

# Теория чисел

## Основной поток

Создал: Низамов Айнур, БПМИ225

Скачать актуальную версию можно нажав по [ссылке](#)

При обнаружении ошибок просьба писать [сюда](#) (не анонимно, но быстро) или [сюда](#) (анонимно, но не очень быстро). Для любителей git предлагаю создавать issue на [GitHub](#)

Если Вам не нравится ТЧ, жалобы принимаются [тут](#)

Версия от 30.03.2023

Всем по котика мяу



# Содержание:

## Лекция 1 (12.01.23)

### 1.0. Введение

### 1.1. Алгоритм Евклида

## Лекция 2 (19.01.23)

### 2.0. Введение

### 2.1. Основная теорема арифметики

### 2.2. Цепные дроби

## Лекция 3 (26.01.23)

### 3.0. Введение

### 3.1. $K$ -я подходящая дробь

## Лекция 4 (02.02.23)

### 4.0. Введение

### 4.1. Сравнения и вычеты

## Лекция 5 (03.02.23)

### 5.0. Введение

### 5.1. Арифметические операции

### 5.2. Много теорем

## Лекция 6 (16.02.23)

### 6.0. Введение

### 6.1. Группы, кольца, поля

## Лекция 7 (02.03.23)

### 7.0. Введение

## Лекция 8 (09.03.23)

### 8.0. Введение

### 8.1. Алгоритм RSA

## Лекция 9 (16.03.23)

### 9.0. Протокол Диффи-Хеллмана построения разделенного ключа

### 9.1. Алгоритм шифрования Эль-Гамала

### 9.2. Квадратичные вычеты

## Лекция 10 (23.03.23)

### 10.0. Введение

### 10.1. Неэлементарные свойства символа Лежандра

Разбор модельного варианта КР

Разбор модельного варианта Экз

# Лекция 1

## 1.0. Введение

$\mathbb{N}$  – натуральные числа

$\mathbb{Z}$  – целые числа

$\mathbb{Q}$  – рациональные числа

$\mathbb{R}$  – вещественные числа

$\mathbb{C}$  – комплексные числа

$\mathbb{A}$  – алгебраические числа (не будут затронуты)

**Обозначение.**  $a \mid b$  (реже  $b \dot{:} a$ )  $\iff \exists c \in \mathbb{Z} : b = ac$  ( $a$  делит  $b$ )

**Свойства:**

- Рефлексивность:  $a \mid a$  ( $a \neq 0$ )
- Транзитивность:  $a \mid b, b \mid c \implies a \mid c$
- $a \mid b \implies \forall c \in \mathbb{Z} \ a \mid bc$
- $a \mid b, a \mid c \implies a \mid b \pm c$

**Теорема 1** (деление с остатком). Пусть  $a \in \mathbb{Z}, b \in \mathbb{N}$ . Тогда  $\exists! q, r \in \mathbb{Z} : a = qb + r, 0 \leq r < b$

**Доказательство.** Возьмем  $n \in \mathbb{Z}, nb \leq a < (n+1)b$ . Положим  $q = n, r = a - nb$ , тогда  $0 \leq r < b$ . Теперь докажем единственность:  $a = q_1b + r_1, a = q_2b + r_2$ . Тогда  $r_1 - r_2 = (q_2 - q_1)b$ . Но  $|r_1 - r_2| < b \implies r_1 - r_2 = 0 \implies q_2 - q_1 = 0$

■

**Деление с остатком:**

1. Однозначное разложение на простые множители (*основная теорема арифметики*)
2. Цепные дроби
3. Вычеты (арифметика остатков)

## 1.1. Алгоритм Евклида

Пусть  $a, b \in \mathbb{Z}, |a| + |b| \neq 0$

Тогда  $(a, b) = \text{НОД}(a, b)$  – наибольший общий делитель.

**Определение.**  $a$  и  $b$  взаимно просты, если  $(a, b) = 1$

**Предложение.** Пусть  $a = qb + r$ . Тогда  $(a, b) = (b, r)$

**Доказательство.**

$$\begin{cases} d \mid a, b \implies d \mid r \\ d \mid b, r \implies d \mid a \end{cases}$$

множество всех общих делителей  $a$  и  $b$  совпадает с  $b$  и  $r$ , значит  $(a, b) = (b, r)$

■

**Алгоритм Евклида.**  $a \in \mathbb{Z}, b \in \mathbb{N}$

$$a = a_0b + r_0 \quad (0 \leq r_0 < b)$$

$$b = a_1r_0 + r_1 \quad (0 \leq r_1 < r_0)$$

$$r_0 = a_2r_1 + r_2 \quad (0 \leq r_2 < r_1)$$

...

$$r_{n-3} = a_{n-1}r_{n-2} + r_{n-1} \quad (0 \leq r_{n-2} < r_{n-1})$$

$$r_{n-2} = a_nr_{n-1} + r_n \quad (r_n = 0), \text{ то есть } r_{n-1} \mid r_{n-2}$$

$$(a, b) \rightarrow (b, r_0) \rightarrow (r_0, r_1) \rightarrow \dots \rightarrow (r_{n-3}, r_{n-2}) \rightarrow (r_{n-2}, r_{n-1}) = r_{n-1}$$

**Теорема 2** (расширенный алгоритм Евклида).

$$\forall a, b \in \mathbb{Z} \quad (|a| + |b| \neq 0) \quad \exists \lambda, \mu \in \mathbb{Z} : (a, b) = \lambda a + \mu b$$

**Доказательство.**  $\forall k \quad r_k = r_{k-2} - a_k r_{k-1}$

$$r_{n-1} = r_{n-3} - a_{n-1}r_{n-2} = \dots = \lambda_k r_k + \mu_k r_{k+1} = \dots = \lambda a + \mu b$$

■

# Лекция 2

## 2.0. Введение

**Лемма (важная).** Пусть  $a, b, c \in \mathbb{Z}$ . Тогда:

$$\begin{cases} a \mid bc \\ (a, b) = 1 \end{cases} \implies a \mid c$$

**Доказательство.**  $\exists \lambda, \mu :$

$$\lambda a + \mu b = 1$$

$$\underbrace{\lambda ac}_{a \mid ac} + \underbrace{\mu bc}_{a \mid bc} = \underbrace{c}_{a \mid c}$$

Левое слагаемое делится на  $a$ , потому что есть множитель  $a$ . Правое слагаемое делится на  $a$  по условию. Тогда и сумма делится на  $a$ . ■

## 2.1. Основная теорема арифметики

**Теорема.** Пусть  $n \in \mathbb{N}, n > 1$ . Тогда  $n$  раскладывается в произведение простых единственным образом с точностью до перестановки множителей.

**Доказательство.** Если  $n$  не имеет *нетривиального разложения*<sup>1</sup>, то оно простое. Если  $n = mk$ , то  $m, k < n$ . Дальше показывается по индукции, что число можно разложить на такие числа, которые не имеют нетривиального разложения (простые). Теперь докажем единственность. Пусть  $n = p_1 \cdot p_2 \cdot \dots \cdot p_a = q_1 \cdot q_2 \cdot \dots \cdot q_b$ . Сократим все одинаковые множители из первого и второго разложения:  $\forall i, j \ p_i \neq q_j$ . Тогда  $(p_1, q_j) = 1$ . По [важной лемме](#):

$$p_1 \mid q_2 \cdot q_3 \cdot \dots \cdot q_b$$

$$p_1 \mid q_3 \cdot \dots \cdot q_b$$

...

$$p_1 \mid q_b$$

$(p_1, q_b) = 1$ , но  $p_1 \neq 1$  – противоречие. ■

Пусть  $n \in \mathbb{N}, n > 1$ . Тогда по [основной теореме арифметики](#):  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ ,  $p_i \neq p_j \ \forall i \neq j$ , где  $p_i$  – простое. Это называется *каноническим разложением  $n$  на простые*.

**Обозначение.**  $\nu_p(n) = \max\{d \in \mathbb{N} \cup \{0\} : p^d \mid n\}$  – степень вхождения  $p$  в  $n$ .

---

<sup>1</sup>Разложение  $n = mk$  называется нетривиальным, если  $m, k < n$  и  $m, k \in \mathbb{N}$

С такими обозначениями разложение на простые множители можно записать так:  
 $n = \prod_{p|n} p^{\nu_p(n)} = \prod_p p^{\nu_p(n)}$  – с какого-то момента  $\nu_p(n)$  будет 0.

## 2.2. Цепные дроби

Вспомним алгоритм Евклида и разложим  $\mathbb{Q}$  в цепную дробь:

$$\left. \begin{array}{l} a = a_0 b + r_0 \\ b = a_1 r_0 + r_1 \\ \dots \\ r_{n-2} = a_n r_{n-1} \end{array} \right| \begin{array}{l} \frac{a}{b} = a_0 + \frac{r_0}{b} = \\ a_0 + \frac{1}{\frac{b}{r_0}} = a_0 + \frac{1}{a_1 + \frac{r_1}{r_0}} = \\ \dots \\ a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n}}} \end{array}$$

Также есть другая, более короткая запись цепной дроби:  $[a_0; a_1, \dots, a_n]$ , где  $a_0 \in \mathbb{Z}$ ,  $a_1, a_2, \dots, a_n \in \mathbb{N}$ ,  $a_n \neq 1$  (последнее видно по алгоритму на предпоследнем шаге: так как  $r_{n-1} < r_{n-2}$ , то  $a_n = \frac{r_{n-2}}{r_{n-1}} \neq 1$ ).

**Обозначение.**  $[\alpha]$  – целая часть  $\alpha$ ,  $\{\alpha\} = \alpha - [\alpha]$  – дробная доля (часть)  $\alpha$

Пусть  $\alpha \in \mathbb{R}$ . Положим  $\alpha_0 = \alpha$ . Рекуррента:  $\alpha_{k+1} = \frac{1}{\{\alpha_k\}}$ ,  $a_k = [\alpha_k]$ ,  $k \in \mathbb{N} \cup \{0\}$

$$\forall n \in \mathbb{N} \cup \{0\} \text{ верно } \alpha = [a_0; a_1, \dots, a_{n-1}, \alpha_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_{n-1} + \frac{1}{\alpha_n}}}}$$

Если у цепной дроби есть период, то над каждой  $a_i$  (которая в периоде) рисуется черта. Например:  $\sqrt{15} = [3; 1, 6, 1, 6, \dots] = [3; \overline{1, 6}]$

**Определение.** Пусть  $\alpha \sim [a_0; a_1, a_2, \dots, a_k, \dots]$ . Тогда для  $k = 0, 1, 2, \dots$  дроби  $\frac{p_k}{q_k} = [a_0; a_1, \dots, a_k]$  называются *подходящими дробями* числа  $\alpha$ .

**Теорема.**  $\forall k \in \mathbb{N} \cup \{0\}$  верно следующее:  $\left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k q_{k+1}} \leq \frac{1}{q_k^2}$

Рекуррентные соотношения:

$$p_k = a_k p_{k-1} + p_{k-2}$$

$$q_k = a_k q_{k-1} + q_{k-2}$$

Все это будет доказано на следующей лекции.

