Семинары по дискретной математике (1 курс, 25-26)

github.com/int28t/hse-se-lecture-notes

Хрыстик Михаил Андреевич

Содержание

1 Листок 4

Малая теорема Ферма

$$a \not\vdots p, p \text{ — простое}$$
$$\Downarrow$$
$$a^{p-1} \equiv 1 \pmod p$$

Утверждение

$$ma \equiv mb \pmod n \Rightarrow a \equiv b \pmod n, \; (m, n) = 1$$

$$ma \equiv mb \pmod n, (m, n) = 1$$
$$\Downarrow$$
$$(ma - mb) \vdots n, \; (m, n) = 1$$
$$\Downarrow$$
$$(a - b) \vdots n$$
$$\Downarrow$$
$$a \equiv b \pmod n$$

1.1 Задача 14

Задача

Найдите остаток от деления числа $\underbrace{111\ldots111}_{105}$ на 107

Решение

$$\underbrace{11\ldots1}_{107} \equiv x \pmod{107} | \cdot 9$$
$$\underbrace{99\ldots9}_{105} \equiv 9x \pmod{107}$$
$$1\underbrace{0\ldots0}_{105} \equiv 9x + 1 \pmod{107} | \cdot 10$$
$$10^{106} \equiv 90x + 10 \pmod{107}$$

По МТФ:

$$90x + 10 \equiv 1 \pmod{107}$$
$$90x \equiv -9 \pmod{107} | : 9$$
$$10x \equiv -1 \pmod{107}$$
$$10x \equiv 106 \pmod{107} | : 2$$
$$5x \equiv 53 \pmod{107}$$

$$5x \equiv 160 \pmod{107} | : 5$$
$$x \equiv 32 \pmod{107}$$

Ответ

32

1.2 Задача 15

Решение

$$1)\ 41^{41^{41}} \equiv 2^{41^{41}} \pmod{13}$$

Построим табличку $[n, 2^n mod 13]$. Заметим что $2^6 \equiv 12 \equiv -1 \pmod{13}$, значит $2^{12} \equiv (2^6)^2 \equiv 1$

$$2)\ 41^{41} \equiv 5^{41} \pmod{12}$$
$$5^2 \equiv 1 \pmod{12}$$
$$3)\ 41 \equiv 1 \pmod{2}$$
$$5^{41} \equiv 5^1 \pmod{12}$$
$$2^{41^{41}} \equiv 2^5 \equiv 6 \pmod{13}$$

Ответ

6

Лемма

Если $b \equiv c \pmod{\phi(n)}$, то $a^b \equiv a^c \pmod{n}$

Теорема Эйлера

$$(a, n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

1.3 Задача 16

Задача о теореме Вильсона

Число $p > 1$ простое тогда и только тогда, когда $(p-1)! \equiv -1 \pmod{p}$

Доказательство

$\Leftarrow$
о/п p — составное
Случай 1: $p = a \cdot b$, $1 < a < b < p$ (то есть p — не квадрат простого числа)

$$\Rightarrow (p-1)! = 1 \cdot 2 \cdot \ldots \cdot a \cdot \ldots \cdot b \ldots (p-1) \vdots p \Rightarrow (p-1)! \equiv 0 \pmod{p} \perp$$

Случай 2: $p = q^2$, q — простое

$$2q < p \Leftrightarrow 2q < q^2 \Leftrightarrow q > 2$$

$$\Rightarrow (p-1)! = 1 \cdot 2 \cdot \ldots q \ldots 2q \ldots (p-1) \vdots p \Rightarrow (p-1)! \equiv 0 \pmod p \perp$$

Случай 3: $p = 4 \Rightarrow (4-1)! \equiv 6 \equiv 2 \not\equiv -1 \pmod 4 \perp$
Во всех случаях получили противоречие

Лемма

$$a \in \mathbb{Z},\ (a,n) = 1 \Rightarrow \exists x \in [1, n-1] : ax \equiv 1 \pmod n$$

$\Rightarrow$
1) Пусть $x \in [1; p-1] \wedge x^2 \equiv 1 \pmod p$

$$x^2 \equiv 1 \pmod p \Leftrightarrow (x^2-1) \vdots p \Leftrightarrow (x-1)(x+1) \vdots p \Leftrightarrow (x-1) \vdots p \vee (x+1) \vdots p \Leftrightarrow$$
$$\Leftrightarrow x = 1 \vee x = p-1$$

2) $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$
Пусть $a, b \in [1; p-1]$, $ax \equiv 1 \pmod 1$, $bx \equiv 1 \pmod p \Rightarrow ax \equiv bx \pmod p (ax-bx) \vdots p \Rightarrow$ $(a-b)x \vdots p$, но $x \in [1; p-1] \Rightarrow (a-b) \vdots p$, но $a, b \in [1; p-1] \Rightarrow a = b \Rightarrow$ числа $2, 3, \ldots, p-2$ разбиваются на пары чисел (a, b) тч $a \cdot b \equiv 1 \pmod p$
Тогда:

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv 1(p-1) \pmod p \equiv -1 \pmod p$$

Случай $p = 2$ на упражнение читателю

1.4 Задача 17

Задача

$$\forall n\ \exists a, d \in \mathbb{N} : a, a+d, a+2d, \ldots, a+(n-1)d \text{ — попарно взаимно просты}$$

