

# Алгебра 1 семестр ПИ,

## Лекция, 10/08/21

Собрано 18 октября 2021 г. в 12:11

---

## Содержание

<b>1. Теория сравнений</b>	<b>1</b>
1.1. Начала теории сравнений . . . . .	1
1.2. Классы вычетов . . . . .	2
1.3. Кольцо классов вычетов . . . . .	3
1.4. Приведенная система вычетов . . . . .	4
1.5. Функция Эйлера . . . . .	4
1.6. Сравнения с одним неизвестным . . . . .	5
1.7. Диофантовы уравнения . . . . .	6
1.8. Системы сравнений . . . . .	6

## 1.1. Начала теории сравнений

**Def. 1.1.1.**  $a$  и  $b$  называются сравнимыми по модулю  $m > 0$ , если они имеют одинаковые остатки при делении на  $m$

$$a \equiv b \pmod{m}, a \equiv b(m), a \stackrel{m}{\equiv} b$$

Утверждение 1.1.2.

$$\Leftrightarrow \begin{cases} a \equiv b \pmod{m} \\ a - b : m \\ a \equiv b + mt \end{cases}$$

Доказательство. 1)  $\Rightarrow$  2)

$$a = mq_1 + r, b = mq_2 + r \Rightarrow a - b = m(q_1 - q_2) : m$$

2)  $\Rightarrow$  3)

$$a - b : m \Rightarrow a - b = mt \Rightarrow a = b + mt$$

3)  $\Rightarrow$  1). Поделим  $a$  и  $b$  на  $m$ :

$$a = mq_1 + r_1, b = mq_2 + r_2$$

$$\begin{aligned} 3) : a = b + mt &\Rightarrow mq_1 + r_1 = mq_2 + r_2 + mt \Rightarrow \\ &\Rightarrow m(q_1 - q_2 - t) = r_2 - r_1 \Rightarrow m | r_2 - r_1 \Rightarrow r_2 - r_1 = 0 \end{aligned}$$

■

Свойства:

1. Рефлексивность.  $a \equiv a \pmod{m}$
2. Симметричность.  $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
3. Транзитивность.  $a \equiv b \pmod{m} \Rightarrow b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Доказательство.

$$a - c = a - b + b - c : m$$

■

4.  $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$
5.  $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$

Доказательство.

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) : m$$

■

$$6. d|a, d|b, d|m, a \equiv b \pmod{m} \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

*Доказательство.*

$$a - b = a_1d - b_1d = my = m_1dt \Rightarrow a_1 - b_1 = m_1t$$

■

$$7. a \equiv b \pmod{m} \Rightarrow ka \equiv kb \pmod{m}$$

$$8. d|a, d|b, (m, d) = 1, a \equiv b \pmod{m} \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$$

*Доказательство.*

$$a = a_1d, b = b_1d, a - b : m \Rightarrow (a_1 - b_1) \cdot d : m \Rightarrow a_1 - b_1 : \frac{m}{d}$$

■

$$9. d|m, a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{d}$$

$$10. a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$$

*Доказательство.*

$$a \equiv b \pmod{m} \Rightarrow a = b + mt \Rightarrow (a, m) = (b, m)$$

■

## 1.2. Классы вычетов

**Def. 1.2.1.** Классом вычетов по  $\pmod{m}$  называется множество чисел, сравнимых с  $a$  по модулю  $m$

$$m = 7, \bar{1} = \{-6, 8, 1, 15, \dots\}$$

$$\bar{a} = \{x | x \equiv a \pmod{m}\}$$

Элементы классов вычетов – **вычеты**. Обычно рассматривают наименьший неотрицательный вычет.

**Def. 1.2.2.** Множество вычетов, взятых по одному из разных классов образуют полную систему вычетов. Например

$$\{0, 1, 2, \dots, m - 1\}$$

**Lm 1.2.3.** Множество из  $m$  чисел, попарно несравнимых по модулю  $m$ , образуют полную систему вычетов.

**Теорема 1.2.4.**  $(a, m) = 1$ . Если  $x$  пробегает полную систему вычетов по  $\pmod{m} \Rightarrow \forall b \rightarrow ax + b$  тоже пробегает полную систему вычетов по  $\pmod{m}$

*Доказательство.*  $x$  принадлежит  $m$  значений  $\Rightarrow ax + b$  принадлежит  $m$  значений.