# Лекция 3

## 3.0. Введение

Давайте разложим  $5 + \frac{1}{3}$  в цепную дробь следующим образом:  $5 + \frac{1}{2 + \frac{1}{1}}$ . Запретим такие  $\frac{1}{1}$ , потому что можно отщепить 1 из числителя и получить исходное число разложение:  $5 + \frac{1}{2 + 1} = 5 + \frac{1}{3}$ .

## 3.1. $K$ -я подходящая дробь

Вспомним прошлую лекцию и дополним определение. Дробь вида  $\frac{p_k}{q_k} = [a_0; a_1, \dots, a_k]$ ,  $p_k, q_k \in \mathbb{Z}, q_k > 0, (p_k, q_k) = 1$  называется  $k$ -й *подходящей дробью*. Докажем некоторые факты, которые остались недоказанными в прошлый раз.

**Теорема** (о рекуррентных соотношениях для числителей и знаменателей подходящих дробей). Пусть заданы последовательности  $\alpha_k$  (хвосты),  $a_k$  (неполные частные). Тогда последовательности  $p$  и  $q$  заданы следующей рекуррентной формулой:

$$p_k = a_k p_{k-1} + p_{k-2}$$

$$q_k = a_k q_{k-1} + q_{k-2}$$

Для удобства можно положить:

$$\begin{pmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Теперь последовательности  $p$  и  $q$  определены  $\forall k \geq 0$

**Теорема** (о континуантах). Пусть  $x_0, x_1, \dots, x_k$  — независимые переменные. Положим:

$$\begin{pmatrix} P_{-1} & P_{-2} \\ Q_{-1} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

А также определим последовательности многочленов ( $\forall k \geq 0$ ):

$$P_k(x_0, \dots, x_k) = x_k P_{k-1}(x_0, \dots, x_{k-1}) + P_{k-2}(x_0, \dots, x_{k-2})$$

$$Q_k(x_0, \dots, x_k) = x_k Q_{k-1}(x_0, \dots, x_{k-1}) + Q_{k-2}(x_0, \dots, x_{k-2})$$

**Обозначение.** Сокращенная запись  $P_k$  предполагает  $P_k(x_0, \dots, x_k)$  (аналогично и для  $Q_k$ ).

**Утверждения:**

1.  $\frac{P_k}{Q_k} = [x_0, \dots, x_k]$
2.  $P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}$
3.  $P_k Q_{k-2} - P_{k-2} Q_k = (-1)^k \cdot x_k$

**Доказательство.**

1. Докажем по индукции по  $k$ :

**База:**  $k = 0$  :

$$P_0(x_0) = x_0 P_{-1} + P_{-2} = x_0$$

$$Q_0(x_0) = x_0 Q_{-1} + Q_{-2} = 1$$

$$\text{откуда } \frac{P_0(x_0)}{Q_0(x_0)} = x_0 = [x_0] \text{ (цепная дробь)} - \text{верно}$$

**Переход:** пусть верно  $\forall k < n$ , докажем для  $k = n$ :

$$\begin{aligned} [x_0; \dots, x_{n-2}, x_{n-1}, x_n] &= [x_0; \dots, x_{n-2}, x_{n-1} + \frac{1}{x_n}]^2 = \frac{P_{n-1}(x_0, \dots, x_{n-2}, x_{n-1} + \frac{1}{x_n})}{Q_{n-1}(x_0, \dots, x_{n-2}, x_{n-1} + \frac{1}{x_n})} = \\ &= \frac{(x_{n-1} + \frac{1}{x_n})P_{n-2}(x_0, \dots, x_{n-2}) + P_{n-3}(x_0, \dots, x_{n-3})}{(x_{n-1} + \frac{1}{x_n})Q_{n-2}(x_0, \dots, x_{n-2}) + Q_{n-3}(x_0, \dots, x_{n-3})} = \frac{(x_{n-1} + \frac{1}{x_n})P_{n-2} + P_{n-3}}{(x_{n-1} + \frac{1}{x_n})Q_{n-2} + Q_{n-3}} = \\ &= \frac{x_n \cdot (x_{n-1} + \frac{1}{x_n})P_{n-2} + P_{n-3}}{x_n \cdot (x_{n-1} + \frac{1}{x_n})Q_{n-2} + Q_{n-3}} = \frac{x_n(x_{n-1}P_{n-2} + P_{n-3}) + P_{n-2}}{x_n(x_{n-1}Q_{n-2} + Q_{n-3}) + Q_{n-2}} = \frac{x_n P_{n-1} + P_{n-2}}{x_n Q_{n-1} + Q_{n-2}} = \\ &= \frac{P_n}{Q_n} = \frac{P_n(x_0, x_1, \dots, x_n)}{Q_n(x_0, x_1, \dots, x_n)} = [x_0; x_1, \dots, x_n] - \text{верно} \end{aligned}$$

2. Докажем по индукции по  $k$ :

**База:**  $k = -1$  :  $P_{-1}Q_{-2} - P_{-2}Q_{-1} = 1 \cdot 1 - 0 \cdot 0 = 1 = (-1)^{-1-1} = (-1)^{-2}$  – верно

**Переход:** пусть верно для  $\forall k < n$ , докажем для  $k = n$ :

$$\begin{aligned} P_n Q_{n-1} - P_{n-1} Q_n &= (x_n P_{n-1} + P_{n-2})Q_{n-1} - P_{n-1}(x_n Q_{n-1} + Q_{n-2}) = x_n P_{n-1} Q_{n-1} + \\ &+ P_{n-2} Q_{n-1} - x_n P_{n-1} Q_{n-1} - P_{n-1} Q_{n-2} = P_{n-2} Q_{n-1} - P_{n-1} Q_{n-2} = -(P_{n-1} Q_{n-2} - \\ &- P_{n-2} Q_{n-1}) = -(-1)^{n-2} = (-1)^{n-1} - \text{верно} \end{aligned}$$

3. Возьмем определитель:

$$\begin{aligned} \begin{vmatrix} P_k & P_{k-2} \\ Q_k & Q_{k-2} \end{vmatrix} &= \begin{vmatrix} P_k - P_{k-2} & P_{k-2} \\ Q_k - Q_{k-2} & Q_{k-2} \end{vmatrix} = \begin{vmatrix} x_k P_{k-1} & P_{k-2} \\ x_k Q_{k-1} & Q_{k-2} \end{vmatrix} = x_k \begin{vmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{vmatrix} = \\ &= x_k (P_{k-1} Q_{k-2} - P_{k-2} Q_{k-1}) = (-1)^{k-2} \cdot x_k = (-1)^k \cdot x_k \end{aligned}$$

■

**Доказательство** теоремы (о рекуррентных соотношениях для числителей и знаменателей подходящих дробей). Положим  $x_0 = a_0, \dots, x_k = a_k$ :

---

<sup>2</sup>Ключевой ход:  $x_{n-1} + \frac{1}{x_n} = [x_{n-1}, x_n] = [x_{n-1} + \frac{1}{x_n}]$  – по алгоритму построения цепной дроби



$$\frac{P_k(a_0, \dots, a_k)}{Q_k(a_0, \dots, a_k)} = [a_0; a_1, \dots, a_k]$$

Заметим, что:

- $P_k(a_0, \dots, a_k), Q_k(a_0, \dots, a_k) \in \mathbb{Z}$
- $Q_k(a_0, \dots, a_k) \in \mathbb{N}$
- $(P_k(a_0, \dots, a_k), Q_k(a_0, \dots, a_k)) = 1$  — следствие пункта 2 из теоремы о континуантах.

Стало быть  $p_k = P_k(a_0, \dots, a_k)$ ,  $q_k = Q_k(a_0, \dots, a_k)$

То есть  $p_k = a_k p_{k-1} + p_{k-2}$ ,  $q_k = a_k q_{k-1} + q_{k-2}$ , так как  $P_k$  и  $Q_k$  удовлетворяли этому. ■

# Лекция 4

## 4.0. Введение

Вспомним 3 утверждения с прошлой лекции:

- $\frac{P_k}{Q_k} = [x_0, \dots, x_k]$
- $P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}$
- $P_k Q_{k-2} - P_{k-2} Q_k = (-1)^k \cdot x_k$

**Следствие** из [теоремы о континуантах](#).

1. Справедливы  $p_k = a_k p_{k-1} + p_{k-2}$ ,  $q_k = a_k q_{k-1} + q_{k-2}$
2.  $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$
3.  $p_k q_{k-2} - p_{k-2} q_k = (-1)^k \cdot a_k$

**Доказательство.** 1 доказывали на прошлой лекции, 2 и 3 мгновенно получаются из утверждений, которые тоже были доказаны на прошлой лекции

■

**Предложение.**

1.  $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \dots < \frac{p_{2k}}{q_{2k}} < \dots \leq \alpha \leq \dots < \frac{p_{2k+1}}{q_{2k+1}} < \dots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$
2.  $\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{p_k q_{k-1} - p_{k-1} q_k}{q_k q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$
3.  $\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}} = \frac{(-1)^k \cdot a_k}{q_k q_{k-2}}$
4.  $q_k \geq 2q_{k-2} \ (\forall k \geq 1)$
5.  $\left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k q_{k+1}} \leq \frac{1}{q_k^2}$
6.  $\left| \alpha - \frac{p_k}{q_k} \right| \geq \frac{a_{k+2}}{q_k q_{k+2}}$

**Доказательство.**

1.  $\forall i = 2n, j = 2m + 1 \quad \frac{p_i}{q_i} < \frac{p_j}{q_j}$  следует из [пункта 2 предложения](#).  $\forall i = 2n \quad \frac{p_i}{q_i} < \frac{p_{i+2}}{q_{i+2}}$  по [пункту 3 предложения](#) верно (знаменатель всегда положительный, а числитель положительный так как  $(-1)^k$  положительный при четном  $k$ ). Аналогично показывается для нечетных индексов.

Далее  $\alpha = [a_0; a_1, \dots, a_k, \alpha_{k+1}]$ . Рассмотрим последние 3 неполных частных:  
 $a_{k-1} + \frac{1}{a_k + \frac{1}{\alpha_{k+1}}}$ . Если обрубим  $\alpha_{k+1}$  (получим  $[a_0; a_1, \dots, a_k]$ ), то знаменатель  
 $a_k + \frac{1}{\underbrace{\alpha_{k+1}}_{>0}}$  уменьшится, значит дробь  $\frac{1}{a_k + \frac{1}{\alpha_{k+1}}}$  увеличится. Следующий знаменатель увеличится, а дробь уменьшится и так далее. Из этого следует:

- $\alpha \geq \frac{p_{2k}}{q_{2k}}$
- $\alpha \leq \frac{p_{2k+1}}{q_{2k+1}}$

Выходит, что все четные не больше  $\alpha$ , а нечетные – не меньше.

2. Даром из [следствия 2 из теоремы о континуантах](#).

