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

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

По МТФ:

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

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

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

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

Доказательство

2 Листок 5

2.1 КТО

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

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 $f(x) \equiv 0 \pmod{7}$

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

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

Примечание

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

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

3 Листок X1

3.1 Задача 11

Решение

c) $(x,y) \in (A \backslash B) \times C \Leftrightarrow (x \in A \backslash B) \wedge (y \in C) \Leftrightarrow (x \in A \wedge x \in \overline{B}) \wedge (y \in C) \Leftrightarrow$
$(x,y) \in (A \times C) \backslash (B \times C) \Leftrightarrow (x,y) \in A \times C \wedge (x,y) \in B \times C \Leftrightarrow$
$\Leftrightarrow (x \in A \wedge y \in C) \wedge \neg(x \in B \wedge y \in C) \Leftrightarrow (x \in A \wedge y \in C) \wedge (\neg(x \in B) \vee \neg(y \in C))$
$\Leftrightarrow (x \in A \wedge y \in C) \wedge (x \notin B \vee y \notin C)$
$\Leftrightarrow (x \in A \wedge y \in C \wedge x \in \overline{B}) \vee (x \in A \wedge y \in C \wedge y \notin C) \Leftrightarrow (x \in A \wedge y \in C \wedge x \in \overline{B})$

3.2 12

Задача

$$A \neq \varnothing, B \neq \varnothing, A \subseteq C, B \subseteq D \Leftrightarrow A \times B \subseteq C \times D$$

$$\boxed{A \subseteq B \Leftrightarrow \forall x (x \in A \to x \in B)}$$

Решение

Необходимость $\Rightarrow$
Пусть $(x,y) \in A \times B \Rightarrow x \in A \wedge y \in B$, но $A \subseteq C, B \subseteq D \Rightarrow x \in C \wedge y \in D \Rightarrow (x,y) \in C \times D$, то есть $A \times B \subseteq C \times D$
Достаточность $\Leftarrow$
Рассмотрим произвольный $x \in A$. Существует $y \in B$, так как $B \neq \varnothing$. Тогда $(x,y) \in A \times B \Rightarrow (x,y) \in C \times D$, так как $A \times B \subseteq C \times D \Rightarrow x \in C$, то есть $A \subseteq C$. Аналогично, $B \subseteq D$. Пусть $B = \varnothing, A = \mathbb{Z}, C = D = \mathbb{N}$
$A \times B = \mathbb{Z} \times \varnothing = \varnothing \ldots$

3.3 13

4 Бинарные отношения

Определение

R — бинарное отношение **между** A и B, если $R \subseteq A \times B$

Определение

$$domR = \{a \in A \mid \exists b : (a,b) \in R\}, rngR = \{b \in B \mid \exists a : (a,b) \in A\}$$

Определение

R — бинарное отношение **на** A, если $R \subseteq A \times A$

Примечание

И первое и второе определение являются частным случаем друг друга. Второе первого тривиально. А первое — частный случай второго если вместо A подставить $A \cup B$

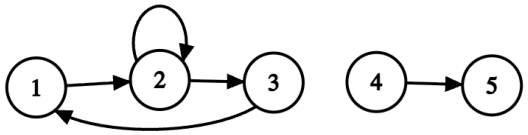
4.1 Лист 7

Задача 1

$$A = \{1,2,3,4\}, B = \mathbb{N}, domR = \{1,2,3,4\}, rngR = \{1,2,3,5\}$$

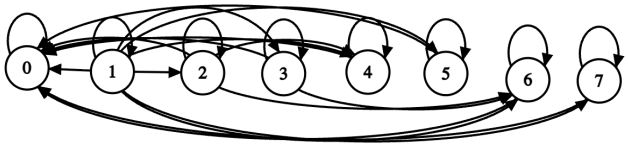
Как рисовать диаграмму R?
$U := domR \cup rngR$

1) Элементы U изобразить точками
2) Провести стрелку от $a \in U$ к $b \in U$, если $(a,b) \in R$



Задача 2

$(a,b) \in \ | \ \Leftrightarrow a|b$ (Вообще, $(a,b) \in R \Leftrightarrow aRb$)



Задача 3

$$R^{-1} = \{(a,b) \mid (b,a) \in R\}, Q \circ P = \{(a,c) \mid \exists b : (a,b) \in P \wedge (b,c) \in Q\}$$

