

# Алгебры

Харитонцев-Беглов Сергей

15 ноября 2021 г.

## Содержание

<b>1. Теория чисел</b>	<b>1</b>
1.1 НОД, делимость, линейные диофантовы уравнения . . . . .	1
<b>2. Продолжение теории чисел</b>	<b>4</b>
2.1 Пара комментариев про предыдущую лекцию . . . . .	4
2.2 Основная теорема арифметики . . . . .	4
<b>3. Кольца вычетов и их друзья</b>	<b>7</b>
3.1 Группы . . . . .	7
3.2 Кольца . . . . .	8
3.3 Построение кольца вычетов . . . . .	8
3.4 Квадратное уравнение . . . . .	10
3.5 Китайская теорема об остатках . . . . .	10
3.6 Группы вычетов и криптографические протоколы . . . . .	15
3.7 Алгоритм RSA . . . . .	16
3.8 Генерация простых, тесты на простоту . . . . .	16
<b>4. Многочлены</b>	<b>18</b>
4.1 Интерполяция . . . . .	21
4.2 Закрываем долг . . . . .	21
<b>5. Евклидовы кольца</b>	<b>23</b>

# 1. Теория чисел

## 1.1. НОД, делимость, линейные диофантовы уравнения

**Определение 1.1.** Диофантовым уравнением называется уравнение, которое можно решить в  $\mathbb{Z}$ .

Рассмотрим линейное диофантово уравнение

$$ax + by = c$$

Если бы мы были в  $\mathbb{R}$ , то решение быстро бы нашлось:  $y = \frac{c-ax}{b}$ . Но в целых штуках такая штука не всегда будет решением, т.к.  $b$  не всегда делит  $c - ax$ .

**Определение 1.2.**  $a$  делится на  $b$  ( $a : b, b|a$ ), если  $\exists c \in \mathbb{Z} : a = bc$ .

Простые свойства:

1.  $\forall a : a : 1$ .
2.  $\forall a : 0 : a$ .
3.  $\forall a, b, c, k, l \in \mathbb{Z} : a : c \wedge b : c \Rightarrow (ka + lb) : c$ .

**Доказательство.**  $a, b : c \Rightarrow \exists d, e : \begin{cases} a = c \cdot d \\ b = c \cdot e \end{cases}$ . Тогда  $ka + lb = k \cdot cd + l \cdot ce = c \cdot (kd + le) \Rightarrow (ka + lb) : c$  □

$$4. \forall k \neq 0, k \in \mathbb{Z} : a : b \iff ak : bk.$$

$$5. a : b \iff a^2 : b^2.$$

$$6. a : b \Rightarrow \begin{cases} |a| \geq |b| \\ a = 0 \end{cases}.$$

$$7. a : b, b : c \Rightarrow a : c.$$

$$8. a : a.$$

$$9. a : b, b : a \Rightarrow a = \pm b.$$

**Теорема 1.1** (О делении с остатком).  $a, b \in \mathbb{Z}, \exists!(q, r) : \begin{cases} q, r \in \mathbb{Z} \\ a = b \cdot q + r \\ 0 \leq r < |b| \end{cases}$

**Доказательство.**

- Единственность. Пусть есть два результата:  $a = b \cdot q_1 + r_1$  и  $a = b \cdot q_2 + r_2$ . Тогда приравняем:  $b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \iff b(q_1 - q_2) = r_2 - r_1 \xrightarrow[r_1 - r_2 < |b|]{r_1, r_2 \in [0; |b|-1]} r_2 - r_1 : b \xrightarrow{\text{Свойство 6}} r_2 - r_1 = 0 \iff r_1 = r_2 \Rightarrow b(q_1 - q_2) = 0 \iff q_1 = q_2$
- Существование. Здесь мы для конкретного  $b$  проверяем, что все  $a$  подходят.

I.  $a \geq 0, b \geq 0$ .

– База:  $a = 0$ .  $0 = b \cdot 0 + 0$ .  $(0, 0)$  – подходит.

– Переход:  $a \rightarrow a + 1$ .

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

$a + 1 = b \cdot q + (r + 1)$ .

\*  $r < b - 1$ . Тогда  $r + 1 < b \Rightarrow (q, r + 1)$  – подходит.

\*  $r = b - 1$ . Тогда  $a + 1 = b \cdot q + b = b \cdot (q + 1) \Rightarrow (q + 1, 0)$  – подходит.

II.  $a < 0, b > 0$ .  $a < 0 \Rightarrow -a > 0$ .

Из I:  $\exists(q, r) : -a = b \cdot q + r$ , где  $0 \leq r < b$ . Соответственно  $a = -bq - r$ .

–  $r = 0$ .  $a = b \cdot q + 0 \Rightarrow (-q, 0)$  – подходит.

–  $r > 0 \Rightarrow r \in [1; b - 1]$ .  $a = -bq - b + b - r = b \cdot (-q - 1) + b - r \Rightarrow (-q - 1, b - r)$  – подходит

III.  $b < 0 \iff -b > 0$ .  $\exists q, r : a = (-b) \cdot q + r$ , где  $0 \leq r < |b|$ , тогда  $a = b(-q) + r \Rightarrow (-q, r)$  – подходит

□

Вернемся к диофантову уравнению  $ax + by = c$ , где  $a, b, c$  фиксированы, а  $x, y$  – переменные. Пусть только  $a, b$  – фиксированы. Тогда подумаем, когда же  $ax + by = c$  имеет решения. Тогда решим задачу: описать  $\{ax + by \mid x, y \in \mathbb{Z}\} =: \langle a, b \rangle$

**Пример.**  $\langle 1, b \rangle = \mathbb{Z}$

**Пример.**  $\langle 4, 6 \rangle =$  четные числа

Заметим:

$$1. \forall m, n \in \langle a, b \rangle : m + n \in \langle a, b \rangle$$

$$2. m \in \langle a, b \rangle \Rightarrow km \in \langle a, b \rangle \forall k$$

**Определение 1.3.** Пусть  $I \subset \mathbb{Z}$ .  $I$  называется идеалом, если

$$\begin{cases} m, n \in I \Rightarrow m + n \in I \text{ (замкнутость по сложению)} \\ m \in I \Rightarrow \forall k \in \mathbb{Z} : k \cdot m \in I \text{ (замкнутость по умножению)} \\ I \neq \emptyset \end{cases}$$

**Пример.**  $\{0\}$  – идеал.

**Пример.**  $\mathbb{Z}$  – идеал (собственный).

**Пример.**  $\langle a, b \rangle$  – идеал, порожденный  $a$  и  $b$ .

$\forall a \in \mathbb{Z} \langle a \rangle = \{ax \mid x \in \mathbb{Z}\}$  – главный идеал (порожденный  $a$ ).

**Пример.**  $\{0\} = \langle 0 \rangle, \mathbb{Z} = \langle 1 \rangle, \langle 4, 6 \rangle = \langle 2 \rangle$

**Теорема 1.2.** В  $\mathbb{Z}$  любой идеал главный.

**Доказательство.**  $I = \{0\}$  – ок. Тогда пусть  $I \neq \{0\}$ . Пусть  $a \in I \wedge a < 0 \Rightarrow -a = (-1)a \in I \wedge -a \in \mathbb{N}$ . То есть  $I \cap \mathbb{N} \neq \emptyset$ . Найдем наименьшее  $r \in I \cap \mathbb{N}$ . Проверим, что  $I = \langle r \rangle$  (тогда  $I$  – главный). Надо проверить  $\langle r \rangle \subset I \wedge I \subset \langle r \rangle$ .

- $x \in \langle r \rangle$ . То есть  $x = r \cdot z$ . Т.к.  $r \in I$ , то  $r \cdot z \in I$  (по определению идеала), т.е.  $\langle r \rangle \subset I$ .
- Пусть  $a \in I$ . Поделим с остатком:  $a = r \cdot q + r_1$ ,  $0 \leq r_1 < r$ , то есть  $r_1 = a - r \cdot q = a + (-q) \cdot r$ . Т.к.  $r \in I \Rightarrow (-q) \cdot r \in I \wedge a \in I \Rightarrow a + (-q) \cdot r \in I$ , т.е.  $r_1 \in I$ . Но!  $0 \leq r_1 < r$ , а  $r$  — минимальное натуральное из  $I$ . Тогда  $r_1 = 0 \Rightarrow a = r \cdot q$ , т.е.  $a \in \langle r \rangle$ , а значит  $I \subset \langle r \rangle$ .

□

**Определение 1.4.** Пусть  $a, b \in \mathbb{Z}$ . Тогда  $d = \text{НОД}(a, b) = \gcd(a, b) = (a, b)$

Докажем единственность.  $\begin{cases} a : d, b : d \\ a : d_1, b : d_1 \end{cases} \iff d : d_1$ . Тогда  $d : d_1 \wedge d_1 : d$ , а значит  $d = \pm d_1$ .

**Теорема 1.3.** 1.  $\forall a, b \exists d = (a, b)$

2.  $\exists x, y \in \mathbb{Z} : d = ax + by$

3.  $ax + by = c$  имеет решение  $\iff c : d$ .

**Доказательство.** Докажем каждый пункт отдельно:

- Рассмотрим  $\langle a, b \rangle$  — идеал. Он главный по предыдущей теореме:  $\exists d \langle a, b \rangle = \langle d \rangle$ .

- $d \in \langle d \rangle = \langle a, b \rangle$ . А значит  $\exists x, y : d = ax + by$ .  
 $a = a \cdot 1 + b \cdot 0 \in \langle a, b \rangle = \langle d \rangle$ , значит  $a : d$ . Аналогично  $b : d$ .  
 С другой стороны пусть  $a : d, b : d$ , тогда  $d = \underbrace{ax}_{:d} + \underbrace{by}_{:d} : d$ .

Пусть  $\exists d_1 : a : d_1 \wedge a : d_1 \Rightarrow d = ax + by : d_1 \Rightarrow d$  — максимальный общий делитель.

- $ax + by = c$  имеет решение  $\iff c \in \langle a, b \rangle = \langle d \rangle$ . А  $c \in \langle d \rangle \iff c : d$ .

□

**Определение 1.5.**  $a, b$  — взаимно просты, если  $(a, b) = 1$ , то есть  $\langle a, b \rangle = \mathbb{Z}$

**Лемма.**  $\begin{cases} ab : c \\ (a, c) = 1 \end{cases} \Rightarrow b : c$ .

**Доказательство.** По условию  $ab : c$ , значит  $\exists x \in \mathbb{Z} : ab = c \cdot x$ .

Так как  $(a, c) = 1$ , то  $\exists y, z \in \mathbb{Z} : ay + cz = 1$ . Тогда домножим все на  $b$  и получим  $aby + czb = b$ .

