25.11.25 — **Цепная дробь** — Синицын Е.А.

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ldots}}}}$$

$$\frac{a}{b} = S_1 + \cfrac{1}{S_2 + \frac{r_2}{r_1}} = S_1 + \cfrac{1}{S_2 + \cfrac{1}{S_3 + \frac{r_3}{r_2}}}$$

$$\frac{a}{b} = S_1 + \frac{r_1}{b}$$
$$\frac{b}{r_1} = S_2 + \boxed{\frac{r_2}{r_1}}$$
$$\boxed{\frac{r_1}{r_2}} = S_3 + \frac{r_3}{r_2}$$
$$\frac{r_2}{r_3} = S_4 + \frac{r_4}{r_3}$$

$$\boxed{\begin{aligned} a &= b \cdot S_1 + r_1 \\ b &= r_1 \cdot S_2 + r_2 \\ r_1 &= r_2 \cdot S_3 + r_3 \\ r_2 &= r_3 S_4 + r_4 \end{aligned}}$$

Пример

1) $\frac{539}{103} = ?$

$539 = 103 \cdot 5 + 24$

$103 = 24 \cdot 4 + 7$

$24 = 7 \cdot 3 + 3$

$7 = 3 \cdot 2 + 5$

$3 = 1 \cdot 3$

Ответ:

$\frac{539}{103} = [5, 4, 3, 2, 3]$

2) $\sqrt{2} - ?$

$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{1}{\alpha_1} \Rightarrow$

$\Rightarrow \alpha_1 = \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{2-1} = \sqrt{2}+1$

$\alpha_1 = 2 + \sqrt{2} - 1 = 2 + \frac{1}{\alpha_2} \Rightarrow \alpha_2 = \sqrt{2} + 1$

$\alpha_2 = \sqrt{2} + 1 = \ldots$

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2}+1}}}}$$

Ответ: $\sqrt{2} = [1; 2, 2, 2, \ldots] = [1; (2)]$

$P_{n+1} = P_n a_{n+1} + P_{n-1}$

$Q_{n+1} = Q_n a_{n+1} + Q_{n-1}$

$[2; 3, 2, 2, 1, 2] = \boxed{\frac{149}{65}}$

n	-1	0	1	2	3	4	5
a_n		2	3	2	2	1	2
P_n	1	2	7	16	39	55	149
Q_n	0	1	3	7	17	24	65

$[2]$: $\frac{P_0}{Q_0} = \frac{2}{1}$; $[2; 3]$: $\frac{P_1}{Q_1} = \frac{7}{3}$; $[2; 3, 2]$: $\frac{P_2}{Q_2} = \frac{16}{7}$

$\frac{P_3}{Q_3} = \frac{39}{17}$ $[2; 3, 2, 2]$; $\frac{P_4}{Q_4} = \frac{55}{24}$ ...; $\frac{P_5}{Q_5} = \boxed{\frac{149}{65}}$ $[2; 3, 2, 2, 1, 2]$

} Подходящие дроби

$ax = b \pmod{m}$

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

P_{n-1} — числитель предпоследней подходящей дроби $\frac{m}{a}$

Пример

$$65x = 2 \pmod{149}$$

$$x = (-1)^5\, 2\cdot 55 \Rightarrow x = 39 \pmod{149}$$

Система сравнений

Китайская теорема об остатках

$$\begin{cases} x = a_1 \pmod{m_1} \\ x = a_2 \pmod{m_2} \\ - \; - \; - \\ x = a_3 \pmod{m_3} \end{cases} \qquad (m_i, m_j) = 1, \quad i \neq j$$

$$x = M_1 b_1 + M_2 b_2 + \ldots + M_n b_n \pmod{M}$$

$$M = m_1 \cdot m_2 \cdot \ldots \cdot m_n \qquad M_i = \frac{M}{m_i} \qquad M_i b_i = a_i \pmod{m_i}$$

Пример

$$\begin{cases} x = 20 \pmod{21} \\ x = 3 \pmod{5} \\ x = 5 \pmod{8} \end{cases}$$

$$M = 21 \cdot 5 \cdot 8 = 840$$

$$40 b_1 = 20 \pmod{21} \Rightarrow 2b_1 = 1 \pmod{21}$$

$$2b_1 = 22 \pmod{21} \Rightarrow b_1 = 11 \pmod{21}$$

$$M_1 = \frac{840}{21} = 40$$

$$M_2 = \frac{840}{5} = 168$$

$$M_3 = \frac{840}{8} = 105$$

$$168 b_2 = 3 \pmod{5} \Rightarrow 3b_2 = 3 \pmod{5} \Rightarrow$$

$$\Rightarrow b_2 = 1 \pmod{5}$$

$$105 b_3 = 5 \pmod{8} \Rightarrow b_3 = 5 \pmod{8}$$

$$x = 40 \cdot 11 + 168 \cdot 1 + 105 \cdot 5 \pmod{840} = 1133 \pmod{840}$$

Ответ: $x = 293 \pmod{840}$

Дискретное логарифмирование

$n \in \mathbb{N}$

Определение

$P_n(a) = \{\min \gamma \in \mathbb{N} : a^\gamma \equiv 1 \pmod n\}$

Определение

g – первообразный элемент по $(\bmod\ n)$

$P_n(g) = \varphi(n)$

Пример

$n = 5 \qquad \varphi(5) = 4$

$1^1 = 1 \qquad P_5(1) = 1$

$2^1 = 2;\ 2^2 = 4;\ 2^3 = 3;\ 2^4 = 1 \pmod 5 \qquad P_5(2) = 4 = \varphi(5)$ 2 – первообразный