3. Даром из [следствия 3 из теоремы о континуантах](#).

$$4. q_k = \underbrace{a_k}_{\geq 1} q_{k-1} + q_{k-2} \geq q_{k-1} + q_{k-2} \geq 2q_{k-2}$$

$$5. \frac{p_k}{q_k} \leq \alpha \leq \frac{p_{k+1}}{q_{k+1}}, \quad \begin{array}{l} \text{если } k - \text{четное} \\ \text{если } k - \text{нечетное} \end{array}. \text{ Вычитаем } \frac{p_k}{q_k} \text{ и получаем что надо.}$$

$$6. \alpha \geq \frac{p_{k+2}}{q_{k+2}} > \frac{p_k}{q_k}, \quad \begin{array}{l} \text{если } k - \text{четное} \\ \text{если } k - \text{нечетное} \end{array}. \text{ Вычитаем } \frac{p_k}{q_k} \text{ и получаем что надо.}$$

■

Еще одно **следствие** из [теоремы о континуантах](#). Пусть  $\alpha = [a_0; a_1, \dots, a_{k-1}, \alpha_k]$ .

$$\text{Тогда } \alpha = \frac{P_k(a_0, \dots, a_{k-1}, \alpha_k)}{Q_k(a_0, \dots, a_{k-1}, \alpha_k)} = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}$$

**Пример.**  $\varphi = \frac{1 + \sqrt{5}}{2}$

$$\varphi^2 = \varphi + 1$$

$$\varphi = 1 + \frac{1}{\varphi}$$

$\varphi = [1; \bar{1}]$  – самая простая цепная дробь для числа из  $\mathbb{R}$

Пусть  $F_k$  –  $k$ -е число Фибоначчи. Положим  $p_k = F_k$ ,  $q_k = F_{k-1}$ . Тогда  $\lim_{k \rightarrow \infty} \frac{p_k}{q_k} = \varphi$

**Приложения к линейным диофантовым уравнениям.**

$a, b \in \mathbb{N}$ ,  $(a, b) = 1$ . Как решить уравнение  $ax + by = c$ ?

Пусть  $\frac{a}{b} = [a_0; a_1, \dots, a_{k-1}, a_k]$ . Тогда  $\frac{p_k}{q_k} = \frac{a}{b}$ ,  $\frac{p_{k-1}}{q_{k-1}} = [a_0; a_1, \dots, a_{k-1}]$

Следовательно  $aq_{k-1} + b(-p_{k-1}) = (-1)^{k-1}$

Значит  $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = (-1)^{k-1} \cdot c \cdot \begin{pmatrix} q_{k-1} \\ -p_{k-1} \end{pmatrix}$  – частичное решение уравнения  $ax + by = c$

## 4.1. Сравнения и вычеты

**Определение.** Пусть  $m \in \mathbb{N}, m \geq 2$  – модуль. Есть  $a, b \in \mathbb{Z}$ . Тогда  $a$  и  $b$  сравнимы по модулю  $m$  если  $m \mid a - b$

**Обозначение.**  $a \equiv b \pmod{m}$ . Реже пишут как  $a \equiv_m b$

**Свойства:**

1. Отношение сравнения является отношением эквивалентности.

2. Пусть выполняются  $\begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases}$ . Тогда верно и  $\begin{cases} a + c \equiv b + d \pmod{m} \\ a - c \equiv b - d \pmod{m} \\ ac \equiv bd \pmod{m} \end{cases}$

3.  $a \equiv b \pmod{m}, \forall c \in \mathbb{N} \implies ac \equiv bc \pmod{mc}$

4.  $a \equiv b \pmod{m}, \forall c \in \mathbb{Z} (c, m) = 1 \iff ac \equiv bc \pmod{m}$

5. Пусть  $f(x) \in \mathbb{Z}[x]$ <sup>3</sup>,  $a \equiv b \pmod{m}$ . Тогда  $f(a) \equiv f(b) \pmod{m}$

**Доказательство.**

1. Чтобы отношение сравнения было отношением эквивалентности, должны выполняться 3 условия. Проверим каждый:

- *Рефлексивность:*  $a \equiv a \pmod{m}$
- *Симметричность:*  $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$
- *Транзитивность:*  $a \equiv b \pmod{m}, b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$

2.  $\begin{cases} m \mid a - b \\ m \mid c - d \end{cases} \implies m \mid (a - b) + (c - d) \implies m \mid (a + c) - (b + d) \implies a + c \equiv b + d \pmod{m}$ . Аналогично для вычитания.

Для умножения:

$$\begin{aligned} \begin{cases} m \mid a - b \\ m \mid c - d \end{cases} &\implies \begin{cases} m \mid c(a - b) \\ m \mid b(c - d) \end{cases} \implies m \mid c(a - b) + b(c - d) \implies m \mid ac - bc + \\ &+ bc - bd \implies m \mid ac - bd \implies ac \equiv bd \pmod{m} \end{aligned}$$

---

<sup>3</sup> $\mathbb{Z}[x]$  – многочлен с целыми коэффициентами от  $x$

3.  $m \mid a - b \iff mc \mid (a - b)c$

4. С одной стороны:  $m \mid a - b \implies m \mid c(a - b)$

С другой стороны:  $m \mid c(a - b) \implies m \mid a - b$  (по [важной лемме](#), так как  $(m, c) = 1$ )

5. Не доказывалось на лекции.



# Лекция 5

## 5.0. Введение

Вспомним что такое сравнимость по модулю:  $a \equiv b \pmod{m} \iff m \mid a - b$

**Определение.** Множество  $a + m\mathbb{Z} = \{a + mt \mid t \in \mathbb{Z}\}$  называется *классом вычетов* числа  $a$  по модулю  $m$ . Еще обозначают как  $\bar{a} = a + m\mathbb{Z}$

**Обозначение.**  $\mathbb{Z}_m = \{a + m\mathbb{Z} \mid a \in \{0, 1, \dots, m-1\}\}$  – множество всех классов вычетов по модулю  $m$ . Также обозначают  $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$

## 5.1. Арифметические операции

Для  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  полагаем:

- $\bar{a} + \bar{b} = \overline{a + b}$
- $\bar{a} \cdot \bar{b} = \overline{ab}$

**Предложение.** Операции корректно определены, то есть  $\forall a_1, a_2, b_1, b_2$  таких, что  $a_1 \equiv a_2 \pmod{m}$ ,  $b_1 \equiv b_2 \pmod{m}$  верно следующее:

$$\begin{cases} a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 \equiv a_2 b_2 \pmod{m} \end{cases}$$

Теперь (при наличии  $m$ )  $a \equiv b \pmod{m} \iff \bar{a} = \bar{b}$

**Определение.** Пусть  $m \in \mathbb{N}$ ,  $m \geq 2$ . Набор из  $m$  чисел  $a_1, a_2, \dots, a_m$  называется *полной системой вычетов*, если  $a_1, a_2, \dots, a_m$  – представители всех различных  $m$  классов вычетов.

**Замечание.** Если  $a \equiv b \pmod{m}$ , то  $(a, m) = (b, m)$ . Поэтому можно говорить о свойстве  $\bar{a}$  быть взаимно простым с  $m$ .

**Определение.** Пусть  $m \in \mathbb{N}$ ,  $m \geq 2$ . Набор  $a_1, a_2, \dots, a_k$  называется *приведенной системой вычетов*, если  $a_1, a_2, \dots, a_k$  – представители всех классов вычетов, взаимно простых с  $m$ .

**Определение.** *Функция Эйлера:*  $\varphi(m) = |\{a \in \mathbb{Z} \mid 1 \leq a < m, (a, m) = 1\}|$

**Обозначение.**  $\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$

## 5.2. Много теорем

**Теорема** (о полной и приведенной системах вычетов). Пусть:

$$\begin{cases} m \in \mathbb{N}, m \geq 2 \\ a \in \mathbb{Z}, (a, m) = 1 \end{cases}$$

1. Если  $b_1, \dots, b_m$  – полная система вычетов по модулю  $m$ , а также  $(a, m) = 1$  и  $c \in \mathbb{Z}$ . Тогда  $ab_1 + c, \dots, ab_m + c$  – тоже полная система вычетов.
2. Если  $b_1, \dots, b_k$  – приведенная система вычетов по модулю  $m$ , а также  $(a, m) = 1$  и  $k = \varphi(m)$ . Тогда  $ab_1, \dots, ab_k$  – тоже приведенная система вычетов.

**Доказательство.**  $\forall i \neq j \ b_i \not\equiv b_j \pmod{m}$ . Следовательно,  $ab_i \not\equiv ab_j \pmod{m}$  (так как если  $ab_i \equiv ab_j \pmod{m} \iff b_i \equiv b_j \pmod{m}$  по 4 свойству сравнений и вычетов – противоречие).

Далее,  $\forall c \in \mathbb{Z}$  при  $ab_i \not\equiv ab_j \pmod{m}$  имеем также  $ab_i + c \not\equiv ab_j + c \pmod{m}$

1. Числа  $ab_1 + c, \dots, ab_m + c$  – представители  $m$  различных классов вычетов.
2. Числа  $ab_1, \dots, ab_k$  – представители  $k$  различных классов вычетов. При этом  $(ab_i, m) = (b_i, m) = 1$  (по важной лемме).

■

**Теорема** (Эйлера). Пусть:

$$\begin{cases} m \in \mathbb{N}, m \geq 2 \\ a \in \mathbb{Z}, (a, m) = 1 \end{cases}$$

Тогда  $a^{\varphi(m)} \equiv 1 \pmod{m}$

**Доказательство.** Пусть  $b_1, \dots, b_k$  – приведенная система вычетов, тогда  $ab_1, \dots, ab_k$  – тоже приведенная система вычетов (по теореме о приведенной системе вычетов). Это значит, что  $\forall i \in \{1, \dots, k\} \exists! j \in \{1, \dots, k\} : b_i \equiv ab_j \pmod{m}$ . Следовательно:

$$\begin{aligned} \prod_{i=1}^k b_i &\equiv \prod_{j=1}^k ab_j \pmod{m} \\ \prod_{i=1}^k b_i &\equiv a^k \prod_{j=1}^k b_j \pmod{m} \end{aligned}$$

.

Но  $\forall l \in \{1, \dots, k\} \ (b_l, m) = 1$ , поэтому можно сократить. Остается  $1 \equiv a^k \pmod{m}$ , где  $k = \varphi(m)$

■

**Следствие** (Малая теорема Ферма). Пусть  $p$  – простое,  $a \in \mathbb{Z}, p \nmid a$ . Тогда  $a^{p-1} \equiv 1 \pmod{p}$

**Доказательство.** При  $m = p$  – простом,  $\varphi(m) = p - 1$ . Далее просто применяем теорему Эйлера. ■

**Теорема (об обратимых вычетах по умножению).** Пусть  $m \in \mathbb{N}$ ,  $m \geq 2$ ,  $a \in \mathbb{Z}$ . Тогда сравнение  $ax \equiv 1 \pmod{m}$  имеет решение  $\iff (a, m) = 1$

**Примечание.** Такое  $a$  называется *обратимым* по модулю  $m$ , а найденный  $x$  – *обратным* к  $a$ .

**Доказательство.** Сравнение  $ax \equiv 1 \pmod{m}$  имеет решение  $\iff \exists b \in \mathbb{Z} : ab \equiv 1 \pmod{m} \iff \exists c \in \mathbb{Z} : ab - 1 = mc \iff ab - mc = 1$ . Получили *линейное диофантово уравнение*, так как  $(a, m) = 1$  ■

**Следствие.** Пусть  $\bar{a} \in \mathbb{Z}_m$  (кольцо). Тогда  $\bar{a}$  обратим по умножению (то есть  $\exists \bar{b} : \bar{a}\bar{b} = \bar{1}$ )  $\iff \bar{a} \in \mathbb{Z}_m^*$

**Замечание.** Если  $\bar{a} \in \mathbb{Z}_m^*$ , то обратный по умножению элемент определен однозначно, то есть  $\exists! \bar{b} : \bar{a}\bar{b} = \bar{1}$

**Доказательство.** Пусть  $ab_1 \equiv 1 \pmod{m}$  и  $ab_2 \equiv 1 \pmod{m}$ . Тогда  $a(b_1 - b_2) \equiv 0 \pmod{m}$ . Но  $(a, m) = 1$ , значит  $b_1 - b_2 \equiv 0 \pmod{m}$ , то есть  $b_1 \equiv b_2 \pmod{m}$  ■

**Теорема (Вильсона).** Пусть  $p$  – простое. Тогда  $(p - 1)! \equiv -1 \pmod{p}$

**Доказательство.**  $\forall a \in \{1, 2, \dots, p - 1\} \exists! b \in \{1, 2, \dots, p - 1\} : ab \equiv 1 \pmod{p}$

Но в некоторых случаях может случиться  $b = a$ . Тогда:

$$a^2 \equiv 1 \pmod{p} \iff p \mid a^2 - 1 = (a - 1)(a + 1) \iff \begin{cases} p \mid a - 1 \\ p \mid a + 1 \end{cases} \iff a \equiv \pm 1 \pmod{p}$$

Получается, что  $2, 3, \dots, p - 2$  разбиваются на пары так, что каждая в произведении дает 1.

