Лекция №2 «Сравнения». Курс A-I

Турашев Артём Сергеевич 619/2

16 сентября 2025

Определение 1. *a, b, $m \in \mathbb{Z}$,* $\quad m \neq 0$

$a \equiv b\,(m)$ $\quad$ (*или по-другому* $\quad a \equiv b \pmod{m}$), $\quad$ *если* $\quad m|b - a$

Пример 1. $b \bmod 2$ $\quad$ (*означает, что каждый* $a \equiv 0;\ 1$)

Лемма 1. "$\equiv (m)$" $-$ *отношение эквивалентности*
(*Упражнение*)

Z разбивается на классы эквивалентности
$\overline{a} \ = \ \{\ \mathrm{n} \in \mathbb{Z} : n \equiv a\,(m)\} = \{n = a + km\}$

Определение 2. *$\overline{a}$ называется классами вычетов по* $\bmod m$, *множество* $\{\overline{a}\}$ *- система вычетов*

Лемма 2. *1)* $\overline{a} = \overline{b} \Leftrightarrow a \equiv b\,(m)$
2) $\overline{a} \neq \overline{b} \Leftrightarrow \overline{a} \cap \overline{b} = \emptyset$
3) $|\{\overline{a} : a \in \mathbb{Z}\}| = m$
(Упражнение)

Определение 3. *{ 0, 1, . . . , m-1 } - полная система вычетов*

Лемма 3. *Пусть* $a \equiv c\,(m)$, $b \equiv d\,(m)$, *тогда*
1) $a + b \equiv c + d\,(m)$
2) $ab \equiv cd\,(m)$
(Упражнение)

Таким образом можем ввести операции на множестве $\{\overline{a}\}$:

$\overline{a} + \overline{b} = \overline{a + b}$

$\overline{a}\ \overline{b} = \overline{ab}$

Лемма 4. *Операции корректно определены*
(Упражнение)

(m) = { km: k $\in \mathbb{Z}$} $-$ множество кратных m чисел (идеал)

$(2) = \{2k : k \in \mathrm{Z}\} -$ идеал

$(2,3) = \{2k_1 + 3k_2,\ k_1, k_2 \in \mathbb{Z}\}$

$\mathbb{Z} -$ КГИ (кольцо главных идеалов)

$(2,3) = (1) = \mathbb{Z}$

Определение 4. *Пусть R - коммутативное кольцо с единицей. Идеалом I кольца R называется $I \in \mathbb{R}$:*
$1) \forall x, y \in I \quad x + y \in I$
$2) \forall x \in I, \forall r \in \mathbb{R} \quad rx \in I$

КГИ $\Leftrightarrow \forall I\, \exists v \in \mathbb{R} \quad I = (v)$

Определение 5. $a,\ b \in \mathbb{R},\ a \equiv b\,(I) \Leftrightarrow a - b \in I$

Множество классов эквивалентности R / I (это множество в общем случае является кольцом)

Случай Z:

$\{\overline{a}\}$ = Z / m Z = Z / (m)

$\overline{a}$ = a + (m)

Пример 2. $n = x^2 + y^2$ *Какие целые числа представимы в виде суммы двух квадратов?*
$p -$ *простое* $p = x^2 + y^2$ *Если* $p \equiv 3\,(4)$, *то не преставимо*

$\square$ *Пусть* $p = x^2 + y^2,\ x, y \in \mathbb{Z}$ (x *и* y *не могут быть одновременно чётными и нечётными*)
Если такое представление $\exists$, *то оно имеет такой вид:*

$$p = (2n)^2 + (2m+1)^2 = 4n^2 + 4m^2 + 4m + 1 \equiv 1\,(4)$$

Перешли: $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$
$p \equiv x^2 + y^2\,(4)$ (*не имеет решений*) $\Rightarrow$ *исходное тоже не имеет решений* $\blacksquare$

Либо возможна в алгебре такая идея (отличная от идеи в предыдущем случае):