Пусть  $x_1 \not\equiv x_2 \pmod{m}$ . Предположим, что  $ax_1 + b \equiv ax_2 + b \pmod{m} \Rightarrow ax_1 \equiv ax_2 \pmod{m} \Rightarrow x_1 \equiv x_2 \pmod{m}$

■

### 1.3. Кольцо классов вычетов

**Def. 1.3.1.** Определим сложение и умножение вычетов по фиксированному модулю  $m$ .

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

**Lm 1.3.2.** Сложение и умножение определены корректно

*Доказательство.*  $a \equiv a_1 \pmod{m}, b \equiv b_1 \pmod{m}$

$$\Rightarrow a + b = a_1 + b_1 \pmod{m}, a \cdot b = a_1 \cdot b_1 \pmod{m} \Rightarrow \bar{a} + \bar{b} = \bar{a}_1 + \bar{b}_1, \bar{a} \cdot \bar{b} = \bar{a}_1 \cdot \bar{b}_1$$

■

**Def. 1.3.3.** Группа  $G$  называется коммутативной (абелевой), Если

$$\forall x, y \in G \rightarrow xy = yx$$

**Теорема 1.3.4.**  $\mathbb{Z}_m$  образует коммутативную группу относительно сложения

*Доказательство.*  $\bar{a} + \bar{b} = \overline{a + b} \in \mathbb{Z}_m$

1.  $(\bar{a} + \bar{b}) + \bar{c} = \overline{a + b + c} = \overline{a + b + c}$   
 $\bar{a} + (\bar{b} + \bar{c}) = \overline{a + b + c} = \overline{a + b + c}$
2.  $\bar{0}. \bar{a} + \bar{0} = \overline{a + 0} = \bar{a}$
3.  $-\bar{a} = \overline{m - a} \Rightarrow \bar{a} - \bar{a} = \overline{a + m - a} = \bar{0}$
4.  $\bar{a} + \bar{b} = \bar{b} + \bar{a}$

■

**Def. 1.3.5.** (Ассоциативным) кольцом называется множество  $R$ , на котором заданы бинарные операции:

1.  $\forall x, y, z \rightarrow (x + y) + z = x + (y + z)$
2.  $\exists 0 \in R : \forall x \in R \rightarrow x + 0 = x$
3.  $\forall x \in R \exists (-x) \in R : x + (-x) = 0$
4.  $\forall x, y \in R \rightarrow x + y = y + x$
5.  $\forall x, y, z \in R \rightarrow (y + z) = xy + xz, (x + y)z = xz + yz$
6.  $\forall x, y, z \in R \rightarrow (xy)z = x(yz)$

*Замечание 1.3.6.*  $\exists 1 \in R : \forall x \in R \rightarrow x \cdot 1 = 1 \cdot x = x$  – кольцо с единицей

$\forall x, y \in R \rightarrow xy = yx$  – коммутативное кольцо

**Теорема 1.3.7.**  $\mathbb{Z}_m$  – коммутативное кольцо с единицей.

*Доказательство.*

$$\bar{a}(\bar{b} + \bar{c}) = \overline{a \cdot (b + c)} = \overline{a(b + c)} = \overline{ab + ac}$$

и т.д.

■

**Def. 1.3.8.** Кольца  $R$ , в котором  $\forall a, b \rightarrow (ab = 0 \Rightarrow a = 0 \vee b = 0)$  называется кольцом без делителей нуля.

Если  $ab = 0$  и  $a, b \neq 0$ , то  $a, b$  – делители нуля

**Def. 1.3.9.** Коммутативное кольцо без делителей нуля – область целостности.

**Теорема 1.3.10.** 1.  $\mathbb{Z}_m$  имеет делители нуля  $\Leftrightarrow m$  – составное число

2.  $\mathbb{Z}_p, p$  – простое – область целостности.