$3^1 = 3;\ 3^2 = 4;\ 3^3 = 2;\ 3^4 = 1 \pmod 5 \qquad P_5(3) = 4 = \varphi(5)$ 3 – первообразный

$4^1 = 4;\ 4^2 = 1 \pmod 5;\ \ P_5(4) = 2 \neq \varphi(5)$

Теорема

$n = 2;\ 4;\ p^\alpha;\ 2p^\alpha;\ 3p^\alpha \qquad p$ – нечётное простое

Поиск первообразных по p

$\varphi(p) = p - 1 = p_1 \cdot p_2$

$g = 2 \qquad 2^{\frac{p-1}{p_1}} = 1 \pmod p$

$g = 3 \ \ldots$

Пример

1) $n = 11 \qquad \varphi(11) = 10 = 2 \cdot 5$

$2^2 = 4 \pmod 4 \qquad 2^5 = 10 \pmod 4 \qquad g = 2$ – первообразный

---

2) $n = 23 \qquad \varphi(23) = 22 = 2 \cdot 11$

$2^2 = 4,\ 2^{11} = 1 \pmod{23} \qquad 4^2 = 16,\ \ 4^{11} = 1 \pmod{23}$

$3^2 = 9,\ 3^{11} = 1 \pmod{23} \qquad 5^2 = 2,\ \ 5^{11} = 22 \pmod{23} \qquad g = 5$

$n = \mathbb{N}$ g - первообразный по $(\mathrm{mod}\ n)$

$a = g^{\beta} (\mathrm{mod}\ n)$ $(a, n) = 1$

$\beta = \mathrm{ind}_g a$ – индекс a по $(\mathrm{mod}\ n)$ с основанием g

Пример

$n = 5$ $g = 3$

$3^1 = 3\ (\mathrm{mod}\ 5) \Rightarrow \mathrm{ind}_3 3 = 1$

$3^2 = 4\ (\mathrm{mod}\ 5) \Rightarrow \mathrm{ind}_3 4 = 2$

$3^3 = 2\ (\mathrm{mod}\ 5) \Rightarrow \mathrm{ind}_3 2 = 3$

$3^4 = 1\ (\mathrm{mod}\ 5) \Rightarrow \mathrm{ind}_3 1 = 0$

Свойства:

1) $a = b\ (\mathrm{mod}\ n) \Rightarrow \mathrm{ind}\, a = \mathrm{ind}\, b\ (\mathrm{mod}\ \varphi(n))$

2) $\mathrm{ind}(ab) = \mathrm{ind}\, a + \mathrm{ind}\, b\ (\mathrm{mod}\ \varphi(n))$

3) $\mathrm{ind}\, a^{\alpha} = \alpha\, \mathrm{ind}\, a\ (\mathrm{mod}\ \varphi(n))$

Пример

1) $n = 1$

$g = 7$

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}\, a$	0	1	8	2	4	9	7	3	6	5

$7x = 9\ (\mathrm{mod}\ 11)$

$\mathrm{ind}\, 7x = \mathrm{ind}\, 9\ (\mathrm{mod}\ 10)$

$\mathrm{ind}\, 7 + \mathrm{ind}\, x = \mathrm{ind}\, 9\ (\mathrm{mod}\ 10)$

$7 + \mathrm{ind}\, x = 6\ (\mathrm{mod}\ 10)$

$\mathrm{ind}\, x = -1\ (\mathrm{mod}\ 10) \Rightarrow \mathrm{ind}\, x = 9\ (\mathrm{mod}\ 10) \Rightarrow x = 6\ (\mathrm{mod}\ 11)$

---

2) $x^{11} + 36 = 0\ (\mathrm{mod}\ 71)$ $n = 71$ $11\, \mathrm{ind}\, x = 29\ (\mathrm{mod}\ 70)$

$x^{11} = -36\ (\mathrm{mod}\ 71)$ $11\, \mathrm{ind}\, x = 99\ (\mathrm{mod}\ 70)$

$x^{11} = 35\ (\mathrm{mod}\ 71)$ $\mathrm{ind}\, x = 9\ (\mathrm{mod}\ 70)$

$\mathrm{ind}\, x^{11} = 29\ (\mathrm{mod}\ 70)$ $x = 47\ (\mathrm{mod}\ 71)$