Следовательно,  $(p - 1)! = 1 \cdot \underbrace{1 \cdot \dots \cdot 1}_{\text{пары}} \cdot (p - 1) = (p - 1) \iff (p - 1)! \equiv -1 \pmod{p}$  ■



# Лекция 6

## 6.0. Введение

Вспомнили, что  $\mathbb{Z}_m = \{a + m\mathbb{Z} \mid a \in \{0, 1, \dots, m-1\}\}$  называется классом вычетов числа  $a$  по модулю  $m$ . А также [все другие теоремы](#).

**Теорема** (*китайская теорема об остатках*). Пусть есть  $m_1, \dots, m_k \in \mathbb{N}$ ,  $m_1, \dots, m_k \geq 2$ ,  $\forall i \neq j (m_i, m_j) = 1$ , а также  $a_1, \dots, a_k \in \mathbb{Z}$ . Тогда система:

$$(*) \begin{cases} x \equiv a_1 \pmod{m_1} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

имеет решение и, более того,  $(*) \iff x \equiv x_0 \pmod{M}$ , где

$$M = \prod_{i=1}^k m_i$$
$$M_i = \frac{M}{m_i}$$
$$x_0 = \sum_{i=1}^k b_i M_i$$

$$b_i \in \mathbb{Z} : b_i M_i \equiv a_i \pmod{m_i}$$

**Доказательство.** Поскольку  $\forall i \neq j (m_i, m_j) = 1$  имеем также  $(m_i, M_i) = 1$ . Следовательно,  $\forall i$  коэффициент  $b_i$  корректно определен (то есть существует) по  $\pmod{m_i}$ .

**Наблюдения:**

1.  $x_0$  удовлетворяет  $(*)$ :  $x_0 = \sum_{i=1}^k b_i M_i \equiv_{m_j} b_j M_j \overset{4}{\equiv} a_j$  — верно для всех  $j$ .
2. Если  $x_1 \equiv x_0 \pmod{M}$ , то  $x_1$  также удовлетворяет  $(*)$ :  $\forall j \ x_1 \equiv_{m_j} x_0 \equiv_{m_j} a_j$
3. Если  $x_1$  удовлетворяет  $(*)$ , то  $x_1 \equiv x_0 \pmod{M}$ .  $\forall j$ :

$$\begin{cases} x_1 \equiv a_j \pmod{m_j} \\ x_0 \equiv a_j \pmod{m_j} \end{cases} \implies x_1 - x_0 \equiv 0 \pmod{m_j}$$

Но  $m_1, \dots, m_k$  попарно взаимно просты. Следовательно  $x_1 - x_0 \equiv 0 \pmod{M}$

■

---

<sup>4</sup>Ключевой переход:  $\sum_{i=1}^k b_i M_i \equiv_{m_j} b_j M_j \pmod{m_j}$ . Так как  $\forall i \neq j (M_i, m_j) = m_j$ , то  $M_i \equiv 0 \pmod{m_j} \implies b_i M_i \equiv 0 \pmod{m_j}$

## 6.1. Группы, кольца, поля

**Определение.** Пусть  $G$  – множество, замкнутое относительно операции " $\circ$ " ( $\forall a, b \in G \exists! c \in G : a \circ b = c$ ).  $G$  называется группой (относительно операции " $\circ$ "), если:

1. Операция *ассоциативна*:  $\forall a, b, c \in G$  верно  $(a \circ b) \circ c = a \circ (b \circ c)$
2. Существует *нейтральный элемент*:  $\exists e \in G : \forall a \in G$  верно  $a \circ e = e \circ a = a$
3. Существует *обратный элемент*:  $\forall a \in G \exists b \in G : a \circ b = b \circ a = e$

**Определение.** Если  $\forall a, b \in G a \circ b = b \circ a$ , то  $G$  называется *коммутативной* (или *абелевой*) группой.

**Определение.** Пусть  $R$  – множество, замкнутое относительно операций " $+$ " и " $\cdot$ ". Тогда  $R$  называется кольцом, если:

1.  $(R, +)$  – абелева группа.
2. Умножение *дистрибутивно*:  $\forall a, b, c \in R$ :

$$\begin{cases} (a + b)c = ac + bc \\ c(a + b) = ca + bc \end{cases}$$

**Замечание.** Иногда требуют в определении кольца еще ассоциативность умножения.

**Определение.** Ассоциативное, коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим, называется *полем*.

**Определение.** Пусть  $(G_1, \circ), (G_2, *)$  – группы. Тогда  $G_1 \cong G_2$  (*изоморфны*), если  $\exists f : G_1 \rightarrow G_2$  такое, что:

1.  $f$  – биекция
2.  $\forall a, b \in G_1 f(a \circ b) = f(a) * f(b)$

**Пример.**  $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$ . Пусть отображение  $f : \mathbb{R} \xrightarrow{\exp} \mathbb{R}_{>0}$ , где:

- $a \in \mathbb{R} : f(a) = e^a$  – инъекция в одну сторону.
- $a \in \mathbb{R}_{>0} : f(a)^{-1} = \ln a$  – инъекция в другую сторону.
- $a, b \in \mathbb{R} : e^{a+b} = f(a+b) = f(a) \cdot f(b) = e^a \cdot e^b$

Инъекции в обе стороны говорят о том, что функция  $f$  является биекцией (по теореме Кантора-Бернштейна).

**Определение.** Пусть  $R_1, R_2$  – кольца. Тогда  $R_1 \cong R_2$ , если  $\exists f : R_1 \rightarrow R_2$  такое, что:

1.  $f$  – биекция
2.  $f(a + b) = f(a) + f(b)$
3.  $f(a \cdot b) = f(a) \cdot f(b)$

**Замечание.** Если  $R_1 \cong R_2$  и  $f$  реализует *изоморфизм*, то  $a \in R_1$  обратим  $\iff f(a) \in R_2$  обратим.

# Лекция 7

## 7.0. Введение

$\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$  – все обратимые. Если  $p$  – простое  $\implies \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

**Определение.** Пусть  $R_1$  и  $R_2$  – кольца. Тогда их *прямым (декартовым) произведением* называется множество  $R_1 \times R_2 = \{(a, b) \mid a \in R_1, b \in R_2\}$

Операции на  $R_1 \times R_2$ :

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

**Упражнение.**  $(a, b)$  обратима в  $R_1 \times R_2 \iff \begin{cases} a \text{ обратима в } R_1 \\ b \text{ обратима в } R_2 \end{cases}$

**Теорема (K.T.O.).** Пусть  $(m, n) = 1$ . Тогда  $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$

**Доказательство.** Рассмотрим отображение

$$f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

$$f : a + mn\mathbb{Z} \rightarrow (a + m\mathbb{Z}, a + n\mathbb{Z})$$

1. Покажем, что  $f$  – инъекция. Пусть  $\exists a \not\equiv b \pmod{mn} : f(a + mn\mathbb{Z}) = f(b + mn\mathbb{Z})$ :

$$\begin{cases} a + m\mathbb{Z} = b + m\mathbb{Z} \\ a + n\mathbb{Z} = b + n\mathbb{Z} \end{cases} \implies \begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$$

Но получаем противоречие:

$$\begin{cases} m \mid a - b \\ n \mid a - b \\ (m, n) = 1 \end{cases} \implies a \equiv b \pmod{mn}$$

2. Поскольку также  $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$ , то  $f$  – биекция.

3. Покажем, что  $f$  сохраняет операции:

$$f(a + b + mn\mathbb{Z}) = (a + b + m\mathbb{Z}, a + b + n\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z}) + (b + m\mathbb{Z}, b + n\mathbb{Z})$$

$$f(ab + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z}) \cdot (b + m\mathbb{Z}, b + n\mathbb{Z})$$

■

**Следствие.**  $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

**Доказательство.**

1.  $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$  – как кольца.
2.  $\mathbb{Z}_{mn}^* \cong (\mathbb{Z}_m \times \mathbb{Z}_n)^*$  – как группы.
3.  $(\mathbb{Z}_m \times \mathbb{Z}_n)^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$  – как группы.

■

**Следствие.** Если  $(m, n) = 1$ , то  $\varphi(mn) = \varphi(m)\varphi(n)$

**Доказательство.** По определению  $|\mathbb{Z}_m^*| = \varphi(m)$ ,  $|\mathbb{Z}_n^*| = \varphi(n)$  – сколько взаимно простых с  $m$  и  $n$  соответственно (и все они обратимы по [теореме об обратимых вычетах](#)). Так как  $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ , следовательно  $\varphi(mn) = \varphi(m)\varphi(n)$

■

**Замечание.** Пусть  $p$  – простое,  $k \in \mathbb{N}$ . Тогда  $\varphi(p^k) = p^k - p^{k-1}$

**Теорема.** Пусть  $n = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$ . Тогда  $\varphi(n) = \prod_{i=1}^s (p_i^{k_i} - p_i^{k_i-1}) = \prod_{i=1}^s p_i^{k_i} \left(1 - \frac{1}{p_i}\right) =$   
 $= n \prod_{i=1}^s \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

**Доказательство.** Очевидно (исходит из следствия и замечания).

■

**Теорема.** Пусть  $F$  – поле,  $f(x) \in F[x] \setminus \{0\}$ . Тогда  $f$  имеет не более  $\deg f$  корней в  $F$ .

**Теорема (Безу).** Пусть  $f(x) = q(x)(x - a) + r(x)$  – деление с остатком  $f(x)$  на  $x - a$  в  $F[x]$ . Тогда  $r(x) = f(a)$ .

