

## Теория чисел и основные алгебраические структуры

- $\mathbb{Z}$  - целые числа  $+$   $-$   $\cdot$   $>$
- $\mathbb{N}$  - натуральные числа
- $\mathbb{R}$  - вещественные числа

**Аксиома индукции.**  $A \subset \mathbb{N}; A \neq \emptyset \Rightarrow$  в  $A$  есть наименьший элемент

**Th.** о делении с остатком

$$\begin{cases} a, b \in \mathbb{Z} \\ b \neq 0 \end{cases} \Rightarrow \exists! q, r \in \mathbb{Z} : a = b \cdot q + r, 0 \leq r < |b|$$

### Доказательство

- Существование

1.  $a > 0, b > 0$  fix  $b$

Пусть не так, есть плохие  $a$  (множество плохих  $a \neq \emptyset$ )

Пусть  $a_0$  - наименьшее плохое, значит  $a_0 - 1$  - хорошее, можно разделить с остатком

$$a_0 - 1 = b \cdot q + r, 0 \leq r < b, \text{ тогда}$$

$$a_0 = (b \cdot q + r) + 1, r + 1 < b$$

$$a_0 = b \cdot (q + 1), \text{ т.е. } a_0 - \text{хорошее}$$

2.  $a < 0, b > 0$

$$-a = b \cdot q + r, 0 \leq r < b$$

$$a = -b \cdot q - r$$

2.1.  $r = 0$

$$a = b \cdot (-q) + 0$$

2.2.  $r > 0$

$$a = b \cdot (-q) - b + b - r = b \cdot (-q - 1) + b - r, 0 < r < b \Rightarrow 0 < b - r < b$$

3.  $b < 0, -b > 0$

$$a = -b \cdot q + r = b \cdot (-q) + r, 0 \leq r < b$$

- Единственность

Пусть  $q, q', r, r'$

$$a = b \cdot q + r$$

$$a = b \cdot q' + r'$$

$$a - a = b \cdot q + r - b \cdot q' - r'$$

$$0 = b \cdot (q - q') + (r - r')$$

$$r' - r = b \cdot (q - q'), q \neq q', |q - q'| \geq 1$$

$$|b \cdot (q - q')| \geq |b|$$

$$r', r \in [0; |b| - 1]$$

$$|r - r'| < |b| - 1 \text{ Противоречие } \Rightarrow q = q', r = r'$$

**Def.**  $a, b \in \mathbb{Z}, a : b(b|a)$ , если  $\exists c \in \mathbb{Z} : a = bc$

**Rem.**  $0 : 0 \forall x \in \mathbb{Z} 0 = 0 \cdot x$

**Основные свойства делимости:**

1.  $0 : a$

2.  $a : 1$
3.  $a, b : c \Rightarrow a + b : c$
4.  $a, k : c \Rightarrow k \cdot a : c$
5.  $a : a$
6.  $a : b, b : a \Rightarrow a = \pm b$
7.  $a : b, b : c \Rightarrow a : c$
8.  $ac : bc, c \neq 0 \Rightarrow a : b$

Доказательство

3.  $a : c \Rightarrow \exists q_a : a = q_a \cdot c$   
 $b : c \Rightarrow \exists q_b : b = q_b \cdot c$   
 $a + b = (q_a + q_b) \cdot c$
6.  $a = bx$   
 $b = ay$   
 $a = a y x$   
 $a = a(xy) \Rightarrow \begin{cases} a = 0, b \neq 0 \\ a \neq 0, xy = 1 \Rightarrow x, y = \pm 1, a = \pm b \end{cases}$
8.  $ac : bc, c \neq 0$   
 $ac = bc \cdot x$   
 $c \cdot a = c \cdot bx \Rightarrow a = bx \ (a : b)$

**Задача:** при каких  $a, b, c \in \mathbb{Z}$  уравнение  $ax + by = c$  имеет решение в целых числах ( $\Leftrightarrow$  из чего состоит  $< a, b >? \ c \in < a, b >?$ )

**Def.** Идеалом называется подмножество  $I \subset \mathbb{Z}$ :

1.  $I \neq \emptyset$
2.  $a, b \in I \Rightarrow a + b \in I$
3.  $a \in I, k \in \mathbb{Z} \Rightarrow a \cdot k \in I$

**Ex. 1**  $c \in \mathbb{Z}$

$< c > = \{n \cdot c\} = \{x \in \mathbb{Z} | x : c\}$  - идеал, порожденный  $c$  - главный идеал

**Ex. 2**  $c_1, c_2 \dots c_k \in \mathbb{Z}$

$< c_1, c_2 \dots c_k > = \{n_1 c_1 + n_2 c_2 + \dots + n_k c_k | n_i \in \mathbb{Z}\}$

**Th.** в  $\mathbb{Z}$  любой идеал - главный

Доказательство

$I$  - идеал в  $\mathbb{Z}$ , хотим  $b \in \mathbb{Z}, I = < b >$

1.  $I = \{0\} = < 0 >$
2.  $\exists a \in I, a \neq 0 \Rightarrow a \in I, a \in \mathbb{N}$ . Рассмотрим наименьший натуральный  $b \in I$   
Докажем  $I = < b >$   
 $< b > \subset I, b \in I, k \cdot b \in I$   
 $a \in I$  делим с остатком  
 $a = bq + r, 0 \leq r < b$   
 $r = a - bq \ b \in I \Rightarrow -bq \in I \Rightarrow a - bq \in I \Rightarrow r \in I$   
 $r \in \mathbb{N}$  - противоречие ( $b$  - наименьшее)  $\Rightarrow r \notin \mathbb{N} \Rightarrow r = 0$

В частности  $\forall a, b \in \mathbb{Z} \exists d : < a, b > = < d >$

**Def.**  $a, b \in \mathbb{Z}$  НОД( $a, b$ ) =  $\gcd(a, b) = (a, b)$  - такое  $d \in \mathbb{Z}$ , что:

1.  $a : d, b : d$
2.  $\forall d' : a : d', b : d' \Rightarrow d : d'$

**Rem.** НОД определен однозначно с точностью до знака

Доказательство

$$\begin{cases} d_1 = (a, b) \Rightarrow a : d_1, b : d_1, d_2 : d_1 \\ d_2 = (a, b) \Rightarrow a : d_2, b : d_2, d_1 : d_2 \end{cases} \Rightarrow d_1 = \pm d_2$$

**Th.**  $a, b \in \mathbb{Z}$

1.  $\exists (a, b) = d$
2.  $\exists x, y \in \mathbb{Z} : ax + by = d$  - линейное представление НОДа
3.  $ax + by = c$  имеет решение  $\Leftrightarrow c : d$

Доказательство 1

Рассмотрим  $I = < a, b >$  - по предыдущей теореме он главный  
 $< d > = < a, b >$

$d = d \cdot 1 \in I \Rightarrow d \in < a, b >$ , т.е.  $\exists x, y : ax + by = d$

$d = (a, b) \begin{cases} a : d' \Rightarrow ax : d'b : d' \Rightarrow by : d' \\ b : d' \end{cases} \Rightarrow d : d'$

$a = a \cdot 1 + b \cdot 0 \in < a, b > = < d > \Leftrightarrow a : d$

Аналогично  $b : d$

Доказательство 3

$$\Rightarrow: c = ax + by \begin{cases} a : (a, b) \\ b : (a, b) \end{cases} \Rightarrow c = ax + by : (a, b)$$

$\Leftarrow$ : Пусть  $c : (a, b) = d$ , т.е.  $c = d \cdot k, k \in \mathbb{Z}$

$$ax + by = d$$

$$a_{new} = ak, b_{new} = bk$$

$$a_{new}x + b_{new}y = dk$$

**Lem.**  $(a, b) = (a, b - a)$

$$\begin{cases} a, b : d \Rightarrow b - a : d \\ a, b - a : d \Rightarrow b = a + (b - a) : d \end{cases} \Rightarrow \text{одинаковые общие делители}$$

**Следствие:**  $b = aq + r \Rightarrow (a, b) = (a, r)$ . Доказывается аналогично лемме

**Алгоритм Евклида:**

1.  $a = bq + r_1$   
 $b = r_1q + r_2$   
 $\dots$
2.  $(a, b) = (r_1, b) = (r_1, r_2) \dots, \exists i \in \mathbb{N} : r_i = 0$
3.  $(a, b) = \dots = (r_k, r_k + 1) = (r_k, 0) = r_k$

**Rem.**  $a_1, a_2 \dots a_k \in \mathbb{Z}$

$\exists (a_1, a_2 \dots a_k) = d \exists x_1 \dots x_k \in \mathbb{Z} :$

$$d = x_1a_1 + x_2a_2 + \dots + x_ka_k$$

Доказательство

Рассмотрим идеал  $\langle a_1, a_2 \dots a_k \rangle \ni d : \langle d \rangle = \langle a_1 \dots a_k \rangle$ . Далее все как при  $k = 2$

**Def.**  $a, b \in \mathbb{Z}$  называются взаимнопростыми, если  $(a, b) = 1$

**Lm.**  $a, b$  - взаимнопросты  $\Leftrightarrow \exists x, y : ax + by = 1$

Доказательство

$$\Rightarrow (a, b) = 1 \Rightarrow \exists x, y : ax + by = 1$$

$$\Leftarrow ax + by = 1 \Rightarrow 1 : (a, b) \quad (a, b) = 1$$

**Lm.** об отбрасывании взаимнопростого множителя

$$a, b, c \in \mathbb{Z} \quad \begin{cases} ab : c \\ (a, c) = 1 \end{cases} \Rightarrow b : c$$

Доказательство

$$ab = cx$$

$$ay + cz = 1 \Rightarrow aby + cbz = b : c$$

**Def.**  $p \in \mathbb{Z}$ .  $p$  называется простым, если

$$1. \quad |p| > 1$$

$$2. \quad p \neq xy \quad |x|, |y| < |p|$$

Ясно, что это равносильно тому, что  $p$  имеет ровно 4 делителя  $(\pm 1, \pm p)$

$$\textbf{Lm. } p - \text{ простое} \Leftrightarrow ab : p \Rightarrow \begin{cases} a : p \\ b : p \end{cases}, |p| > 1$$

Доказательство

$$\Leftarrow p = xy \Rightarrow xy : p \Rightarrow \begin{cases} x : p \\ y : p \end{cases} \Rightarrow \begin{cases} |x| \geq p \\ |y| \geq p \end{cases}$$

$$\Rightarrow \text{Пусть } p - \text{ простое, } ab : p$$

$$\begin{cases} (a, p) = 1 \Rightarrow b : p \\ (a, p) = p \Rightarrow a : p \end{cases}$$

**Основная теорема арифметики**

$$x \in \mathbb{Z}, x \neq 0$$

$$1. \quad \exists p_1, p_2 \dots p_k - \text{ простые } > 0$$

$$\varepsilon = \text{sgn}(n)$$

$$a_1, a_2 \dots a_k \in \mathbb{N}$$

$$x = \varepsilon p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}, p_i \neq p_j$$

$$2. \quad \text{Это разложение единственное с точностью до порядка сомножителей}$$

$$x = \varepsilon_1 p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

$$x = \varepsilon_2 q_1^{b_1} q_2^{b_2} \dots q_l^{b_l}$$

$$p_i, q_i > 0, \text{ тогда } \varepsilon_1 = \varepsilon_2, k = l$$

$$\exists \{i_1, i_2 \dots i_k\} = \{1, 2 \dots k\} :$$

$$p_{i_1} = q_1 \quad a_{i_1} = b_1, p_{i_2} = q_2 \quad a_{i_2} = b_2$$

Доказательство

Будем доказывать единственность и существование разложения  $n = p_1 p_2 \dots p_s, p_i$  - простые,  $n \in \mathbb{N}$

1. Существование:

Пусть есть плохие  $n$  (множество плохих непусто)

$n_0$  - наименьшее плохое

- $n_0$  - простое

$$p_1 = n_0, s = 1$$

$$n_0 = p_1 \text{ ??} \Rightarrow n_0 - \text{хорошее}$$

- $n_0$  - составное  $\Rightarrow n_0 = n_1 n_2, n_1, n_2 < n_0$

$$n_1, n_2 - \text{хорошие} \Leftrightarrow \begin{cases} n_1 = p_1 p_2 \cdots p_k, p_i - \text{простое} \\ n_2 = q_1 q_2 \cdots q_s, q_i - \text{простое} \end{cases} \Rightarrow n_0 = n_1 n_2 = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_s \Rightarrow n_0 - \text{хорошее}$$

2. Единственность:

