmod{m} \Rightarrow a_i n n^* \equiv a'_i n n^* \pmod{k}$

$\Rightarrow a_i \equiv a'_i$ ,  $b^i \equiv b'_i \pmod{m}$ .

□

**Следствие.** В условиях теоремы 9.3. Решение сравнения

$f(x) \equiv 0 \pmod{m}$ ,  $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$  сводится к отысканию всех решений каждого из сравнений  $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ ,  $1 \leq i \leq t$  ( $\Diamond$ ).

Если  $\nu(p_i^{\alpha_i})$  - число решений ( $\Diamond$ ), то число  $\nu(m)$  решений исходного сравнения равно произведению  $\nu(p_1^{\alpha_1}) \dots \nu(p_t^{\alpha_t})$

## Полиномиальные сравнения

Пусть  $m \geq 2$ ,  $n \geq 2$  - целые числа,  $f(x) = a_n x^n + \dots + a_1 x + a_0$  - полином с целыми коэффициентами, причем  $a_n \not\equiv 0 \pmod{m}$ . Если  $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$  - каноническое разложение, то по следствию теоремы 9.1 решение сравнения  $f(x) \equiv 0 \pmod{m}$  сводится к решению каждого из сравнений  $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ , то есть достаточно рассмотреть случай, когда  $m = p^\alpha$ ,  $p$  - простое,  $\alpha \geq 1$ . Вначале рассмотрим случай  $\alpha = 1$ , то есть случай простого модуля:  $m = p$ .

**Теорема 9.4.** Сравнение  $f(x) \equiv 0 \pmod{p}$  равносильно сравнению степени не выше  $p - 1$ .

*Доказательство.* Пусть  $n \geq p$ , поделим  $f(x)$  с остатком на  $x^p - x$   
 $\Rightarrow f(x) = (x^p - x)h(x) + g(x)$ , где  $g(x)$  - полином степени  $\leq p - 1$  с целыми коэффициентами  $\Rightarrow (x^p - x)h(x) + g(x) \equiv 0 \pmod{p} \Rightarrow$  по малой теореме Ферма (следствие теоремы 8.6)  $x^p - x \equiv 0 \pmod{p}$  при любом  $x \Rightarrow$  сравнение равносильно  $g(x) \equiv 0 \pmod{p}$ .  $\square$

**Теорема 9.5.** (Теорема Лагранжа) Пусть  $2 \leq n \leq p - 1$ ,  $p$  - простое. Если сравнение  $f(x) = a_n x^n + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$  имеет более чем  $n$  решений, то все коэффициенты  $f(x)$  делятся на  $p$ .

*Доказательство.* Пусть имеется  $(n + 1)$  класс вычетов по модулю  $p$ , удовлетворяющий сравнению, пусть  $x_1, \dots, x_{n+1}$  - произвольные представители этих классов:  $f(x_i) = pN_i$ ,  $N_i$  - целое. Тогда

$$\begin{cases} a_0 + a_1 x_1 + \dots + a_n x_1^n = pN_1, \\ a_0 + a_1 x_2 + \dots + a_n x_2^n = pN_2, \\ \vdots \\ a_0 + a_1 x_{n+1} + \dots + a_n x_{n+1}^n = pN_{n+1}. \end{cases}$$

Рассмотрим это как систему линейных уравнений с неизвестными  $a_0, \dots, a_n$   
 $\Rightarrow a_k = \frac{\Delta_k}{\Delta}$

$$\Delta = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^n \\ 1 & x_2 & x_2^2 & \dots & x_2^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_{n+1} & x_{n+1}^2 & \dots & x_{n+1}^n \end{vmatrix} = \prod_{1 \leq j < i \leq n+1} (x_j - x_i)$$

Ни одна из разностей  $x_j - x_i$  не делится на  $p \Rightarrow \Delta$  не делится на  $p$ .  $\Delta_k$  получается из  $\Delta$  заменой  $k$ -го столбца на столбец, которой состоит из  $pN_1, pN_2, \dots, pN_{n+1}$   
 $\Rightarrow p \mid \Delta_k \Rightarrow p \mid a_k, \forall k$ .  $\square$

**Теорема 9.6.** (Теорема Вильсона)

Для любого простого  $p$  выполнено:  $(p-1)! + 1 \equiv 0 \pmod{p}$

*Доказательство.* Если  $p = 2$ , то очевидно. Пусть  $p \geq 3$ . Рассмотрим  $f(x) = (x-1)(x-2)\dots(x-(p-1)) - (x^{p-1} - 1)$ . Степень  $f(x)$  не выше чем  $(p-2)$ . Но всякий вычет  $x \equiv a \pmod{p}$ ,  $a = 1, \dots, p-1$  является решением сравнения  $f(x) \equiv 0 \pmod{p} \Rightarrow$  по теореме Лагранжа (9.5) все коэффициенты делятся на  $p$ . В частности,  $(-1)^{p-1}(p-1)! + 1 \equiv 0 \pmod{p} \Rightarrow (p-1)! - 1 \equiv 0 \pmod{p}$ . □

(Упражнение) Верно и обратное  $(n-1)! + 1 \equiv 0 \pmod{n} \Rightarrow n$  - простое.

Значит теорему Вильсона можно рассматривать как критерий простоты числа.

**Определение 9.1.** Пусть  $f(x) = a_n x^n + \dots + a_1 x + a_0$ . Производной многочлена  $f(x)$  назовем многочлен, который определяется формулой:

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1.$$

**Лемма 9.1.** Пусть  $f(x) = a_n x^n + \dots + a_1 x + a_0$  - многочлен с целыми коэффициентами, и пусть  $\Delta$  - целое число. Тогда при любом  $x$  справедливо равенство:  $f(x+\Delta) - f(x) = \Delta \cdot a f'(x) + \Delta^2 g(x)$ , где  $g(x)$  - некоторый многочлен с целыми коэффициентами.

*Доказательство.*

$$\begin{aligned} f(x+\Delta) - f(x) &= \sum_{k=0}^n a_k ((x+\Delta)^k - x^k) = \\ &= \sum_{k=0}^n a_k (x^k + k x^{k-1} \Delta + C_k^2 x^{k-2} \Delta^2 + \dots + C_k^k \Delta^k - x^k) = \\ &= \Delta \sum_{k=1}^n k a_k x^{k-1} + \Delta^2 g(x) = \Delta f'(x) + \Delta^2 g(x) \end{aligned}$$

□