Коллоквиум по теории чисел.

Титилин Александр

1 Делимость

$$a, b \in \mathbb{Z}.$$

$$a \vdots b := \exists \alpha \in \mathbb{Z} : a = \alpha b.$$

Теорема 1.

$$a, b, c \in \mathbb{Z}.$$

$$a \vdots b \wedge b \vdots c \implies a \vdots c.$$

Доказательство.

$$\exists \alpha, \beta \in \mathbb{Z}.$$

$$a = \alpha b \wedge b = \beta c \implies a = \alpha\beta c.$$

□

Теорема 2.

$$a, b, c \in \mathbb{Z}.$$

$$a \vdots c \wedge b \vdots c \implies (a \pm b) \vdots c.$$

Доказательство.

$$\exists \alpha, \beta \in \mathbb{Z}.$$

$$a = \alpha c \wedge b = \beta c.$$

$$a \pm b = c(\alpha \pm \beta).$$

□

Теорема 3. *Каждое натуральное число больше единицы делится хотя бы на одно простое число.*

Доказательство. Рассуждаем по индукции. Для 2 теорема верна, так как 2 простое число. Теперь предположим, что теорема верна для всех чисел меньше n. Если n простое, то теорема верна, иначе $n = ab$, $a < n$. a делится на простое число. n делится на простое по теореме 1. □

Теорема 4. *Существует бесконечно много простых чисел.*

Доказательство. Пусть простых чисел конечное число $p_1, p_2 \dots p_k$ Рассмотрим число $n = p_1p_2p_3 \dots p_k+1$. n не простое число и не делится ни на одно простое, получили противоречие. □

Теорема 5. *Каждое натуральное число > 1 число может быть единсвенным образом записано в виде произвдения степеней простых чисел.*

Доказательство. □

2 НОД

Если $a \vdots c \wedge b \vdots c$. c называется общим делителем.

Лемма 6.

$$\forall a, b \in \mathbb{Z}.$$

$$\gcd(a, b) = \gcd(a - b, b).$$

Доказательство.

$$a, b \in \mathbb{Z}.$$

$$a \vdots c \wedge b \vdots c \implies a - b \vdots c.$$

□

Теорема 7.

$$m \vdots n \implies \gcd(m, n) = n.$$

Теорема 8.

$$\gcd(am, an) = |a| \gcd(m, n).$$

3 Деление с остатком

Теорема 9.

$$a, b \in \mathbb{Z}, b \neq 0.$$

$$\exists! q, r \in \mathbb{Z}, r = 0..|b| - 1.$$

$$a = qb + r, r = 0 \dots |b| - 1.$$

Доказательство. Единственность.

$$a = bq_1 + r_1.$$

$$a = bq_2 + r_2.$$

$$b(q_1 - q_2) = r_1 - r_2.$$

$$|b(q_1 - q_2)| = |r_1 - r_2|.$$

□

Теорема 10.

$$a, b \in \mathbb{Z}.$$

$$d = \gcd a, b.$$

$$\exists \alpha, \beta \in \mathbb{Z}.$$

$$\alpha a + \beta b = d.$$

Доказательство. Рассмотрим множество $M = \{ax + by | x, y \in \mathbb{Z} \wedge ax + by > 0\}$. $ax \,\vdots\, d \wedge by \,\vdots\, d \implies \forall \delta \in M \ \delta \,\vdots\, d$. $d = \min M$ □

Следствие 10.1.

$$\gcd(a, b) = 1 \iff \exists x, y \in \mathbb{Z} \ ax + by = 1.$$

Теорема 11.

$$a, b \in \mathbb{Z}.$$

$$ab \,\vdots\, c \wedge \gcd(b, c) = 1 \implies a \,\vdots\, c.$$

Доказательство.

$$ab = \alpha c.$$

$$bx + ny = 1 \implies (ab)x + (ay)n = a.$$

□

4 Сравнение по модулю

$$n \in \mathbb{N}, n \neq 1.$$

$$a, b \in \mathbb{Z}.$$

$$a \equiv b \pmod{n} := a - b \,\vdots\, n.$$

Теорема 12. *Если*

$$a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}.$$

то

- $a + c \equiv b + d \ (\mathrm{mod}\ n)$
- $ac \equiv bd \ (\mathrm{mod}\ n)$

Доказательство.

$$a - b = \alpha n.$$

$$c - d = \beta n.$$

- $$(a + c) - (b + d) = n(\alpha + \beta).$$

•
$$ac - bd = ac - ad - bd + ad = a(c - d) - d(a - b) = (a\beta)n - (d\alpha)n.$$

□

Теорема 13. • $a \equiv a \pmod{n}, \forall a \in \mathbb{Z}, n \neq 1 n \in \mathbb{N}$

• $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$

• $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$

Доказательство. • $a - a = 0, 0 \vdots n$

•
$$a - b = pn.$$
$$b - a = -(a - b) = -pn.$$

•
$$a - b = \alpha n.$$
$$b - c = \beta n.$$
$$a - c = n(\alpha + \beta).$$

□

Теорема 14. $\gcd a, n = 1 \implies \exists x \ ax \equiv 1 \pmod{n}$

Доказательство.
$$\alpha a + \beta n = 1.$$
$$\alpha a - 1 = \beta n.$$

□

Теорема 15. $\gcd a, n = 1 \wedge a * b \equiv a * c \pmod{n} \implies b \equiv c \pmod{n}$

5 Классы вычетов

$\{b \mid b \in \mathbb{Z}, b \equiv a \pmod{n}\}$ – класс вычетов a по модулю n. $(a = 0..n - 1)$

Теорема 16. *Два класса вычетов по одному модулю или совпадают или их пересечение пустое множество.*

Теорема 17 (Малая теорема Ферма)**.** *Пусть p простое число, $a \in \mathbb{Z}$ a не делится на p, тогда*
$$a^{p-1} \equiv 1 \pmod{p}.$$

Доказательство. Пусть a_k – остаток от деления ka на p, где $k = 1, 2, \dots, p-1$. ak не делится на p,с среди a_k нет нулей. Рассмотрим $\forall n, m \in \{1, 2, \dots, p-1\}, n \neq m$. $an - am \neq 0$. Таким образом множество $a_1, a_2, \dots, a_{p-1}$ совпадает с множеством $\{1, 2, \dots, p-1\}$.

$$a_1 a_2 a_3 \dots a_{p-1} = (p-1)!.$$

$$a^{p-1}(p-1)! = a * 2a * \dots * (p-1)a \equiv (p-1)! \pmod p.$$

□

$\varphi(n)$ – функция Эйлера, количество натуральных чисел меньше n взаимнопростых с ним. Если n – простое, то $\varphi(n) = n - 1$

Теорема 18 (Эйлера)**.** *a взаимно просто с n. Тогда* $a^{\varphi(n)} \equiv 1 \pmod n$

Доказательство. Рассмотрим $A = \{k_1, k_2, \dots, k_{\varphi(n)}\}$ – множество всех чисел, взаимно простых с n. Теперь рассматриваем набор всех остатков от деления $\forall k \in A$ на a. Нулей и одинаковых чисел в таком наборе нет. Этот набор совпадает с A

$$a^{\varphi(n)} k_1 k_2 \dots k_{\varphi(n)} = ak_1 * ak_2 * \dots * a * k_{\varphi(n)} \equiv k_1 k_2 \dots k_{\varphi(n)} \equiv 1 \pmod n.$$

□

Теорема 19. $\gcd m, n = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$