Пусть есть плохие  $n$

$n_0$  - наименьшее из плохих

$$\begin{cases} n_0 = p_1 p_2 \cdots p_k \\ n_0 = q_1 q_2 \cdots q_s \end{cases} \quad p_i, q_i - \text{простые}$$

$$p_1 p_2 \cdots p_k = n_0 : q_1 \Rightarrow \begin{bmatrix} p_1 : q_1 \\ p_2 \cdots p_k : q_1 \end{bmatrix} \Rightarrow \begin{bmatrix} p_1 : q_1 \\ p_2 : q_1 \\ p_3 \cdots p_k : q_1 \end{bmatrix} \Rightarrow \cdots \Rightarrow \begin{bmatrix} p_1 : q_1 \\ p_2 : q_1 \\ \cdots \\ p_k : q_1 \end{bmatrix}$$

$$\exists p_i : q_1$$

$$p_i, q_1 > 0, q_1 \neq 1 \Rightarrow q_1 = p_i$$

Итак:  $\exists i : p_i = q_1 \Rightarrow p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_k = q_2 q_3 \cdots q_s = n_1, n_1 < n_0 \Rightarrow n_1 - \text{хорошее} \Rightarrow \text{разложения } p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_k \text{ и } q_2 q_3 \cdots q_s \text{ совпадают ??}$

$n = \varepsilon p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, p_1 < p_2 < \cdots < p_k$  - каноническое разложение

$n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ , почти все  $v_p(n) = 0$

$v_p(n)$  - степень вхождения  $p$  в  $n$

Свойства степени вхождения:

$$1. v_p(ab) = v_p(a) + v_p(b)$$

$$2. v_p(a+b) \geq \min(v_p(a), v_p(b))$$

$$\text{если } v_p(a) \neq v_p(b), \text{ то } v_p(a+b) = \min(v_p(a), v_p(b))$$

**Rem.**  $v_p(a)$  - это такое  $n$ , что  $a : p_n, a \not: p^{n+1}$

Доказательство

1. Напишем разложения:

$$a = p^{v_p(a)} \cdot \prod_{q \neq p} q^{v_q(a)}$$

$$b = p^{v_p(b)} \cdot \prod_{q \neq p} q^{v_q(b)}$$

$$ab = p^{v_p(a)+v_p(b)} \cdot \prod_{q \neq p} q^{v_q(a)+v_q(b)}$$

$$a = p^n x, b = p^m y$$

$$\text{НУО } n \geq m$$

$$a+b = p^m p^{n-m} x + p^m y = p^m (p^{n-m} x + y) : p^m = p^{\min(n,m)}$$

$$n \neq m, p^{n-m} x : p \Rightarrow p^{n-m} x + y \not: p \Rightarrow p^m (p^{n-m} x + y) \not: p^{m+1}$$

$$m = v_p(a+b)$$

### Следствия из ОТА

Утверждение:  $a = \prod_{p_i \in \mathbb{P}} p_i^{a_i}$ ,  $b = \prod_{p_i \in \mathbb{P}} p_i^{b_i}$

Тогда

1.  $a : b \Leftrightarrow a_i \geq b_i \forall i$
2.  $\exists c : a = c^k \Leftrightarrow a_i : k \forall i$
3. Число  $a$  имеет  $\tau(a) = \prod (a_i + 1)$  натуральных делителей

Доказательство

1.  $a = bx, x = \prod p_i^{x_i}$   
 $\prod p_i^{a_i} = \prod p_i^{b_i} \cdot \prod p_i^{x_i} = \prod p_i^{b_i + x_i} \Leftrightarrow a_i = b_i + x_i \forall i \Leftrightarrow a_i \geq b_i \forall i$
2. Упражнение

$$3. |\{ \text{делители } a \}| = |\{ p_1^{b_1} p_2^{b_2} \dots p_s^{b_s} \mid \begin{matrix} b_1 \in \{0, 1 \dots a_1\} \\ b_2 \in \{0, 1 \dots a_2\} \\ \dots \\ b_s \in \{0, 1 \dots a_s\} \end{matrix} \}| = |\{(b_1 \dots b_s) \mid b_i \leq a_i\}| = |\{0 \dots a_1\} \times \{0 \dots a_2\} \times \dots \times \{0 \dots a_s\}| = (a_1 + 1)(a_2 + 1) \dots (a_s + 1)$$

**Def.**  $c$  - наименьшее общее кратное  $a, b$   
 $a, b, c \in \mathbb{Z}$  если

1.  $c : a, c : b$
2.  $c' : a, c' : b \Rightarrow c' : c$

Утверждение  $a = \prod p_i^{a_i}, b = \prod p_i^{b_i}$   
 $(a, b) = \prod p_i^{\min(a_i, b_i)}$   
 $\exists [a, b] = \prod p_i^{\max(a_i, b_i)}$

Доказательство

1.  $\min(a_i, b_i) \leq a_i$   
 $\leq b_i$   
 $\prod p_i^{a_i} : \prod p_i^{\min(a_i, b_i)}$ , т.е.  $a, b : \prod p_i^{\min(a_i, b_i)}$   
 $a, b : \prod p_i^{c_i} \forall i \begin{matrix} c_i \leq a_i \\ c_i \leq b_i \end{matrix} \Rightarrow c_i \leq \min(a_i, b_i) \Rightarrow \prod p_i^{\min(a_i, b_i)} : \prod p_i^{c_i}$
2. НОК - аналогично

### Отступление

Решаем диофантовы уравнения

$x^2 - y^2 = 100$   $(x - y)(x + y) = 2^2 \cdot 5^2 \Rightarrow$  знаем  $(x - y), (x + y)$  (находим их из разложения 100)  $\Rightarrow$  находим  $x, y$

Отступление от теории чисел

## Основные алгебраические структуры

**Def.** Группой называется пара  $(G, *)$ , где  $G$  - множество,  $*$  - бинарная операция на  $G$ , такая, что:

1.  $(a * b) * c = a * (b * c)$  - ассоциативность
2.  $\exists e : a * e = e * a = a, e$  - нейтральный элемент
3.  $\forall a \in G \exists a^{-1} : a * a^{-1} = a^{-1} * a = e$

Если  $a * b = b * a$  (коммутативность), то  $G$  - абелева (коммутативная) группа

**Rem.** Простейшие свойства группы

1. Нейтральный элемент единственный
2. Обратный элемент единственный
3.  $a, b \in G$ 
  - $a * x = b * x \Rightarrow a = b$  - свойство сокращения
  - Уравнения  $a * x = b$  и  $x * a = b$  имеют единственное решение

### Доказательство (?)

- $a * x = b * x$   
 $(a * x) * x^{-1} = (b * x) * x^{-1}$   
 $a * (x * x^{-1}) = b * (x * x^{-1})$   
 $a * e = b * e$   
 $a = b$
- $a * x = b$   
 $a^{-1} * (a * x) = a^{-1} * b$   
 $(a^{-1} * a) * x = a^{-1} * b$   
 $e * x = a^{-1} * b$   
 $x = a^{-1} * b$
- $x * a = b$   
 $\dots$   
 $x = b * a^{-1}$

Главный пример ассоциативной, но не коммутативной операции – композиция

$f : A \rightarrow B$

$$\{(a, f(a)) \mid \begin{matrix} a \in A \\ f(a) \in B \end{matrix}\}$$

$g : B \rightarrow C$

$b \in B; g(b) \in C$

$a \rightarrow f(a) \rightarrow g(f(a)) \in C$

$g \circ f : A \rightarrow C$

$(g \circ f)(x) = g(f(x)) \quad \forall x \in A$

**Rem.** Если  $C \neq A$ , то  $f \circ g$  не существует

$A \rightarrow B \rightarrow C \rightarrow D$

$h \circ (g \circ f) : A \rightarrow D$

$(h \circ g) \circ f : A \rightarrow D$

и  $h \circ (g \circ f) = (h \circ g) \circ f$

$\forall a \in A \quad (h \circ (g \circ f))(a) = h(g(f(a))) = ((h \circ g) \circ f)(a)$

**Def.**  $M$  – множество

$End(M) = \{f : M \rightarrow M\}$

Тогда на  $End(M)$  определена бинарная ассоциативная операция  $\circ$

$f, g : M \rightarrow M; f \circ g : M \rightarrow M \rightarrow M$

$End(M)$  замкнуто относительно композиции

**Аксиомы:**

1. Ассоциативность есть

2.  $id_m(x) = x \forall x \in M$

$$(f \circ id_m)(x) = f(id_m(x)) = f(x)$$

$$(id \circ f)(x) = id(f(x)) = f(x)$$

Т.е.  $f \circ id = f$  и  $id \circ f = f$

$id_m$  – нейтральный элемент

**Rem.** Если в определение группы взять только аксиомы 1 и 2, то  $G$  – моноид.  $End(M)$  – моноид

$$fix f(x) = a$$

$$g(f(x)) = f(a) - fix$$

$$g \circ f \neq id_m \forall g$$

**Th.**  $f : M \rightarrow M$  имеет обратное  $\Leftrightarrow f$  – биекция

Т.е.  $\forall y \in M f(x) = y$  имеет единственно решение

$$f^{-1}(y) = x$$

$$f^{-1} \circ f(x) = f^{-1}(y) = x$$

$$f \circ f^{-1}(y) = f(x) = y$$

$$\begin{cases} f^{-1} \circ f = id \\ f \circ f^{-1} = id \end{cases} \Rightarrow f^{-1} - \text{биекция}$$

**Def.**  $M$  – множество

$$S(M) \subset End(M)$$

$$S(M) = \{f \in End(M) | f - \text{биекция}\}$$

$S(M)$  – симметрическая группа на множестве  $M$ , группа относительно  $\circ$

**Rem.**  $id$  – биекция;  $id^{-1} = id$

$$M = \{1, 2 \dots n\}$$

$S(M) = S_n$  – симметричная группа (группа перестановок)

**Def.** Кольцом называется тройка  $(R, +, \cdot)$ , где

$R$  – множество

$+, \cdot$  – бинарные операции на  $R$  ( $|R| > 1$ )

Такие, что:

1.  $(R, +)$  – абелева группа

$$\bullet a + b = b + a$$

$$\bullet (a + b) + c = a + (b + c)$$

$$\bullet \exists 0 : a + 0 = a$$

$$\bullet \forall a \exists (-a) : a + (-a) = 0$$

5.  $a \cdot (b + c) = a \cdot b + a \cdot c$  – дистрибутивность  
 $(b + c) \cdot a = b \cdot a + c \cdot a$

6.  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  – у нас выполняется всегда

$$7. \exists 1 : a \cdot 1 = 1 \cdot a = a$$

$$8. a \cdot b = b \cdot a$$

$$9. \forall a \in R, a \neq 0 \exists a^{-1} : a \cdot a^{-1} = 1$$

Если выполняется 1-6, это ассоциативное кольцо

Если выполняется 1-7, это ассоциативное кольцо с 1

Если выполняется 1-6 и 8, это (ассоциативное) коммутативное кольцо

Если выполняется 1-8, это (ассоциативное) коммутативное кольцо с 1

Если выполняется 1-9, это поле

Если выполняется 1-7 и 9, это тело

**Простейшие свойства колец:**



1.  $a \cdot 0 = 0$
2.  $a \cdot (-1) = -a$

**Rem.**  $R$  – поле  $\Rightarrow \forall a, b \neq 0 \ a : b$

$$a = b \cdot \frac{a}{b} = b \cdot (a \cdot b^{-1})$$

Значит бессмысленны понятия простых, разложения на простые

## Кольца вычетов

$M, \{(a, b)\} \subset M \times M$  – отношения на множестве  $M$   
 $aRb$

- $aRb \Rightarrow bRa$  – симметричность
- $aRb, bRc \Rightarrow aRc$  – транзитивность
- $aRa$  – рефлексивность

Если выполняются все 3 пункта, то это отношения эквивалентности

$R$  – отношения эквивалентности

$a \in M$

$\bar{a} = \{b \in M | aRb\}$  – класс Эквивалентности  $a$

**Th.** Любые два класса эквивалентности  $\bar{a}, \bar{b}$  : 
$$\begin{cases} \bar{a} \cap \bar{b} = \emptyset \\ \bar{a} = \bar{b} \end{cases}$$

В итоге  $M = \bigcup \bar{a}$  – разбиение на классы

**Def.**  $a, b, n \in \mathbb{Z}$   $a$  сравнимо с  $b$  по модулю  $n$ , если  $(a - b) : n$  обозначается  $a \equiv b \pmod{n} \Rightarrow \mathbb{Z}$  разбивается на классы эквивалентности. Обозначение:  $R$  – отношение,  $M/R$  – множество классов эквивалентности,  $\sim$  – эквивалентность  $M/\sim$  – множество классов эквивалентности – фактормножество

### Доказательство

P:  $a - a = 0 : n \Rightarrow a \equiv a$

C:  $a \equiv b \Rightarrow a - b : n \Rightarrow b - a : n \Rightarrow b \equiv a$

T: 
$$\begin{cases} a \equiv b \\ b \equiv c \end{cases} \Rightarrow \begin{cases} a - b : n \\ b - c : n \end{cases} \Rightarrow a - c = (a - b) + (b - c) : n \Rightarrow a \equiv c$$

**Rem.**  $a \equiv b \Leftrightarrow a$  и  $b$  имеют одинаковые остатки от деления на  $n$

### Доказательство

$\Leftarrow$  Упражнение

$$\Rightarrow \begin{cases} a = q_a \cdot n + r \\ b = q_b \cdot n + r \end{cases} \Rightarrow a - b = n(q_a - q_b) + 0 \Rightarrow a \equiv b$$

$$(r_1 - r_2 \neq 0 \Rightarrow 0 < |r_1 - r_2| < n; r_1 - r_2 \not\equiv 0 \pmod{n})$$

Элементы  $\mathbb{Z}/\equiv$  – вычеты (классы вычетов) по модулю  $n$

$$\bar{3} = \{3; 3 \pm n; 3 \pm 2n \dots\}$$

Из Rem  $\Rightarrow |\mathbb{Z}/\equiv| = n$

$$\mathbb{Z}/\equiv = \{\bar{0}; \bar{1} \dots \bar{n-1}\}$$

Обозначается  $\mathbb{Z}/n\mathbb{Z}$

**Свойства сравнений:**

$$\begin{cases} a \equiv b \\ c \equiv d \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \\ ac \equiv bd \end{cases}$$

### Доказательство

1.  $(a + c) - (b + d) = (a - b) + (c - d) : n$
2.  $ac \equiv bc$ , т.к.  $ac - bc = c(a - b) : n$   
 $ad \equiv bd$ , т.к.  $ad - bd = d(a - b) : n$

По транзитивности  $ac \equiv bc \equiv bd$

$$a \equiv b \Leftrightarrow \bar{a} = \bar{b} \text{ в } \mathbb{Z}/n\mathbb{Z}$$

Каноническое отображение:

$$\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$

$$a \mapsto \bar{a} = \{a + nk | k \in \mathbb{Z}\}$$

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2} \dots \overline{n-1}\}$$

$$\begin{cases} a \equiv b \\ c \equiv d \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \\ ac \equiv bd \end{cases}$$

Эти свойства позволяют перенести на  $\mathbb{Z}/n\mathbb{Z}$  структуру кольца:

$$\bar{a} + \bar{b} := \overline{a + b}$$

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Зачем для этого свойства?