А значит  $\begin{cases} aby : c \\ czb : c \end{cases} \Rightarrow b : c$

□

## 2. Продолжение теории чисел

### 2.1. Пара комментариев про предыдущую лекцию

1. Для любого набора  $a_1, \dots, a_n \in \mathbb{Z}$   $\exists \gcd(a_1, \dots, a_n)$  и  $\exists x_1, \dots, x_n : \text{НОД} = x_1 a_1 + \dots + x_n a_n$ .  
НОД - такое  $d$ , что  $\langle a_1, \dots, a_n \rangle = \langle d \rangle$ .
2. Алгоритм Евклида.
  - $(a, b) = (a, b - a)$ , но и  $b = a \cdot q + r$ , тогда  $(a, b) = (a, r)$ .
  - Пусть  $r = b \bmod a$ ,  $x_1, x_2 \in \mathbb{N}$ . Сделаем последовательность  $x_{n+1} = x_{n-1} \bmod x_n$ . Тогда  $(x_1, x_2) = (x_3, x_4) = \dots$ . Заметим, что  $x_n$  — убывает.
  - Тогда существует такое  $x_n$ , что  $(x_1, x_2) = (x_n, 0) = x_n$ .

### 2.2. Основная теорема арифметики

**Определение 2.1.**  $x \in \mathbb{Z}, x \neq \pm 1$ , тогда  $x$  — простое число, если  $x = x_1 x_2 \iff \begin{cases} x_1 = \pm 1 \\ x_2 = \pm 1 \end{cases} \forall x_1, x_2$

**Свойство \*.**  $x$  — обладает свойством \*,  $\iff x \neq \pm 1 \wedge ab : x \Rightarrow \begin{cases} a : x \\ b : x \end{cases}$

**Утверждение 2.1.**  $p$  — простое  $\iff p$  — обладает свойством \*.

**Доказательство.**

- $\Leftarrow$  Пусть  $p = x_1 x_2$ . Тогда  $x_1 x_2 : p$  по \*:  $\begin{cases} x_1 : p \\ x_2 : p \end{cases}$ . Пусть  $x_1 = py$ .  $p = x_1 x_2 = pyx_2$ .  $1 = yx_2 \Rightarrow x_2 = \pm 1$ . Получили определение простого числа.
- $\Rightarrow$ . Пусть  $p$  — простое и  $ab : p$ .  $d = (a, p)$ ,  $p$  — простое  $\Rightarrow d = p \vee d = 1$ .  
 $d = p \Rightarrow a : p$ .  $d = 1 \wedge (a, p) = 1$ , по лемме  $ab : p \wedge (a, p) = 1 \Rightarrow b : p$ .

□

**Теорема 2.2** (Основная теорема арифметики). Пусть  $n \in \mathbb{Z}, n \neq 0$ . Тогда  $n$  единственным образом с точностью до перестановки сомножителей, представимо в виде ( $p_i$  — простые,  $p_i > 0$ )

$$n = \varepsilon p_1 p_2 \dots p_k, \varepsilon = \pm 1 = \text{sign}(n).$$

Или, иными словами, существует единственное каноническое разложение:

$$n = \varepsilon p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}, \varepsilon = \pm 1 = \text{sign}(n), a_i > 0, p_1 < p_2 < \dots < p_k.$$

**Доказательство.**

1. Существование. От противного. Пусть  $\exists$  нераскладываемое число. Рассмотрим минимальное такое число.
  - $x = 1$  — пустое произведение. Противоречие.

- $x = p$  — произведение из 1 члена. Противоречие.
- $x = x_1 x_2$ .  $x_1, x_2 \neq \pm 1 \Rightarrow x_1, x_2 < x \Rightarrow x_1, x_2$  — раскладываемые. Или  $x_1 = p_1 p_2 \dots p_n, x_2 = q_1 q_2 \dots q_m \Rightarrow x = p_1 p_2 \dots p_n q_1 q_2 \dots q_m$ .

2. Единственность. Пусть есть плохие числа.  $X$  — минимальное из них.  $q_1 q_2 \dots q_n = X = p_1 p_2 \dots p_m$ . Значит  $p_1 p_2 \dots p_m : q_1 \Rightarrow p_1 : q_1 \vee p_2 \dots p_m : q_1$ . Тогда  $\exists p_i : q_1$ . Тогда можно поделить на  $q_1$ , но  $p_i$  — простое, тогда  $p_i = q_1$ . Рассмотрим  $X' = \frac{X}{q_1}$ .  $q_2 q_3 \dots q_n = X' = p_1 p_2 \dots p_{i-1} p_{i+1} \dots p_m$ .  $X' < X$ , значит разложения  $X'$  равны, а значит, т.к.  $p_i = q_1$ , то равны и исходные разложения. Получили противоречие.

□

Контр-примеры для О. Т. А:

1. Рассмотрим  $2\mathbb{Z}$  — множество четных чисел. Теперь 6 — простое, как и все  $(4k + 2)$ .

Теперь как разложить на простые 60?  $60 = 2 \cdot 30$ , а также  $60 = 6 \cdot 10$ .

2.  $\mathbb{Z} \cup \{\sqrt{5}\} = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ . Заметим, что  $\mathbb{Z} \subset \mathbb{Z}\{\sqrt{5}\}$

$$4 = 2 \cdot 2 = \overbrace{(\sqrt{5} - 1)}^{\text{простое}} \overbrace{(\sqrt{5} + 1)}^{\text{простое}}$$

**Определение 2.2.**  $n \in \mathbb{Z}, n \neq 0, p$  — простое, тогда степень вхождения  $(V_p(n) = k)$   $p$  в  $n$  —  $\max\{k \mid n : p^k\}$

В терминах разложения:  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ .  $V_p(n) = a_i$ , а если  $p$  нет в разложении, то  $V_p(n) = 0$ .

Свойства:  $V_p(n)$

1.  $V_p(xy) = V_p(x) + V_p(y)$
2.  $V_p(x + y) \geq \min(V_p(x), V_p(y))$ , а если  $V_p(x) \neq V_p(y)$ , то строгое равенство

**Доказательство.**  $V_p(x) = a, V_p(y) = b$  и  $x = p^a \cdot \tilde{x}, y = p^b \cdot \tilde{y}$ .

Не умаляя общности:  $a \geq b$ . Тогда  $x + y = p^a \tilde{x} + p^b \tilde{y} = p^b (p^{a-b} \tilde{x} + \tilde{y})$ . Если  $a > b$ , то  $\underbrace{p^{a-b} \tilde{x}}_{:p} + \tilde{y}$

не делится на  $p$ . А значит  $V_p(x + y) = \min(V_p(x), V_p(y))$ . В случае же равенства, получаем  $p^b \cdot (\tilde{x} + \tilde{y})$ , для которого уже  $V_p(x + y) \geq \min(V_p(x), V_p(y))$  □

Еще следствия из О. Т. А.

1.  $x : y \Rightarrow V_p(x) \geq V_p(y) \forall$  простого  $p$
2.  $x = p_1^{a_1} \dots p_n^{a_n}, y = p_1^{b_1} \dots p_n^{b_n} \Rightarrow (x, y) = p_1^{\min(a_1, b_1)} \dots p_n^{\min(a_n, b_n)}$
3.  $x = z^k \iff \forall$  простого  $p \ V_p(x) : k$
4. Количество натуральных делителей  $x = \prod x_i^{a_i}$  равно  $\tau(x) = \prod (a_i + 1)$

**Доказательство.** Делители  $X$  однозначно соотносятся с  $\{(b_1, b_2, \dots, b_n) \mid 0 \leq b_i \leq a_i\}$  □

5.  $\sigma(x)$  — сумма натуральных делителей  $x$ . Тогда  $\sigma(x) = \frac{\prod (p_i^{a_i+1} - 1)}{\prod (p_i - 1)}$ .

**Доказательство.**  $\frac{\prod (p_i^{a_i+1}-1)}{\prod (p_i-1)} = \prod \frac{p_i^{a_i+1}-1}{p_i-1} = \prod (1+p_i+\dots+p_i^{a_i})$  = раскроем скобки. = сумма делителей.  $\square$

6.

**Определение 2.3.**  $m$  — НОК (LCM,  $[a, b]$ ), если  $m : a, m : b$  и  $\forall n \ n : a \wedge n : b \Rightarrow n : m$

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

7.  $a, b \in \mathbb{Z} \ (a, b) = 1 \ ab = c^k \Rightarrow \exists c_1, c_2 \ a = c_1^k, b = c_2^k$

### 3. Кольца вычетов и их друзья

Рассмотрим  $a^2 - b^2 = 15^{2021} \iff (a-b)(a+b) = 3^{2021} \cdot 5^{2021} \Rightarrow \begin{cases} a+b = 3^k \cdot 5^l \\ a-b = 3^{2021-k} \cdot 5^{2021-l} \end{cases} \Rightarrow$   
 $a = \frac{3^k \cdot 5^l + 3^{2021-k} \cdot 5^{2021-l}}{2}.$

Уравнение  $81a^2 - 169b^2 = 15^{2021}$  — тоже решается. А вот  $a^2 - 2b^2 = 15^{2021} \iff (a - \sqrt{2}b)(a + \sqrt{2}b) = 3^{2021}5^{2021}$  уже не решается в целых числах. Если вылезать, то надо расписывать разложение  $a + \sqrt{2}b$ , "3", "5" и единственность разложения на множители.

Еще один пример:  $a^2 + b^2 = 15^{2021}$ . Посмотрим на остатки от деления на 4:  $a^2, b^2 \pmod 4 \in \{0, 1\}$ ,  $15^{2021} \pmod 4 = 3$ . Но для этого нам нужно понимать что-то про кольцо вычетов по модулю.

#### 3.1. Группы

**Определение 3.1.** Группой называется пара  $(G, *)$ , где  $G$  — множество, а  $*$  :  $G \times G \rightarrow G$  — бинарная операция, так что выполнены свойства:

1.  $\forall a, b, c \in G : (a * b) * c = a * (b * c)$ . Ассоциативность.
2.  $\exists e \in G : \forall a \in G a * e = e * a = a$ . Существование нейтрального элемента.
3.  $\forall a \in G \exists a^{-1} : a * a^{-1} = a^{-1} * a = e$ . Существование обратного элемента.