Q, R $\to \mathbb{C}$

Теорема 1. $ax \equiv b\,(m)$ *разрешимо* $\Leftrightarrow d = (a, m) | b$

$\square$
$\Rightarrow$: $\exists x_0 :\ ax_0 \equiv b\,(m) \quad ax_0 - b = my_0 \quad d|a,\ d|m\ \to d|ax_0 - my_0 = b$
$\Leftarrow$: $d = (a, m),\ d|b$ (*это то же самое что* $b = cd$)
$\exists x_0, y_0 :\ d = ax_0 - my_0$ (*это то же самое что* $d = (a, m)$)
$b = cd = a(x_0 c) - m(y_0 c)$ *Перейдём по модулю m и получим решение нашего сравнения.*

Дополнение к утверждению: если d $|b$, а $x_0 -$решение, то есть в точности d решений:
$x_0,\ x_0 + m'$ (где $m' = m/d$), $x_0 + 2m',\ \ldots,\ x_0 + (d-1)m'$

Пусть x_0, x_1 — решения $ax_0 \equiv b\,(m),\ ax_1 \equiv b\,(m)$

$a(x_0 - x_1) \equiv 0\,(m) \Leftrightarrow a(x_0 - x_1) = mk$

$d|b,\ d$ — наибольший общий делитель, $d = (a, m)$;

$a = a'd \quad m = m'd \quad (a', m') = 1$

$a'(x_0 - x_1) = m'k \quad m'|a'(x_0 - x_1) \to m'|x_0 - x_1$

$x_1 = x_0 + k'm' \quad (x_0,\ x_0 + m',\ \ldots,\ x_0 + (d-1)m'$ — попарно несравнимы по модулю $m)$

$x_0 + km' \equiv x_0 + lm'\,(m)$

$m'(k - l) \equiv 0\,(m)$

$m|m'(k-l),\ m' < m$ (причём m и m' — взаимно простые) $\to m|k - l \quad (0 \le k,\ l \le d - 1 < m) \to k = l$ ∎

Следствие. *1) (a, m) = 1, то* $ax \equiv b\,(m)$ *имеет единственное решение*
2) $m = p$ — *простое число, то* $\forall a \not\equiv 0\,(p) \quad (a, p) = 1 \to \forall a \not\equiv 0\,(p) \quad \exists x : ax \equiv 1(p)$ *(то есть иными словами* $\mathbb{Z}/p\mathbb{Z}$ *— поле)*

Определение 6. *R - кольцо с единицей*
$e \in \mathbb{R}$ *называется единицей, если он обратим, то есть если:* $\exists f \in \mathbb{R} : ef = 1$

Следствие. *1)* $a \in \mathbb{Z}/m\mathbb{Z}$ *— единица (обратим)* $\Leftrightarrow (a, m) = 1$

Пример 3. *0, 1* $\in \mathbb{Z}/2\mathbb{Z}$

Следствие. *2) число единиц в* $Z/mZ = \varphi(m)$ *(где* φ *— обозначение функции Эйлера)*

Определение 7. *{* $\overline{a}$*: (a, m) = 1} называется приведенной системой вычетов*

Теорема 2. *(Эйлер) (a, m) = 1* $\to a^{\varphi(m)} \equiv 1\,(m)$

□ *Пусть* $r_1, \ldots, r_{\varphi(m)}$ *— приведенная система вычетов* $ar_1, \ldots, ar_{\varphi(m)}$ *—*
тоже приведенная система вычетов

$\prod_{i=1}^{\varphi(m)} (ar_i) \equiv \prod_{i=1}^{\varphi(m)} r_i\,(m)$

$a^{\varphi(m)} \prod r_i \equiv \prod r_i\,(m)$

Получается, что $a^{\varphi(m)} \equiv 1\,(m)$ ∎

□ *Второй вариант доказательства:* $\mathbb{R}^*$ *— единица кольца, группа. Таким образом* $(\mathbb{Z}/m\mathbb{Z})^*$ *— группа,* $\varphi(m)$ *— порядок* $\to \forall a \in (\mathbb{Z}/m\mathbb{Z})^* \quad a^{\varphi(m)} \equiv 1\,(m)$ ∎