Пусть  $x, y$  – классы

$$\begin{aligned} \text{Строим } x + y : \text{выбираем } a : \bar{a} = x \\ b : \bar{b} = y \quad x + y := \overline{a + b} \end{aligned}$$

Нужно показать, что результат не зависит от выбора  $a$  и  $b$

$$\begin{cases} \bar{a} = \bar{c} \\ \bar{b} = \bar{d} \end{cases} \Leftrightarrow \begin{cases} a \equiv c \\ b \equiv d \end{cases} \Rightarrow a + c \equiv c + d \Leftrightarrow \overline{a + b} = \overline{c + d}$$

С умножением аналогично

**Th.**  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  – коммутативное ассоциативное кольцо с 1

### Доказательство

Надо проверить 8 аксиом, очев

$$\text{Пусть } v \in \mathbb{Z}/n\mathbb{Z} \quad f(x) = bx$$

$$f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$

Как устроена?

В  $\mathbb{Q}$ :  $f(x) = bx$  – биекция ( $b \neq 0$ )

В  $\mathbb{Z}$ :  $f(x) = bx$  – инъекция, но не сюръекция

- $bx = by \Rightarrow x = y$
- Не все числа вида  $bx$

**Утверждение**  $f$  – биекция  $\Leftrightarrow (a, n) = 1$ ;  $\bar{a} = b$ , иначе это даже не инъекция

### Доказательство

- $(b, n) = 1 \Rightarrow \exists y, z : by + nz = 1$

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1} \dots \overline{n-1}\} \quad b = \bar{a}$$

$$\text{Значения } f : \overline{0a}, \overline{1a} \dots \overline{(n-1)a}$$

$$\text{Заметим, что если } \overline{ka} = \overline{la}, \text{ т.е. } ka \equiv la, \text{ то } \begin{cases} (k-l)a \equiv n \\ (a, n) = 1 \end{cases} \Rightarrow k-l \equiv n \Rightarrow \bar{k} = \bar{l}$$

Таким образом  $f$  – инъективно  $\Rightarrow \overline{0a}, \overline{1a} \dots \overline{(n-1)a}$  – попарно различные классы  $\Rightarrow$  это  $\{\bar{0}, \bar{1} \dots \overline{n-1}\} \Rightarrow f$  – сюръекция

**Упражнение:** доказать сюръективность напрямую через  $ay + bz = 1$

- Пусть  $(a, n) = d \neq 1$

$$a = dz; \quad n = dy$$

Положим  $x = \bar{y} \in \mathbb{Z}/n\mathbb{Z}$

Тогда  $f(x) = vx = \overline{dz} \cdot \bar{y} = \overline{dzy} = \overline{dy} \cdot \bar{z} = 0 \cdot \bar{z} = 0$  и  $f(0) = 0$

$x \neq \bar{0} = \{0 + nk | k \in \mathbb{Z}\} \Rightarrow f - \text{неинъективна}$

**Следствие**  $p$  – простое,  $\mathbb{Z}/p\mathbb{Z}$  – поле

### Доказательство

Пусть  $\bar{a} \neq \bar{0}$ , т.е.  $a \not\equiv 0 \pmod{p} \Rightarrow (a, p) = 1$ , т.е.  $x \rightarrow \bar{a} \cdot x$  сюръективно

то есть  $\exists b \in \mathbb{Z} : \bar{a} \cdot \bar{b} = 1 \Rightarrow \bar{b} = \bar{a}^{-1}$ , т.е.  $y \rightarrow \bar{a}$  есть обратный  $\Rightarrow \mathbb{Z}/p\mathbb{Z}$  – поле

Как найти этот обратный?

$\bar{a} \cdot \bar{x} = \bar{1}$ ;  $ax \equiv 1 \Leftrightarrow ax = 1 + py \Leftrightarrow ax - py = 1$  – линейное представление НОДа, т.е.  $x, y$  существуют

Пусть  $n$  – составное:  $n = pq$ ;  $p, q > 1$

$$\bar{p} \cdot \bar{q} = \bar{0}$$

$\bar{p}, \bar{q} \neq \bar{0}$  – кольцо с делителями нуля

**Def.** Область целостности – кольцо без делителей нуля

**Lem.**

1. Любое поле – область целостности
2. В области целостности  $\begin{cases} ab = ac \\ a \neq 0 \end{cases} \Rightarrow b = c$

### Доказательство

1.  $K$  – поле;  $a, b \in K : ab = 0$

Пусть  $a \neq 0 \Rightarrow \exists a^{-1}$

$$a^{-1} \cdot ab = a^{-1} \cdot 0 = 0, \text{ т.е. } b = 0$$

$$\text{Итак } ab = 0 \Rightarrow \begin{cases} a = 0 \\ b = 0 \end{cases}$$

2.  $ab = ac$ ;  $a \neq 0 \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$

**Rem.**  $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$

$$ax + by = c; \quad (a, b) = 1$$

$$ax = c - by$$

$$ax \equiv c$$

$$\bar{a} \cdot \bar{x} = \bar{c} \text{ в } \mathbb{Z}/b\mathbb{Z}$$

$$\exists! \bar{x}_0 : (\bar{a}, \bar{b}) = 1$$

$$ax \equiv c \Leftrightarrow x \equiv x_0, \text{ т.е. } x = x_0 + bk, k \in \mathbb{Z}$$

Тогда  $y = \dots$

$$\text{Утверждение } \begin{cases} (m, n) = 1 \\ a, b \in \mathbb{Z} \end{cases} \Rightarrow$$

$$1. \exists x \in \mathbb{Z} : \begin{cases} \bar{x} = \bar{a} \text{ в } \mathbb{Z}/m\mathbb{Z} \\ \bar{x} = \bar{b} \text{ в } \mathbb{Z}/n\mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} x - a : m \\ x - b : n \end{cases}$$

2. Пусть  $x_0$  – такое, тогда все  $x$ , удовлетворяющие условию, это  $\bar{x}_0$  в  $\mathbb{Z}/mn\mathbb{Z}$

### Доказательство

$$1. x - a : m, \text{ т.е. } \begin{cases} x - a = my \\ x - b = nz \end{cases}$$

$my + a = x = nz + b \Rightarrow my - nz = b - a$  – имеет решение, т.к.  $(m, n) = 1 \Rightarrow \exists$  соответствующие  $x, y$

2. В  $\mathbb{Z}/m\mathbb{Z}$   $\bar{x} = \bar{a} = \bar{x}_0$

В  $\mathbb{Z}/n\mathbb{Z}$   $\bar{x} = \bar{b} = \bar{x}_0$

$$\text{Т.е. } \begin{cases} x \equiv x_0 \pmod{m} \\ x \equiv x_0 \pmod{n} \end{cases} \Leftrightarrow \begin{cases} x - x_0 : m \\ x - x_0 : n \\ (a, b) = 1 \end{cases} \Leftrightarrow x - x_0 : mn \Leftrightarrow \bar{x} = \bar{x}_0 \text{ в } \mathbb{Z}/mn\mathbb{Z}$$

Смысл: каждой паре остатков по модулю  $m$  и по модулю  $n$  соответствует единственный остаток по модулю  $mn$

$m = 3; n = 5$

	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

Биекция между  $\mathbb{Z}/15\mathbb{Z}$  и  $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

**Отступление:** произведение групп и колец

**Def.**  $R_1, R_2$  – кольца

Их произведение – это  $(R_1 \times R_2, +, \cdot)$ , где  $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$

$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$

**Утверждение** это и правда кольцо (аксиомы наследуются)

### Доказательство

Очев

**Rem.**  $R_1 \times R_2$  – не область целостности  $(1, 0) \cdot (0, 1) = (0, 0)$

с группами аналогично:

$G_1, G_2$  – группы  $\Rightarrow G_1 \times G_2$  – группа

$(g_1, g_2) \cdot (g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$

Хотим сказать

$(m, n) > 1 \Rightarrow \mathbb{Z}/mn\mathbb{Z}$  и  $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  – это одно и то же

**Def.**  $R_1, R_2$  – кольца

Изоморфизм между  $R_1$  и  $R_2$  – биекция

$f : R_1 \rightarrow R_2$  такая, что

$$1. f(a + b) = f(a) + f(b)$$

$$2. f(ab) = f(a)f(b)$$

$$3. f(1) = 1$$

$R_1$  и  $R_2$  изоморфны, если существует изоморфизм

$G_1, G_2$  – группы

Изоморфизм  $f : G_1 \rightarrow G_2$  – биекция:

$$f(xy) = f(x) \cdot f(y) \quad \forall x, y \in G_1$$

$G_1$  и  $G_2$  изоморфны, если  $\exists$  изоморфизм  $f : G_1 \rightarrow G_2$

$G_1 \cong G_2$ . Аналогично  $R_1 \cong R_2$  ( $R_1, R_2$  – кольца)

**Rem.**  $e_1, e_2$  – нейтральные элементы в  $G_1, G_2$ ;  $f$  – изоморфизм  $\Rightarrow f(e_1) = e_2$

$$e_1 \cdot e_1 = e_1$$

$$\begin{cases} f(e_1 \cdot e_1) = f(e_1) \\ f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1) \end{cases} \Rightarrow f(e_1) \cdot f(e_1) = f(e_1) \cdot e_2 \Rightarrow f(e_1) = e_2$$

Аналогично  $f(a^{-1}) = f(a)^{-1}$

**Rem2.** Здесь биективность не важна

**Def.** Гомоморфизм отображение  $f : G_1 \rightarrow G_2 : f(xy) = f(x) \cdot f(y) \quad \forall x, y \in G_1$

**Def.** Гомоморфизм колец:  $f : R_1 \rightarrow R_2$

$$f(xy) = f(x) \cdot f(y) \quad \forall x, y \in R_1$$

$$f(x + y) = f(x) + f(y)$$

**Def.** Гомоморфизм колец с 1: требуем еще  $f(1_{R_1}) = 1_{R_2}$

**Def.** Изоморфизм между множествами  $f : M_1 \rightarrow M_2$  – биекция

$f : \mathbb{Z} \rightarrow \mathbb{Z} \quad f(x) = kx \quad x \in \mathbb{Z}$

$\begin{cases} k(x+y) = kx + ky \\ k(xy) \neq kx \cdot ky \end{cases} \Rightarrow f - \text{не гомоморфизм колец } (k \neq 1), \text{ но гомоморфизм групп}$

А если  $k = \pm 1 \Rightarrow$  изоморфизм

$G$  – группа  $f : G \rightarrow G \quad f(g) = g^{-1}$  – биекция  $\Rightarrow$  изоморфизм, если  $G$  – абелева

$\begin{cases} f : \mathbb{R} \rightarrow \mathbb{R} \\ f(x) = e^x \\ e^{x+y} = e^x \cdot e^y \end{cases} \Rightarrow f - \text{гомоморфизм, но точнее это } f : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \cdot), \text{ но не изоморфизм}$

$g : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \cdot)$  – изоморфизм

$g(x) = e^x$

**Th.** Китайская теорема об остатках

1.  $(m, n) = 1 \quad Z/mnZ \cong Z/mZ \times Z/nZ$
2.  $m_1, m_2 \dots m_k \in Z \quad (m_i, m_j) = 1$   
 $Z/m_1 m_2 \dots m_k Z \cong Z/m_1 Z \times \dots \times Z/m_k Z$
3.  $\forall a_1, a_2 \dots a_n \in Z; \quad m_1, m_2 \dots m_n \in Z : (m_i, m_j) = 1$   
 $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} - \text{имеет решение в } Z, \text{ единственное по модулю } m_1 m_2 \dots m_n$

