

# Алгебры

Харитонцев-Беглов Сергей

31 октября 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 вычета и их друзья</b>	<b>6</b>
3.1 Группы . . . . .	6
3.2 Кольца . . . . .	7
3.3 Построение кольца вычетов . . . . .	7
3.4 Квадратное уравнение . . . . .	9
3.5 Китайская теорема об остатках . . . . .	9
3.6 Группы вычетов и криптографические протоколы . . . . .	13
3.7 Алгоритм RSA . . . . .	14
3.8 Генерация простых, тесты на простоту . . . . .	14

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

**Доказательство.**  $a, b : c \Rightarrow \exists d, e : \begin{matrix} a = c \cdot d \\ b = c \cdot e \end{matrix}$ . 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.  $a : b \Rightarrow \begin{cases} |a| > |b| \\ a = 0 \end{cases}$ .
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:  $b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \iff b(q_1 - q_2) = r_2 - r_1 \xrightarrow{r_1, r_2 \in [0; |b|-1]} [|r_1 - r_2| < |b|] r_2 - r_1 : b \Rightarrow r_2 - r_1 = 0 \iff r_1 = r_2 \Rightarrow b(q_1 - q_2) = 0 \iff q_1 = q_2$

• Существование.

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.

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

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

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

**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.  $r \in I \Rightarrow (-q) \cdot r \in I \wedge q \in I \Rightarrow a + (-q) \cdot r \in I$ , т.е.  $r_1 \in I$ . Но!  $0 < r_1 < r$ , 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  $d$  — 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  $d = \underbrace{ax}_{:d} + \underbrace{by}_{:d} : d$ .

- $ax + by = c$  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.**  $x \in \mathbb{Z}, x \neq 1$ , тогда  $x$  — простое число, если  $x = x_1 x_2 \iff \begin{cases} x_1 = \pm 1 \\ x_2 = \pm 1 \end{cases} \quad \forall x_1, x_2$

**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  $p$  — простое и  $p = x_1 x_2$ . Тогда  $x_1 x_2 : p$  по \*,  $\begin{bmatrix} x_1 : p \\ x_2 : p \end{bmatrix}$ . Пусть  $x_1 = py$ .  $p = x_1 x_2 = py x_2$ .  $1 = y x_2 \Rightarrow x_2 = \pm 1$ .

- $\Rightarrow$ . Пусть  $p$  — простое и  $ab : p$ .  $d = (a, p)$ ,  $d = d \cdot d_1$ ,  $p$  — 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)

$$n = \epsilon p_1 p_2 \dots p_n, \epsilon = \pm 1 = \text{sign}(n), p_1 < p_2 < \dots < p_n.$$

**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.
- $x = x_1 x_2$ .  $x_1, x_2 = \pm 1 \Rightarrow x_1, x_2 < X \Rightarrow x_1, x_2$  — 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  $X' = \frac{X}{q_1}$ .  $q_2 q_3 \dots q_n = X' = p_1 p_2 \dots p_k$ .  $X' < X$ , значит  $q = p$ . А значит противоречие.  $\square$

Контр-примеры для О. Т. А:

1. Рассмотрим  $2\mathbb{Z}$  — множество четных чисел. Теперь 6 — простое. 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  $\mathbb{Z} \subset \mathbb{Z}\{\sqrt{5}\}$

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

**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:  $V_p(n)$

- $V_p(xy) = V_p(x) + V_p(y)$
- $V_p(x+y) = \min(V_p(x), V_p(y))$ , и если  $V_p(x) \neq V_p(y)$

**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  $\underbrace{p^{a-b} \tilde{x} + \tilde{y}}_{:p}$

не делится на  $p$ . А значит  $V_p(x+y) = \min(V_p(x), V_p(y))$ .  $\square$

Еще следствия из О. Т. А.

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

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

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 вычета и их друзья

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

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 чисел. 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 по кольцо вычетов по модулю.

#### 3.1. Группы

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

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

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

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

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

**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  $(b + c) \cdot a = b \cdot a + b \cdot c$ . 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

6.  $a \cdot b = b \cdot a$

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

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

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

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

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

**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  $n \mid a - b$ . Эквивалентное определение:  $a$  и  $b$  имеют одинаковые остатки по модулю  $n$ .

Докажем, что сравнимость по модулю — отношение эквивалентности.

- $a \equiv a \pmod{n} \iff n \mid 0$
- $n \mid a - b \iff n \mid b - a \Rightarrow a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$ .
- Транзитивность...