Раздел Китайская теорема об остатках (КТО)

Лемма 5. *$a_1, \dots, a_t \quad a_i|n$, они попарно взаимно просты, то есть $(a_i, a_j) = 1 \to a_1...a_t|n$ (Упражнение)*

Теорема 3. *(Китайская теорема об остатках (КТО)) Пусть $m = m_1...m_t,\ (m_i, m_j) = 1,\ i \neq j. \quad b_1, \dots, b_t \in \mathbb{Z}$. Тогда система уравнений:*

$$\begin{cases} x \equiv b_1\,(m_1), \\ \qquad\quad \dots, \\ x \equiv b_t\,(m_t). \end{cases}$$

разрешима (то есть имеет решение). Если x, y – решение, то $x \equiv y\,(m)$

$\square \quad n_i = m/m_i$ *По лемме* $(n_i, m_i) = 1 \quad \exists r_i, s_i : r_i m_i + s_i n_i = 1$, *где* $e_i = s_i n_i$

$e_i \equiv 1\,(m_i) \quad e_i \equiv 0\,(m_j), \quad j \neq i$

Возьмём $x = \sum_{i=1}^{t} b_i e_i \quad x \equiv b_i e_i\,(m_i)$

y – *другое решение*

$x - y \equiv 0\,(m_i) \Leftrightarrow m_i|x - y\ \to m = \prod m_i|x - y \qquad \blacksquare$

Кольцо многочленов

F - поле

Определение 8. *F[x] = $\{f = a_0 + a_1 x + \dots + a_n x^n \quad a_i \in F,\ a_n \neq 0\}$*

deg f = n (степень f = n)

Лемма 6. *F[x] - кольцо (коммутативное с единицей)
(Упражнение)*

Определение 9. $f \in F[x] \qquad f$ – *унитарный, если* $a_n = 1$

f – *неприводимый, если* $g|f \to g \in F \vee g = f$

f = gh
(f, g) = d - НОД $\qquad$ d $|f \qquad d|h \qquad d'|f \qquad d'|h \quad \to \quad d'|d$

Лемма 7. $f \in F[x],\ deg\, f > 1 \to f(x) = \prod p(x)\ (p$ – *неприводимый*$)$

$\square$ *как в* $\mathbb{Z}$, *только вместо* $|.|\ deg\,(.) \qquad \blacksquare$

Лемма 8. $\forall f, g \in F[x],\ g \neq 0 \quad \exists h, r \in F[x] \quad f = gh + r$, *где либо* $r = 0$ *либо* $deg\, r < deg\, f$
(Упражнение)

Лемма 9. *1) F[x] - КГИ, $\quad$ 2)f, g $\in F[x] \quad \exists d \in F[x] \quad (f, g) = (d) \quad d$ – НОД (f, g)
(Упражнение)*

Лемма 10. *1) (f, g) = 1* $\Leftrightarrow \exists r, s \in F[x] \quad rf + sg = 1$
$2)(f, g) = 1,\ f|gh \rightarrow f|h$
$3)p -$ *неприводимый,* $p|fg \ \rightarrow\ p|f \vee p|h$

Определение 10. *p(x)* $\in F[x]-$*неприводимый,* $f(x) \in F[x] \quad f(x) = p(x)^a f_1(x)$ *(где* $f_1(x)-$ *какой-то другой многочлен)*

$\mathrm{pf}_1: \quad a = \nu_{p(x)}(f(x))$ (или по-другому $ord_{p(x)}(f(x))$)

Лемма 11. $\nu_p(fg) = \nu_p(f) + \nu_p(g)$

Теорема 4. $\forall f \in F[x]\ \exists!\ f(x) = c\prod_{p-\text{неприводим}} p(x)^{a(p)}, \quad a(p) = \nu_p(f)$ *(где c−константа)*