Несколько примеров:

1.  $(\mathbb{Z}, +)$ ,  $e = 0$ ,  $a^{-1} = -a$ .
2.  $(\mathbb{Q} \setminus 0, \cdot)$ ,  $e = 1$ ,  $a^{-1} = \frac{1}{a}$ .
3.  $(2^M, \Delta)$ ,  $e = \emptyset$ ,  $A^{-1} = A$ .

**Определение 3.2.** Группа  $G$  называется абелевой, если  $\forall x, y \in G : x * y = y * x$ .

**Пример Главный пример группы.** Пусть  $G = S(M) = \{f : M \rightarrow M \mid f \text{ — биекция}\}$ , операция — композиция функций

- Ассоциативность — упражнение.
- Нейтральный элемент —  $f(x) = x$ , тождественное отображение.
- $f^{-1}$  = обратная функция. Она существует, так как  $f$  — биекция.

Получили группы по композиции.

**Пример.**  $M = \{1, 2, 3\}$ .  $f_1, f_2 : M \rightarrow M$  — биекция.  $f_1$  — меняет местами 1 и 2:  $1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3$ ,  $f_2$  переставляет по циклу:  $1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 1$ .  $f_2 \circ f_1 : 1 \rightarrow 3, 2 \rightarrow 2, 3 \rightarrow 1$ .  $f_1 \circ f_2 : 1 \rightarrow 1, 2 \rightarrow 3, 3 \rightarrow 2$ . Ну значит группа не абелева.

Докажем простейшие свойства групп:

1.  $\exists!$  нейтральный элемент.

**Доказательство:** заметим, что  $e_1 = e_1 * e_2 = e_2$



2.  $\exists!$  обратный элемент.

**Доказательство:** пусть  $b, c$  — обратные к  $a$ . Тогда  $(b * a) * c = e * c = c$ , но при этом  $b * (a * c) = b * e = b$ . Значит  $b = c$ .

3.  $a * b = a * c \iff b = c$

**Доказательство:**  $a * b = a * c \iff (a^{-1} * a) * b = (a^{-1} * a) * c \iff e * b = e * c \iff b = c$

### 3.2. Кольца

**Определение 3.3.** Кольцо — тройка  $(R, +, \cdot)$  ( $R$  — множество,  $+, \cdot : R \times R \rightarrow R$ ), такая что:

1–4.  $(R, +)$  — абелева группа. Нейтральный элемент обозначается  $0$ , обратный к  $a$  —  $-a$ .

5.  $a \cdot (b + c) = a \cdot b + a \cdot c$  и  $(b + c) \cdot a = b \cdot a + c \cdot a$ . Дистрибутивность.

**Определение 3.4.** Кольцо  $R$  называется ассоциативным, если выполнено

6.  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ .

**Определение 3.5.** Кольцо  $R$  называется коммутативным, если

7.  $a \cdot b = b \cdot a$

**Определение 3.6.** Кольцо  $R$  называется кольцом с  $1$ , если

8.  $\exists 1 \in R : 1 \cdot a = a \cdot 1 = a$

**Пример.**  $(\mathbb{Z}, +, \cdot)$  — коммутативное ассоциативное кольцо с  $1$ .

**Определение 3.7.** Коммутативное ассоциативное кольцо с  $1$  называется полем, если выполнена

9.  $\forall a \in R \setminus \{0\} \exists b \in R \ ab = 1 \wedge 1 \neq 0$

**Пример.**  $(\mathbb{Q}, +, \cdot)$  — поле, а вот  $(\mathbb{Z}, +, \cdot)$  — не поле.

### 3.3. Построение кольца вычетов

**Определение 3.8.** Пусть  $a, b \in \mathbb{Z}$ , говорят, что  $a$  сравнимо с  $b$  по модулю  $n$  ( $a \equiv b \pmod{n}$ ), если  $(a - b) : n$ . Эквивалентное определение:  $a$  и  $b$  имеют одинаковые остатки по модулю  $n$ .

Докажем, что сравнимость по модулю — отношение эквивалентности.

- $a \equiv a \pmod{n} \iff 0 : n$
- $(a - b) : n \iff (b - a) : n \Rightarrow a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$ .
- $(a - b) : n \wedge (b - c) : n \Rightarrow (a - b + b - c) : n \iff (a - c) : n$

Наблюдение.  $a \in \mathbb{Z} \Rightarrow \bar{a} = \{b \mid a \equiv b\} = \{a + kn \mid k \in \mathbb{Z}\}$ .  $\mathbb{Z} = \bar{0} \cup \bar{1} \dots$

**Определение 3.9.** Фактор множества по отношению  $\equiv$  обозначается  $\mathbb{Z}/n\mathbb{Z}$ .

$\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ . Элементы  $\mathbb{Z}/n\mathbb{Z}$  называются классами вычетов по модулю.

$$1. a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \iff a + c \equiv b + d \pmod{n} \wedge ac \equiv bd \pmod{n}.$$

$$\text{Доказательство } (a + c) - (b + d) = \underbrace{(a - b)}_{\vdots n} - \underbrace{(d - c)}_{\vdots n} \vdots n.$$

$$\text{Доказательство } ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) \vdots n.$$

Значит класс суммы и произведения зависит только от классов множителей и слагаемых.

**Теорема 3.1.** Пусть  $n \in \mathbb{N}$ . Тогда класс  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ , где  $\overline{a} + \overline{b} = \overline{a + b} \wedge \overline{a} \cdot \overline{b} = \overline{a \cdot b}$  — ассоциативное коммутативное кольцо с единицей.

**Доказательство.** Все аксиомы — следствия из  $\mathbb{Z}$ . Докажем для примера  $(\overline{a} + \overline{b}) + \overline{c} = \overline{a + b + c} = \overline{a} + \overline{b + c} = \overline{a} + (\overline{b} + \overline{c})$ .  $\square$

Закон сокращения не очень работает в кольце вычетов по модулю:  $2 \cdot 1 = 2 \cdot 4 \pmod{6}$ , но  $1 \not\equiv 4 \pmod{6}$ .

**Определение 3.10.** Пусть  $R$  — коммутативное ассоциативное кольцо с единицей. Тогда  $\forall a \in R: a$  — делитель нуля  $\Rightarrow \exists b \neq 0: ab = 0$ .

**Пример.**  $n$  — составное:  $n = p_1 p_2$ ,  $n$  в  $\mathbb{Z}/n\mathbb{Z}$   $\overline{p_1 p_2} = \overline{n} = 0$ . Значит  $p_1, p_2$  — делители нуля.

**Лемма.**  $\forall a, b, c \in R: ab = ac \wedge a$  — не делитель нуля  $\Rightarrow b = c$ .

**Доказательство.**  $ab = ac: ab - ac = 0 \iff a(b - c) = 0$ .  $a$  — не делитель нуля  $\Rightarrow b - c = 0 \iff b = c$ .  $\square$

**Лемма.**  $a \in R: a$  — обратим  $\Rightarrow a$  — не делитель нуля.

**Доказательство.** Пусть  $ab = 0 \Rightarrow a^{-1}(ab) = a^{-1} \cdot 0; (a^{-1}a)b = 0 \Rightarrow b = 0$ .  $\square$

**Замечание.** Обратное неверно: в  $\mathbb{Z}$  2 — не делитель нуля, но  $\frac{1}{2} \notin \mathbb{Z}$ .

**Теорема 3.2.**  $\forall a \in \mathbb{Z}: \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ . Тогда:

1.  $\overline{a}$  — обратим  $\iff (a, n) = 1$
2.  $\overline{a}$  — делитель нуля  $\iff (a, n) \neq 1$ .

**Доказательство.**  $\overline{a}$  — обратим  $\iff \exists \overline{b}: \overline{a}\overline{b} = \overline{1} \iff \exists b: ab = 1 \pmod{n} \iff \exists b: ab - 1 \vdots n \iff \exists b, k: ab - 1 = nk \iff \exists b, k: ab - nk = 1 \iff (a, n) = 1$ .

$(a, n) = 1 \Rightarrow \overline{a}$  — обратим  $\Rightarrow$  не делитель нуля.

$(a, n) = d > 1, a = dx$ . Тогда  $\overline{a} \cdot \overline{\frac{n}{d}} = \overline{dx} \overline{\frac{n}{d}} = \overline{nx} = \overline{0}$  и  $\overline{\frac{n}{d}} \neq 0$ . Значит  $0 < |\frac{n}{d}| < n$ .  $\square$

**Следствие.**  $n$  — простое  $\Rightarrow \mathbb{Z}/n\mathbb{Z}$  — поле.

**Доказательство.** Достаточно проверить существование обратного.  $\overline{a} \neq \overline{0} \iff a \not\equiv 0 \iff (a, n) = 1 \iff a$  — обратим.  $\square$

**Определение 3.11.**  $\forall$  ассоциативного кольца с 1  $R: R$  — называется кольцом без делителей нуля (область целостности), если делитель нуля только 0.  $ab = 0 \iff a = 0 \vee b = 0$ .

**Замечание.**  $R$  — область  $\Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$  ( $a \neq 0$ ).

Вернемся к диофантову уравнению  $ax + by = c$ ,  $(a, b) = 1$ . Тогда  $ax = c \pmod{b}$  и  $by = c \pmod{a}$ . Тогда  $\overline{ax} = \overline{c}$  в  $\mathbb{Z}/b\mathbb{Z} \xrightarrow{(a, b)=1} \overline{x} = \overline{a}^{-1} \overline{c} \pmod{b}$ . Тогда  $x = x_0 + kb$ .

### 3.4. Квадратное уравнение

Посмотрим на  $x^2 + px + q = 0$  в  $\mathbb{Z}/n\mathbb{Z}$ . Работает ли  $x_{1,2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$ . Есть проблемки:

1.  $p^2 - 4q$  — не квадрат в  $\mathbb{Z}/n\mathbb{Z}$  (нет решений).
2.  $2 = 0$ . Или  $\nexists 2^{-1}$  (нельзя поделить на два).
3.  $n$  — не простое. Тогда из  $(x - x_1)(x - x_2) = 0$  не следует, что  $x = x_1 \vee x = x_2$ . Пример:  $x^2 - 1 = 0 \pmod{8}$

### 3.5. Китайская теорема об остатках

Чтобы решать такие уравнения можно свести к простым модулям при помощи китайской теоремы об остатках.