### Доказательство

Индукция по  $k$ . База  $k = 2$

- База: строим  $\varphi : Z/mnZ \rightarrow Z/mZ \times Z/nZ$

$$\overline{a_{mn}} \rightarrow (\overline{a_m}, \overline{a_n})$$

$$(\overline{a_{mn}} = \overline{b_{nm}} \Rightarrow \overline{a_m} = \overline{b_m})$$

$\varphi$  – гомоморфизм:

$$\varphi(x+y) = \varphi(\overline{a_{mn}} + \overline{b_{mn}}) = \varphi(\overline{a+b_{mn}}) = (\overline{a+b_m}, \overline{a+b_n}) = (\overline{a_m} + \overline{b_m}, \overline{a_n} + \overline{b_n}) = (\overline{a_m}, \overline{a_n}) + (\overline{b_m}, \overline{b_n}) = \varphi(x) + \varphi(y)$$

$\varphi$  – биекция (смотри утверждение перед табличкой  $3 \times 5$ )

$$\forall a, b \exists x : \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \quad \text{и все такие } x \text{ имеют вид } x = x_0 + kmn$$

- Переход  $k \rightarrow k+1$

$m_1, m_2 \dots m_{k+1}$  попарно взаимнопросты  $\Rightarrow (m_1 m_2 \dots m_k, m_{k+1}) = 1 \Rightarrow$  по базе

$$Z/m_1 m_2 \dots m_{k+1} Z \cong Z/m_1 m_2 \dots m_k Z \times Z/m_{k+1} Z$$

По индукционному предположению  $Z/m_1 \dots m_k \cong Z/m_1 Z \times \dots \times Z/m_k Z$

$$\text{Итого } Z/m_1 \dots m_{k+1} Z \cong Z/m_1 \dots m_k Z \times Z/m_{k+1} Z \cong (Z/m_1 Z \times Z/m_2 Z \times \dots \times Z/m_k Z) \times Z/m_{k+1} Z \cong Z/m_1 Z \times \dots \times Z/m_k Z \times Z/m_{k+1} Z$$

**Rem.**  $(A \times B) \times C \neq A \times B \times C$

$$((a, b), c) \rightarrow (a, b, c)$$

- $\varphi$  – сюръективно, т.е.  $\forall y_1 \dots y_n \quad y_i \in Z/m_i Z$   
 $\exists z \in Z/m_1 \dots m_n Z : \varphi(z) = (y_1, y_2 \dots y_n)$

Возьмем  $y_i = \overline{a_i}$   $a_i \in Z$   $z = \overline{x m_1} \cdots m_n \Rightarrow \begin{cases} \overline{x m_1} = y_1 \\ \overline{x m_2} = y_2 \\ \dots \end{cases}$ , т.е.  $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \end{cases}$

Единственность  $x$  по модулю  $m_1 \cdots m_n$  – инъективность  $\varphi$

"Явная формула" для  $\varphi^{-1}$

Найдем  $\varphi^{-1}(1_{m_1}, 0_{m_2} \cdots 0_{m_k})$  это  $\overline{a}$ :  $a - 1 : m_1$   
 $a : m_2, \dots, m_k \Leftrightarrow a : m_2 \cdots m_k$

$a = m_2 \cdots m_k \cdot y$ ;  $m_2 \cdots m_k \cdot y - 1 = m_1 x$

$m_2 \cdots m_k \cdot y - m_1 x = 1$ . Далее ищем  $y$

$a = a_1$   $\varphi(\overline{a_1}) = (1, 0 \cdots 0)$

Аналогично находим  $\varphi(\overline{a_i}) = (0, 0 \cdots 1_{m_i} \cdots 0)$

Теперь  $\forall \overline{b_1}, \overline{b_2}, \dots, \overline{b_k}$  ( $b_i \in Z/m_i Z$ )

$\varphi(\overline{a_1 b_1} + \overline{a_2 b_2} + \cdots + \overline{a_k b_k}) = \varphi(\overline{b a_1}) + \varphi(\overline{b_2 a_2}) + \cdots + \varphi(\overline{b_k a_k}) = b_1 \varphi(\overline{a_1}) + b_2 \varphi(\overline{a_2}) + \cdots + b_k \varphi(\overline{a_k}) = b_1(1, 0 \cdots 0) + b_2(0, 1, 0 \cdots 0) + \cdots + b_k(0 \cdots 0, 1)$

**Rem.**  $\varphi(3x) = \varphi(\overline{x + x + x}) = \overline{3\varphi(x)}$

**Def.**  $G$  – группа.  $a \in G$ , порядок  $a$  –  $\min k \in N : a^k = e$ . Если такого  $k$  нет, то порядок  $= \infty$ . Обозначение:  $\text{ord}(a)$

**Lm.**

1.  $\text{ord}(a)$  – количество различных элементов в последовательности  $(e, a, a^2, a^3 \cdots)$
2.  $\text{ord}(a) = \infty \Rightarrow$  все элементы различны
3.  $\text{ord}(a) = k \in N$ , тогда  $a^m = a^n \Leftrightarrow m \equiv n \pmod{k}$

#### Доказательство

1. 2, 3  $\Rightarrow$  1 – упражнение

2.  $\text{ord}(a) = \infty$   $a^m = a^n$ , НУО  $m > 0$

$a^m \cdot a^{m-n} = a^n \cdot e \Rightarrow a^{m-n} = e$ ;  $m - n \in N$ , но  $\text{ord}(a) = \infty$  ???

3.  $\text{ord}(a) = k$   $m, n \in N$

$m = q_m \cdot k + r_m$ ;  $n = q_n \cdot k + r_n$

$$\begin{cases} a^m = a^{q_m \cdot k + r_m} = (a^k)^{q_m} \cdot a^{r_m} = a^{r_m} \\ a^n = a^{r_n} \\ r_m = r_n \end{cases} \Rightarrow a^m = a^n \Rightarrow a^{r_m} = a^{r_n} \Rightarrow a^{r_m - r_n} = e \text{ ???}$$

**Th.** Теорема Лагранжа

$G$  – группа,  $|G| = n$  ( $|G|$  – порядок группы)

$a \in G$ ;  $\text{ord}(a) = k \Rightarrow n : k$

#### Доказательство

Нарисуем оргграф  $\forall x \in G : x \rightarrow ax$

$\forall x \rightarrow$  цикл  $x \rightarrow ax \rightarrow a^2 x \rightarrow \cdots \rightarrow a^k x = x$

Все элементы  $G$  разбились на циклы длины  $k \Rightarrow n : k$

**Следствие:** малая теорема Ферма

$G = (Z/pZ)^*$ ;  $|(Z/pZ)^*| = p - 1$

$\text{ord}(\overline{a}) = k \Leftrightarrow \overline{a}^k = \overline{1}$ ;  $p - 1 : k$

$a^{p-1} = (\overline{a}^k)^{\overline{1}} = \overline{1}$

В  $Z/pZ$   $\overline{a}^{p-1} = \overline{1}$   $a \not\equiv 0 \Rightarrow a^{p-1} \equiv 1 \pmod{p} \Leftrightarrow a^{p-1} - 1 : p$

**Th.** Переформулировка теоремы Лагранжа

$G$  – конечная  $\Rightarrow a^{|G|} = e$

$e, a, a^2 \dots$  преиодична с периодом  $|G|$ , но возможно это не наименьший период  
 $G = (Z/pZ)^* \Rightarrow a^{p-1} = 1$  в  $Z/pZ \Leftrightarrow a^{p-1} \equiv 1 \pmod{p} \ (\forall a \not\equiv p)$

Или  $a \in Z; a^p - a : p \Leftrightarrow a(a^{p-1} - 1) : p \Leftrightarrow \begin{cases} a : p \\ a^{p-1} - 1 : p \end{cases}$

Что с произвольным  $n$ ? Хотим  $a^k \equiv 1 \pmod{n}$

$(a, n) \neq 1 \Rightarrow (a^k, n) \neq 1 \Rightarrow a^k \not\equiv 1 \pmod{n} \ (\forall k > 0) \Rightarrow$  вопрос имеет смысл только для  $(a, n) = 1 \Rightarrow \bar{a}$  – обратим в  $Z/nZ$

По теореме Лагранжа  $b \in (Z/nZ)^* \Rightarrow b^{|(Z/nZ)^*|} = 1$

Переформулировка:  $(a, n) = 1 \Rightarrow a^{|(Z/nZ)^*|} \equiv 1 \pmod{n}$  – теорема Эйлера

**Def.** Функция Эйлера  $\varphi(n) = |(Z/nZ)^*|$

**Rem.**  $\varphi(n) = \{x \in \{0, 1, \dots, n-1\} | (x, n) = 1\}$

**Ex.**  $p$  – простое. Знаем  $(Z/pZ)^* = (Z/pZ) \setminus \{0\}$

$\varphi(p) = p - 1$

Как найти  $\varphi(n)$ ?  $n = p_1^{a_1} p_2^{a_2} \dots$

**Rem1.**  $p$  – простое  $\Rightarrow \varphi(p^k) = \{x \in \{0, 1, \dots, p^k - 1\} | (p^k, x) = 1\} = \{x = 0 \dots p^k - 1 | x \not\equiv p\} = p^k - \{x = 0 \dots p^k - 1 | x \equiv p\} = p^k - \frac{p^k}{p} = p^k - p^{k-1}$

**Rem2.** Мультипликативность  $\varphi$

$m, n \in N \ (m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n)$

$\varphi$  – мультипликативная функция

**Remrem.**  $\tau(n)$  – количество делителей,  $\sigma(n)$  – сумма делителей. Обе эти функции тоже мультипликативны (упражнение)

**Явная формула для функции Эйлера**

$$\varphi(n) = \varphi(p_1^{a_1} \dots p_k^{a_k}) = \varphi(p_1^{a_1}) \dots \varphi(p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1-1}) \dots (p_k^{a_k} - p_k^{a_k-1}) = p_1^{a_1} (1 - \frac{1}{p_1}) \dots p_k^{a_k} (1 - \frac{1}{p_k}) = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} (1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}) = n (1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}) = n \prod_{p \in P: p|n} (1 - \frac{1}{p})$$

**Ex.**  $\varphi(600) = 600 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 160$

**Rem.**  $a^{\varphi(n)} = 1 \ (\forall a \in (Z/nZ)^*)$

$n : p, q \Rightarrow$  показатель  $\varphi(n)$  можно улучшить

$n = 105 = 3 \cdot 5 \cdot 7 \Rightarrow \varphi(n) = 2 \cdot 4 \cdot 6 = 48$

По теореме Эйлера  $(a, 105) = 1 \Rightarrow a^{48} \equiv 1 \pmod{105}$

$$\text{На самом деле (применим МТФ)} \ (a, 105) = 1 \Rightarrow a \not\equiv 3, 5, 7 \Rightarrow \begin{cases} a^2 \equiv 1 \pmod{3} \\ a^4 \equiv 1 \pmod{5} \\ a^6 \equiv 1 \pmod{7} \end{cases} \Rightarrow \begin{cases} a^{12} \equiv 1 \pmod{3} \\ a^{12} \equiv 1 \pmod{5} \\ a^{12} \equiv 1 \pmod{7} \end{cases} \Rightarrow \Rightarrow a^{12} \equiv 1 \pmod{105}$$

### Доказательство мультипликативности

Знаем:  $(m, n) = 1 \Rightarrow Z/mnZ \cong Z/mZ \times Z/nZ \Rightarrow \varphi(ab) = \varphi(a) \cdot \varphi(b)$

$\varphi$  – изоморфизм.  $x$  – обратим  $\Leftrightarrow \varphi(n)$  – обратим

$x$  – обратим  $\Leftrightarrow \exists y : x \cdot y = 1. \varphi(xy) = \varphi(x) \cdot \varphi(y) = 1 = \varphi(1) \Rightarrow \varphi$  – обратим

Обратно:  $\varphi(x)$  – обратим.  $\varphi(x) \cdot z = 1 \Rightarrow \varphi^{-1}(\varphi(x) \cdot z) = \varphi^{-1}(1). \varphi^{-1}(\varphi(x)) \cdot \varphi^{-1}(z) = \varphi^{-1}(1) \Rightarrow x$  – обратим

**Следствие:**  $(Z/mnZ)^* = (Z/mZ \times Z/nZ)^*$

**Утверждение.**  $R_1, R_2$  – кольца.  $(R_1 \times R_2)^* = R_1^* \times R_2^*$

### Доказательство

$$(r_1, r_2) \in R_1 \times R_2 \text{ – обратим} \Leftrightarrow \exists (s_1, s_2) : (r_1, r_2)(s_1, s_2) = 1_{R_1 \times R_2} \Leftrightarrow (r_1 s_1, r_2 s_2) = (1_{R_1}, 1_{R_2}) \Leftrightarrow \begin{cases} \exists s_1 : r_1 s_1 = 1 \\ \exists s_2 : r_2 s_2 = 1 \end{cases} \Leftrightarrow \Leftrightarrow \begin{cases} r_1 \in R_1^* \\ r_2 \in R_2^* \end{cases}$$