Доказательство

2 Листок 5

2.1 КТО

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k}. \end{cases} \qquad \begin{array}{l} (m_i, m_j) = 1 \text{ при } i \neq j \\ M = m_1 \cdot \ldots \cdot m_k, \quad M_i = \dfrac{M}{m_i} \\ b_i \text{ — числа, такие что } M_i b_i \equiv a_i \pmod{m_i} \end{array}$$

Тогда $\exists!$ решение $(*) : x \equiv M_1 b_1 + \ldots + M_k b_k \pmod M$

2.2 Задача 4

Задача 4

$$\begin{cases} x \equiv 12 \pmod{15} \\ x \equiv 8 \pmod{17} \\ x \equiv 3 \pmod{8} \end{cases}$$

Решение

$$M = 15 \cdot 8 \cdot 17 = 2040$$

$$M_1 = 136$$

$$136b_1 \equiv 12 \pmod{15}$$

$$b_1 \equiv 12 \pmod{15}$$

$$M_2 = 120$$

$$120b_2 \equiv 8 \pmod{17}$$

$$b_2 \equiv 8 \pmod{17}$$

$$M_3 = 255$$

$$255b_3 \equiv 3 \pmod{8}$$

$$-b_3 \equiv 3 \pmod{8}$$

$$b_3 \equiv -3 \pmod{8}$$

$$x \equiv 136 \cdot 12 + 120 \cdot 8 - 255 \cdot 3 = 1827 \pmod{2040}$$

Ответ

1827

Пример

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 11 \pmod{13} \\ x \equiv 6 \pmod{8} \end{cases} \Leftrightarrow \begin{cases} x \equiv -2 \pmod{9} \\ x \equiv -2 \pmod{13} \\ x \equiv -2 \pmod{8} \end{cases} \Leftrightarrow \begin{cases} (x+2) \vdots 9 \\ (x+2) \vdots 13 \ (x+2) \vdots 8 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow (x+2) \vdots 936 \Leftrightarrow x \equiv -2 \pmod{936} \equiv -2 \equiv 934$$

2.3 Задача 5

Задача 5

$$f(x) = x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{35}$$

Сколько решений и найти все решения

Решение

$$f(x) \equiv 0 \pmod{35} \Leftrightarrow \begin{cases} f(x) \equiv 0 \pmod 5 \\ f(x) \equiv 0 \pmod 7 \end{cases}$$

1) Решим $f(x) \equiv 0 \pmod 5$

$$x \equiv 0 : f(x) \equiv 9 \not\equiv 0 \pmod 5 \perp$$
$$x \equiv 1 : f(x) \equiv 20 \equiv 0 \pmod 5 \checkmark$$
$$x \equiv 2 : f(x) \equiv 57 \not\equiv 0 \pmod 5 \perp$$
$$x \equiv 3 : f(x) \equiv 168 \not\equiv 0 \pmod 5 \perp$$
$$x \equiv 4 : f(x) \equiv f(-1) \equiv 0 \pmod 5 \checkmark$$

2) Решим $f(x) \equiv 0 \pmod 7$

$$x \equiv 0 : f(x) \equiv 9 \not\equiv 0 \pmod 7 \perp$$
$$x \equiv 1 : f(x) \equiv 20 \not\equiv 0 \pmod 7 \perp$$
$$x \equiv 2 : f(x) \equiv 57 \not\equiv 0 \pmod 7 \perp$$
$$x \equiv 3 : f(x) \equiv 168 \equiv 0 \pmod 7 \checkmark$$
$$x \equiv 4 : f(x) \equiv f(-3) \equiv 12 \not\equiv 0 \pmod 7 \perp$$
$$x \equiv 5 : f(x) \equiv f(-2) \equiv -7 \equiv 0 \pmod 7 \checkmark$$
$$x \equiv 6 : f(x) \equiv f(-1) \equiv 0 \pmod 7 \checkmark$$

$$\Leftrightarrow \begin{cases} \left[\begin{array}{l} x \equiv 1 \pmod 5 \\ x \equiv 4 \pmod 5 \end{array}\right. \\ \left[\begin{array}{l} x \equiv 3 \pmod 7 \\ x \equiv 5 \pmod 7 \\ x \equiv 6 \pmod 7 \end{array}\right. \end{cases} \Leftrightarrow \left[\begin{array}{l} \begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases} \\ \begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases} \\ \begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases} \\ \begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases} \\ \begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases} \\ \begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases} \end{array}\right. \Leftrightarrow \underbrace{\left[\begin{array}{l} x \equiv 31 \pmod{35} \\ x \equiv 26 \pmod{35} \\ x \equiv 6 \pmod{35} \\ x \equiv 24 \pmod{35} \\ x \equiv 19 \pmod{35} \\ x \equiv 34 \pmod{35} \end{array}\right.}_{\text{ответ}}$$

Примечание

$$ax \equiv b \pmod n \Rightarrow ax + by = c$$

$$ax \equiv b \pmod n \Leftrightarrow |ax - b| \,\vdots\, n \Leftrightarrow ax - b = ny \Leftrightarrow ax - ny = b$$