Вопрос такой: как связаны  $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/mn\mathbb{Z}$ . Пусть  $P_m : \mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z}$ , а  $P_{mn} : \mathbb{Z} \mapsto \mathbb{Z}/mn\mathbb{Z}$ ,  $P_m, P_{mn}$  — гомоморфизмы соответствующих колец.

**Определение 3.12.** Гомоморфизмом колец  $f : R_1 \mapsto R_2$  называется такое отображение, что  $\forall r_1, r_2 \in R_1 : f(r_1 + r_2) = f(r_1) + f(r_2), f(r_1 r_2) = f(r_1) \cdot f(r_2), f(1) = 1$ .

**Определение 3.13.** Гомоморфизмом группы  $f : G_1 \mapsto G_2$  называется такое отображение, что  $\forall g_1, g_2 \in G_1 : f(g_1 g_2) = f(g_1) \cdot f(g_2)$ .

**Замечание.**  $f$  — гомоморфизм групп  $G_1, G_2 \Rightarrow f(e_{G_1}) = e_{G_2}$ . В частности  $f$  — гомоморфизм колец  $R_1, R_2 \Rightarrow f(0_{R_1}) = 0_{R_2}$ .

**Доказательство.**  $f(e_{G_1}) = f(e_{G_1} \cdot e_{G_1}) = f(e_{G_1}) \cdot f(e_{G_1}); e_{G_2} \cdot f(e_{G_1}) = f(e_{G_1}) \cdot f(e_{G_1}); e_{G_2} = f(e_{G_1})$   $\square$

Существует такой гомоморфизм колец  $P_{mn,m}$ , что  $P_{mn,m} \cdot P_{mn} = P_m$  (тут подразумевается композиция гомоморфизмов)

**Доказательство.** Предъявим такой гомоморфизм:  $P_{mn,m}(\overline{a_{mn}}) = \overline{a_m}$ .  $\square$

**Корректность.**  $\overline{a_{mn}} = \overline{b_{mn}} \iff a \equiv b \pmod{mn} \iff a - b : mn \Rightarrow a - b : m \Rightarrow \overline{a_m} = \overline{b_m}$   $\square$

Аналогично существует гомоморфизм  $P_{mn,n}$ . То есть  $\overline{a_{mn}} \mapsto (\overline{a_m}, \overline{a_n})$  — отображение. То есть  $\mathbb{Z}/mn\mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ . Отступление.

**Определение 3.14.**  $R_1, R_2$  — кольца. Рассмотрим  $(R_1 \times R_2, +, \cdot) : (r_1, r_2) +_{R_1 \times R_2} (r'_1, r'_2) := (r_1 +_{R_1} r'_1, r_2 +_{R_2} r'_2)$ , где  $+_{R_1 \times R_2}, +_{R_1}, +_{R_2}$  — операции сложения для соответствующих множеств. То же самое для умножения. Тогда  $R_1 \times R_2$  — тоже кольцо, т.к. соответствующие свойства операций унаследуются, что можно проверить самостоятельно. Но заметка: если  $R_1$  и  $R_2$  были областями целостности, то их произведение областью целостности почти никогда не будет.

Итак мы построили гомоморфизм  $\mathbb{Z}/mn\mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ , назовём его  $i_{m,n}$ . Подумаем про его свойства. Во-первых заметим, что слева  $mn$  элементов, но и справа  $mn$  элементов!

**Определение 3.15.** Биактивный гомоморфизм (групп, колец, ...) (называется изоморфизмом,  $\cong$ ) если каждым  $a_i$  задано ровно одно  $b_j$  и наоборот.

**Теорема 3.3** (Китайская теорема об остатках). Пусть  $(m, n) = 1$ , тогда  $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ .

**Доказательство.**

1.  $i_{m,n}$  — инъективно. Пусть  $i_{m,n}(\overline{a_{m,n}}) = (\overline{a_m}, \overline{a_n})$ ,  $i_{m,n}(\overline{b_{n,m}}) = (\overline{b_m}, \overline{b_n}) \Rightarrow a - b : m \wedge a - b : n \xrightarrow{(n,m)=1} a - b : mn$ .
2. Раз  $i_{m,n} : \mathbb{Z}/nm\mathbb{Z} \mapsto \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  инъективно и  $|\mathbb{Z}/nm\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}|$ , то  $i_{m,n}$  — сюръективно, а значит и биективно.

□

**Теорема 3.4** (КТО 2).  $m_1, m_2, m_3, \dots, m_n \in \mathbb{Z} \wedge (m_i, m_j) = 1 \Rightarrow \mathbb{Z}/m_1, m_2, \dots, m_n\mathbb{Z} \mapsto \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \dots$  — изоморфизм колец.

**Теорема 3.5** (КТО без колец).  $\forall m_1, \dots, m_n \in \mathbb{Z} : \forall i, j (m_i, m_j) = 1, \forall a_1, \dots, a_n \Rightarrow \exists x_0 \in \mathbb{Z} : x \equiv a_1 \pmod{m_1} \wedge \dots \wedge x \equiv a_n \pmod{m_n} \iff x \equiv x_0 \pmod{\prod_i m_i}$

То есть по факту мы хотим получить обратную функцию к  $f_{m_1, m_2, \dots} : \overline{a_{m_1 m_2 m_3}} \mapsto (\overline{a_{m_1}}, \overline{a_{m_2}}, \overline{a_{m_3}})$ . Пусть тогда  $g = f^{-1}$ . Заметим, что  $g$  — гомоморфизм колец. Раз  $g$  сохраняет операции, то  $g(\bar{x}, \bar{y}, \bar{z}) = g(\bar{x}, 0, 0) + g(0, \bar{y}, 0) + g(0, 0, \bar{z}) = \bar{x}g(1, 0, 0) + \bar{y}g(0, 1, 0) + \bar{z}g(0, 0, 1)$ .

$$\text{Пусть } x = g(1, 0, 0) \iff \begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ x \equiv 0 \pmod{m_3} \end{cases} \iff \begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2 m_3} \end{cases}.$$

В группе  $\forall a \neq e \forall x : ax \neq x$ . Тогда посмотрим группу  $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \supset \{(a, 0) \mid a \in \mathbb{Z}/m\mathbb{Z}\} \cong \mathbb{Z}/m\mathbb{Z}$ .

Тогда для любого  $n \in \mathbb{N} : n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}$ .

**Пример.** Для того, чтобы решить  $b^2 = a$  надо решить  $b_i^2 = a$  для все составляющих.

**Определение 3.16.** Пусть  $C$  — группа ( $a \in C$ ), тогда порядок элемента  $a$ :  $\text{ord}(a) = \{\min k \in \mathbb{N} \mid a^k = 1\}$ . А если такого  $k$  нет, то  $\text{ord}(a) = \infty$

**Лемма.** Пусть  $G$  — группа ( $a \in G$ ).  $\langle a \rangle = \{a, a^2, \dots; a^{-1}, (a^{-1})^2, \dots, e\} = \{a^k \mid k \in \mathbb{Z}\}$ . Тогда  $(\langle a \rangle, *)$  — группа.

**Доказательство.** Проверим замкнутость относительно операций: 0-рной ( $\{\} \rightarrow e$ ), унарной  $a \rightarrow a^{-1}$ , бинарной  $(a, b) \rightarrow a * b$ .

- $e = a^0 \in \langle a \rangle$
- $b \in \langle a \rangle. b = a^k \Rightarrow b^{-1} = a^{-k} \in \langle a \rangle$ .
- $b, c \in \langle a \rangle. b = a^k, c = a^l \Rightarrow bc = a^{k+l} \in \langle a \rangle$ .

□

**Определение 3.17.**  $\langle a \rangle$  называется циклической группой, порожденной  $a$ .  $G$  — циклическая группа  $\iff \exists a \in G : G \cong \langle a \rangle$

**Теорема 3.6** (О классификации циклических групп).  $\text{ord } a = \infty \Rightarrow \langle a \rangle \cong (\mathbb{Z}, +)$ .  $\text{ord } a = k \in \mathbb{N} \Rightarrow \langle a \rangle \cong (\mathbb{Z}/k\mathbb{Z}, +)$

**Доказательство.**  $f : (\mathbb{Z}, +) \rightarrow \langle a \rangle$ . То есть  $k \mapsto a^k$ .  $f(k+l) = a^{k+l} = a^k \cdot a^l = f(k) + f(l)$ , т.е.  $f$  — гомоморфизм. А ещё  $f$  — сюръекция по определению циклической группы.

Докажем инъективность. Пусть  $a^k = a^l \iff a^{k-l} \cdot a^l = ea^l \iff a^{k-l} = e$ . Но  $\text{ord } a = \infty$ ! Значит  $k - l = 0$ .

Теперь  $\text{ord } a \neq \infty$ . Тогда построим  $f : \mathbb{Z}/k\mathbb{Z} \rightarrow \langle a \rangle$ , то есть  $\overline{m}_k \mapsto a^m$ .

Корректность:  $\overline{m}_k = \overline{n}_k \Rightarrow (m - n) : k$ . То есть  $m = n + k \cdot l$ . Значит  $a^m = a^{n+k \cdot l} \iff a^m = a^n \cdot a^{kl} = a^n$ .

Аналогично первому случаю доказываем, что  $f$  — гомоморфизм и сюръекция.

Инъективность:  $f(\overline{m}) = f(\overline{n}) \iff a^m = a^n \iff a^{m-n} = e, m - n = qk + r, 0 \leq r < k$ ;  $a^{qk+r} = e \iff (a^k)^q \cdot a^r = e \iff a^r = e$ , но  $r < k$ , а  $k$  — наименьшая натуральная степень обращения элемента в единицу, а значит  $r = 0$ , т.е.  $f(\overline{n}) = f(\overline{m}) \iff (m - n) : k$ , т.е. мы имеем дело с одним классом эквивалентности.

□

Простыми словами, если  $\text{ord } a = \infty \Rightarrow$  в последовательности  $\{a^i\}$  — элементы не повторяются. А если  $\text{ord } a \neq \infty$ , то элементы повторяются с периодом  $k$ , а внутри периода элементы не повторяются.