Важно: композиция некоммутативна
Обратим внимание, что это некорректная запись. Также требуется указать чему принадлежат a, c в начале задания множества

$$P \circ P = \{(a,c) \mid \exists b : (a,b) \in P \wedge (b,c) \in P\} = \{(a,c) \mid \exists b : a \text{ — сын } b \wedge b \text{ — сын } c\} =$$

$$= \{(a,c) \mid a \text{ — внук } c\}.\ P \circ P \text{ — быть внуком}$$

$P^{-1} = \{(a,b) \mid (b,a) \in P\} = \{(a,b) \mid b \text{ — сын } a\} = \{(a,b) \mid a \text{ — отец } b\}.\ aP^{-1}b$—$a$ отец b

$$P^{-1} \circ P = \{(a,c) \mid \exists b : (a,b) \in P \wedge (b,c) \in P^{-1}\} =$$

$$= \{(a,c) | \exists b : a \text{ — сын } b \wedge b \text{ — отец } c\} = \{(a,c) | a \text{ — брат } c \vee a = c\}$$

$$P \circ P^{-1} = \{(a,c) | \exists b : (a,b) \in P^{-1} \wedge (b,c) \in P\} = \{(a,c) | \exists b : a \text{ — отец } b \wedge b \text{ — сын } c\} \Rightarrow$$

$$\Rightarrow aP \circ P^{-1}b - a = b. \text{ у } a \text{ есть сын}$$

Задача 4

а) $\leqslant \circ <$

$$= \overbrace{\{(a,c) \mid \exists b : a < b \wedge b \leqslant c\}}^{X} = (*) = \overbrace{\{(a,c) \mid a < c\}}^{Y} =<$$

Докажем $(*)$:

Пусть $(a,c) \in X \Rightarrow \exists b : (a < b) \wedge (b \leqslant c) \Rightarrow \exists b : a < b \leqslant c \Rightarrow a < c \Rightarrow (a,c) \in Y (X \subseteq Y)$

Пусть $(a,c) \in Y \Rightarrow a < c \Rightarrow a < c \leqslant c \Rightarrow \exists b (= c) : a < b \wedge b \leqslant c \Rightarrow (a,c) \in X (Y \subseteq X)$

Ответ: $<$

б) $< \circ <$

$$= \underbrace{\{(a,c) \mid \exists b : a < b \wedge b < c\}}_{X} = \underbrace{\{(a,c) \mid a + 1 < c\}}_{Y}$$

Пусть $(a,c) \in X \Rightarrow \exists b : a < b < c \Rightarrow \exists b : a + 1 \leqslant b \wedge b < c \Rightarrow\Rightarrow a + 1 < c \Rightarrow (a,c) \in Y \Rightarrow X \subseteq Y$

Пусть $(a,c) \in Y \Rightarrow a + 1 < c \Rightarrow a < a + 1 \wedge a + 1 < c \Rightarrow \exists b (= a + 1) : a < b \wedge b < c \Rightarrow (a,c) \in X \Rightarrow Y \subset X$

Ответ: $(a,b) \in< \circ <$, если $a + 1 < b$

в) $< \circ <^{-1}$

$$= \{(a,c) \mid \exists b : (a,b) \in <^{-1} \wedge b < c\} =$$

$$[(a,b) \in <^{-1} \Leftrightarrow (b,a) \in < \Leftrightarrow b < a \Leftrightarrow a > b]$$

$$= \{(a,c) \mid \exists b : a > b \wedge \ b < c\} = \underbrace{(\mathbb{N} \backslash \{0\}) \times (\mathbb{N} \backslash \{0\})}_{\textbf{Ответ}}$$

г) $<^{-1} \circ <$

$$= \{(a,c) \mid \exists b : a < b \wedge b > c\} = \underbrace{\mathbb{N} \times \mathbb{N}}_{\textbf{Ответ}}$$

$Id_A = \{(a,a) \mid a \in A\}$
$Q \circ P = \{(a,c) \mid \exists b : (a,b) \in P \wedge (b,c) \in Q\}$

Задача 5

Проговорили устно

$P \subseteq A \times B, \overline{P} = A \times B \backslash P$. Замечание: $\overline{P} \neq P^{-1}$, например $(<^{-1}) = (>), (\overline{<}) = \geqslant$

Задача 6

а)

$$(a, b) \in (\overline{P})^{-1} \Leftrightarrow (b, a) \in \overline{P} \Leftrightarrow (b, a) \notin P \Leftrightarrow (a, b) \in \overline{(P^{-1})}$$