*Доказательство.* " $\Rightarrow$ ".  $m = n \cdot k, \bar{n} \cdot \bar{k} = \bar{0}$  в  $\mathbb{Z}_m$

" $\Leftarrow$ ".  $\bar{n} \cdot \bar{k} = \bar{0} \Rightarrow n \cdot k \equiv 0 \pmod{m}$

Предположим, что  $m$  – простое  $\Rightarrow m|n \vee m|k \Rightarrow \bar{n} = \bar{0} \vee \bar{k} = \bar{0}$ . Но  $\bar{n}$  и  $\bar{k}$  – делители нуля, т.е.  $\bar{n}, \bar{k} \neq \bar{0} \Rightarrow m$  – составное.

1)  $\Rightarrow$  2)

■

## 1.4. Приведенная система вычетов

**Def. 1.4.1.** Вычеты, выбранные из полной системы вычетов и взаимно-простые с модулем  $m$  образуют приведенную систему вычетов

**Def. 1.4.2.** Количество вычетов в приведенной системе вычетов обозначается  $\varphi(m)$  – функция Эйлера.

**Lm 1.4.3.** Если  $p$  – простое, то

$$\varphi(p) = p - 1$$

**Теорема 1.4.4.**  $(a, m) = 1, x$  пробегает приведенную систему вычетов  $\Rightarrow ax$  тоже пробегает приведенную систему вычетов по  $\pmod{m}$

*Доказательство.*  $x \rightarrow \varphi(m), ax \rightarrow \varphi(m)$

$(ax, m) = (a, m) = 1 \Rightarrow ax$  набор чисел из  $\varphi(m)$ , взаимно-простых с  $m \Rightarrow \{ax\}$  – приведенная система вычетов.

■

## 1.5. Функция Эйлера

**Lm 1.5.1.**  $p$  – простое,  $\alpha > 0$

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

*Доказательство.*  $1, 2, 3, \dots, p, 2p, 3p, \dots, p \cdot p, \dots, p^\alpha - 1$ . Выбросим из этого множества числа, делящиеся на  $p$ . Таких чисел будет ровно количество коэффициентов при  $p$  до  $p^\alpha$ , т.е.  $p^{\alpha-1}$

■

**Def. 1.5.2.** Функция  $\Theta : \mathbb{N} \rightarrow \mathbb{N}$  называется мультипликативной, если

$$(a, b) = 1 \Rightarrow \Theta(ab) = \Theta(a) \cdot \Theta(b)$$

**Теорема 1.5.3** (Мультипликативность функции Эйлера).  $\varphi$  мультипликативна

*Доказательство.*  $(a, b) = 1$

$$\begin{array}{ccccccc} 1 & 2 & 3 & \dots & b \\ b+1 & b+2 & b+3 & \dots & 2b \\ \dots & \dots & \dots & \dots & \dots \\ (a-1)b+1 & (a-1)b+2 & (a-1)b+3 & \dots & ab \end{array}$$

Количество чисел, взаимно-простых с  $b : \forall$  строка :  $kb+r, k=0, \dots, a-1, 1 \leq r \leq b$ . Рассмотрим  $k$ -ю строку:  $(kb+r, b) = 1 \Rightarrow (r, b) = 1$ . Количество чисел  $kb+r : (kb+r, b) = 1 = \varphi(b) \Rightarrow$  есть  $\varphi(b)$  столбцов, в которых числа  $(kb+r, b) = 1$ . Найдем в этих столбцах числа, взаимно-простые с  $a$ .  $\forall$  столбец :  $xb+r, x=0, \dots, a-1 \Rightarrow xb+r$  – полная система вычетов по  $\pmod{a} \Rightarrow$  среди  $\{xb+r\}$  чисел, взаимно-простых с  $a = \varphi(a) \Rightarrow$  всего чисел, взаимно-простых с  $ab = \varphi(a) \cdot \varphi(b)$

■

*Следствие 1.5.4.*  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  – каноническое разложение  $\Rightarrow \varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot \dots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k-1})$

*Замечание 1.5.5.*  $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdot \dots \cdot (1 - \frac{1}{p_k})$