**Следствие.** Если  $f(a) = 0$ , то  $x - a \mid f(x)$  в  $F[x]$ .

**Доказательство.** По индукции (по  $\deg f$ ):

**База:**  $\deg f = 1$  :

$$0 = f(x) = c(x - a) \iff x = \frac{a}{c}$$

**Переход:** Пусть  $a$  – корень  $f$ . Тогда  $f(a) = 0$ . По [теореме Безу](#)  $f(x) = q(x)(x - a)$ .

Ключевое наблюдение: если  $f(b) = 0$ , то либо  $q(b) = 0$ , либо  $b = a$  (так как в поле нет делителей 0).

$\deg g(x) = \deg f(x) - 1$ , по предположению индукции корней  $q(x)$  не больше  $\deg q$ .

■

# Лекция 8

## 8.0. Введение

**Следствие.** Пусть  $p$  – простое. Тогда  $\mathbb{Z}_p^*$  – циклическая группа, то есть  $\exists g \in \mathbb{Z} : Z_p^* = \{\bar{g}^0, \bar{g}^1, \bar{g}^2, \dots, \bar{g}^{p-2}\}$

**Определение.** Пусть  $m \in \mathbb{N}, m \geq 2$ , а также  $a \in \mathbb{Z}, (a, m) = 1$ . Показателем числа  $a$  по модулю  $m$  называется  $\text{ord}_m(a) = \min\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod{m}\}$

**Определение.** Пусть  $G$  – группа (по умножению),  $a \in G$ . Порядком элемента  $a$  называется  $\text{ord}(a) = \min\{k \in \mathbb{N} \mid a^k = 1\}$

**Утверждение.** Пусть  $a \in \mathbb{Z}, (a, m) = 1$ . Тогда  $\text{ord}_m(a) = \text{ord}(\bar{a})$

**Теорема (почти Лагранжа).** Пусть  $G = \mathbb{Z}_m^*, \bar{a} \in G$ . Тогда  $\text{ord}_m(a) \mid \varphi(m)$

**Доказательство.** Пусть  $\text{ord}_m(a) = d, |G| = n = \varphi(m)$ . Поделим с остатком  $n$  на  $d$ :

$$n = q \cdot d + r, \quad 0 \leq r < d$$

Тогда  $\bar{a}^r = \bar{a}^{n-qd} = \bar{a}^n \cdot (\bar{a}^d)^{-q} = \bar{1}$

Следовательно  $r = 0$ , то есть  $d \mid n = \varphi(m)$

■

**Определение.** Пусть  $g \in \mathbb{Z}, (g, m) = 1$ . Тогда  $g$  называется *первообразным корнем* (ПК) по  $(\text{mod } m)$ , если  $\text{ord}_m(g) = \varphi(m)$ . То есть если  $\bar{g}$  – образующая группы  $\mathbb{Z}_m^*$ .

**Теорема.**  $g$  – ПК  $(\text{mod } m) \iff \forall q \mid \varphi(m) \quad g^{\frac{\varphi(m)}{q}} \not\equiv 1 \pmod{m}$ , где  $q$  – простое.

**Доказательство.**

1.  $\implies$ :  $g$  – ПК  $(\text{mod } m) \implies \text{ord}_m(g) = \varphi(m) \implies \forall q \mid \varphi(m) \quad g^{\frac{\varphi(m)}{q}} \not\equiv 1 \pmod{m}$

2.  $\impliedby$ : Пусть  $\text{ord}_m(g) = d$ . Знаем, что  $d \mid \varphi(m)$ . Если  $d < \varphi(m)$ , то  $\exists q$  – простое:

- $q \mid \varphi(m)$ ,
- $d \mid \frac{\varphi(m)}{q}$

Следовательно, для такого  $q$ :

$$g^{\frac{\varphi(m)}{q}} \equiv (g^d)^{\frac{\varphi(m)}{qd}} \equiv 1 \pmod{m}$$

■

**Определение.** Пусть  $p$  – простое,  $g$  – ПК  $(\text{mod } p)$ ,  $a \equiv g^x \pmod{p}$ ,  $0 \leq x \leq p-2$ . Такой  $x$  называется *дискретным логарифмом* числа  $a$  по основанию  $g$  по  $(\text{mod } p)$ .

**Предложение.** Пусть  $m = pq$ ,  $p$  и  $q$  – различные нечетные простые. Тогда  $\forall a \in \mathbb{Z}$ ,  $(a, m) = 1$  :

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$$

**Доказательство.** Заметим, что  $\varphi(m) = (p-1)(q-1)$ , откуда:

$$\begin{cases} p-1 \mid \frac{\varphi(m)}{2} \\ q-1 \mid \frac{\varphi(m)}{2} \end{cases}$$

Далее по МТФ:

$$\begin{cases} a^{p-1} \equiv 1 \pmod{p} \\ a^{q-1} \equiv 1 \pmod{q} \end{cases} \implies a^{\frac{(p-1)(q-1)}{2}} \equiv 1 \pmod{\frac{p}{q}} \implies a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$$

■

## 8.1. Алгоритм RSA

Пусть  $m = pq$ ,  $p$  и  $q$  – большие различные простые. Тогда  $\varphi(m) = (p-1)(q-1)$ . Подберем  $e$  и  $d$  такие, что  $ed \equiv 1 \pmod{\varphi(m)}$ . Тогда:

- $e$  и  $m$  являются открытыми (их знают все)
- $d$  и  $\varphi(m)$  знает только создатель

Если отправитель хочет отправить сообщение  $N$ , то он отправляет  $N^e \pmod{m}$ . Получатель делает  $(N^e)^d \equiv N^{ed} \equiv N^{k\varphi(m)+1} \equiv (N^{\varphi(m)})^k \cdot N \equiv 1^k \cdot N \equiv N \pmod{m}$

Это шифрование хорошо тем, что модуль сложно факторизовать, потому что оно состоит из произведения двух больших простых чисел.

Примерно также работает Электронная Цифровая Подпись.

# Лекция 9

## 9.0. Протокол Диффи-Хеллмана построения разделенного ключа

Пусть  $p$  – простое,  $g$  – ПК  $(\text{mod } p)$  (известно всем).

А придумывает  $a \in \mathbb{Z}$  такое, что  $(a, p-1) = 1$  и передает Б  $g^a \pmod{p}$

Б придумывает  $b \in \mathbb{Z}$  такое, что  $(b, p-1) = 1$  и передает А  $g^b \pmod{p}$

Получаем  $s \equiv g^{ab} \pmod{p}$  – секрет, известный лишь А и Б.

## 9.1. Алгоритм шифрования Эль-Гамала

Пусть  $p$  – простое,  $g$  – ПК  $(\text{mod } p)$  (известен всем).

Б хочет передать  $N \in \mathbb{Z}, 1 \leq N < p$

1. А придумывает секретную экспоненту  $d \in \mathbb{N}, (d, p-1) = 1$  и вычисляет  $h \equiv g^d \pmod{p}$
2. А передает Б переменные  $p, g, h$
3. Б придумывает сессионный ключ  $k \in \mathbb{N}, (k, p-1) = 1$
4. Б вычисляет  $g^k \pmod{p}$ ,  $h^k \cdot N \pmod{p}$  и передает их А
5. А вычисляет  $(g^k)^{-d} \cdot h^k \cdot N \equiv_{\text{mod } p} g^{-kd} \cdot g^{kd} \cdot N \equiv_{\text{mod } p} N$

## 9.2. Квадратичные вычеты

**Определение.** Пусть  $p$  – нечетное простое,  $a \in \mathbb{Z}$ . Функция  $a$  по  $p$

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \equiv 0 \pmod{p} \\ 1, & \text{если } a \not\equiv 0 \pmod{p} \text{ и } x^2 \equiv a \pmod{p} \text{ разрешимо} \\ -1, & \text{если } x^2 \equiv a \pmod{p} \text{ не разрешимо} \end{cases}$$

называется *символом Лежандра*.

**Определение.** Если сравнение  $x^2 \equiv a \pmod{p}$  разрешимо, то  $a$  называется *квадратичным вычетом*. Иначе называется *квадратичным невычетом*.

**Предложение.** Пусть  $p$  – нечетное простое. Тогда по модулю  $p$  существует ровно  $\frac{p-1}{2}$  квадратичных вычетов.



**Доказательство.** Поймем когда  $a^2 \equiv b^2 \pmod{p}$

$$a^2 \equiv b^2 \pmod{p} \iff p \mid a^2 - b^2 \iff p \mid (a-b)(a+b) \iff \begin{cases} p \mid a-b \\ p \mid a+b \end{cases} \iff a \equiv \pm b \pmod{p}$$

Следовательно, квадратов среди вычетов  $1, 2, \dots, p-1$  будет ровно  $\frac{p-1}{2}$  ■

**Теорема (критерий Эйлера).** Пусть  $p$  – нечетное простое,  $a \in \mathbb{Z}$ ,  $p \nmid a$ . Тогда:

1.  $a$  – квадратичный вычет  $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$
2.  $a$  – квадратичный невычет  $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

**Доказательство.** Заметим, что  $\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

- $\implies$  Пусть  $a \equiv b^2 \pmod{p}$ . Тогда  $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$
- $\Leftarrow$  Рассмотрим  $f(x) = x^{\frac{p-1}{2}} - 1$ . Из первого утверждения следует, что все ненулевые квадратичные вычеты являются корнями  $f(x) \pmod{p}$

В силу предложения квадратичных вычетов ровно  $\frac{p-1}{2}$ . Следовательно, квадратичные невычеты не являются корнями  $f(x) \pmod{p}$ . То есть если  $a$  – квадратичный невычет, то  $a^{\frac{p-1}{2}} \not\equiv 1 \implies a^{\frac{p-1}{2}} \equiv -1$  ■

**Следствие.**  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

**Свойства символа Лежандра:**

1.  $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2.  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
3.  $\left(\frac{1}{p}\right) = 1$ ,  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
4.  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$
5. Пусть  $p, q$  – простые нечетные. Тогда:  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}$

# Лекция 10

## 10.0. Введение

Вспомним символ Лежандра. Пусть  $p$  – нечетное простое,  $a \in \mathbb{Z}$ :

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a \mid p \\ 1, & a - \text{квадратичный вычет} \\ -1, & a - \text{квадратичный невычет} \end{cases}$$

## 10.1. Неэлементарные свойства символа Лежандра

**Лемма (Гаусса).** Пусть  $p$  – нечетное простое,  $a \in \mathbb{Z}$ ,  $p \nmid a$ . Определим  $r_k, \varepsilon_k$  следующим образом: для  $k = 1, 2, \dots, \frac{p-1}{2}$  положим  $ak \equiv \varepsilon_k r_k \pmod{p}$ , где  $\varepsilon_k = \pm 1$ ,  $1 \leq r_k \leq \frac{p-1}{2}$

Тогда  $\left(\frac{a}{p}\right) = \prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k = (-1)^t$ , где  $t$  – количество отрицательных  $\varepsilon_k$

**Доказательство.** Перемножим  $ak$  по всем  $k = 1, 2, \dots, \frac{p-1}{2}$ :

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \left(\prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k\right) \cdot \left(\prod_{k=1}^{\frac{p-1}{2}} r_k\right) \pmod{p}$$

Заметим, что  $r_1, \dots, r_{\frac{p-1}{2}}$  – перестановка чисел  $1, \dots, \frac{p-1}{2}$

