Оглавление

Лекция 5

06.10.2023

0.1 Степень вхождения простого числа

Определение 1. $v_p(n)$ — степень вхождения $p \in P$ в разложение n на простые множители.

Т.е. $v_p(n) = k$, если $n \vdots p^k$ и $n \not\vdots p^{k+1}$.

Пример. $v_2(12) = 2$, $v_2(15) = 0$, $v_2(16) = 4$.

Свойство.

1. $v_p(nm) = v_p(n) + v_p(m)$.
2. $a, b \in \mathbb{N}$. Тогда $a = b \Leftrightarrow v_p(a) = v_p(b)$
3. $a \vdots b \Leftrightarrow v_p(a) \geq v_p(b) \forall p \in P$
4. $v_p((a, b)) = min(v_p(a), v_p(b))$ $v_p([a, b]) = max(v_p(a), v_p(b))$

Глава 1

Сравнения и классы вычетов

Определение 2. $m \in \mathbb{N}$. Числа a и b называют сравнивыми по модулю m, если $a - b \vdots m$.

Обозначение. $a \equiv b \mod m$ $a \underset{m}{\equiv} b$.

Теорема 1. Сравнение по модулю m — отношение эквивалентности.

Доказательство.

1. $a \equiv a \mod m \Leftrightarrow a - a \vdots m \Leftrightarrow 0 \vdots m$ — рефлексивное.
2. $a \equiv b \mod m \Rightarrow (a - b) \vdots m \Rightarrow (-1)(a - b) \vdots m \Rightarrow b - a \vdots m \Rightarrow b \equiv a \mod m$ — симметричное.
3. $a \equiv b \mod m, b \equiv c \mod m \Rightarrow (a - b) \vdots m, (b - c) \vdots m \Rightarrow (a - b) + (b - c) \vdots m \Rightarrow a - c \vdots m \Rightarrow a \equiv c \mod m$ — транзитивное.

$\square$

Определение 3. $a \in \mathbb{Z}, m \in \mathbb{N}$. Классом вычетов по модулю m называется множество $\overline{a}_m = \{b \in \mathbb{Z} \mid a \equiv b \mod m\}$.

Определение 4. Набор чисел называется полной системой вычетов по модулю m, если в него входят по одному представителю из каждого класса вычетов

Пример. $m = 5$. Полные системы вычетов:
$\{0, 1, 2, 3, 4\}$
$\{-2, -1, 0, 1, 2\}$
$\{5, 11, -13, 3, 4\}$

Свойство. (Арифметические свойства сравнений)

Пусть $a \equiv b \mod m$ и $c \equiv d \mod m$, тогда:

1. $a + c \equiv b + d \mod m$
   $a - c \equiv b - d \mod m$
2. $ac \equiv bd \mod m$

Доказательство. 1. $(a + c) - (b + d) = \underset{\vdots m}{(a - b)} + \underset{\vdots m}{(c - d)} \Rightarrow$
   $\Rightarrow a + c \equiv b + d \mod m$
   Аналогично для разности.
2. $ac - bd = ac - bc + bc - bd = c\underset{\vdots m}{(a - b)} + b\underset{\vdots m}{(c - d)} \Rightarrow ac \equiv bd \mod m$

□

Замечание. $2 \equiv 12 \mod 10, 1 \not\equiv 6 \mod 10$

Свойство. (Решение линейного сравнения)
Пусть $a, b \in \mathbb{Z}, m \in \mathbb{N}, (a, m) = 1$, Тогда:

1. Сравнение $ax \equiv b \mod m$ имеет решение.
2. Если x_1, x_2 — решения, то $x_1 \equiv x_2 \mod m$.

Пример. $3x \equiv 2 \mod 5$
$x_0 = 4$ — решение, множество решений: $x \equiv 4 \mod 5$

Доказательство. Докажем первое, затем второе.

1. (a, m) $= 1 \Rightarrow \exists u, v : au + mv = 1 \Rightarrow$
   $\Rightarrow au \equiv 1 \mod m \Rightarrow a(bu) \equiv b \mod m$
   $x = bu$ — решение.
2. $\begin{cases} ax_1 \equiv b \mod m \\ ax_2 \equiv b \mod m \end{cases} \Rightarrow ax_1 \equiv ax_2 \mod m \Rightarrow a(x_1 - x_2) \vdots m \Rightarrow$
   $x_1 - x_2 \vdots m \Rightarrow x_1 \equiv x_2 \mod m$

□

Определение 5. Определим сложение и умножение на множестве классов вычетов по модулю m:

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

Пример. $m = 5$

$\overline{2} + \overline{3} = \overline{5} = \overline{0}$
$\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$

Теорема 2. (Кольцо вычетов) Пусть $m > 1, m \in \mathbb{N}$. Рассмотрим классы вычетов по модулю m.

1. Сумма и произведение определены корректно, т.е. результат не зависит от выбора представителей.

2. Классвы вычетов образуют коммутативное и ассоциативное кольцо с единицей.

3. Кольцо классов вычетов является полем $\Leftrightarrow m$ — простое.

Доказательство. Приведем доказательство только для суммы, для произведения доказательство строится аналогично.

1. $\begin{cases} a_1, a_2 \text{ — представители одного класса} \\ b_1, b_2 \text{ — представители одного класса} \end{cases} \Rightarrow \begin{cases} a_1 \equiv a_2 \mod m \\ b_1 \equiv b_2 \mod m \end{cases} \Rightarrow$
   $a_1 + b_1 \equiv a_2 + b_2 \mod m$ — $a_1 + b_1$ и $a_2 + b_2$ в одном классе.