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  $\overline{a+b} = \overline{a} + \overline{b} \wedge \overline{a \cdot b} = \overline{a} \cdot \overline{b}$  — ассоциативное коммутативное кольцо с единицей.

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

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  $\forall a \in R : a \text{ — делитель} \Rightarrow \exists b \neq 0 : ab = 0$ .

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

**Лемма.**  $\forall a, b, c \in R ab = ac \wedge a \text{ — не делитель } 0 \Rightarrow b = c$ .

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

**Лемма.**  $a \in Ra$  — обратим  $\Rightarrow a$  — не делитель 0.

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

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

$(a, n) = d > 1, a = dx$ . Тогда  $\overline{a} \cdot \overline{\frac{n}{d}} = \overline{dx} \overline{\frac{n}{d}} = \overline{nx} = 0$  и  $\overline{\frac{n}{d}} \neq 0$ . Значит  $9 < |\frac{n}{d}| < n$ .  $\square$

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

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

**Определение 3.11.**  $\forall$  ассоциативного кольца с 1  $R$ :  $R$  — называется кольцом без делителей 0 (область целостности), если делитель 0 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  $ax + by = 1, (a, b) = 1$ . Тогда  $ax = c \pmod{b}$  и  $by = c \pmod{a}$ . Тогда  $\overline{ax} = \overline{c}$  в  $\mathbb{Z}/n\mathbb{Z} \xrightarrow{(a,b)=1} \overline{x} = \overline{a}^{-1} \overline{c} \pmod{b}$ . 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  $\mathbb{Z}/n\mathbb{Z}$  (не решений).
2.  $2 = 0$ . Или  $\nexists 2^{-1}$  (нельзя поделить на два).
3.  $n$  — не простое. Тогда  $(x - x_1)(x - x_2) \dots = 0$ . Тогда 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  $P_{mn} : \mathbb{Z} \mapsto \mathbb{Z}/mn\mathbb{Z}$ .

**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 групп  $f : G_1 \mapsto G_2$  называется такое отображение, что  $\forall g_1, g_2 : f(g_1 g_2) = f(g_1) \cdot f(g_2)$ .

**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.**  $f(e_{G_1}) = f(e_{G_1} \cdot e_{G_1}) = f(e_{G_1}) \cdot f(e_{G_1})$ . Дальше сокращаем. □

Существует  $P_{mn,m} : P_{mn,m} \cdot P_{mn} = P_m$ .

**Доказательство.**  $P_{mn,m}(\overline{a_{mn}}) = \overline{a_m}$ . □

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

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  $(R_1 \times R_2, +, \cdot) : (r_1, r_2) +_{R_1 \times R_2} (r'_1, r'_2) := (r_1 +_{R_1} r'_1, r_2 +_{R_2} r'_2)$ . То же самое для умножения. Тогда  $R_1 \times R_2$  — тоже кольцо.

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

**Определение 3.15.** Биективный 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  $i_{m,n}(\overline{a_{m,n}}) = (\overline{a_m}, \overline{a_n}), i_{m,n}(\overline{b_{m,n}}) = (\overline{b_m}, \overline{b_n}) \Rightarrow a - b : m \wedge a - b : n \xrightarrow{(n,m)=1} a - b : mn$ .
2.  $i_{m,n} : a \mapsto B$  инъективно:  $|A| = |B| \Rightarrow i_{m,n}$  — сюръективно.

□

**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).  $\forall m_1, \dots, m_n \in \mathbb{Z}, \forall a_1, \dots, a_n (m_i, m_j) = 1 \Rightarrow \exists x_0 \in \mathbb{Z} x \equiv a_1 \pmod{m_1} \wedge \dots \wedge x \equiv a_n \pmod{m_n} \iff x \equiv x_0 \pmod{\prod_i m_i}$

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

**Доказательство.**  $f : (\mathbb{Z}, +) \rightarrow \langle a \rangle$ . То есть  $k \mapsto a^k$ .  $f(k+l) = a^{k+l} = a^k \cdot a^l = f(k) + f(l)$ . Тогда  $f$  — 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  $a^m = a^{n+k \cdot l} \iff a^m = a^n \cdot a^{kl} = a^m$ .

Суръективность/инъективность: смотри выше. Или ниже, ну тут бан короче.

□

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 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) —  $x \rightarrow a_x$ ).  $x \rightarrow ax \rightarrow a^2x \rightarrow a^3x \rightarrow \dots \rightarrow a^kx \rightarrow x$ , так как для  $\forall i, j \leq k : a^i x = a^j x \Rightarrow a^i = a^j$ .