Действительно, если  $r_k \equiv r_l \pmod{p}$ , то:

$$ak \equiv \pm al \pmod{p}$$

$$p \mid a(k \pm l) \pmod{p}$$

$$p \mid k \pm l \pmod{p}$$

$$|k \pm l| \leq p-1 < p \implies k = l$$

Значит  $\left(\frac{p-1}{2}\right)! = \prod_{k=1}^{\frac{p-1}{2}} r_k$ . Тогда  $\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}} \equiv_p \prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k$

■

**Теорема.**  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{[\frac{p+2}{4}]}$ <sup>5</sup>

---

<sup>5</sup>  $\left[\frac{p+2}{4}\right]$  – целая часть от деления

**Доказательство.** Применим [лемму Гаусса](#) для  $a = 2$ . Тогда  $ak$  примет все четные значения на отрезке  $[2, p]$ . Все  $ak$ , лежащие на интервале  $\left(\frac{p}{2}, p\right)$  являются отрицательными  $\varepsilon_k r_k$ . На интервал  $\left(\frac{p}{2}, p\right)$  перешли все  $k$ , которые были на  $\left(\frac{p}{4}, \frac{p}{2}\right)$ . А значит, что  $t$  равно количеству целых чисел на интервале  $\left(\frac{p}{4}, \frac{p}{2}\right)$ . Их ровно столько:

$$1 + \left[ \frac{p-1}{2} - \frac{p}{4} \right] = 1 + \left[ \frac{p-2}{4} \right] = \left[ 1 + \frac{p-2}{4} \right] = \left[ \frac{p+2}{4} \right]$$

■

**Теорема** (квадратичный закон взаимности Гаусса). Пусть  $p, q$  – нечетные простые. Тогда  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}$

**Лемма** (следствие из леммы Гаусса). Пусть  $p$  – нечетное простое,  $a \in \mathbb{Z}$  и  $a$  – нечетное. Тогда  $\left(\frac{a}{p}\right) = (-1)^S$ , где  $S = \sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{ak}{p} \right]$

**Доказательство.** Заметим, что  $\left[ \frac{ak}{p} \right]$  – неполное частное.

$$ak = \left[ \frac{ak}{p} \right] \cdot p + \rho_k, \quad 1 \leq \rho_k \leq p-1$$

По модулю 2 получаем:  $k \equiv \left[ \frac{ak}{p} \right] + \rho_k \pmod{2}$

Просуммируем по  $k = 1, 2, \dots, \frac{p-1}{2}$ :

$$(*) \quad \frac{p^2-1}{8} \equiv \sum_{k=1}^{\frac{p-1}{2}} k \equiv \underbrace{\sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{ak}{p} \right]}_S + \sum_{k=1}^{\frac{p-1}{2}} \rho_k$$

Заметим, что:

$$\rho_k \equiv \underbrace{ak}_{\varepsilon_k r_k} \pmod{p}, \text{ то есть } \rho_k = \begin{cases} r_k, & \text{если } 1 \leq \rho_k \leq \frac{p-1}{2} \\ p - r_k, & \text{если } \frac{p+1}{2} \leq \rho_k \leq p-1 \end{cases}$$

Значит,  $\rho_k \equiv \begin{cases} r_k, & \text{если } \varepsilon_k = 1 \\ r_k - 1, & \text{если } \varepsilon_k = -1 \end{cases} \pmod{2}$

ВЫХОДИТ  $(*) \iff \sum_{k=1}^{\frac{p-1}{2}} k \equiv S + \sum_{k=1}^{\frac{p-1}{2}} r_k - t \pmod{2} \implies S \equiv t \pmod{2}$ , так как  $\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{\frac{p-1}{2}} r_k$

То есть  $\left(\frac{a}{p}\right) = (-1)^t = (-1)^S$

■

**Доказательство** (квадратичного закона взаимности Гаусса). Отложим по горизонтали  $p$ , а по вертикали  $q$ . Возьмем целую точку  $1 \leq k \leq \frac{p-1}{2}$ . Посчитаем сколько точек вида  $(k, l)$  при целом  $l$  и  $0 < l \leq$  "точки на диагонали  $(0, 0) - (p, q)$ ". Их ровно  $\left[ \frac{qk}{p} \right]$ . Теперь сделаем тоже самое для вертикальной оси:  $\left[ \frac{pl}{q} \right]$ .

Всего точек в прямоугольнике  $\frac{p-1}{2} \cdot \frac{q-1}{2} = \frac{(p-1)(q-1)}{4}$ . Складывая количество точек в треугольниках ниже/выше диагонали получаем  $S_1 + S_2$ , где

$$S_1 = \sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{qk}{p} \right]$$

$$S_2 = \sum_{l=1}^{\frac{q-1}{2}} \left[ \frac{pl}{q} \right]$$

Выходит  $S_1 + S_2 = \frac{(p-1)(q-1)}{4}$  (на диагонали нет целых точек, так как  $p \neq q$ ).

Остается вспомнить, что  $\left( \frac{p}{q} \right) = (-1)^{S_2}$ ,  $\left( \frac{q}{p} \right) = (-1)^{S_1}$

Таким образом, при  $p \neq q$ :

$$\left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = (-1)^{S_1+S_2} = (-1)^{\frac{(p-1)(q-1)}{4}}$$

■

**Определение.** Пусть  $p$  – нечетное число,  $p = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ ,  $a \in \mathbb{Z}$

Тогда  $\left( \frac{a}{p} \right) = \prod_{i=1}^k \left( \frac{a}{p_i} \right)^{\alpha_i}$  называется *символом Якоби*.

# Разбор модельного варианта КР

1. Опишите все натуральные числа  $n$ , при которых дробь  $\frac{4n^2 + n + 1}{2n + 1}$  является сократимой.

**Sol.** Заметим, что исходное утверждение эквивалентно  $(4n^2 + n + 1, 2n + 1) \neq 1$   
По Алгоритму Евклида будем делить многочлен на многочлен:

$$(4n^2 + n + 1, 2n + 1) \rightarrow (2n + 1, -n + 1) \rightarrow (-n + 1, 3) = x \neq 1$$

Получаем  $x = 3$ , так как это единственный делитель  $\neq 1$ . Значит:

$$3 \mid -n + 1 \iff -n + 1 \equiv 0 \pmod{3} \rightarrow n \equiv 1 \pmod{3}, n \in \mathbb{N}$$

**Ans.**  $n \equiv 1 \pmod{3}, n \in \mathbb{N}$

2. Найдите в явном виде число  $\alpha$ , если  $\alpha = [1; \overline{1, 6, 1, 2}]$

**Sol.** Вспомним алгоритм построения цепной дроби и по ней будем отщеплять не максимальное возможное целое число, а то, которое записано на текущей позиции в дроби:

$$\alpha = 1 + (\alpha - 1) = 1 + \frac{1}{\frac{1}{\alpha - 1}}$$

$$\frac{1}{\alpha - 1} = 1 + \frac{1 - (\alpha - 1)}{\alpha - 1} = 1 + \frac{1}{\frac{\alpha - 1}{-\alpha + 2}}$$

$$\frac{\alpha - 1}{-\alpha + 2} = 6 + \frac{\alpha - 1 - 6(-\alpha + 2)}{-\alpha + 2} = 6 + \frac{1}{\frac{-\alpha + 2}{7\alpha - 13}}$$

$$\frac{-\alpha + 2}{7\alpha - 13} = 1 + \frac{-\alpha + 2 - (7\alpha - 13)}{7\alpha - 13} = 1 + \frac{1}{\frac{7\alpha - 13}{-8\alpha + 15}}$$

$$\frac{7\alpha - 13}{-8\alpha + 15} = 2 + \frac{7\alpha - 13 - 2(-8\alpha + 15)}{-8\alpha + 15} = 2 + \frac{1}{\frac{-8\alpha + 15}{23\alpha - 43}}$$

Дальше раскладывать не нужно, так как разложение идет по циклу, а значит  $\frac{-8\alpha + 15}{23\alpha - 43}$  равен  $\frac{1}{\alpha - 1}$ . Приравняем и решим уравнение:

$$\frac{-8\alpha + 15}{23\alpha - 43} = \frac{1}{\alpha - 1}$$

$$(-8\alpha + 15)(\alpha - 1) = 23\alpha - 43$$

$$-8\alpha^2 + 15\alpha + 8\alpha - 15 = 23\alpha - 43$$

$$8\alpha^2 = 28$$

$$\alpha = \sqrt{\frac{28}{8}} = \sqrt{\frac{7}{2}}$$

**Ans.**  $\sqrt{\frac{7}{2}}$

3. Найдите подходящую дробь вида  $\frac{p_k}{q_k}$  числа  $\sqrt{11}$  с наименьшим индексом  $k$ , удовлетворяющую неравенству

$$\left| \sqrt{11} - \frac{p_k}{q_k} \right| < 10^{-4}$$

**Sol.** Будем раскладывать  $\sqrt{11}$  в цепную дробь и находить  $a_i$ . Далее, по [теореме о рекуррентных соотношениях](#) будем искать  $p_i$  и  $q_i$ . Потом по [пункту 5 предложения](#) оценим погрешность. Сначала цепная дробь:

$$\sqrt{11} = 3 + (\sqrt{11} - 3) = 3 + \frac{1}{\frac{1}{\sqrt{11}-3}}$$

$$\frac{1}{\sqrt{11}-3} = \frac{\sqrt{11}+3}{(\sqrt{11}-3)(\sqrt{11}+3)} = \frac{\sqrt{11}+3}{2} = 3 + \frac{\sqrt{11}-3}{2} = 3 + \frac{1}{\frac{2}{\sqrt{11}-3}}$$

$$\frac{2}{\sqrt{11}-3} = \frac{2(\sqrt{11}+3)}{(\sqrt{11}-3)(\sqrt{11}+3)} = \sqrt{11}+3 = 6 + (\sqrt{11}-3) = 6 + \frac{1}{\frac{1}{\sqrt{11}-3}}$$

Защиклились, значит  $\sqrt{11} = [3; \overline{3, 6}]$ . Теперь ищем  $p_i, q_i$ :

$p_0 = a_0 p_{-1} + p_{-2} = 3 \cdot 1 + 0 = 3$	$q_0 = a_0 q_{-1} + q_{-2} = 3 \cdot 0 + 1 = 1$
$p_1 = a_1 p_0 + p_{-1} = 3 \cdot 3 + 1 = 10$	$q_1 = a_1 q_0 + q_{-1} = 3 \cdot 1 + 0 = 3$
$p_2 = a_2 p_1 + p_0 = 6 \cdot 10 + 3 = 63$	$q_2 = a_2 q_1 + q_0 = 6 \cdot 3 + 1 = 19$
$p_3 = a_3 p_2 + p_1 = 3 \cdot 63 + 10 = 199$	$q_3 = a_3 q_2 + q_1 = 3 \cdot 19 + 3 = 60$
можем не считать	$q_4 = a_4 q_3 + q_2 = 6 \cdot 60 + 19 = 379$

Проверяем погрешность:

$$\left| \sqrt{11} - \frac{199}{60} \right| \leq \frac{1}{60 \cdot 379} = \frac{1}{22740} < \frac{1}{10^4} = 10^{-4}$$

**Ans.**  $\frac{199}{60}$

4. Опишите все решения уравнения Пелля  $x^2 - 14y^2 = 1$  в натуральных числах.