**Теорема 3.7** (Теорема Лангранжа). Пусть  $G$  — группа.  $\forall G$  —  $n$ -элементная группа, тогда  $\forall a \in G : n : \text{ord } a$

**Доказательство.** Пусть  $\text{ord } a = k$ . Рассмотрим отображение  $m_a(x) = ax$ .  $m_a G \rightarrow G$ . Нарисуем граф отображений (вершины — элементы  $G$ , ребра (стрелки) —  $x \rightarrow ax$ ).  $x \rightarrow ax \rightarrow a^2x \rightarrow a^3x \rightarrow \dots \rightarrow a^{k-1}x \rightarrow a^kx = x$ , так как для  $\forall i, j < k : a^i x = a^j x \Rightarrow i = j$ .

Значит все элементы  $G$  разбиваются на циклы длины  $k$ . Следовательно  $n : k$ .

□

**Следствие.**  $G$  — конечная группа ( $a \in G$ )  $\Rightarrow a^{|G|} = e$

**Доказательство.**  $\text{ord } a = k$ .  $n = k \cdot l$  по теореме Лагранжа. Тогда  $a^n = a^{k \cdot l} = (a^k)^l = e^l = e$  □

**Пример.**  $(\mathbb{Z}/p\mathbb{Z}, +)$ .  $\overline{a}^x = \underbrace{\overline{a} + \overline{a} + \overline{a} + \overline{a}}_{x \text{ раз}} = \overline{xa}$ .

**Пример.**  $p$  — простое.

$G := (\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \cdot)$ .  $|G| = p - 1$ . Тогда  $a^{p-1} = 1$ . Малая теорема Ферма.

На языке сравнений:  $a \in \mathbb{Z}, a : p \Rightarrow a^{p-1} - 1 : p \iff a^{p-1} \equiv 1 \pmod{p}$ .

**Пример.**  $(\mathbb{Z}/p\mathbb{Z}, +)$  — циклическая группа. А вот с  $G$  из предыдущего пункта — тоже, если  $p$  — простое. Но не очев.

**Утверждение 3.8.**  $G$  — группа ( $|G| = n$ ).  $G$  — циклическая  $\iff \exists a \in G : \text{ord } a = n$ . МТФ:  $\overline{a}, \overline{a}^2, \dots$  — периодична с периодом  $p - 1$ . Утверждение:  $\exists \overline{a} : p - 1$  — наименьший период этой последовательности.

**Замечание.** Пусть  $G$  — группа,  $|G| = p$  — простое. Тогда  $G \cong (\mathbb{Z}/p\mathbb{Z}, +)$ .  $G$  — циклическая.

**Доказательство.** Возьмем  $a \neq e$ . Тогда  $p : \text{ord}(a) \Rightarrow \text{ord}(a) = 1 \vee \text{ord}(a) = p \Rightarrow a = e \vee \langle a \rangle = G \Rightarrow G$  — циклическая  $\Rightarrow G \cong (\mathbb{Z}/p\mathbb{Z}, +)$ . □

**Определение 3.18.**  $R$  — ассоциативное кольцо, тогда  $R^* = \{a \in R | \exists a^{-1}\}$  — группа обратимых элементов.

Проверим, что  $R^*$  — группа.

- Проверим замкнутость.  $a, b \in R^* \Rightarrow \exists a^{-1} \exists b^{-1} : (ab)^{-1} = b^{-1}a^{-1}$ .

- $1 \in R^*$ .
- $a \in R^* : \exists a^{-1} \Rightarrow \exists (a^{-1})^{-1} = a$ , значит  $a^{-1} \in R^*$ .

**Замечание.**  $a^n = 1 \Rightarrow a \in R^*$ . Т.к. тут записано, что  $a \cdot a^{n-1} = 1$  — то есть он обратим.

**Определение 3.19.** Рассмотрим  $R = \mathbb{Z}/n\mathbb{Z}$ . Тогда  $R^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists \bar{b} : \bar{a}\bar{b} = 1\} = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$ . Тогда  $|R^*| = \varphi(n)$  — функция Эйлера.

**Теорема 3.9** (Теорема Эйлера).  $\forall b \in (\mathbb{Z}/n\mathbb{Z})^* = b^{\varphi(n)} = 1$

**Теорема 3.10** (Теорема Эйлера).  $\forall a \in \mathbb{Z} : (a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Эффективно вычислим  $\varphi(n)$ :

1.  $n = p^k$ ,  $p$  — простое.

$$\varphi(n) = \{x \in \{1, \dots, p^k\} \mid (x, p^k) = 1\} = \{x \in \{1, \dots, p^k\} \mid x \not\equiv 0 \pmod{p}\} = p^k - |\{p, 2p, \dots, p^k\}| = p^k - p^{k-1}.$$

2.  $n$  — составное.  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

По КТО:

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}).$$

. Тогда заметим, что

$$(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^* = (\mathbb{Z}/p_1\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^*.$$

Так как если  $(x_1, \dots, x_k)$  — обратим, то  $x_i$  — обратимы.

Из этого получаем, что

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = |(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^*| = \prod_{i=1}^k |(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*|.$$

Получили формулу из а). Применим её:

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) = n \cdot (1 - \frac{1}{p_1}) \cdot \dots \cdot (1 - \frac{1}{p_k}).$$

**Теорема 3.11** (Теорема о первообразном корне).  $p \in \mathbb{Z}$  — простое  $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^*$  — циклическая.

**Доказательство.** В ноябре. □

Посмотрим на устройство  $\mathbb{Z}/p\mathbb{Z}$ .  $\exists a \in \mathbb{Z} : \{\bar{a}, \bar{a}^2, \dots, \bar{a}^{p-1}\} = \{\bar{1}, \dots, \overline{p-1}\}$ .

Тогда как устроены  $(\mathbb{Z}/n\mathbb{Z})^*$  в общем случае?

Отступление: группа, порожденная множеством.

**Определение 3.20.** Подгруппа группы  $G$  — пара  $(H, *)$ , где  $H \subset G$ ,  $*$  — замкнуто относительно  $H$ . Обозначается  $\leq$ .

**Определение 3.21.** Подгруппа группы  $G$  порожденная множеством  $S$  ( $S \subset G$ ) — наименьшая по включению подгруппа  $G$ , содержащая все элементы  $S$ .

$$\langle S \rangle = \bigcap_{H \leq G, S \subset H} H.$$

**Замечание.**  $\forall I \forall H_\alpha, \dots, H_\omega, \alpha, \dots, \omega \in I : H_i \leq G \Rightarrow \bigcap_{i \in I} H_i \leq G$

**Доказательство.** Рассмотрим  $e (\forall i \in I H_i \text{ — группа} \Rightarrow e \in H_i) \Rightarrow e \in \bigcap_{i \in I} H_i$ .

$\forall x \in \bigcap_{i \in I} (\forall i \in I x^{-1} \in H_i) \Rightarrow x^{-1} \in \bigcap_{i \in I} H_i \Rightarrow \bigcap_{i \in I} H_i \text{ — группа (ассоциативность гарантируется определением подгруппы).}$   $\square$

**Теорема 3.12.**  $\forall S \subset G : \langle S \rangle = \{a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k} \mid \forall i \in I a_i \in S \wedge \varepsilon_i = \pm 1\}$ , т.е. все возможные произведения элементов из  $S$  и обратных к ним (элементы в произведении могут повторяться,  $k$  произвольное, не фиксировано)

**Доказательство.**

1. Пусть  $a_1, a_2, \dots, a_k \in S$ . Тогда для любой  $H \leq G$   $H \supseteq S$  верно:

- (a)  $a_i \in H$ .
- (b)  $a_i^{\varepsilon_i} \in H$ , так как  $H$  замкнута относительно  $^{-1}$
- (c)  $a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_k^{\varepsilon_k} \in H$ , так как  $H$  замкнуто относительно  $\cdot$ .

Значит  $H \supset \langle S \rangle \Rightarrow \langle S \rangle \subseteq H$ .

С другой стороны, сама группа  $\langle S \rangle$ , которую мы описали в предыдущей теореме, является корректной подгруппой  $G$ , т.е.  $H = \langle S \rangle \Rightarrow H \supset S \wedge H \leq G$ . Следовательно:

$$\bigcap_{H \leq G, S \subset H} H = \langle S \rangle.$$

$\square$

**Теорема 3.13.**  $(\mathbb{Z}/n\mathbb{Z})^*$  — циклическая  $\iff \begin{cases} n = p^k & p > 2 \text{ — простое} \\ n = 2p^k & \text{см. выше} \\ n = 2 \vee n = 4 \end{cases}$ .

$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ . Тогда  $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^*$ .

**Утверждение 3.14.**  $G_1, G_2, G$  — группы (конечные).

- 1.  $G \cong G_1 \times G_2$ .  $(|G_1|, |G_2|) \neq 1 \Rightarrow G$  — не циклическая.
- 2.  $(|G_1|, |G_2|) = 1$  и  $G_1, G_2$  — циклическая  $\Rightarrow G_1 \times G_2$  — циклическая. (КТО).

**Доказательство.** Пусть  $(|G_1|, |G_2|) > 1$ . Тогда  $\forall a \in G_1, b \in G_2$   $a^{|G_1|} = e_{G_1} \wedge b^{|G_2|} = e_{G_2} \Rightarrow (a, b)^{\text{lcm}(|G_1|, |G_2|)} = (e, e) \Rightarrow \forall x \in G_1 \times G_2 : \text{ord}(x) \leq \text{lcm}(|G_1|, |G_2|) < |G_1| \cdot |G_2| = |G_1 \times G_2| \Rightarrow G_1 \times G_2$  — не циклическая.  $\square$

**Замечание.**  $a^{\varphi(n)} = 1$ . Точна ли оценка  $\varphi(n)$ ? Если  $(\mathbb{Z}/n\mathbb{Z})^*$  — циклическая (например,  $n$  — простое). Тогда да. Иначе пусть  $n = pq$ ,  $p, q$  — простые. Тогда по Эйлеру  $a^{(q-1)(p-1)} = 1$ , а на самом деле  $a^{\frac{(q-1)(p-1)}{2}} = 1$ .

Теперь докажем теорему о том, в каких случаях мультипликативная группа вычетов циклическая.

**Доказательство.**  $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ . Тогда  $|(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*| = p_i^{\alpha_i} - p_i^{\alpha_i-1} : 2$ , кроме случая  $p_i = 2, \alpha_i = 1$ .

Поэтому, если  $k > 2$  или  $k = 2$   $p_1^{\alpha_1}, p_2^{\alpha_2} \neq 2^1 \Rightarrow \text{gcd}$  у размеров групп не взаимно просты  $\Rightarrow (\mathbb{Z}/n\mathbb{Z})^*$  — не циклическая.

