Алгебра 1 семестр ПИ,
Лекция, 10/08/21

Собрано 13 октября 2021 г. в 11:37

Содержание

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*

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

Утверждение 1.1.2.

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

Доказательство. 1) $\Rightarrow$ 2)

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

2) $\Rightarrow$ 3)

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

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

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

$$3) : a = b + mt \Rightarrow mq_1 + r_1 = mq_2 + r_2 + mt \Rightarrow$$
$$\Rightarrow m(q_1 - q_2 - t) = r_2 - r_1 \Rightarrow m | r_2 - r_1 \Rightarrow r_2 - r_1 = 0$$

■

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.

   $$a - c = a - b + b - c \vdots m$$

   ■

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.

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

   ■

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.

$$a - b = a_1 d - b_1 d = my = m_1 dt \Rightarrow a_1 - b_1 = m_1 t$$

∎

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.

$$a = a_1 d, b = b_1 d, a - b \vdots m \Rightarrow (a_1 - b_1) \cdot d \vdots m \Rightarrow a_1 - b_1 \vdots m$$

∎

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*

$$m = 7, \overline{1} = \{-6, 8, 1, 15, ...\}$$

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

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*

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

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 $\pmod m$ $\Rightarrow \forall b \to ax + b$ 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.*

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

Lm 1.3.2. Сложение и умножение определены корректно

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

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

■

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

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

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

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

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

■

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

1. $\forall x, y, z \to (x + y) + z = x + (y + z)$

2. $\exists 0 \in R : \forall x \in R \to x + 0 = x$

3. $\forall x \in R\ \exists (-x) \in R : x + (-x) = 0$

4. $\forall x, y \in R \to x + y = y + x$

5. $\forall x, y, z \in R \to (y + z) = xy + xz, (x + y)z = xz + yz$

6. $\forall x, y, z \in R \to (xy)z = x(yz)$

Замечание 1.3.6. $\exists 1 \in R : \forall x \in R \to x \cdot 1 = 1 \cdot x = x$ – кольцо с единицей
$\forall x, y \in R \to xy = yx$ – коммутативное кольцо

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

Доказательство.

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

и т.д. ■

Def. 1.3.8. *Кольца R, в котором $\forall a, b \to (ab = 0 \Rightarrow a = 0 \lor b = 0)$ 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. "$\Rightarrow$". $m = n \cdot k, \overline{n} \cdot \overline{k} = \overline{0}$ в $\mathbb{Z}_m$
"$\Leftarrow$". $\overline{n} \cdot \overline{k} = \overline{0} \Rightarrow n \cdot k \equiv 0 \pmod{m}$
Предположим, что m – простое $\Rightarrow m|n \vee m|k \Rightarrow \overline{n} = \overline{0} \vee \overline{k} = \overline{0}$. Но $\overline{n}$ и $\overline{k}$ – делители нуля, т.е. $\overline{n}, \overline{k} \neq 0 \Rightarrow m$ – 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 обрузуют 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. $x \to \varphi(m), ax \to \varphi(m)$
$(ax, m) = (a, m) = 1 \Rightarrow ax$ 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. $1, 2, 3, ..., p, 2p, 3p, ..., p \cdot p, ..., p^\alpha - 1$. Выбросим из этого множества числа, делящиеся на p. Таких чисел будет ровно количество коэффициентов при p до p^α, т.е. $p^{\alpha-1}$ ■

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

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