**Следствие:**  $|(Z/mZ \times Z/nZ)^*| = |(Z/mZ)^* \times (Z/nZ)^*| = |(Z/mZ)^*| \cdot |(Z/nZ)^*|$

Итого:  $\varphi(mn) = \varphi(m) \cdot \varphi(n)$

Вопрос:  $p \in P$ .  $\exists$  ли  $\bar{a} \in Z/pZ : \{\bar{a}, \bar{a}^2 \dots\} = \{\bar{1}, \bar{2} \dots \overline{p-1}\}$

**Def.**  $(G, \cdot)$  – группа;  $a \in G$

$\langle a \rangle = \{a^k | k \in Z\}$  – группа, порожденная элементом  $a$

**Утверждение.** Это действительно группа (относительно  $\cdot$ )

### Доказательство

- Замкнутость.  $x, y \in \langle a \rangle$   
 $x = a^e; y = a^m \Rightarrow xy = a^{e+m} \in \langle a \rangle$
- Ассоциативность – очев
- $\exists e \in G; e = a^0 \in \langle a \rangle$
- $x \in \langle a \rangle \Rightarrow x = a^k \Rightarrow x^{-1} = a^{-k} \in \langle a \rangle$

$\langle a \rangle$  – подгруппа в  $G$ . Может быть  $\langle a \rangle = G$  или  $\langle a \rangle \neq G$

**Def.** Если  $\exists a \in G : \langle a \rangle = G \Rightarrow G$  называется циклической

**Th.**  $G$  – циклическая

1.  $|G| = \infty \Rightarrow G \cong (Z, +)$
2.  $|G| = n < \infty \Rightarrow G \cong (Z/nZ, +)$

### Доказательство

$G = \langle a \rangle$ . Знаем:  $\text{ord}(a) = k \Rightarrow$  в  $\langle a \rangle$   $k$  элементов. Иначе ( $\text{ord}(a) = \infty$ )  $\Rightarrow$  все  $\{a^k | k \in Z\}$  попарно различны

1. Строим гомоморфизм  
 $\varphi: Z \rightarrow G; k \rightarrow a^k$   
 Это биекция (см. выше) и  $\varphi(x+y) = a^{x+y} = a^x \cdot a^y = \varphi(x) \cdot \varphi(y)$  – точно гомоморфизм
2. ( $k = n$ )  $\text{ord}(a) = n$ .  $\langle a \rangle = \{e, a, a^2 \dots a^{n-1}\}$   
 $(a^n = e; a^{-1} = a^{n-1})$   
 $\varphi: Z/nZ \rightarrow \langle a \rangle; \bar{p} \rightarrow a^p$  – биекция и гомоморфизм (упражнение)  
 Корректность:  $q: \bar{p} = \bar{q} \Rightarrow p - q : n$   
 $p = q + ln \Rightarrow a^p = a^{q+ln} = a^q \cdot (a^n)^l = a^q \Rightarrow a^p = a^q$

**Ex.**  $(Z/3Z)^* = \langle 2 \rangle: \bar{2}^2 = 1$  ( $\text{ord}(\bar{2}) = 2$ )

Изоморфизм:  $(Z/2Z, +) \rightarrow (Z/3Z, \cdot)$

$\bar{0}_2 \leftrightarrow \bar{1}_3$

$\bar{1}_2 \leftrightarrow \bar{2}_3$

$(Z/5Z)^* = \{1, 2, 3, 4\} = \langle \bar{2} \rangle$  ( $\text{ord}(2) = 4$ ). Поэтому  $(Z/5Z)^* \cong (Z/4Z, +)$

**Th.**  $p \in P \Rightarrow (Z/pZ)^*$  – циклическая

**Следствие.**  $(Z/pZ)^* \cong (Z/(p-1)Z, +)$

$\exists a \in Z : \langle \bar{a} \rangle = \{1, 2 \dots p-1\}$

$a$  называется первообразным корнем по модулю  $p$

$a$  – первообразный корень  $\text{mod } p \Leftrightarrow \text{ord}(\bar{a}) = p-1$ , т.е.  $|\langle \bar{a} \rangle| = p-1 = |(Z/pZ)^*|$

**Lm.**  $G$  – группа  $|G| = N$ .  $f: G \rightarrow G: f(a) = a^k$

Тогда  $f_k$  – биекция  $\Leftrightarrow (k, N) = 1$



## Доказательство

Только  $\Leftarrow$ :

$(k, N) = 1 \Rightarrow \exists x, y : xk + yN = 1 \Rightarrow \forall a \in G; a = a^1 = a^{xk+yN} = (a^k)^x \cdot (a^N)^y$  по переформулировке теоремы  
Лагранжа  $= (a^k)^x \Rightarrow f_x$  – обратное к  $f_k$

## Алгоритм RSA (шифрование с открытым ключом)

Алиса (А) хочет получать сообщения от Боба (В)

А придумывает  $p, q$  – простые (достаточно большие)  $N = pq$

$\varphi(N) = (p-1)(q-1)$ . А выбирает  $x : (x, \varphi(N)) = 1$  и  $y : (x-y) \equiv 1 \pmod{\varphi(N)}$

Тогда как в Лм.  $f_x(a) = a^x; f_y(a) = a^y$  – взаимно обратные отображения

А сообщает В  $x$

В хочет послать А сообщение.  $a \in (Z/NZ)^*$

Шифрование:  $a \rightarrow a^x = b$  и посылает А

А получает  $b = a^x$ , вычисляет  $b^y = a$

Что нужно чтобы дешифровать  $b$ ? Надо знать  $y$

$N, x$  известны всем.  $xy \equiv 1 \pmod{\varphi(N)}$

$yx + \varphi(N)z = 1$  – линейное Диофантово уравнение. Легко решается зная  $x, \varphi(N)$

Нужно сделать так, чтобы  $\varphi(N)$  было сложно узнать

Вопрос: как найти большие простые числа?

$p$  – большое натуральное число. Как проверить, что  $p$  – простое?

Рассмотрим  $n \in \mathbb{N}$ .  $n-1 = p_1^{a_1} \dots p_s^{a_s}$ , т.е.  $n = \prod p_i^{a_i} + 1$ . Простое ли  $n$ ?

**Th.** Тест Люка

Пусть  $n = \prod p_i^{a_i} + 1, a \in \mathbb{Z}$

$$\begin{cases} a^{n-1} \equiv 1 \pmod{n} \\ a^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n} \end{cases} \Rightarrow n - \text{простое}$$

## Доказательство

В  $(Z/nZ)^*$   $\text{ord}(a) = ?$

$$\begin{cases} a^{n-1} \equiv 1 \Leftrightarrow n-1 : \text{ord}(a) \\ a^{\frac{n-1}{p_i}} \not\equiv 1 \Leftrightarrow \frac{n-1}{p_i} \not: \text{ord}(a) \end{cases} \Rightarrow n-1 = \text{ord}(a) \Rightarrow |(Z/nZ)^*| \geq |<a>| = n-1$$

$\varphi(n) \geq n-1 \Leftrightarrow 1, 2 \dots n-1$  взаимнопросты с  $n \Rightarrow n$  – простое

Вопрос: какая доля  $a \in \{1, 2 \dots n\}$  удовлетворяет условию Люка, если  $n$  – простое?

$a \in \{1 \dots n-1\} \Rightarrow \bar{a} \in (Z/nZ)^*$ . Какова вероятность:  $\text{ord}(\bar{a}) = n-1$ ?

Знаем:  $n$  – простое  $\Rightarrow (Z/nZ)^*$  – циклическая.  $(Z/nZ)^* = \langle b \rangle$   $\text{ord}(b) = n-1$

$\forall a \in (Z/nZ)^* \exists k : b^k = a; k \in \{1, 2 \dots n-1\}$

**Утверждение:**  $\text{ord}(a) = n-1 \Leftrightarrow (k, n-1) = 1$

**Следствие:** Доля подходящих под тест Люка  $a = \frac{\varphi(n-1)}{n-1} = p \in [0; 1]$

Делаем тест Люка  $s$  раз  $\Rightarrow \begin{cases} \text{попадетс} \text{я хорошее } a \Rightarrow n - \text{простое} \\ \text{все время плохие } a \Rightarrow (1-p)^s \rightarrow 0 \end{cases}$

**Lm.**  $\text{ord}(x) = n \Rightarrow \text{ord}(x^k) = \frac{n}{(n,k)}$  (утверждение: частный случай)

$$(n, k) = d \Rightarrow \begin{cases} n = dn_1 \\ k = dk_1 \end{cases} \Rightarrow (x^k)^{\frac{n}{(n,k)}} = (x^{dk_1})^{n_1} = 1^{n_1} = 1$$

Пусть  $(x^k)^l = 1; x^{kl} = 1 \Leftrightarrow kl : \text{ord}(x) \Leftrightarrow dk_1 l : dn_1 \Leftrightarrow k_1 b : n_1 \Leftrightarrow l : n_1$ , т.е.  $n_1 = \min(l)$

**Нестойкость простых из теста Люка**

Пусть  $p, q$  – простые получены тестом Люка, т.е. у  $p-1$  и  $q-1$  маленькие простые множители

$N = pq$ . Как зная все разложить  $N$ ?

$$a \in N; \begin{cases} \text{ord}_p(a) = p_1^{b_1} \dots p_k^{b_k} \\ \text{ord}_q(a) = p_1^{c_1} \dots p_k^{c_k} \end{cases}$$

$$\begin{cases} A = \min(x|x! : \text{ord}_p(a)) \\ B = \min(x|x! : \text{ord}_q(a)) \end{cases} \Rightarrow A, B \text{ не очень большие, скорее всего } A \neq B$$

Враг считает  $d_k = (a^{k!} - 1, n)$ . НУО  $A < B$ . Тогда  $d_A = p$ ;  $a := \frac{N}{b}$ . Взломано

### Тест Ферма:

$n \in \mathbb{Z}$ ;  $a \in \{1 \dots n-1\}$ .  $n$  тестируем,  $a$  – случайное

$a^{n-1} \not\equiv 1 \pmod{n} \Rightarrow n$  – составное

$a^{n-1} \equiv 1 \pmod{n} \Rightarrow n$  – может быть простое

( $n = 15$ ;  $n-1 = 14$ ;  $4^{14} \equiv 1 \pmod{15}$ ), но 15 не простое)

$a$  – свидетель простоты  $\pmod{n}$ , если  $a^{n-1} \equiv 1 \pmod{n}$

**Утверждение:** (упражнение) если не все числа  $\{1 \dots n-1\}$  – свидетели, то свидетелей  $\leq$  половины

$a$  – свидетель,  $b$  не свидетель  $\Rightarrow ab$  не свидетель. В этом случае за  $s$  тестов  $p(\text{неудачи}) \leq (\frac{1}{2})^s \rightarrow 0$

Проблема:  $\exists n$  – составные :  $\forall a \in (\mathbb{Z}/n\mathbb{Z})^*$  – свидетель простоты

Это числа Кармайкла. Наименьшее такое число  $n = 561 = 3 \cdot 11 \cdot 17$

$$a \in \{3, 11, 17\}; \begin{cases} a^2 \equiv 1 \pmod{3} \\ a^{10} \equiv 1 \pmod{11} \\ a^{16} \equiv 1 \pmod{17} \end{cases} \Rightarrow a \equiv 1 \pmod{561} \Rightarrow a^{560} \equiv 1 \pmod{561}, \text{ но } 561 \text{ не простое}$$

### Тест Рабина-Миллера:

$p \in \mathbb{Z}$ ;  $p-1 = 2^m \cdot l$ ;  $l \not\equiv 2$

$a \in \mathbb{Z}$ ;  $a \not\equiv p$ . Рассмотрим в  $\mathbb{Z}/p\mathbb{Z}$  последовательность  $\bar{a}^l, \bar{a}^{2l} \dots \bar{a}^{2^{m-1}l} = \bar{a}^{p-1} = 1$

**Утверждение:** Если  $p$  – простое, то  $\begin{cases} \bar{a}^l = 1 \\ \exists k : \bar{a}^{2^k l} = -1 \end{cases} (*)$

### Доказательство

Пусть  $a^l \neq 1$ ;  $a^{p-1} = 1 \Rightarrow \exists k : \bar{a}^{2^k l} \neq 1$ ;  $\bar{a}^{2^{k+1}l} = 1$

$$\Rightarrow \text{в } \mathbb{Z}/p\mathbb{Z} \ x \neq 1; \ x^2 = 1 \Rightarrow (x-1)(x+1) = 0 \Rightarrow \begin{cases} x-1 = 0 \\ x+1 = 0 \end{cases} \Rightarrow x = -1$$

\* – условия Рабина-Миллера для числа  $a$

Знаем:  $\exists a \not\equiv p$ . Рабин-Миллер для  $a$  не выполнен  $\Rightarrow p$  – составные

**Th.** Если все  $a = 1, 2 \dots \sqrt[p]{p}$  свидетели Рабина-Миллера  $\Rightarrow p$  – простое

**Th.** Если все  $a = 1, 2 \dots c \cdot \log^2 p$  свидетели  $\Rightarrow p$  – простое. (следует из гипотезы Римана)

**Th.**  $n$  – составное  $\Rightarrow$  свидетелей Рабина-Миллера  $\leq \frac{\varphi(n)}{4}$

**Следствие:** делаем  $s$  ходов.  $p(\text{неудачи}) = (\frac{1}{4})^s \rightarrow 0$

## Квадратичные вычеты

$\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ . Как решать уравнения в  $\mathbb{Z}/p\mathbb{Z}$ ?