Остались случаи  $k = 1, n = p^a$  и  $k = 2, n = 2 \cdot p^a$ .

Случай  $n = 2p^a, p \neq 2$ .  $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^a\mathbb{Z})^* = (\mathbb{Z}/p^a\mathbb{Z})^*$  — свели к случаю 1.

Пусть  $n = p^a$ .  $p = 2, a = 1, 2$  — очев.  $a > 2 \Rightarrow (\mathbb{Z}/2^a\mathbb{Z})^*$  — не циклическая. Пусть циклическая, тогда  $(\mathbb{Z}/2^a\mathbb{Z})^* = \langle x \rangle$ ,  $\text{ord } x = 2^{a-1}$ . Тогда в  $(\mathbb{Z}/2^a\mathbb{Z})^*$ :  $y^2 = 1 \iff \exists k(x^k)^2 = 1 \iff x^{2k} = 1$ .  $2k : 2^{a-1} \wedge k : 2^{a-2} \xrightarrow{x \in (0; 2^{a-1})} k = 0 \vee k = 2^{a-2}$ .  $y^2$  — имеет два решения. Но!  $1^2 = (-1)^2 = (2^{a-1} \pm 1)^2 = 1$ . 4 решения. Противоречие.

Теперь, если  $p \neq 2$ , то группа будет циклической. А дальше на лекции произошёл кек следующего вида: доказать для случая  $n = p^1$  довольно тяжело, будет потом или вообще не будет, в общем хз, а доказательство для случая  $n = p^a$  выводится «позже..., это довольно элементарная выкладка..., выводится уже какими-то совсем такими ручными манипуляциями» из случая  $n = p$ , но как конкретно — сказано не было, какая досада.  $\square$

**Теорема 3.15.**  $a \in (\mathbb{Z}/p\mathbb{Z})^*$ . Тогда  $x^2 = a$  имеет решение  $\iff a^{\frac{p-1}{2}} = 1$

**Доказательство.**

- $\Rightarrow$ .  $a = x^2 \Rightarrow a^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$  (МТФ).
- $\Leftarrow$ .  $a^{\frac{p-1}{2}} = 1$ .  $\exists c : (\mathbb{Z}/p\mathbb{Z})^* = \langle c \rangle$ .  $\exists k : a = c^k$ . Тогда  $a^{\frac{p-1}{2}} = (c^k)^{\frac{p-1}{2}} \iff c^{\frac{k(p-1)}{2}} = 1$  Та как  $\text{ord } \frac{k(p-1)}{2} : p-1$ . Тогда  $\frac{k}{2} \in \mathbb{Z}$ , то есть  $k = 2l$ .  $a = c^{2l} = (c^l)^2$ .

$\square$

### 3.6. Группы вычетов и криптографические протоколы

Главное отображение, которое нас интересует —  $p_k : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^* : p_k(x) = x^k$ .

Заметим, что если  $(p-1, k) = 1 \Rightarrow p_k$  — биекция:  $p_k^{-1}(x) = x^l$ , где  $l : kl = 1 \pmod{p-1}$ .  $x \rightarrow x^k \rightarrow (x^k)^l = x^{kl} = x^1 = x$ .  $x \rightarrow (x^l) \rightarrow (x^l)^k = x$ .

А если  $(p-1, k) \neq 1$ , то  $p_k$  — не биекция. Если  $p-1 = k \cdot s$  и  $g$  — первообразный корень, то  $\text{ord } g = p-1$  и  $(g^s)^k = 1$ . Тогда  $1^k = 1$  — не инъекция, т.к. несколько элементов перешли в единицу.

Классический протокол шифровки: протокол с закрытым ключом (ключ — способ шифровки / дешифровки).

Пусть Алиса(А) и Боб(В) хотят обмениваться информацией. Хотят придумать закрытый ключ путем пересылки сообщений.

Протокол Диффи-Хеллмана: А и В хотят сгенерировать закрытый ключ  $m \in \mathbb{N}$ .

1. Придумывают большое число  $p$ , объявляется всем
2. Придумывают  $a$  — первообразный корень по модулю  $p$ :  $\text{ord}_p(a) = p-1$ , тоже объявляется всем
3. А: берет  $x \in \mathbb{Z}$  (лучше  $(x, p-1) = 1$ ) и посылает  $a^x \pmod{p}$ ,  $x$  остаётся в тайне
4. В: берет  $y \in \mathbb{Z}$ ,  $a^y \pmod{p}$ ,  $a^y$  отправляет,  $y$  остаётся в тайне
5. А вычисляет  $(a^x)^y = a^{xy} \pmod{p}$ .
6. В: вычисляет  $(a^y)^x = a^{xy} \pmod{p}$ .

Получили ключ  $a^{xy}$ .

Чтобы взломать надо найти  $x, y$ . Если есть  $x$ , то посчитать  $a^x$  просто, а вот наоборот — сложно, т.е. троллинг заключается в трудности вычисления дискретного логарифма (общая концепция — односторонние функции).



### 3.7. Алгоритм RSA

RSA — Rivest, Shamir, Adleman.

RSA — шифрование с открытым ключом:

1. А: придумывает  $p, q$  — большие простые. Вычисляет  $\varphi(pq) = (p-1)(q-1)$ .  $p, q, (p-1)(q-1)$  — закрытая часть ключа.
2. Выбирает  $d \in \mathbb{Z}$   $(d, p-1) = (d, q-1) = 1$ .  $p, q, d$  — закрытая часть.
3. Открытый ключ  $n = pq$  и  $e \in \mathbb{Z} : de \equiv 1 \pmod{(p-1)(q-1)}$ . Решение Л.Д.У.
4. В: хочет послать сообщение  $(x \in \mathbb{Z}, (x, n) = 1)$  А: он посылает  $x^e \pmod{n}$ .
5. А: получает  $y = x^e$  и вычисляет  $y^d = (x^e)^d = x^{ed} = x^{k \cdot \varphi(n) + 1} = x \pmod{n}$ .

Устойчивость: чтобы взломать, надо знать  $(p-1)(q-1)$ , то нам надо просто знать  $p, q$ . Но мы не умеем делать это быстро.

### 3.8. Генерация простых, тесты на простоту

**Теорема 3.16.**  $\pi(n)$  — количество простых на  $[1, n]$ . Тогда  $\lim_{n \rightarrow +\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$ .

**Следствие.** Случайное число на  $1, n$  — простое с вероятностью  $\frac{1}{\ln n}$

Способ генерации: возьмем  $p_1, p_2, \dots, p_k$  — простые (небольшие). Попробуем  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} + 1$ , где  $a_i$  — произвольные степени. Получили число Люка.

**Теорема 3.17** (Тест Люка). Пусть  $b \in \mathbb{Z}$ , такое что  $b^{n-1} \equiv 1 \pmod{n}$  и  $b^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n}$ . Тогда  $n$  — простое.

**Доказательство.**  $b^{n-1} \equiv 1 \Rightarrow \text{ord}_n(\overline{b_n})$  — делитель  $n-1$ .

$b^{\frac{n-1}{p_i}} \not\equiv 1 \Rightarrow \text{ord}_n(\overline{b_n})$  — не делитель  $\frac{n-1}{p_i}$  для любого  $p_i \Rightarrow \text{ord}(\overline{b_n}) = n-1 \Rightarrow |(\mathbb{Z}/n\mathbb{Z})^*| \geq n-1 \Rightarrow n$  — простое.  $\square$

**Замечание.**  $n$  — простое,  $b$  — подходит  $\iff b$  — первообразный корень. Их  $\varphi(n-1)$ . Пусть  $\varphi(n-1) > \frac{n-1}{10}$ , значит через  $k$  тестов будет вероятность проиграть  $(\frac{9}{10})^k$ , что мало.

**Замечание.** Числа Люка — неоч для RSA:  $n = pq, p, q$  — числа Люка. Такие числа с большой вероятностью факторизуются: Выбираем  $a \in \mathbb{Z}$ , дальше  $a \rightarrow a^2 \rightarrow (a^2)^3 \rightarrow \dots$ , то есть вычисляем  $a^{k!} \pmod{n}$ . Помним, что  $p-1 = \prod p_i^{a_i}, q-1 = \prod p_i^{b_i}$ .

Рассмотрим  $K_p = \min\{a^{k!} \equiv 1 \pmod{p} \mid k \in \mathbb{N}\}$ .

$k_p, k_q$  — не велики. Действительно:  $k_p : p-1 = \prod p_i^{a_i}$ , а  $p_i$  — довольно маленькие.

Скорее всего  $k_p \neq k_q$ . Не умаляя общности считаем  $k_p < k_q$ , тогда  $(a^{k_p!}, n) = p$ .

Тест Ферма:  $n \in \mathbb{N}, a \in [1, \dots, n-1]$ . Если  $a^{n-1} \not\equiv 1 \pmod{n}$ , значит  $n$  — составное.

**Определение 3.22.** Если  $n$  — составное, но  $a^{n-1} \equiv 1 \pmod{n}$ , то  $a$  — свидетель простоты.

Если  $n$  — составное, то или свидетелей  $\leq \frac{\varphi(n)}{2} \leq \frac{n-1}{2}$ , или любое взаимно простое с  $a$  является свидетелем простоты. Свидетели образуют подгруппу, а значит либо это вся группа, либо там  $\leq \frac{\varphi(n)}{2}$  элементов.

Пусть там меньше половины, тогда после  $k$  итераций вероятность проиграть  $\frac{1}{2^k}$ , что довольно хорошо.

Тест Рабина-Миллера. Пусть  $n - 1 = 2^s \cdot m$ . Тогда, если  $n$  — простое, то  $x^2 \equiv 1 \pmod{n} \Rightarrow x = \pm 1 \pmod{n}$ . Тогда берем  $a \in (\mathbb{Z}/n\mathbb{Z})^*$ . Считаает  $a^m, (a^m)^2, \dots, (a^m)^{2^{s-1}}$ . Так как  $n$  — простое  $\Rightarrow$  или  $a^m = 1$ , или есть  $-1$ , а потом  $1$ .

Условие Миллера-Рабина работает для  $\forall a \in [1.. \sqrt[7]{n}]$  или  $\in [1.. \log^2 n]$ , если верим в гипотезу Римана.