**Sol.** Алгоритм следующий: раскладываем  $\sqrt{14}$  в цепную дробь, находим период цепной

дроби (пусть равен  $k$ ) и ищем общее решение с помощью  $p_{k-1}$  и  $q_{k-1}$  (ниже будет формула).

Разложим  $\sqrt{14}$  в цепную дробь. Это делается как в предыдущем номере, поэтому сразу:  $\sqrt{14} = [3; \overline{1, 2, 1, 6}]$ . Период четный и равен 4. Найдем  $p_3, q_3$ :

$$\frac{p_3}{q_3} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}} = 3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}} = 3 + \frac{1}{1 + \frac{1}{3}} = 3 + \frac{3}{4} = \frac{15}{4} \implies p_3 = 15, q_3 = 4$$

Получаем все решения уравнения:

$$x_n + \sqrt{14}y_n = \left(p_3 + \sqrt{14}q_3\right)^n = \left(15 + 4\sqrt{14}\right)^n$$

**Примечание.** Если бы период был нечетный, то возвели бы в степень  $2n$ .

**Ans.**  $(x_n, y_n) \in \mathbb{N} : x_n + \sqrt{14}y_n = \left(15 + 4\sqrt{14}\right)^n$

**5.** Решите сравнение  $79x \equiv 3 \pmod{101}$

**Sol.** Исходное сравнение можно записать как диофантово уравнение:

$$79x = 101k + 3, k \in \mathbb{Z}$$

Будем решать такое диофантово уравнение с помощью [алгоритма Евклида](#), а также восстановим коэффициенты  $\lambda a + \mu b = 1$  при помощи [расширенного алгоритма Евклида](#). В данном случае  $a = 101, b = 79$ . Решаем:

$$(101, 79) =^1 (79, 22) =^2 (22, 13) =^3 (13, 9) =^4 (9, 4) =^5 (4, 1)$$

$$\begin{array}{llllll} 1. & 101 & = & a & = & a_0 \cdot b + r_0 & = & 1 \cdot 79 + 22 \\ 2. & 79 & = & b & = & a_1 \cdot r_0 + r_1 & = & 3 \cdot 22 + 13 \\ 3. & 22 & = & r_0 & = & a_2 \cdot r_1 + r_2 & = & 1 \cdot 13 + 9 \\ 4. & 13 & = & r_1 & = & a_3 \cdot r_2 + r_3 & = & 1 \cdot 9 + 4 \\ 5. & 9 & = & r_2 & = & a_4 \cdot r_3 + r_4 & = & 2 \cdot 4 + 1 \end{array}$$

Основная рекуррента это  $r_i = r_{i-2} - a_i r_{i-1}$ , при этом для удобства возьмем  $a = r_{-2}, b = r_{-1}$ . Идем обратно расширенным алгоритмом Евклида:

$$\begin{aligned} r_4 &= r_2 - a_4 r_3 = r_2 - 2r_3 = r_2 - 2(r_1 - a_3 r_2) = r_2 - 2r_1 + 2r_2 = 3r_2 - 2r_1 = \\ &= 3(r_0 - a_2 r_1) - 2r_1 = 3r_0 - 3r_1 - 2r_1 = 3r_0 - 5r_1 = 3r_0 - 5(b - a_1 r_0) = \\ &= 3r_0 - 5b + 15r_0 = 18r_0 - 5b = 18(a - a_0 b) - 5b = 18a - 18b - 5b = 18a - 23b \end{aligned}$$

Вышло  $\lambda = 18, \mu = -23$ . Найдем все решения:  $x \equiv_{101} \mu \cdot 3 \equiv_{101} -69 \equiv_{101} 32$

**Ans.**  $x \equiv 32 \pmod{101}$

6. Найдите остаток от деления числа  $10^{14^{104}}$  на 19.

**Sol.** Хотим найти  $x$  в сравнении  $10^{14^{104}} \equiv x \pmod{19}$ . Для этого перепишем левую часть:

$$10^{14^{104}} \equiv_{19} 10^{18k+a} \equiv_{19} 10^{18k} \cdot 10^a \equiv_{19} 1^k \cdot 10^a \equiv_{19} 10^a$$

**Примечание.**  $10^{18} \equiv 1 \pmod{19}$  по [малой теореме Ферма](#), так как  $19 \nmid 10$ .

Приравняем показатели степени:  $14^{104} = 18k + a$ . Отсюда перейдем к сравнению  $14^{104} \equiv a \pmod{18}$ . Теперь есть 2 разных решения: в лоб и идейное. Рассмотрим каждое.

**6.1.** Воспользуемся бинарным возведением в степень по модулю 18. Для этого разложим 104 в двоичную запись:  $104 = 1101000_2$ . По [алгоритму](#):

Основание	Текущая степень	Результат ( $a$ )
14	$1101000_2$	1
16	$110100_2$	1
4	$11010_2$	1
16	$1101_2$	16
4	$110_2$	16
16	$11_2$	4
4	$1_2$	16

Получаем  $a = 16 \implies 10^{16} \equiv x \pmod{19}$ . Дальше делим  $10^{16}$  столбиком на 19 и получаем остаток 4.

**6.2.** Заметим что  $14^6 \equiv 1 \pmod{9}$  – это верно по [теореме Эйлера](#):  $14^{\varphi(9)} \equiv 1 \pmod{9}$ , так как  $(14, 9) = 1$ , при этом  $\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 6$ . Тогда:

$$14^{103} \equiv_9 14^{6 \cdot 17 + 1} \equiv_9 14^{6 \cdot 17} \cdot 14 \equiv_9 1^{17} \cdot 14 \equiv_9 14 \iff 14^{103} \equiv 14 \pmod{9}$$

Домножаем сравнение на 2 по [3 свойству сравнений](#):

$$14^{103} \equiv 14 \pmod{9} \rightarrow 2 \cdot 14^{103} \equiv 28 \pmod{18}$$

Теперь на 7 по [4 свойству сравнений](#) (так как  $(7, 18) = 1$ ):

$$2 \cdot 14^{103} \equiv 28 \pmod{18} \rightarrow 14 \cdot 14^{103} \equiv 196 \pmod{18} \rightarrow 14^{104} \equiv 16 \pmod{18}$$

Получили такой же корень. Вместо деления столбиком можно решить диофантово уравнение:

$$10^{16} \equiv x \pmod{19} \rightarrow 10^{18} \equiv 100x \pmod{19} \rightarrow 100x \equiv 1 \pmod{19} \rightarrow 100x = 19k + 1$$

**Ans.** 4



7. Докажите, что число  $1105 = 5 \cdot 13 \cdot 17$  является числом Кармайкла.

**Proof.** Составное число  $n$  называется числом Кармайкла, если  $\forall a \in \mathbb{Z}$  такого что  $(a, n) = 1$ , справедливо  $a^{n-1} \equiv 1 \pmod{n}$ .

Можно разбить на систему из 3 модулей (интуитивно понятно, по сути можно сказать, что следует из КТО):

$$\begin{cases} a^{1104} \equiv 1 \pmod{5} \\ a^{1104} \equiv 1 \pmod{13} \\ a^{1104} \equiv 1 \pmod{17} \end{cases}$$

Распишем для первого сравнения:

$$a^{1104} \equiv (a^4)^{276} \equiv 1^{276} \equiv 1 \pmod{5}$$

Осталось понять почему  $a^4 \equiv 1 \pmod{5}$ . Такой переход разрешен по [малой теореме Ферма](#) если  $5 \nmid a$ . От противного:  $5 \mid a$ ,  $5 \mid 1105 \implies (a, 1105) \geq 5$ , что противоречит условию  $(a, 1105) = 1$ .

Для остальных сравнений аналогично. ■

8. Найдите все основания  $a$ , для которых  $15$  – (сильно) псевдопростое число.

**Sol.** Нечетное число  $n = d \cdot 2^s + 1$  с нечетным  $d$  называется сильно псевдопростым по основанию  $a$ , если выполнено одно из условий:

- $a^d \equiv 1 \pmod{n}$
- $a^{d \cdot 2^r} \equiv -1 \pmod{n}$  для некоторого  $0 \leq r < s$

В нашем случае  $d = 7$ ,  $s = 1$ , а значит  $r = 0$ . Условие единственное:  $a^7 \equiv \pm 1 \pmod{15}$ . Заметим, что если в ответ включили  $a$ , то и включаем  $a + 15k$ ,  $\forall k \in \mathbb{Z}$ :

$$(a + 15k)^7 \equiv_{15} a^7 + \underbrace{a^6 \cdot 15k}_{\equiv 0} + \underbrace{a^5 \cdot (15k)^2}_{\equiv 0} + \dots + \underbrace{(15k)^7}_{\equiv 0} \equiv_{15} a^7$$

Поэтому рассмотрим только  $a \in \{0, 1, \dots, 14\}$ . Более элегантного решения, чем просто перебрать все основания и честно проверить я не придумал. Тогда подойдут только эти:

$$\begin{aligned} a = 1 : \quad 1^7 &\equiv 1 \pmod{15} \\ a = 14 : \quad 14^7 &\equiv -1 \pmod{15} \end{aligned}$$

**Ans.**  $a \equiv 1 \pmod{15}$ ,  $a \equiv 14 \pmod{15}$

9. Решите систему сравнений

$$\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 7 \pmod{12} \\ x \equiv 1 \pmod{13} \end{cases}$$

**Sol.** Перепишем сравнения и приравняем:

$$x = 11k + 2 = 12p + 7 = 13t + 1$$

Теперь решим несколько диофантовых уравнений (в 5 задаче описано подробнее):

$$11k + 2 = 13t + 1$$

$$13t - 11k = 1$$

$$13 = 11 + 2 \implies 11 = 5 \cdot 2 + 1 \implies 1 = (11 - 5 \cdot 2) = 11 - 5(13 - 11) = 6 \cdot 11 - 5 \cdot 13$$

$$\begin{cases} 13t - 11k = 1 \\ -5 \cdot 13 + 6 \cdot 11 = 1 \end{cases} \implies 13(t + 5) = 11(k + 6) \implies t = 11m - 5, k = 13m - 6 \implies$$

$$\implies x = 13(11m - 5) + 1 = 143m - 64 = 12p + 7$$

$$143m - 12p = 71$$

$$143m - 12p = 1$$

$$1 = 12 - 11 = 12 - (143 - 11 \cdot 12) = 12 \cdot 12 - 1 \cdot 143$$

$$\begin{cases} -71 \cdot 143 + 12 \cdot 71 \cdot 12 = 1 \\ 143m - 12p = 71 \end{cases} \implies 143(m + 71) = 12(p + 12 \cdot 71) \implies$$

$$\implies m = 12y - 71, p = 143 \cdot y - 12 \cdot 71 \implies$$

$$\implies x = 143(12y - 71) - 64 = 143 \cdot 12y - 143 \cdot 71 - 64 =$$

$$= 11 \cdot 12 \cdot 13y - 11 \cdot 13 \cdot (12 \cdot 6 - 1) - 64 =$$

$$= 11 \cdot 12 \cdot 13(y - 6) + 143 - 64 = 79 \pmod{11 \cdot 12 \cdot 13}$$

**Ans.**  $79 \pmod{11 \cdot 12 \cdot 13}$

10. Решите в натуральных числах уравнение  $\varphi(3^x 5^y) = 120$

**Sol.** Ниже приведены 2 свойства функции Эйлера, которые помогут в решении задачи:

$$\varphi(nm) = \varphi(n) \cdot \varphi(m), \quad \forall n, m \quad (n, m) = 1$$

$$\varphi(p^k) = p^k - p^{k-1} \text{ для простого } p$$

Заметим, что  $(3^x, 5^y) = 1$ , так как в их факторизации нет одинаковых чисел. Тогда:

$$\begin{aligned}\varphi(3^x 5^y) &= \varphi(3^x) \cdot \varphi(5^y) = (3^x - 3^{x-1})(5^y - 5^{y-1}) = 3^{x-1}(3 - 1) \cdot 5^{y-1}(5 - 1) = \\ &= 8 \cdot 3^{x-1} \cdot 5^{y-1} = 120 \implies 3^{x-1} \cdot 5^{y-1} = 3 \cdot 5 = 15\end{aligned}$$

Тут уже видно, что  $x = y = 2$ .