1. Линейные  $\bar{a}x = \bar{b} \Leftrightarrow ax \equiv b \pmod{p} \Leftrightarrow ax - py = b$

2. Квадратные  $ax^2 + bx + c = 0$ ;  $a \neq 0$

$x^2 + sx + q = 0$ . Если  $p \neq 2$ , то

$$(x + \frac{s}{2})^2 + (q - \frac{s^2}{4}) = 0 \Leftrightarrow y^2 = k, \text{ где } y = x + \frac{s}{2}; \quad -k = q - \frac{s^2}{4}$$

Как понять, что  $\exists y : y^2 \equiv k \pmod{p}$  в  $\mathbb{Z}/p\mathbb{Z}$

Или для каких  $p \exists y : (y^2 - k : p)$

Если такой  $y$  существует,  $k$  называется квадратичным вычетом по модулю  $p$ . ( $k \neq 0$ )

$$\text{Символ Лежандра } \left(\frac{a}{p}\right) = \begin{cases} 1, & a - \text{квадратичные вычет} \\ -1, & a - \text{не квадратичные вычет} \\ 0, & a : p \end{cases}$$

**Утверждение:**  $\exists$  ровно  $\frac{p-1}{2}$  квадратичных вычетов и  $\frac{p-1}{2}$  квадратичных неравенства

### Доказательство

$$1, 2 \dots p-1$$

$$1^2, 2^2 \dots (p-1)^2$$

Сколько различных вычетов во второй строке? Заметим:  $x^2 = y^2 \Rightarrow (x-y)(x+y) = 0 \Leftrightarrow \begin{cases} x = y \\ x = -y \end{cases} \Rightarrow$   
при возведении в квадрат вычеты склеиваются, попадая  $\Rightarrow$  ровно  $\frac{p-1}{2}$  квадратов  $\Rightarrow p-1 - \frac{p-1}{2} = \frac{p-1}{2}$   
не квадратов

$$\text{Мультипликативность: } \forall a, b. \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

### Доказательство

$$\left(\frac{ab}{p}\right) = 0 \Leftrightarrow ab : p \Leftrightarrow \begin{cases} a : p \\ b : p \end{cases} \Leftrightarrow \begin{cases} \left(\frac{a}{p}\right) = 0 \\ \left(\frac{b}{p}\right) = 0 \end{cases}$$

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = 1 \Rightarrow \begin{cases} a = x^2 \\ b = y^2 \end{cases} \Rightarrow ab = (xy)^2 \Rightarrow \left(\frac{ab}{p}\right) = 1$$

$$\left(\frac{a}{p}\right) = 1; \left(\frac{b}{p}\right) = 1 \Rightarrow \exists x : a = x^2; b \neq y^2 \forall y$$

$$\text{Пусть } \begin{cases} ab = z^2 \\ a = x^2 \end{cases} \Rightarrow b = \left(\frac{z}{x}\right)^2 \text{ ???}$$

$$\left(\frac{a}{p}\right) = -1; \left(\frac{b}{p}\right) = -1$$

$b_1, b_2 \dots b_{\frac{p-1}{2}}$  – квадраты, все остальные не квадраты

Идем  $ab_1, ab_2 \dots ab_{\frac{p-1}{2}}$  – не квадраты (все, т.к. их  $\frac{p-1}{2}$ )  $\Rightarrow$  все остальные квадраты

$$\{ab_1, ab_2 \dots ab_{p-1}\} = \{1, 2 \dots p-1\}$$

**Утверждение:** Квадратичный закон взаимности

$$\text{Если } p, q - \text{нечетные простые} \Rightarrow \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \dots \frac{q-1}{2}}$$

$R$  – коммутативное кольцо с 1

$f(x) = 3x^2 + 2x$  имеет смысл в любом кольце с 1, т.к.  $f(x) = (1+1+1) \cdot x \cdot x + (1+1) \cdot x$

**Ех.**  $g, f : Z/pZ \rightarrow Z/pZ$

$$\begin{cases} f(x) = x \\ g(x) = x^p \end{cases} \Rightarrow \text{по МТФ одна и та же функция, но многочлены различные}$$

$$x^2 + 2x + 5 \rightarrow (1, 2, 5)$$

## Формальные степенные ряды

**Def.** Пусть  $R$  – коммутативное кольцо с 1. Кольцом формальных степенных рядов  $R[[x]]$  называется множество  $f : Z_{\geq 0} \rightarrow R; \{a_0, a_1, a_2 \dots | a_i \in R\}$  с операциями  $+, \cdot$

Ряд:  $a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$

$$(a_0, a_1, a_2 \dots) + (b_0, b_1, b_2 \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \dots)$$

$(a_i) \cdot (b_i) = (c_i)_{i=0}^\infty$ ;  $c_i = \sum_{k=0}^i a_k b_{i-k}$  – правило свертки

**Th.**  $R[[x]]$  – коммутативное кольцо с 1

### Доказательство

Очев – аксиомы сложения:  $(0, 0 \dots) = 0_{R[[x]]}$

$1_{R[[x]]} = (1, 0, 0 \dots)$

$(a + b) \cdot c$  – очев (покоординатно)

$$ab = ba : (ab)_i = \sum_{k=0}^i a_k b_{i-k} = \sum_{l=0}^i a_{i-l} b_l = \sum_{l=0}^i b_l a_{i-l} = (ba)_i$$

Ассоциативность:  $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ ;  $f, g, h \in R[[x]]$

$f = (a_0, a_1, a_2 \dots a_i \dots)$ ;  $f_i = a_i$

$$\begin{aligned} ((f \cdot g) \cdot h)_n &= \sum_{k=0}^n (fg)_k h_{n-k} = \sum_{k=0}^n \left( \sum_{i=0}^k f_i g_{k-i} \right) h_{n-k} = \sum_{k=0 \dots n; i=0 \dots k} f_i g_{k-i} h_{n-k} = \sum_{p,q,r \geq 0; p+q+r=n} (f_p g_q) h_r = \\ &= \sum_{p,q,r \geq 0; p+q+r=n} f_p (g_q h_r) = \sum_{p,q,r \geq 0; p+q \leq n} f_p (g_q h_{n-p-q}) = \sum_{r=0}^n f_p \left( \sum_{q=0}^r g_q h_{(n-p)-q} \right) = \sum f_p (gh)_{n-p} = (f(gh))_n \end{aligned}$$

**Lem.**  $\exists$  инъективный гомоморфизм колец

$$\begin{aligned} i : R &\rightarrow R[[x]] \\ a &\rightarrow (a, 0, 0 \dots) \end{aligned}$$

### Доказательство

$$\text{Нужно доказать } \begin{cases} \text{инъективность} \\ i(x+y) = i(x) + i(y) \\ i(xy) = i(x) \cdot i(y) \\ i(1) = 1 \end{cases} \quad - \text{ все очев}$$

В умножении  $(a, 0, 0 \dots) \cdot (b, 0, 0 \dots) = (ab, 0, 0 \dots)$

**Def.**  $x = (0, 1, 0, 0 \dots)$

$$\text{Lem. } a \in R \begin{cases} ax = (0, a, 0, 0 \dots) \\ x^2 = (0, 0, 1, 0, 0 \dots) \\ x^k = (0, 0, 0 \dots 1, 0, 0 \dots) \end{cases}$$

$(a_0, a_1, a_2 \dots a_k, 0, 0 \dots) = a_0 + a_1 x + a_2 x^2 + \dots a_k x^k$  – следствие из леммы и правила сложения

**Def.**  $f \in R[[x]]$  называется многочленом, если  $\exists N : \forall n > N \ f_n = 0$

**Обозначение:** множество многочленов обозначается  $R[x]$

**Lem.**  $R[x]$  – подкольцо в  $R[[x]]$

### Доказательство

$0, 1 \in R[x]$  – очев

$(a_n) \in R[x] \Rightarrow (-a_n) \in R[x]$  – тоже очев

$$\begin{aligned} (b_i), (a_i) \in R[x] \Rightarrow (b_i + a_i) \in R[x] &\begin{cases} \exists N_1 : a_n = 0; \ n > N_1 \\ \exists N_2 : b_n = 0; \ n > N_2 \end{cases} \Rightarrow (a+b)_n = 0; \ n > \max(N_1; N_2) \ (a \cdot b)_n = 0 = \\ = \sum_{i=0}^n a_i b_{n-i}; \ n > N_1, N_2 \Rightarrow &\begin{cases} i > N_1 \\ n-i > N_2 \end{cases} \Rightarrow a_i b_{n-i} = 0 \ \forall i \Rightarrow (ab)_n = 0 \end{aligned}$$

**Th.**  $S$  – коммутативное кольцо;  $f : R \rightarrow S$  – гомоморфизм (e.g.  $R = S$ ;  $f = id$ );  $s \in S$ . Тогда  $\exists! f_s : R[x] \rightarrow S$  продолжающий  $f$

$$f_s|_R = f; \quad f_s \circ i = f; \quad f_s(x) = s$$

### Доказательство

$$g \in R[x] \Rightarrow g = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

$$\text{Положим } f_s(g) = f(a_0) + f(a_1)s + f(a_2)s^2 + \dots + f(a_n)s^n$$

$$f_s(gh) = f_s(g) \cdot f_s(h) - \text{муторная проверка}$$

Сложение – очев проверка

Единственность – очев

**Rem.**  $f_s$  называется гомоморфизм эвалюации

**Rem.**  $R = S$ ;  $f \rightarrow f(s)$  – значение многочлена в точке  $S$

$f \in R[x]$ ;  $P(f) : R \rightarrow R : a \rightarrow f(a)$  – полиномиальная функция, заданная  $f$

Знаем: может быть такое, что  $f_1 \neq f_2$ , но  $P(f_1) = P(f_2)$  (e.g.  $x^p$  и  $x$  в  $Z/pZ$ )

$$\text{Степень многочлена: } f = \sum_{i \in \mathbb{Z}_{\geq 0}} a_i x^i$$

$$\deg(f) = \max\{i | a_i \neq 0\}; f \neq 0$$

$$\deg(0) = -\infty$$

Свойства степени:

$$1. \deg(f + g) \leq \max(\deg(f), \deg(g))$$

$$\deg(f + g) = \max(\deg(f), \deg(g)) \text{ если } \deg(f) \neq \deg(g)$$

$$2. \deg(fg) = \deg(f) + \deg(g)$$

$$f = \sum a_i x^i; g = \sum b_j x^j$$

Тогда  $(fg)_s = 0$  при  $s > n + m$

$$(fg)_{n+m} = a_{n+m}b_0 + a_{n+m-1}b_1 + \dots + a_nb_m + a_{n-1}b_{m+1} \dots = a_nb_m$$

Итого:  $(fg)_{n+m} = a_nb_m \neq 0 \Rightarrow \deg(fg) = \deg(f) + \deg(g)$  – но верно только если  $R$  – область целостности, т.к. нет делителей нуля

Далее  $R$  – область целостности, еще лучше:  $R = K$  – поле

**Следствие:**  $R$  – область целостности  $\Rightarrow R[x]$  – область целостности

**Th.** О делении с остатком

$K$  – поле,  $f, g \in K[x] (g \neq 0)$ , тогда  $\exists! q, r \in K[x] : f = gq + r; \deg(r) < \deg(g)$

**Def.**  $a$  – корень  $f$ , если  $f(a) = 0$

**Th.** Теорема Безу: остаток от деления  $f$  на  $(x - a)$  равен  $f(a)$ . В частности  $a$  – корень  $f \Leftrightarrow f : x - a$