2. Нейтральный по сложению: $\overline{0} : \overline{0} + \overline{x} = \overline{x + 0} = \overline{x}$

   Нейтральный по умножению: $\overline{1} : \overline{1} \cdot \overline{x} = \overline{1 \cdot x} = \overline{x}$

   Свойства ассоциативности и коммутативности очевидны. Докажем, например, ассоциативность:

   $(\overline{x} \cdot \overline{y}) \cdot \overline{z} = \overline{xy} \cdot \overline{z} = \overline{xyz} = \overline{x} \cdot \overline{yz} = \overline{x} \cdot (\overline{y} \cdot \overline{z})$

3. ассоциативное коммутативное кольцо с единицей является полем $\Leftrightarrow \forall \overline{a} \neq \overline{0}$ есть обратный по умножению.

   (a) Пусть $m \in P, \overline{a} \neq \overline{0}$
   $\overline{a} \neq \overline{0} \Rightarrow a \not\vdots m \underset{m \in P}{\Rightarrow} (a, m) = 1$
   Из решения линейного сравнения следует, что $\exists x : ax \equiv 1 \mod m \Rightarrow \overline{a} \cdot \overline{x} = 1 \Rightarrow \overline{x} = \overline{a}^{-1}$

   (b) Пусть $m \notin P$. Тогда $\exists a, b : m = ab, 1 < a, b < m$
   Докажем, что $\nexists\, \overline{a}^{-1}$
   Предположим, что есть, тогда: $\overline{x} = \overline{a}^{-1}$
   $\overline{b} = 1 \cdot \overline{b} = \overline{x} \cdot \overline{a} \cdot \overline{b} = \overline{x} \cdot \overline{ab} = \overline{x} \cdot \overline{m} = \overline{x} \cdot \overline{0} = \overline{0}$ — противоречие.

□

Обозначение. Кольцо вычетов по модулю m обозначается $\mathbb{Z}_m$ или $\mathbb{Z}/m\mathbb{Z}$.

Теорема Вильсона и малая теория Ферма

Теорема 3. (Теорема Вильсона) Пусть $p \in P$, тогда $(p-1)! \equiv -1 \mod p$.

Доказательство. 2 случая:

1. случай p $=$ 2: $(p-1)! = 1 \equiv -1 \mod 2$
2. случай p $>$ 2: Рассмотрим поле $\mathbb{Z}_p$
   (a) Нужно доказать, что $(p-1)! = 1 \in \mathbb{Z}_p$.
   - $1, 2, \ldots, p-1$ - ненулевые элементы $\mathbb{Z}_p$.
   - у каждого элемента есть обратный по умножению.

   (b) Докажем, что $x = \overline{x}^{-1}$ выполнено только при $x = 1, x = p-1$: $x = \overline{x}^{-1} \Leftrightarrow x \cdot x = \overline{x}^{-1} \cdot x \Leftrightarrow x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0 \underset{\text{обл. целост.}}{\Leftrightarrow} \left[\begin{array}{l} x-1=0 \\ x+1-0 \end{array}\right. \Leftrightarrow \left[\begin{array}{c} x=1 \\ x=p-1 \end{array}\right.$

   (c) Все элементы, кроме 1 и $p-1$ распадаются на пары, обратные друг другу:
   $1 \cdot 2 \cdot \ldots \cdot (p-1) = 1 \cdot (p-1) \cdot (x_1 \cdot \overline{x_1}^{-1}) \cdot (x_2 \cdot \overline{x_2}^{-1}) \cdot \ldots = p-1 = 1$

□

Лемма 1. Пусть $p \in P$. Тогда $\forall a \in \mathbb{Z}_p, a \neq 0$ набор элементов:
$0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a$ — перестановка элементов $0, 1, \ldots, p-1$.
Другая формулировка:
Если $a \not| p$, то $0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a$ — полная система вычетов по $\mod p$.

Доказательство. Докажем, что элементы $0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a$ — различны.

Предположим, что не различны, тогда $\exists i, j : i \neq j, i \cdot a = j \cdot a \Rightarrow (i-j) \cdot a = 0 \Rightarrow i = j$ — противоречие.

$0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a$ — р шт. различных элементов в $\mathbb{Z}_p \Rightarrow$ это все элементы $\mathbb{Z}_p$. □

Пример. $p = 5, a = 3$
$\{0 \cdot 3, 1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3\} = \{0, 3, 6, 9, 12\}$

Теорема 4. (Малая теорема Ферма) Пусть $p \in P, a \in \mathbb{Z}, a \not\vdots\, p$. Тогда
$a^{p-1} \equiv 1 \mod p$.

Доказательство. Рассмотрим наборы $0, 1, \ldots p-1$ и $0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a$ — совпадающие по лемме 1

Выкинем 0 из наборов, тогда $1, \ldots, p-1$ — перестановка $1 \cdot a, \ldots, (p-1) \cdot a$.

Перемножим:

$$\begin{aligned} 1 \cdot 2 \cdot \ldots \cdot (p-1) &= (1 \cdot a) \cdot (2 \cdot a) \cdot \ldots \cdot ((p-1) \cdot a) \\ 1 \cdot 2 \cdot \ldots \cdot (p-1) &= a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \\ 1 &= a^{p-1} \quad \text{в } \mathbb{Z}_p \end{aligned}$$

□