**Ans.**  $x = y = 2$

# Разбор модельного варианта Экз

1. Выясните, разрешимо ли сравнение

(a)  $x^2 \equiv 92 \pmod{431}$ ;    (b)  $x^2 \equiv 2 \pmod{143}$ .

**Sol.** (a) 431 простое число, поэтому по критерию Эйлера:

$$92^{\frac{431-1}{2}} \equiv 1 \pmod{431} \iff 92 - \text{квадратичный вычет, то есть имеет решение}$$

Возведем бинарным возведением в степень и получим:  $92^{215} \equiv 1 \pmod{431}$ . А значит, сравнение разрешимо.

**Ans.** Да.

**Sol.** (b)  $143 = 11 \cdot 13$ , поэтому сравнение надо разбить на систему:

$$\begin{cases} x^2 \equiv 2 \pmod{11} \\ x^2 \equiv 2 \pmod{13} \end{cases}$$

Понятно, чтобы исходное сравнение было разрешимо, надо чтобы каждое из сравнений было разрешимо. Проверим по критерию Эйлера:

$$2^5 = 32 \equiv -1 \pmod{11} - \text{квадратичный невычет}$$

Второе сравнение проверять нет смысла, ответ уже отрицательный.

**Ans.** Нет.

2. Вычислите сумму символов Лежандра  $\sum_{x=1}^{102} \left( \frac{20x+23}{103} \right)$ .

**Sol.** Давайте докажем, что  $20x+23 \pmod{103}$  при  $x = 0, 1, \dots, 102$  — это перестановка чисел  $0, 1, \dots, 102$ :

$$20x + 23 \equiv 20y + 23 \pmod{103}$$

$$20x \equiv 20y \pmod{103}$$

$$103 \mid 20(x - y)$$

$$103 \mid x - y, \text{ так как } (20, 103) = 1$$

$$x < 103, y < 103 \implies |x - y| < 103 \implies x = y$$

■

Тогда  $\sum_{x=0}^{102} \left( \frac{20x+23}{103} \right) = 0$ , потому что есть 51 квадратичный вычет, 51 квадратичный невычет и ровно один 0 (по предложению). Остается вычесть случай, когда  $x = 0$  :  
$$\left( \frac{20 \cdot 0 + 23}{103} \right) = \left( \frac{23}{103} \right)$$

По критерию Эйлера  $\left(\frac{23}{103}\right) = 23^{51} \pmod{103}$ . Бинарно возведем в степень и получим 1. Тогда:

$$\sum_{x=1}^{102} \left(\frac{20x+23}{103}\right) = \sum_{x=0}^{102} \left(\frac{20x+23}{103}\right) - \left(\frac{23}{103}\right) = 0 - 1 = -1$$

**Ans.**  $-1$

**3.** Найдите

- (a) все первообразные корни по модулю 7 на промежутке от -3 до 3;
- (b) все первообразные корни по модулю 14 на промежутке от -7 до 7;
- (c) какой-нибудь первообразный корень по модулю 98.

**Sol.** (a) Знаем, что  $\varphi(7) = 6$ .  $g$  является первообразным корнем по  $(\text{mod } 7)$ , если для любого  $p \mid 6$  верно  $g^{\frac{6}{p}} \not\equiv 1 \pmod{7}$ . Таких подходящих  $p$  всего 2: это 2 и 3  $\left(\frac{6}{p} \text{ тоже } 2 \text{ и } 3\right)$ .

Теперь найдем такие  $g$ . Ими могут быть только простые числа меньше 7: 2, 3, 5. Проверим:

$g = 2$	$2^2 = 4 \equiv 4 \pmod{7}$	$2^3 = 8 \equiv 1 \pmod{7}$	не подходит
$g = 3$	$3^2 = 9 \equiv 2 \pmod{7}$	$3^3 = 27 \equiv 6 \pmod{7}$	подходит
$g = 5$	$5^2 = 25 \equiv 4 \pmod{7}$	$5^3 = 125 \equiv 6 \pmod{7}$	подходит

**Ans.**  $-2, 3$

**Sol.** (b) Делаем тоже самое как в прошлом примере. Получаем  $\varphi(14) = \varphi(2)\varphi(7) = 6$ , также  $\frac{6}{p}$  равен 2 и 3. Но не забываем, что  $(g, m) = 1$ , поэтому 2 и 7 не подходят.

Проверяем:

$g = 3$	$3^2 = 9 \equiv 9 \pmod{14}$	$3^3 = 27 \equiv 13 \pmod{14}$	подходит
$g = 5$	$5^2 = 25 \equiv 11 \pmod{14}$	$5^3 = 125 \equiv 13 \pmod{14}$	подходит
$g = 11$	$11^2 = 121 \equiv 9 \pmod{14}$	$11^3 = 1331 \equiv 1 \pmod{14}$	не подходит
$g = 13$	$13^2 = 169 \equiv 1 \pmod{14}$	можно не считать	не подходит

**Ans.** 3, 5

**Sol.** (c) Найдем  $\varphi(98) = \varphi(2) \cdot \varphi(7^2) = 42$ . Факторизуем:  $42 = 2 \cdot 3 \cdot 7$  – это те простые, которые делят  $\varphi(98)$ . Значит при возведении  $g$  в степень  $\frac{42}{2} = 21$ ,  $\frac{42}{3} = 14$  и  $\frac{42}{7} = 6$  это не должно быть сравнимо с 1 по  $(\text{mod } 98)$ :

$$\begin{cases} g^6 \not\equiv 1 \pmod{98} \\ g^{14} \not\equiv 1 \pmod{98} \\ g^{21} \not\equiv 1 \pmod{98} \end{cases}$$

Будем перебирать простые и подставлять в систему (однако стоит помнить, что 2 и 7 не подходят). Вероятность везения достаточно велика.

**Ans.** Любой из  $\{3, 5, 17, 33, 45, 47, 59, 61, 73, 75, 87, 89\}$

4. Найдите количество целых чисел  $x$  на промежутке от 1 до 1024, удовлетворяющих сравнению  $x^{12} \equiv 625 \pmod{1024}$ .

**Sol.**

$$\begin{aligned}x^{12} &\equiv 625 \pmod{1024} \\x^{12} - 5^4 &\equiv 0 \pmod{1024} \\(x^6 + 5^2)(x^6 - 5^2) &\equiv 0 \pmod{1024} \\(x^6 + 5^2)(x^3 + 5)(x^3 - 5) &\equiv 0 \pmod{1024}\end{aligned}$$

Заметим, что нам нужны только  $x \equiv 1 \pmod{2}$ , иначе все скобки будут нечетными, их произведение тоже нечетное, что нас не устраивает. Рассмотрим первую скобку:

- Она делится на 2 (нечетное + нечетное)
- Теперь покажем, что не делится на 4:

$$\begin{aligned}x^6 + 25 &\not\equiv 0 \pmod{4} \\(x^6 - 1) + (25 + 1) &\not\equiv 0 \pmod{4} \\(x^6 - 1) + 2 &\not\equiv 0 \pmod{4} \\(x^3 + 1)(x^3 - 1) &\not\equiv 2 \pmod{4} \\\frac{(x^3 + 1)(x^3 - 1)}{2} &\not\equiv 1 \pmod{2}\end{aligned}$$

Действительно,  $x^3 + 1$  и  $x^3 - 1$  четные числа, поэтому левая часть сравнения четная. Значит, исходная скобка не делится на 4.

Поэтому делим все сравнение на 2:

$$(x^3 + 5)(x^3 - 5) \equiv 0 \pmod{512}$$

Рассмотрим случай  $x \equiv 1 \pmod{4}$ . Тогда первая скобка делится на 2, но не на 4. Первое утверждение очевидно, второе:

$$\begin{aligned}x^3 + 5 &\not\equiv 0 \pmod{4} \\x^3 &\not\equiv 3 \pmod{4} \\1 &\not\equiv 3 \pmod{4}\end{aligned}$$

Так же разделим сравнение на 2:

$$x^3 - 5 \equiv 0 \pmod{256}$$

$$x^3 \equiv 5 \pmod{256}$$

Фанфакт с ДЗ:  $m = 2^\alpha \implies \text{ord}_{2^\alpha}(5) = 2^{\alpha-2}$ . В нашем случае  $\text{ord}_{256}(5) = 64$ . Тогда, если сравнение имеет решение, то  $x$  представимо в виде  $5^k$ :

$$5^{3k} \equiv 5 \pmod{256}$$

$$3k \equiv 1 \pmod{64}$$

Это сравнение имеет ровно одно решение: даже не важно какое.

Главное, что  $x$  в сравнении  $x^3 \equiv 5^k \pmod{256}$  нечетный, так как  $5 \cdot \dots \cdot 5 \pmod{\text{четное}}$  является нечетным числом. Тогда случай  $x \equiv 3 \pmod{4}$  является полностью таким же, за исключением, что корни там  $-x$  (разделив на 2 можно понять почему). Отметим, что  $x \not\equiv -x \pmod{256}$ , так как они оба нечетные, а в сумме дают 256.

Так как период корней 256, то на интервале от 1 до 1024 их будет по 4 для каждого случая, следовательно подходящих  $x$  ровно 8 (различность было доказано выше).

**Ans.** 8

5. Пусть  $p$  – простое,  $p \geq 5$ . Пусть  $P$  – произведение всех положительных первообразных корней по модулю  $p$ , не превосходящих  $p$ . Докажите, что

$$P \equiv 1 \pmod{p}$$

**Proof.** Пусть  $g$  – первообразный корень. Тогда  $g^{-1} = g^{p-2}$  тоже первообразный корень, потому что  $(p-2, 1) = 1$  (а значит является образующей группы). При  $p \geq 5$  получаем  $g \neq g^{p-2}$ , то есть это различные первообразные корни.

Значит все первообразные корни делятся на пары. Перемножим их в каждой паре:

$$g \cdot g^{p-2} = g^{p-1} \equiv 1 \pmod{p} \text{ по МТФ, так как } g \nmid p$$

Получается произведение всех пар тоже  $\equiv 1 \pmod{p}$

■