### Доказательство

По теореме о делении с остатком

$$f = (x - a)q + r; \deg(r) < \deg(x - a) = 1 \Rightarrow \begin{cases} \deg(r) = 0 \\ r = 0 \end{cases} \Leftrightarrow r = c \in K$$

$$f(x) = (x - a)q(x) + k$$

$$f(a) = (a - a)q(a) + k = k$$

TODO

$$f = ax^n + f_1; f \circ \deg(f_1) < n$$

$$g = bx^m + g_1; \deg(g_1) < m$$

$$\tilde{f} = f - \frac{a}{b}x^{n-m}g = ax^n + f_1 - ax^n - \frac{a}{b}x^{n-m}g_1 = f_1 - \frac{a}{b}x^{n-m}g_1$$

$$\deg(\tilde{f}) < n \text{ по и.п. } \exists \tilde{q}, \tilde{r} : \tilde{f} = g \cdot \tilde{q} + \tilde{r}; \deg(\tilde{r}) < \deg(g)$$

$$\text{Тогда } f = \tilde{f} + \frac{a}{b}x^{n-m}g = g(\tilde{q} + \frac{a}{b}x^{n-m}) + \tilde{r}$$

$$\text{Положим } q = \tilde{q} + \frac{a}{b}x^{n-m}; r = \tilde{r}$$

**Th.**  $k$  – поле,  $f \in k[x], \deg(f) = n \in \mathbb{Z} \Rightarrow f$  имеет не более  $n$  корней

### Доказательство

Индукция по  $n$ . База  $n = 1$  – очев

$$n \rightarrow n + 1. \deg(f) = n + 1$$

1. У  $f$  0 корней.  $0 \leq n + 1$

2. У  $f$  есть корень  $a \Rightarrow f = (x - a)\tilde{f}$

$$b - \text{корень } f \Leftrightarrow (b - a)\tilde{f}(b) = a \Leftrightarrow \begin{cases} b - a = 0 \\ \tilde{f}(b) = 0 \end{cases} \Leftrightarrow \begin{cases} b = a \\ b - \text{корень?} \end{cases}$$

По и.п.  $\deg(\tilde{f}) = n$ . У  $\tilde{f}$  не больше  $n$  корней, у  $f \leq n + 1$  корня

**Th.** О формальном и функциональном равенстве

1.  $k$  – поле.  $f, g \in k[x]$ ;  $a_1 \dots a_n \in k$ ;  $n > \max(\deg(f), \deg(g))$

$$f(a_i) = g(a_i) \forall i \Leftrightarrow f = g$$

2.  $k$  – бесконечно,  $f(a) = g(a) \forall a \in k \Rightarrow f = g$

$$1 \Rightarrow 2 : \text{возьмем любые } a_1 \dots a_n \in k : n > \max(\deg(f), \deg(g))$$

### Доказательство

1.  $h := f - g$ ;  $\deg(h) \leq \max(\deg(f), \deg(g)) < n$

При этом  $h(a_i) = f(a_i) - g(a_i) = 0$ ;  $a_1 \dots a_n$  – корни  $h$ ,  $n > \deg(h) \Rightarrow h = 0 \Leftrightarrow f = g$

**Rem.**  $f, g \in \mathbb{Z}/p\mathbb{Z}[x]$ ;  $\deg(f), \deg(g) < p \Rightarrow$  по предыдущей теореме  $f \neq g$  как функции  
 $|\{f | \deg f < p\}| = |\{a_0 + a_1x + \dots + a_{p-1}x^{p-1}\}| = p^p$

$$\text{Функций: } \begin{cases} f(0) = b_0 \\ f(1) = b_1 \\ \vdots \\ f(p-1) = b_{p-1} \end{cases} \Rightarrow \text{всего } p^p$$

**Lm.**  $a_1, a_2 \dots a_k$  – корни  $f : a_i \neq a_j \Rightarrow f \div (x - a_1)(x - a_2) \dots (x - a_k)$

## Интерполяция

**Def.**  $k$  – поле. Интерполяционные данные

$x$	$x_1 \dots x_n \in k$	$x_i \neq x_j$
$f(x)$	$y_1 \dots y_n \in k$	

Интерполяционная задача: построить  $f \in k[x]$  такую, что  $f(x_i) = y_i \forall i$

**Th.**

1.  $\forall$  интерполяционная задача имеет решение

2. Оно единственно при ограничении  $\deg(f) < n$  (а вообще бесконечно много)

### Доказательство

2. Пусть  $f_1, f_2$  – два решения.  $\deg(f_i) < n$

По теореме о формальном и функциональном равенстве  $f_1 = f_2$  ( $f_1(x_i) = y_i = f_2(x_i)$ )

1. Рассмотрим  $L_i(x) = \frac{(x-x_1)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)}{(x_i-x_1)\dots(x_i-x_{i-1})(x_i-x_{i+1})\dots(x_i-x_n)}$

$$L_i = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)}$$

$$L_i(x_i) = 1; \text{ при } i \neq j \quad L_i(x_j) = 0$$

$$\deg(L_i) = n - 1$$

$$\text{Положим } f = \sum y_i L_i$$

$$\forall k \quad f(x_k) = \sum y_i L_i(x_k) = y_k L_k(x_k) + \sum y_i L_i(x_k) = y_k$$

$$\text{Итог: } f = \sum_{i=1}^n \frac{y_i \prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)} - \text{интерполяционная формула Лагранжа}$$

**Rem.** Это все КТО:

$$\text{Интерполяционная задача} \Leftrightarrow \begin{cases} f \equiv y_1 \pmod{x - x_1} \\ \vdots \\ f \equiv y_n \pmod{x - x_n} \end{cases}$$

Вернемся к теории чисел

**Th.**  $(Z/pZ)^* = \langle a \rangle$ .  $\exists a : \{\bar{a}, \bar{a}^2, \bar{a}^3 \dots\} = \{\bar{1}, \bar{2} \dots\}$ .  $a$  – первообразный корень по модулю  $p$

Надо доказать:  $\exists a \in (Z/pZ)^* : \text{ord}(a) = p - 1$

**LmA.**  $\forall n \in N \sum_{d|n} \varphi(d) = n$

**Доказательство LmA:**

$$\{1, 2, \dots, n\} = A_{d_1} \cup A_{d_2} \dots; A_d = \{x \leq n | (x, n) = d\}$$

$$|A_d| = |\{dy \leq d \cdot \frac{n}{d} | (dy, d \frac{n}{d}) = d\}| = |\{y \leq \frac{n}{d} | (y, \frac{n}{d}) = 1\}| = \varphi(\frac{n}{d})$$

$$\text{Тогда } n = |\{1 \dots n\}| = \sum_{d|n} |A_d| = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{x|n} \varphi(x)$$

**LmB.**  $\forall d$  – делителя  $n$  в  $(Z/pZ)^*$  есть либо 0, либо  $\varphi(d)$  элементов порядка  $d$

**Доказательство LmB:**

Пусть  $a \in (Z/pZ)^* : \text{ord}(a) = d$

$a^d = 1$ ;  $1, a, a^2 \dots a^{d-1}$  попарно различны

Заметим:  $\text{ord}(b) = d \Rightarrow b^d = 1 \Rightarrow b \in \{1, a, a^2 \dots a^{d-1}\}$ , так как иначе у многочлена  $x^d - 1$   $d$  корней в  $Z/pZ$   
 $b = a^k$ ;  $\text{ord}(b) = d$ ;  $b^l \neq 1$  при  $l < d \Leftrightarrow a^{kl} \neq 1$  при  $l < d \Leftrightarrow kl \not\equiv 0 \pmod{d}$  при  $l < d \Leftrightarrow (k, d) = 1 - \varphi(d)$  вариантов

### Доказательство (Th.)

Докажем:  $d$  – делитель  $p - 1 \Rightarrow$  в  $(Z/pZ)^*$  ровно  $\varphi(d)$  элементов порядка  $d$  (в частности  $d = p - 1 \Rightarrow$  есть элементы порядка  $p - 1$ )

По LmA.  $p - 1 = \sum_{d|p-1} \varphi(d)$ , но  $p - 1 = |(Z/pZ)^*| = |\bigcup_{d|p-1} B_d| = \sum |B_d|$ , где  $B_d = \{a | \text{ord}(a) = d\}$

$$p - 1 = \sum_{d|p-1} |B_d| = \sum_{d|p-1} \varphi(d) \Rightarrow |B_d| = \varphi(d). \text{ В частности } |B_{p-1}| = \varphi(p - 1) > 0$$

Хотим ОТА для многочленов ...

**Def.** Область целостности  $R$  называется евклидовым кольцом, если  $\exists \varphi : R \setminus \{0\} \rightarrow Z_{\geq 0}$  (евклидова норма),

такая, что  $\forall a, b \in R, b \neq 0 \exists q, r : a = bq + r \begin{cases} \varphi(r) < \varphi(b) \\ r = 0 \end{cases}$

**Смысл.** В евклидовом кольце можно делать алгоритм евклида (понижая  $\varphi$ )

**Def.**  $R$  – область целостности.  $R$  – евклидово, если  $\exists \varphi : R \setminus \{0\} \rightarrow Z_{\geq 0}$  – евклидова норма

$$\forall a, b \in R, b \neq 0; \exists q, r : a = b \cdot q + r \begin{cases} r = 0 \\ \varphi(r) < \varphi(b) \end{cases}$$

**Th.** В евклидовом кольце любой идеал главный

### Доказательство

$I$  – идеал в  $R$ ;  $I \neq \{0\}$  (иначе  $I = \langle 0 \rangle$ )

Рассмотрим  $i \in I : \varphi(i)$  – минимальна

$$\text{Тогда } \forall a \in I \ a = q \cdot i + r \begin{cases} \varphi(r) < \varphi(i) \\ r = 0 \end{cases}$$

Но  $r = a - q \cdot i \in I \Rightarrow \varphi(r) \geq \varphi(i) \Rightarrow r = 0$ , т.е.  $a = qi \forall a \in I$ , т.е.  $I \in \langle i \rangle \Rightarrow I = \langle i \rangle$

**Def.** Область целостности в которой любой идеал главный, называется областью главных идеалов (ОГИ)

**Д-ли:**  $\forall$  евклидово кольцо

**Rem.** Обратное неверно (сложно)

**Ex.** Пусть  $R = Z[x]$ , тогда  $R$  – не ОГИ

$I = \langle 2, x \rangle = \{f \in Z[x] | f(0) : 2\}$  – идеал

$I \neq \langle f \rangle$ , т.к.  $\begin{cases} 2 \vdots f \\ x \vdots f \end{cases} \Rightarrow f = \pm 1$ , но  $\pm 1 \in I!!!$   $(2, x) = 1$ , но  $\nexists g, h : 2 \cdot g + x \cdot h = 1$   
 $R = Q[x], R[x], Z/pZ[x]$  – все ок, т.к. это поля  $\Rightarrow K[x]$  евклидово  $\Rightarrow$  ОГИ

**Def.**  $R$  – область целостности,  $a \vdots b$ , если  $\exists c : a = bc$

**Rem.**  $a \vdots c, c \neq 0 \Rightarrow$  частное в определении однозначно (т.к. в области целостности верен закон сохранения)  
 $Z/4Z, 2 = 2 \cdot 1 = 2 \cdot 3???$

**Def.**  $a \in R \Rightarrow a$  называется неразложимым, если

1.  $a \neq 0, a \notin R^*$
2.  $a = bc \Rightarrow \begin{cases} b \in R^* \\ c \in R^* \end{cases}$

**Def.**  $a, b$  называются ассоциированными ( $a \sim b$ ), если выполнено одно из определений

1.  $a \vdots b, b \vdots a$
2.  $a = b\varepsilon; \varepsilon \in R^*$

**Rem.** В  $Z a \sim b \Leftrightarrow |a| = |b|$

**Rem.** Это отношение эквивалентности (очев из первого определения)

**Упражнение:**  $3 \Rightarrow 1, 2$  у  $a, b$  одинаковые делители

$3'$ : у  $a, b$  одинаковые кратные

**Def.** Область целостности  $R$  называется факториальной, если любой  $a \in R \setminus \{0\}$  представляется в виде произведения не разложимых единственным образом с точностью до порядка множителей и ассоциированности

**Ex.**  $a = p_1 p_2 p_3; p_1, p_2, p_3$  – неразложимые.  $\varepsilon, \mu, \alpha \in R^*$

$a = (\varepsilon p_2 \mu)(\alpha p_3 \mu^{-1} \alpha^{-1})(\varepsilon^{-1} \alpha p_1)$ ;  $\varepsilon p_2 \mu \sim p_2$  – неразложимый (упр) и т.д.