Но Рабин заметил, что вероятность ошибиться для составного  $\frac{\varphi(n)}{4}$

## 4. Многочлены

Теперь мы многочлены будем рассматривать как самостоятельные элементы, а не как функции, ведь сами многочлены можно складывать и умножать! Причем свойства умножения и сложения удовлетворяет требованием кольца! Получили **Кольцо многочленов над кольцом  $\mathbb{R}$** .

Но сначала рассмотрим немного другую штуку: **кольцо формальных степенных рядов** (отличие будет позже).

**Определение 4.1.** Пусть  $R$  — ассоциативное коммутативное кольцо. Тогда кольцо формальных степенных рядов  $R[[x]]$  — тройка  $(R^{\mathbb{Z}_{\geq 0}}, +, \cdot)$ .

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

$$\cdot \text{ (Правило свертки): } (a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (a_0 b_0, a_0 b_1 + b_1 b_0, \dots), \text{ по факту: } (a_i) \cdot (b_i) = (c_i), c_n := \sum_0^n a_k b_{n-k}$$

Так же можно представлять  $(a_0, a_1, a_2, \dots) \iff a_0 + a_1 x + a_2 x^2 + \dots$ . То есть, если неформально, то правило свертки — обычное раскрытие скобок.

**Определение 4.2.**  $R^{\mathbb{Z}_{\geq 0}} = \{f : \mathbb{Z}_{\geq 0} \rightarrow R\} = \{(a_0, a_1, \dots) | a_i \in R\}$

**Теорема 4.1.**  $R[[x]]$  — ассоциативное, коммутативное кольцо. Причем, если  $R$  с единицей, то  $R[[x]]$  — кольцо с единицей.

**Доказательство.** Заметим, что все аксиомы доказываются супер просто, ведь сложение у нас просто по координатам. Тогда получили очевидность коммутативности и ассоциативности  $+$  (следует из коммутативности и ассоциативности  $R$ ). В качестве нуля берется  $0 = (0, 0, 0, \dots)$ . Обратный элемент —  $-(a_0, a_1, a_2, \dots) = (-a_0, -a_1, -a_2, \dots)$

Дистрибутивность — упражнение (из дистрибутивности  $R$ ).

Коммутативность произведения:  $c_n = \sum_0^n a_k b_{n-k} = \sum a_k b_l$ , где  $k, l \geq 0 \wedge k + l = n$ . Тогда  $c_n = \sum_{l=0}^n a_{n-l} b_l = \sum_{l=0}^m b_l a_{n-l}$  — формула свертки для  $b \cdot a$ .

Если  $\exists 1_R$ , то  $(1_R, 0_R, 0_R, \dots)$  — нейтральный относительно  $\cdot$  в  $R[[x]]$  (упражнение).

Ассоциативность (упражнение на смирение духа):  $\forall f, g, h \in R[[x]] (f \cdot g) \cdot h = f \cdot (g \cdot h)$ . Введем много обозначений:  $f = (a_n), g = (b_n), h = (c_n), f \cdot g = (d_n), g \cdot h = (e_n), (f \cdot g) \cdot h = (k_n), f \cdot (g \cdot h) = (l_n)$

Хотим доказать, что  $k_n = l_n \forall n \in \mathbb{Z}_{\geq 0}$ . Тогда

$$k_n = \sum_{i=0}^n d_i c_{n-i} = \sum_{i=0}^n \left( \sum_{j=0}^i a_j b_{i-j} \right) c_{n-i}.$$

Воспользуемся дистрибутивностью:

$$k_n = \dots = \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq i}} a_j b_{i-j} c_{n-i}.$$

Определим  $s := i - j, t := n - i$ , тогда

$$k_n = \dots = \sum_{\substack{j, s, t \geq 0 \\ j + s + t = n}} a_j b_s c_t.$$

Аналогично для  $l_n$ :

$$l_n = \dots = \sum_{\substack{j, s, t \geq 0 \\ j + s + t = n}} a_j b_s c_t.$$

□

**Замечание.** Если  $R$  — не коммутативное кольцо, то стоит различать  $ax^2$ ,  $x^2a$ ,  $xa$ .

**Замечание.** Существует инъективный гомоморфизм колец  $i : R \rightarrow R[[x]] : a \rightarrow (a, 0, 0, 0, \dots)$ . Это можно проверить.

Тогда не умаляя общности считаем, что  $R$  содержится в  $R[[x]]$  (в качестве подкольца).

**Замечание.** Положим по определению  $x := (0, 1, 0, 0, 0, \dots)$ .

Тогда (упражнение на индукцию)  $x^n := (0, 0, \dots, \overbrace{1}^n, 0, 0, \dots)$  (1 стоит на  $n$ -ой позиции в нумерации с нуля)

Тогда, если  $f = (a_0, a_1, a_2, \dots, a_n, 0, 0, 0)$  ( $a_i$  при  $i > n$  равно 0).

Тогда  $f = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \dots + a_n \cdot x^n$ .

**Замечание.**  $(a_0, a_1, a_2, \dots) \cdot \underbrace{(0, 1, 0, \dots)}_x = (0, a_0, a_1, \dots)$

**Следствие.**  $f : x. f = (a_i) \wedge a_0 = 0 \Rightarrow 1 \nmid f$ .

**Теорема 4.2.**  $f = (a_i). f \in R[[x]] \iff a_0 \in R^*$ . В частности:  $R$  — поле  $\Rightarrow f$  — обратим  $\iff f \nmid x$ .

**Доказательство.**

•  $\Rightarrow$ .  $(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (1, 0, 0, \dots)$ .

$1 = a_0 b_0 \Rightarrow a_0 \in R^*$ .

•  $\Leftarrow$ : будем вычислять последовательность  $(b_0, b_1, \dots)$ .  $a_0 \in R^*$ , тогда:

$a = a_0 b_0 \Rightarrow b_0 = a_0^{-1} = \frac{1}{a_0}$ .  $0 = a_0 b_1 + a_1 b_0 \Rightarrow \frac{-a_1 b_0}{a_0}$ . И так далее.

$0 = \sum_{i=0}^n a_i b_{n-i}$ .  $b_n = (-\sum_{i=1}^n a_i b_{n-i}) a_0^{-1}$ .

Построили метод построения  $b$ , причем все хорошо!

□

**Пример.**  $f = (1, 1, 1, 1, \dots) = 1 + x + x^2 + x^3 + \dots$ . Тогда  $\frac{1}{1+x+x^2+\dots} = 1-x$ . Тогда  $1+x+x^2+x^3+\dots = \frac{1}{1-x}$ .

**Теорема 4.3.** Подмножество в  $R[[x]]$   $R[x] = \{(a_0, a_1, \dots) \mid \exists N \forall n > N : a_n = 0\}$  — финитные последовательности, образуют подкольцо с единицей, называемое **кольцом многочленов** (вот и то самое отличие от формальных степенных рядов)).

**Доказательство.** Замкнутость по  $+$ :  $a_n = 0$  при  $n > N_1$  и  $b_n = 0$  при  $n > N_2$ . Тогда при  $n > \max(N_1, N_2)$   $a_n + b_n = 0$ .

Замкнутость по  $\cdot$ :  $a_n = 0, n > N_1$  и  $b_n = 0, n > N_2$ . Тогда при  $n > N_1 + N_2$ :  $c_n = \sum_{i+j=n} a_i b_j = 0$ . Так как при  $i+j = N > N_1 + N_2 \Rightarrow i > N_1 \vee j > N_2$ .

$1 \in k[x]!!!$

□

**Определение 4.3.**  $f \in k[x]$  степенью  $f$  называется  $\deg f = \{\max k : a_k \neq 0\}$ . Причем  $\deg 0 = -\infty$

**Свойства.**

1.  $\deg(f+g) \leq \max(\deg f, \deg g)$ . Причем  $\deg f \neq \deg g \rightarrow \deg(f+g) = \max(\deg f, \deg g)$ .

2.  $\deg(f \cdot g) \leq \deg f + \deg g$ , а если  $R$  — область целостности, то  $\deg(fg) = \deg f + \deg g$ .

**Следствие.**  $R$  — область целостности  $\Rightarrow R[x]$  — область целостности.

Теперь у нас  $K$  — поле.

**Теорема 4.4** (О делении с остатком).  $f, g \in K[x]$   $g \neq 0$ . Тогда  $\exists! q, r \in K[x] : f = g \cdot q + r, \deg r < \deg g$ .

**Доказательство.** Формальное доказательство будет в конспекте, который должен скинуть Антипов. Здесь только кукареки.

Идея: в целых числах операция деления: вычитание, пока это возможно.

Многочлены:  $f = ax^m + \dots, g = bx^l, m \geq l$ .  $f \rightsquigarrow f - \frac{a}{b}x^{m-l} \cdot g = ax^m f + \dots$ . Получили сумму чего-то кратного  $g$  + какой-то остаток.  $\square$

**Следствие.**  $R$  — коммутативное, ассоциативное кольцо  $a \in R$ . Тогда  $\exists$  гомоморфизм колец  $R[x] \rightarrow R : a_0 + a_1x + \dots + a_nx^n \mapsto a_0 + a_1 \cdot a + \dots + a_n a^n$  — гомоморфизм эвалюации.

С другой стороны  $f \in R[x]$  — полиномиальная функция.  $F_f : R \rightarrow R$   $a \mapsto \text{ev}_a(f)$ .

**Следствие.**  $f, g \xrightarrow[\text{Эвклида}]{\text{Алгоритм}} h = (f, g)$   $h = u_1f + u_2g$ . А значит, у  $\gcd$  корнями будут общие корни  $f$  и  $g$ .

**Определение 4.4.**  $f \in R[x]$ .  $a \in R$  — корень  $f$ , если  $F_f(a) = 0$ .

**Теорема 4.5** (Безу).  $K$  — поле.  $f \in K[x]$ .  $a \in K$ .  $f = (x - a)g + r$  — деление с остатком.

$$1. r = f(a).$$

$$2. r = 0 \iff f : (x - a) \text{ (тут } r \text{ можно заменить на } f(a), \text{ сути не меняет)}$$

**Доказательство.**  $f = (x - a) \cdot g + r, \deg r < \deg(x - a) = 1 \Rightarrow \deg r = 0 \vee \deg r = -\infty \iff r = c \in K$ .

$$F_f(a) = F_{x-a}(a)F_g(a) + F_r(a). f(a) = (a - a)g(a) + r \iff r = f(a). \quad \square$$

**Следствие.**  $\deg f = n, f \in K[x], f \neq 0 \Rightarrow$  существует не более  $n$  корней  $f$  в  $K$ .

**Доказательство.** По индукции по  $n$ .

- База  $n = 0$   $f = r \neq 0$  — 0 корней.

