Практическое занятие 12

Решение сравнений 1 степени

ITMO University

Сравнение 1-й степени с одним неизвестным:

$$a \cdot x = b \ (mod \ n) \qquad (1)$$

Определение

Решением сравнения (1) называется класс x по модулю n, состоящий из чисел, удовлетворяющих этому сравнению.

Число решений сравнения (1) – число классов по модулю n, удовлетворяющих этому сравнению.

d = НОД (a,n)

Теорема

1. $d \nmid b \Rightarrow$ сравнение (1) не имеет решений.

2. $d = 1 \Rightarrow$ сравнение (1) имеет единственное решение.

3. $d \mid b \Rightarrow$ сравнение (1) имеет d решений по модулю n.

Все эти решения образуют один класс по модулю $\frac{n}{d}$:

$$x = \alpha \ (mod \ \frac{n}{d})$$

Числа этого класса образуют d классов по модулю n.

Решения сравнения (1) имеют вид:

$$x_1 = \alpha \pmod{n}$$

$$x_2 = \alpha + 1 \cdot \frac{n}{d} \pmod{n}$$

$$x_3 = \alpha + 2 \cdot \frac{n}{d} \pmod{n}$$

$$\dots$$

$$x_d = \alpha + (d-1) \cdot \frac{n}{d} \pmod{n}$$

Метод цепных дробей

$c \in \boldsymbol{R}$, q_1 – наибольшее целое, не превосходящее c.

Цепной дробью называется число, записанное в виде

$$c = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{s-1} + \cfrac{1}{c_s}}}},$$

где $q_1, q_2, \ldots, q_{s-1} \in \boldsymbol{Z}$, $c_s > 1$.

- c – иррациональное число $\Rightarrow$ всякое c_s иррационально и дробь бесконечная
- c – рациональное число $\Rightarrow$ дробь конечная

$$\frac{k}{l} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_{m-1} + \cfrac{1}{q_m}}}},$$

где $k \in \mathbf{Z}$, $l \in \mathbf{N}$, НОД$(k,l)=1$.

Дроби

$$\delta_1 = q_1$$

$$\delta_2 = q_1 + \frac{1}{q_2}$$

$$\delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} \quad \dots$$

называются подходящими дробями.

Алгоритм вычисления подходящих дробей

$P_0=1,\ Q_0=0$

$P_1=q_1,\ Q_1=1$

$\delta_1 = \frac{P_1}{Q_1} = q_1$

$\delta_s = \frac{P_s}{Q_s}$

$P_s = q_s P_{s-1} + P_{s-2}$

$Q_s = q_s Q_{s-1} + Q_{s-2}$

$s = 2, 3, 4, \ldots$

$$ax = b \ (mod\ n)$$

Теорема

Если $\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \ldots, \frac{P_{m-1}}{Q_{m-1}}, \frac{P_m}{Q_m}$

– последовательность подходящих дробей разложения $\frac{n}{a}$ в цепную дробь и НОД(a,n)=1, то решением сравнения является класс

$$x = (-1)^{m-1} P_{m-1}\ b \ (mod\ n)$$