**Th.** ОГИ – факториальна

Ключевые свойства:

1.  $\begin{cases} (a, b) = 1 \\ ac \vdots b \end{cases} \Rightarrow c \vdots b$
2.  $p$  – неразложимый  
 $ab \vdots p \Rightarrow \begin{cases} a \vdots p \\ b \vdots p \end{cases} \Rightarrow$  единственность разложения

### Доказательство

Единственность доказывается по той же схеме, что и в  $Z$

Существование – неочев /без доказательства/

У нас  $R = K[x]$  – существование разложения очевидна (индукция по  $\deg(f)$ )

Что значит в  $K[x] f \sim g? f = \varepsilon g, \varepsilon \in K[x]^*$

**Lem.**  $K[x]^* = K \setminus \{0\}$ .  $\deg(f) > 0, \forall g \deg(fg) \geq \deg(f) > 0$  или  $fg = 0 (fg \neq 1)$

Поэтому  $f \sim g \Leftrightarrow \exists k \in K^* : f = kg$

$\deg(f) = 0, f = k \sim 1$ , для  $f$  разложение пустое ( $\deg(f) > 0$  – непустое)

**Def.**  $f$  называется уникальным, если  $\exists n = \deg(f) : f = x^n + \sum_{i=0}^{n-1} a_i x^i$

В  $\forall$  классе ассоциативности  $\exists!$  уникальный многочлен

Итого:  $\forall f \in K[x] \exists! a \in K, p_1, p_2 \dots p_l$  – уникальные неразложимые:  $f = ap_1 p_2 \dots p_l$

$p_1, p_2 \dots p_l$  – единственные с точностью до перестановки множителей



# Производная

**Def.**  $R$  – коммутативное кольцо:  $D : R \rightarrow R$  называется дифференцированием, если

1.  $\forall f, g \in R \ D(f + g) = D(f) + D(g)$
2.  $\forall f, g \in R \ D(f \cdot g) = f \cdot D(g) + g \cdot D(f)$  – правило Лейбница

**Def.**  $R$  – кольцо,  $f \in R[x] : f = \sum a_n x^n$  тогда по определению  $D(f) = f' = \sum n a_n x^{n-1}$  ( $n \cdot a_n = a_n + a_n + \dots + a_n$  ( $n$  раз))

**Def.**  $f \in R[x]$ . Положим  $D(f)(x) = \frac{f(x)-f(y)}{x-y}|_{x=y}$

Упражнение:  $def1 \Leftrightarrow def2$

$$\frac{ax^n - ay^n}{x-y} = a \frac{(x-y)(x^{n-1} + x^{n-2}y + \dots + y^{n-1})}{x-y} \Big|_{x=y} = na \cdot y^{n-1}$$

**Def./Th.**  $K$  – бесконечное поле  $f \in K[x]$ ,  $a \in K$ ,  $\exists q, r : f = (x-a)^2 \cdot q + r$  ( $\deg(r) < 2$ )

$$f = (x-a)^2 \cdot q(x) + k(x-a) + m_a \quad (x=a; \ m_a = f(a))$$

**Утв.** отображение  $a \rightarrow K_a$  – полиномиальная функция, соответствующий многочлен называется производной (а именно  $f'$  из Def1. задает эту функцию)

$$\text{Утв. } f = (x-a)^2 q_f(x) + f'(a)(x-a) + f(a); \ g = (x-a)^2 q_g(x) + g'(a)(x-a) + g(a)$$

$$\text{Сложим: } f+g = (x-a)^2(q_f+q_g) + (f'(a)+g'(a))(x-a) + f(a)+g(a)$$

$$f \cdot g = (x-a)^2((x-a)^2 q_f q_g + q_f g'(a)(x-a) + q_g f'(a)(x-a) + f'(a)g'(a)) + (f'(a)g(a) + f(a)g'(a))(x-a) + f(a)g(a),$$

но коэффициенты при  $x-a$  равен  $(fg)'(a)$

Пусть  $K$  – поле,  $f \in K[x]$ ;  $a$  – корень  $f$

$a$  – корень кратности  $l$ , если  $V_{(x-a)}(f) = l$ , т.е.  $f : (x-a)^l, \ f : (x-a)^{l+1}, \ f = (x-a)^l \tilde{f} : \tilde{f}(a) \neq 0$

$a$  – кратный корень, если  $l > 1$  (иначе простой)

**Th.**  $f \in K[x]$ ,  $a$  – корень кратности  $l$  ( $l \geq 1$ ), тогда

1.  $a$  – корень кратности  $\geq l-1$  в многочлене  $f'$
2. Если  $1+1+\dots+1 \neq 0$  в  $K \Rightarrow a$  – корень кратности  $= l-1$  в  $f'$
3.  $a$  – кратный корень  $f \Leftrightarrow a$  – корень  $\gcd(f, f')$

## Доказательство

1.  $f = (x-a)^l \tilde{f}; \ \tilde{f}(a) \neq 0$   
 $f' = ((x-a)^l)' \tilde{f} + (x-a)^l \tilde{f}' = l(x-a)^{l-1} \tilde{f} + (x-a)^l \tilde{f}' = (x-a)^{l-1} (l \tilde{f} + (x-a) \tilde{f}') \Rightarrow a$  – корень кратности хотя бы  $l-1$
2.  $1 \cdot l \neq 0$  в  $K$ , т.е.  $l \neq 0$  в  $K \Rightarrow l \tilde{f} \neq 0 \Rightarrow (l \tilde{f} + (x-a) \tilde{f}')(a) \neq 0$   
т.е.  $f' = (x-a)^{l-1} g, \ g(a) \neq 0 \Rightarrow$  кратность ровно  $l-1$

**Ex.**  $Z/pZ \ f = x^p, \ 0$  – корень кратности  $p$

$$f' = px^{p-1} = 0 \text{ – корень кратности } \infty \ 0 : x^n \forall n$$

**Def.**  $K$  – поле. Характеристика  $K$  –  $\text{char}(K) = \begin{cases} \text{ord}_{(K,+)}(1), & \text{если оно не } \infty \\ 0 & \end{cases}$

**Ex.**  $\text{char}(Q) = \text{char}(Z) = 0; \ \text{char}(Z/pZ) = p$

**Th.**  $\text{char}(K) = 0$  или простое число

## Доказательство

Пусть  $n = pq, \ p, q > 1$

Если  $n$  единиц  $= 0 \Rightarrow$  т.к.  $K$  – поле  $\Rightarrow$  О.Ц.  $\Rightarrow \begin{cases} p=0 \\ q=0 \end{cases} \Rightarrow n$  – не минимальное

**Rem.** Любое поле характеристики 0 содержит подполе, изоморфное  $Q$ . Поле характеристики  $p$  содержит подполе, изоморфное  $Z/pZ$

**Th.**  $K$  – поле,  $a \in K; \ f \in K[x]$ , тогда  $\exists! a_0, a_1, a_2 \dots a_n; \ n = \deg f : f = \sum a_i (x-a)^i; \ f = \sum a_i (x-0)^i = \sum a_i x^i$

## Доказательство

Индукция по  $\deg f$ . База очев

Переход:  $n \rightarrow n + 1$

$$f = (x - a)q + f(a) \text{ по и.п. } q = \sum_{i=0}^n b_i(x - a)^i$$

$$f = (x - a) \sum b_i(x - a)^i + a_0 = \sum b_i(x - a)^{i+1} + a_0, \text{ положим } a_i = b_{i-1} \text{ при } i > 0$$

**Th.** Формула Тейлора:

$K$  – поле,  $f \in K[x]$ ,  $\text{char}(K) = 0$  или  $\text{char}(K) > \deg f$

Определим последовательность многочленов:  $f^{(0)} = f$ ;  $f^{(n+1)} = (f^{(n)})'$

$$\text{Тогда } f = \sum \frac{f^{(k)}(a)}{k!} (x - a)^k$$

## Доказательство

Знаем:  $f = \sum a_i(x - a)^i$  (\*). Хотим  $a_i = \frac{f^{(i)}(a)}{i!}$

$$((x - a)^k)' = k(x - a)^{k-1}$$

$$\text{Тогда } f = (x - a)^k; f^{(1)} = k(x - a)^{k-1}; f^{(k)} = k!(x - a)^0 = k!; f^{(l)} = 0, l > k$$

Применим к \* дифференцирование  $k$  раз и эвалюируем в  $a$

$$f^{(k)}(a) = \sum ((a_i(x - a)^i)^{(k)}(a))$$

$$\text{При } i < k: ((a_i(x - a)^i)^{(k)}(a)) = 0$$

$$\text{При } i > k: ((a_i(x - a)^i)^{(k)}(a)) = c \cdot (x - a)^{i-k}. \text{ Эвалюация в } a \text{ дает } 0$$

$$\text{При } i = k: (a_i k!)(a) = a_i k!$$

$$\text{Итого: } f^{(k)}(a) = a_k k! \Rightarrow a_k = \frac{f^{(k)}(a)}{k!}$$

## Расширения полей и комплексные числа

Пусть  $K$  – поле,  $f \in K[x]$ ,  $f$  – неразложим,  $\deg f > 1$

Надо  $K = Q$ ;  $f = x^2 - 2$

$Q \rightarrow Q(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in Q\}$ ;  $Q \rightarrow R$  – новые поля

$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$  – разложение!!!

Хотим уметь строить новое поле  $L \supset K$  такое, что в  $L$  у  $f$  есть корень  $\Rightarrow$  раскладывается на множители

Конструкция: положим  $g \equiv h \pmod{f}$ , если  $g - h : f$

Это отношение эквивалентности и можно перейти к  $K[x]/f$  – множество классов эквивалентности

$K[x]/f$  – кольцо вычетов по модулю  $f$

**Th.** Упражнение:  $f$  – неразложимый многочлен  $\Rightarrow K[x]/f$  – поле

$$g = f \cdot q + r; \deg r < \deg f$$

$$\bar{g} = \bar{r} = \{a_0 + a_1 x + \dots + a_{n-1} x^{n-1} | a_i \in K\}$$

$$\text{Все } \bar{a}_0 - \text{различны и } \bar{a}_0 + \bar{a}'_0 = \overline{a_0 + a'_0} \text{ и } \bar{a}_0 \cdot \bar{a}'_0 = \overline{a_0 \cdot a'_0}$$

Можно считать, что  $K[x]/f$  содержит  $K$  как подполе

$L = K[x]/f$ . В  $L$   $f$  имеет корень:

$$f = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + a_n x^n$$

$$\bar{0} = \bar{f} = \sum \bar{a}_i \cdot \bar{x}^i = \sum \bar{a}_i (\bar{x})^i = \sum a_i \bar{x}^i = f(\bar{x})$$

$f$  имеет корень в  $L$ :  $f = (x - \bar{x})(\dots)$

**Ex. (основной)**  $K = R$ ;  $f = x^2 + 1$  – неразложим

$$R[x]/(x^2 + 1) = \{ax + b | a, b \in R\}$$

$$ax + b + cx + d = (a + c)x + (b + d)$$

$$ax + b \cdot cx + d = (ax + b)(cx + d) = acx^2 + (ad + bc)x + bd \text{ делим на } x^2 + 1$$

$$\text{Получаем } acx^2 + ac - ac + (bc + ad)x + bd = ac(x^2 + 1) + (bc + ad)x - ac + bd = \overline{(bc + ad)x - ac + bd}$$

$R[x]/(x^2 + 1) \cong R \times R$  ( $(a + bx) \leftrightarrow (a, b)$ ) со следующими операциями

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

$$\overline{x} \rightarrow (0, 1)$$

$$\overline{x^2} = -1 \rightarrow (-1, 0); \overline{x} = i$$

Итого:  $C = R[x]/(x^2 + 1) = \{a + bi | a, b \in R\}$  – поле комплексных чисел

$$R = \{a + 0 \cdot i | a \in R\} \subset C \text{ – подполе } C$$

В общем случае  $Z = a + bi$ ;  $a = \operatorname{Re}(z)$ ,  $b = \operatorname{Im}(z)$  – вещественная и мнимая часть соответственно  
 $i$  – мнимая единица

$$x^2 + 1 = x^2 - (-1) = x^2 - i^2 = (x - i)(x + i)$$

**Следствие.** Любой квадратный трехчлен из  $R[x]$  раскладывается на линейные множители в  $C$ .  $f = (x - c)^2 - D = (x - c - \sqrt{D})(x - c + \sqrt{D})$   
 $D = -k$ ;  $k > 0 \Rightarrow \sqrt{D} = i\sqrt{k}$

**Th.** Основная теорема алгебры:  $\forall f \in C[x] \ f = c(x - a_1) \dots (x - a_n)$  – имеет  $n$  комплексных корней с учетом кратности

Знаем: существует биекция  $R \times R \leftrightarrow$  точки на плоскости

А еще есть биекция  $C \leftrightarrow$  точки на плоскости

А еще есть биекция  $C \leftrightarrow$  вектора, отложенные из 0

Вот как-то так и думайте, а по-другому не думайте

**Def.**  $|a + bi| = \sqrt{a^2 + b^2}$  – модуль комплексного числа

$$z \rightarrow |\overrightarrow{0x}| = \sqrt{a^2 + b^2}$$

Симметричный относительно  $\overrightarrow{0x}$  вектор  $\rightarrow a - bi$

**Def.**  $a + bi = a - bi$  – сопряженное число

Свойства модуля и сопряжения:

1.  $\overline{\overline{z}} = z$
2.  $z + \overline{z} = 2\operatorname{Re}(z)$
3.  $z \cdot \overline{z} = |z|^2$

Резюмируем что-то:  $z, \overline{z}$  – корни многочлена  $x^2 - 2ax + (a^2 + b^2) \in R[x]$

4.  $|z_1 z_2| = |z_1| \cdot |z_2| \Leftrightarrow |z_1 z_2|^2 = |z_1|^2 \cdot |z_2|^2 \Leftrightarrow z_1 \overline{z_1} z_2 \overline{z_2} = (z_1 z_2)(\overline{z_1 z_2})$  – следует из 6
5.  $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
6.  $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$

**Rem.** 3)  $\Rightarrow C$  – поле, т.к.  $z \neq 0 \Rightarrow |z| \neq 0 \Rightarrow z^{-1} = \frac{\overline{z}}{|z|^2}$