- Переход  $n \rightarrow n + 1$ :

$$\deg f = n + 1. \text{ Нет корней } \Rightarrow 0 \leq n + 1.$$

Существует  $a$  — корень.  $f = (x - a)\tilde{f}, \deg \tilde{f} = n$ . У  $\tilde{f}$  не более  $n$  корней  $\Rightarrow$  у  $f$  не более  $n + 1$  корня.

С другой стороны  $b$  — корень  $f \Rightarrow f(b) = 0$ .  $(b - a)\tilde{f}(b) = 0 \xrightarrow{k-\text{о. п.}} b - a = 0 \vee \tilde{f} = 0 \iff b = a \vee b$  — корень  $\tilde{f}$ . Таких не более  $n$ , а значит у  $f$  не более  $n + 1$  корня.  $\square$

$f \in K[x]$ .  $f \rightsquigarrow F_f : K \rightarrow K$  — полиномиальная функция. Верно ли  $F_f = F_g \Rightarrow f = g$ ?

**Теорема 4.6** (Теорема о формальном и функциональном равенстве). Пусть  $K$  — поле,  $f, g \in K[x]$ ,  $|K| > \max(\deg f, \deg g)$ , например,  $K$  — бесконечно. Тогда  $F_f = F_g \Rightarrow f = g$ .

**Доказательство.**  $F_f = F_g \Rightarrow f(k) = g(k) \forall k \in K \Rightarrow (f - g)(k) = 0 \forall k \in K$ . По свойствам степени знаем, что  $n := \deg(f - g) \leq \max(\deg f, \deg g)$   
 $|K| > \max(\deg f, \deg g) \geq n \Rightarrow f - g = 0 \iff f = g$ .  $\square$

**Замечание.**  $K = \mathbb{Z}/8\mathbb{Z}$ . Тогда у  $x^2 = 1$  4 корня:  $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ . А у  $x^2 - 2x = 0$  корня  $\bar{0}, \bar{2}, \bar{4}, \bar{6}$ .  $x^2 - 1)(x^2 - 2x) = 0 \iff x^4 + 2x = 2x^3 + x^2$  как функции. При этом  $\max(\deg) = 4 < 8$ .

**Замечание.**  $\mathbb{Z}/p\mathbb{Z}$ :  $x^p = x - ???$

**Замечание.** Рассмотрим  $\mathbb{Z}/p\mathbb{Z}[x]$  — бесконечное кольцо.  $f \rightsquigarrow F_f: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$  — не более  $p^p$  отображений.  $\mathbb{Z}/p\mathbb{Z}[x]_{p-1} = \{f \mid \deg f \leq p-1\}$ .

$$\mathbb{Z}/p\mathbb{Z}[x]_{p-1} \leftrightarrow \{\text{отображения } \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}\}.$$

## 4.1. Интерполяция

**Определение 4.5.** Интерполяционная задача в поле  $K$  называется набор данных  $x_1, x_2, \dots, x_n \in K$  ( $x_i \neq x_j$ ),  $y_1, y_2, \dots, y_n \in K$ .

Задача заключается в поиске  $f \in K[x]: f(x_i) = y_i \forall 1..n$ .

$x_i$  — узлы интерполяции.

**Теорема 4.7.** Любая интерполяционная задача с  $n$  узлами имеет единственное решение  $f_0$  среди множеств степени  $< n$ .

**Доказательство.**

- Единственность. Пусть  $f_0, f_1$  — два решения.  $\deg(f_i) < n$ .

$f_0(x_c) = y_c = f_1(x_c)$ . Тогда возьмем  $g := f_0 - f_1$ . Заметим, что у него  $n$  корней, но  $\deg < n$ . Значит  $f_0 = f_1$

- Существование: рассмотрим задачу  $\chi_i: \chi_i(x_i) = 1, \chi_i(x_j) = 0$ , если  $i \neq j$ . Её решение:  $L_i = \frac{(x-x_1)(x-x_2)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)}{(x_i-x_1)(x_i-x_2)\dots}$  — в числителе условие на 0, в знаменателе на 1.

Тогда  $f_0 := y_1 L_1 + y_2 L_2 + \dots + y_n L_n$ . Тогда для  $\forall i: f_0(x_i) = y_1 L_1(x_i) + \dots$  во всех слагаемых, кроме  $y_i \cdot L_i(x_i)$  равно 0, а данное слагаемое равно  $y_i$ .

$\square$

**Определение 4.6.** Интерполяционный полином Лагранжа:  $f_0 = \sum_i \frac{y_i \prod_{j \neq i} (x-x_j)}{\prod_{j \neq i} (x_i-x_j)}$ , если  $\deg f_0 < \max(\deg L_i) = n-1$

## 4.2. Закрываем долг

**Теорема 4.8.**  $(\mathbb{Z}/p\mathbb{Z})^*$  — циклическая группа, то есть  $\exists a \in \mathbb{Z}/p\mathbb{Z}: \{a, a^2, \dots, a^{p-1}\} = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$ , то есть  $\text{ord } a = p-1$ ,  $a$  — первообразный корень.

**Лемма.** Пусть  $a \in G$  — группа,  $\text{ord } a = d$ . Тогда  $\text{ord}(a^k) = \frac{d}{(d,k)}$

**Доказательство.**  $(a^k)^l = e \iff a^{kl} = e \iff kl : \text{ord}(a) = d$ . Тогда, если  $k = (d,k) \cdot k'$  и  $d = (d,k)d'$ , то  $(d,k) \cdot k' \cdot l : (d,k) \cdot d' \iff k' \cdot l : d' \xrightarrow{(k',d')=1} l : d' = \frac{d}{(d,k)}$   $\square$

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

**Доказательство.** Пусть  $d_1, d_2, \dots, d_k$  — все натуральные делители  $n$ .  $n = |\{1, 2, \dots, n\}| =: |A|$ .

Разобьем множество  $A = A_1 \cup A_2 \cup \dots \cup A_k$ , причем  $A_i \cap A_j = \emptyset$  и  $|A_i| = \varphi(d_i)$  (тогда докажем лемму).

$A_i = \{a \in A \mid (a, n) = \frac{n}{d_i}\}$ . Заметим,  $d_1, \dots, d_k$  — все делители  $n \Rightarrow \frac{n}{d_1}, \dots, \frac{n}{d_k}$  — все делители  $n$ . И понятно, что  $\forall a \ (a, n)$  — какой-то делитель  $n$ .

Поэтому  $A = A_1 \cup A_2 \cup \dots \cup A_k$   $A_i \cap A_j = \emptyset$ .

$a \in A_i \iff (a, n) = \frac{n}{d_i}$ . Значит  $a = \frac{n}{d_i}k$ ,  $(\frac{n}{d_i}k, n) = \frac{n}{d_i} \iff (\frac{n}{d_i}k, \frac{n}{d_i}d_i) = \frac{n}{d_i} \iff (k, d_i) = 1$ .

Тогда  $|A_i| = |\{k \mid k \leq d_i \wedge (k, d_i) = 1\}| = \varphi(d_i)$ .  $\square$

**Лемма.** Количество элементов порядка  $d$  в  $(\mathbb{Z}/p\mathbb{Z})^*$  равно либо 0, либо  $\varphi(d)$ .

**Доказательство.** Например,  $p-1 \not\equiv d \Rightarrow$  кол-во равно 0.

Пусть  $\exists a: \text{ord } a = d$   $a^d = 1$ ,  $a, a^2, \dots, a^d = 1$  — различные элементы. Тогда  $\forall k = 1..d$   $(a^k)^d = (a^d)^k = 1$ , то есть это  $d$  решений  $x^d = 1$ . Других решений нет, так как  $x^d - 1$  имеет  $\leq d$  корней.

Пусть  $\text{ord } b = d \Rightarrow b^d = 1 \Rightarrow b = a^k$ ,  $k = 1..d$ . Тогда по предыдущей лемме  $\text{ord } a^k = \frac{d}{(d, k)} \Rightarrow (d, k) = 1$ .

Тогда  $(k, d) = 1 \Rightarrow \text{ord}(a^k) = d$ . То есть все элементы порядка  $d$  это  $\{a^k \mid 1 \leq k \leq d \wedge (k, d) = 1\}$ .  $\square$

*Доказательство теоремы.*  $B_d \subset (\mathbb{Z}/p\mathbb{Z})^*$ , такие что  $B_d = \{x \in (\mathbb{Z}/p\mathbb{Z})^* \mid \text{ord } x = d\}$ ,  $B_0 = \{0\}$ .

Тогда получится, что  $(\mathbb{Z}/p\mathbb{Z}) = B_0 \cup B_{d_1} \cup \dots \cup B_{d_k}$ ,  $d_i$  — делители  $p-1$  (со звездочкой без нуля).

$p-1 = |(\mathbb{Z}/p\mathbb{Z})^*| = \sum |B_{d_i}|$  по лемме 3 каждое слагаемое 0 или  $\varphi(d_i)$ , а по лемме 2  $p-1 = \sum_{i=1}^k \varphi(d_i)$ . А значит в первой сумме каждое слагаемое  $\varphi(d_i)$ .

В том числе  $|B_{p-1}| = \varphi(p-1) \neq 0$ , то есть  $\exists$  элементы порядка  $p-1$ .  $\square$

**Замечание.**  $K$  — не область целостности  $\Rightarrow$  не выполняется ОТА для многочленов.

$$\mathbb{Z}/8\mathbb{Z}: x^2 - 1 = (x-1)(x+1) = (x-3)(x+3)$$

## 5. Евклидовы кольца

**Определение 5.1.**  $A$  — область целостности, тогда  $A$  называется евклидовым, если  $\exists \varphi: A \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ , такой что  $\forall a, b \in A, b \neq 0 \exists q, r: a = bq + r$ , причем  $\varphi(r) < \varphi(b)$

**Пример.**  $\mathbb{Z}$  — евклидово.  $\varphi(x) = |x|$ .

**Пример.**  $K$  — поле.  $K[x]$  —  $\varphi(f) = \deg f$

**Пример.**  $\mathbb{Z}[\sqrt{2}]$  — евклидово.  $\mathbb{Z}[\sqrt{5}]$  — неевклидово.