**Теорема 1.5.6** (Теорема Эйлера).  $(m, a) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

*Доказательство.*  $r_1, r_2, \dots, r_{\varphi(m)}$  – приведенная система вычетов по  $\pmod{m}$   
 $\Rightarrow ar_1, ar_2, \dots, ar_{\varphi(m)}$  – приведенная система вычетов по  $\pmod{m}$ . Пусть  $ar_i = \rho_i$

$$\Rightarrow ar_1 \cdot ar_2 \cdot \dots \cdot ar_{\varphi(m)} = \rho_1 \rho_2 \cdot \dots \cdot \rho_{\varphi(m)}$$

$$a^{\varphi(m)} r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} = \rho_1 \cdot \rho_2 \cdot \dots \cdot \rho_{\varphi(m)} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

■

**Теорема 1.5.7** (Теорема Ферма).  $p$  – простое,  $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

*Доказательство.*  $\varphi(p) = p - 1$

■

**Def. 1.5.8.**  $\mathbb{Z}_m^* = \{r : 0 \leq r < m, (r, m) = 1\}$  – приведенная система вычетов по  $\pmod{m}$

**Теорема 1.5.9.**  $\mathbb{Z}_m^*$  – коммутативная группа по умножению

*Доказательство.*  $r_1, r_2 \in \mathbb{Z}_m^*$ .  $(r_1, m) = (r_2, m) = 1 \Rightarrow (r_1 \cdot r_2, m) = 1 \Rightarrow r_1 \cdot r_2 \in \mathbb{Z}_m^*, 1 \in \mathbb{Z}_m^*$   
 $r \in \mathbb{Z}_m^*$ , то  $r^{-1} = r^{\varphi(m)-1} \Rightarrow r^{\varphi(m)-1} \cdot r = r^{\varphi(m)} \equiv 1 \pmod{m}$

■

## 1.6. Сравнения с одним неизвестным

**Def. 1.6.1.**  $f(x) \equiv 0 \pmod{m}$ . Решением этого сравнения называется  $x_0 : f(x_0) \equiv 0 \pmod{m}$ .

Решения  $x_1$  и  $x_2$  называются эквивалентными, если  $x_1 \equiv x_2 \pmod{m}$

Решить сравнение – найти решений из полной системы вычетов.

**Теорема 1.6.2** (Решение линейного сравнения).  $ax \equiv b \pmod{m}, (a, m) = d$

1.  $d \nmid b \Rightarrow$  решений нет.

2.  $d \mid b \Rightarrow \exists d$  решений :  $x = x_0 + m_1 t, t = 0, 1, \dots, d - 1, m_1 = \frac{m}{d}, x_0$  – какое-то решение

*Доказательство.* 1. Очевидно

2. Если  $(a, m) = 1, x$  пробегает полную систему вычетов по  $\pmod{m} \Rightarrow ax$  – полная система вычетов по  $\pmod{m} \Rightarrow \exists x_0 : ax_0 \equiv b \pmod{m}$

Если  $(a, m) = d, a = a_1 d, m = m_1 d, b = b_1 d, (a_1, m_1) = 1$

$a_1 x \equiv b_1 \pmod{m_1} - \exists$  решение  $x_0 : a_1 x_0 \equiv b_1 \pmod{m_1}$ .  $x = x_0 + m_1 t$  – решение  $ax \equiv b \pmod{m}$

$$a(x_0 + m_1 t) = a_1 d x_0 + a_1 d m_1 t \equiv b_1 d \pmod{m}$$

Посмотрим, какие решения принадлежат полной системе вычетов, т.е.  $0 \leq x_0 + m_1 t < m$ .

Ясно, что такие решения будут при  $t = 0, 1, \dots, d - 1$ .

■

**Теорема 1.6.3** (Методы решения  $ax \equiv b \pmod{m}$ ,  $(a, m) = 1$ ). 1.  $ax \equiv b \pmod{m} \Rightarrow x \equiv a^{\varphi(m)-1} \cdot b \pmod{m}$

2.  $ax \equiv b \pmod{m} \Rightarrow x \equiv (-1)^n p_{n-1} \cdot b \pmod{m}$   
 $\frac{m}{a}$  – непрерывная дробь,  $p_{n-1}$  – числитель  $(n-1)$ -й подходящей дроби,  $\frac{p_n}{q_n} = \frac{m}{a}$