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

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

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

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

**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:  $\bar{a}, \bar{a}^2, \dots$  — периодична с периодом  $p - 1$ . Утверждение:  $\exists \bar{a} : p - 1$  — 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  $\Rightarrow G \cong (\mathbb{Z}/p\mathbb{Z}, +)$ .  $\square$

**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.

Рассмотрим  $R = \mathbb{Z}/n\mathbb{Z}$ . Тогда  $R^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} | \exists \bar{b} : \bar{a}\bar{b} = 1\} = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} | (a, n) = 1\}$ . 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.

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

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 3.19.**  $G$ -группа  $S \subset G$  — подгруппа, порожденная множеством  $S$ .

1. Наименьшая (по включению) подгруппа  $G$ , содержащая  $S$ .

**Замечание.**  $H$  — подгруппа  $G$ :  $H \leq G$ .

**Замечание.**  $\{H_i\}_{i \in I} : H_i \leq G \Rightarrow \bigcap H_i \leq G$ .

2. (Явное описание).  $\langle S \rangle = \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_k^{\varepsilon_k} \mid a_i \in S, \varepsilon = \pm 1\}$ .

Докажем, что 1) равно 2).

**Доказательство.**

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

(а)  $a_i \in H$ .

(б)  $a_i^{\varepsilon_i} \in H$ , так как  $H$  замкнута относительно  $^{-1}$

(с)  $a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_k^{\varepsilon_k} \in H$ , так как  $H$  замкнуто относительно  $\cdot$ .

Значит  $H \supset \langle S \rangle \Rightarrow \langle S \rangle \subset \prod_{H \leq G \wedge H \supset S} H$ .

С другой стороны  $H = \langle S \rangle \Rightarrow H \supset S \wedge H \leq G$ .  $\langle S \rangle$  — подгруппа:

$$(a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k}) \cdot (b_i^{\mu_i}) = \prod_i ???.$$

□

**Теорема 3.12.**  $(\mathbb{Z}/n\mathbb{Z})^*$  — 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  $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^*$ .

Общее утверждение:  $G_1, G_2, G$  — 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).

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.

**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  $a^{\frac{(q-1)(p-1)}{2}} = 1$ .

**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  $k = 2, p_1^{\alpha_1}, p_2^{\alpha_2} \neq 2^1 \Rightarrow p_i^{\alpha_i} - p_i^{\alpha_i-1}$  — не циклическая  $\Rightarrow (\mathbb{Z}/n\mathbb{Z})^*$  — не простое. Остались случаи  $k = 1, n = p^a, k = 2, n = 2 \cdot p^a$ .

Случай  $n = 2p^a, p \neq 2$ .  $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/p^a\mathbb{Z})^* = (\mathbb{Z}/p^a\mathbb{Z})^*$  — 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  $(\mathbb{Z}/2^a\mathbb{Z})^*$ :  $y^2 = 1 \iff \exists k(x^k)^2 = 1 \iff x^{2k} = 1$ .  $2k : 2^{a-1} \wedge 2k : 2^{a-2} \Rightarrow k = 0 \vee k = 2^{a-2}$ .  $y^2$  — имеет два решения.  $\square$

**Теорема 3.13.**  $a \in (\mathbb{Z}/p\mathbb{Z})^*$ . 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.

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

Чтобы взломать надо найти  $x, y$ . Если есть  $x$ , то посчитать  $a^x$  просто, а вот наоборот — сложно.

Получили ключ  $a^{xy}$ .

### 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 3.14.**  $\pi(n)$  — 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 Тест Люка.

**Теорема 3.15** (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  $b$  — простое.

**Доказательство.**  $b^{n-1} \equiv 1 \Rightarrow \text{ord}_n(\bar{b})$  — делитель  $n - 1$ .  $b^{\frac{n-1}{p_i}} \not\equiv 1 \Rightarrow \text{ord}_n(\bar{b})$  — не делитель  $\frac{n-1}{p_i}$  для любого  $p_i \Rightarrow \text{ord}_n(\bar{b}) = n - 1 \Rightarrow |(\mathbb{Z}/n\mathbb{Z})^*| \geq n - 1 \Rightarrow n$  — 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  $\left(\frac{9}{10}\right)^k$ , 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:  $k_p \leq \prod p_i^{a_i}$ .

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 3.20.** 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  $a \in (\mathbb{Z}/n\mathbb{Z})^*$ . Считаю  $a^m, (a^m)^2, \dots, (a^m)^{2^{s-1}}$ . Так как  $n$  — простое  $\Rightarrow$  или  $a^m = 1$ , или есть  $-1$ , а потом 1.

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

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