*Доказательство.*  $p_k \cdot q_{k-1} - p_{k-1} \cdot q_k = (-1)^{k-1}$ .  $k = n$

$$m \cdot q_{n-1} - p_{n-1} \cdot a = (-1)^{n-1} \Rightarrow -p_{n-1} \cdot a \equiv (-1)^{n-1} \pmod{m}$$

$$ap_{n-1}b = (-1)^n b \pmod{m} \Rightarrow a \cdot (-1)^n p_{n-1} \cdot b \equiv b \pmod{m} \Rightarrow x \equiv (-1)^n p_{n-1} \cdot b \pmod{m}$$

■

## 1.7. Диофантовы уравнения

**Def. 1.7.1.** Уравнение вида

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b$$

где  $a_i \in \mathbb{Z}$ ,  $x_i$  – переменные и  $\exists i : a_i \neq 0$ , называется диофантовым.

**Lm 1.7.2.**  $ax + by = c$ ,  $a, b \neq 0$ . Если  $x_0 : ax_0 \equiv c \pmod{b} \Rightarrow (x_0, \frac{ax_0 - c}{b})$  – решения уравнения

*Доказательство.*  $by \equiv c - ax$  при  $x = x_0$  и  $c - ax : b \Rightarrow \frac{c - ax_0}{b} \in \mathbb{Z}$

■

**Теорема 1.7.3.**  $ax + by = c$ ,  $d = (a, b)$ ,  $d|c$ . Пусть  $(x_0, y_0)$  – какое-то решение  $\Rightarrow$  все решения:

$$\begin{cases} x = x_0 - \frac{b}{d}t \\ y = y_0 + \frac{a}{d}t \end{cases}, t \in \mathbb{Z}$$

## 1.8. Системы сравнений

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

**Теорема 1.8.1** (Китайская теорема об остатках).  $(m_i, m_j) = 1, i \neq j$ . Тогда

1. Решение системы существует:

$$x \equiv \frac{M}{m_1} \cdot M'_1 b_1 + \frac{M}{m_2} \cdot M'_2 b_2 + \dots + \frac{M}{m_k} \cdot M'_k b_k \pmod{M}$$

$$M = m_1 \cdot m_2 \cdot \dots \cdot m_k, M'_i : M'_i \cdot \frac{M}{m_i} \equiv 1 \pmod{m_i}$$

2. Решение единственно

*Доказательство.* 1. Подставим в  $i$ -е уравнение:

$$x \equiv \frac{M}{m_i} M'_i b_i \pmod{m}_i \Rightarrow x \equiv b_i \pmod{m}_i$$

2. Без доказательства. ■

**Теорема 1.8.2** (Теорема Вильсона).  $p$  – простое  $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$

*Доказательство.* " $\Rightarrow$ ".  $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$  – группа,  $a \in \mathbb{Z}_p^*$

$$a^2 = 1 \Rightarrow a = \pm 1, 1 \cdot 2 \cdot \dots \cdot (p-1) \Rightarrow 1 \cdot (p-1) \equiv -1 \pmod{p}$$

$$a \neq a^{-1} \Rightarrow 2 \cdot \dots \cdot (p-2) = 1$$

" $\Leftarrow$ ". Предположим, что

$$k|p, k > 1, k \neq p \Rightarrow k < p \Rightarrow 1 \cdot 2 \cdot \dots \cdot (p-1) \div k \Rightarrow (p-1)! \equiv 0 \pmod{p}$$
■

*Алгоритм 1.8.3* (Алгоритм RSA). 1. Выбираем  $p, q$  – простые

2.  $n = p \cdot q, \varphi(n) = (p-1)(q-1)$

3. Выбираем  $e : (e, \varphi(n)) = 1$

4. Решаем  $e \cdot d \equiv 1 \pmod{\varphi(n)} \Rightarrow$  находим  $d$

Шифрование:

1.  $m$  – текст (в виде цифрового кода)

2.  $c \equiv m^e \pmod{n} \Rightarrow c$  – шифр

Ключи:

- $(e, n)$  – открытый ключ
- $(d, n)$  – закрытый ключ

Дешифрование:

$$c^d \equiv m^{ed} \equiv m \pmod{n}$$

Трудность  $n = p \cdot q$ .