Гл. 2. Быстр. вычисления

§2.1 Базовые алгоритмы (по Панкратовой)

§2.2. Алгоритмы умножения

$* U \in \mathbb{Z}$

Разлож. по основ. в : $U = \sum_{i=0}^{n-1} \underbrace{u_i}_{\in \mathbb{Z}_в} b^i \quad \| \quad U(X) = \sum_{i=0}^{n-1} u_i X^i$

$X \leftrightarrow в$ – не явл-ся изоморф.

$\mathbb{Z}_в[X] \not\cong \mathbb{Z}$

КТО:

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

$n_1, n_2, \dots, n_k$ – попарно вз. пр

Тогда ∃-ем общее реш. сист

по mod $n_1 \cdot n_2 \cdot \dots \cdot n_k$

① Метод Карацубы - Офмана

$\exists\ U(X),\ V(X) \in \mathbb{F}_p[X]$

$\deg U,\ \deg V \leq 2m-1$

$$U(X) = U_1(X)\cdot X^m + U_0(X)$$
$$V(X) = V_1(X)\cdot X^m + V_0(X)$$

$\deg U_1,\ \deg U_0,\ \deg V_1,\ \deg V_0 \leq m-1$

$$U\cdot V = U_1V_1\cdot X^{2m} +$$
$$+\Big((U_1+U_0)(V_1+V_0) - U_1V_1 - U_0V_0\Big)\cdot X^m +$$
$$+ U_0V_0$$

$\Rightarrow$ 3 умнож.

$$O\left(3^{\lfloor \log n+1\rfloor}\right) = O\left(n^{\log 3}\right) \approx O\left(n^{1,58}\right)$$

$$\times \begin{matrix} U_1X^m + U_0 \\ V_1X^m + V_0 \end{matrix}$$

$\Rightarrow$ 4 умнож. мн-ов ст. $m-1$

$$\left\{\begin{matrix} 1+X+X^2 \\ \times X^2 \end{matrix}\right. \Leftrightarrow (1;1;1;0;0)$$

$$X^2+X^3+X^4 \Leftrightarrow (0;0;1;1;1)$$

X $m > 2^b$

b - основание (разрядность).

② Метод Шенхаге

✱ $M = m_0 \cdot \ldots \cdot m_{k-1}$.

$$\mathbb{Z}/M\mathbb{Z} \cong \mathbb{Z}/m_0\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_{k-1}\mathbb{Z}$$

$\mathbb{Z}/M\mathbb{Z} = \mathbb{Z}_M$

✱ 2 числа длины $\leq \frac{\log M}{2}$.

(1) Переход к представл. сомножит. в $\mathbb{Z}/m_i\mathbb{Z}$

(2) Вычисл. произвед. сомножит. по mod m_i

(3) Восстановл. произвед. по кто по mod M.

∃ на вход подаем max разм. n ⇒

⇒ на выход размер $\leq 2n$

✱ k – попарно вз. пр. числ: $m_0, \ldots, m_{k-1}$ | ← на практике – степень двойки

$M = \prod_{i=0}^{k-1} m_i$ длины $> 2n$

Умножим U и V по mod N

‼ $M > (N-1)^2$.

(1) $U \equiv u_i \pmod{m_i}$

$V \equiv v_i \pmod{m_i}$ $\quad i = \overline{0; k-1}$

Вычисл. $M_i = m_0 \cdot \ldots \cdot m_{i-1} \cdot m_{i+1} \cdot \ldots \cdot m_{k-1}$

$N_i = M_i^{-1} \pmod{m_i}$

Нахожд. вычетов по mod m_i

$m_0; m_1; m_2; m_3; \dots, m_{k-2}; m_{k-1}$

- $m_0 m_1$; $m_2 m_3$; $m_4 m_5$; ...
- $m_0 m_1 m_2 m_3$; $m_4 m_5 m_6 m_7$; ..
- :

$$W = U \cdot V \equiv \sum_{i=0}^{k-1} w_i M_i N_i \pmod{M}$$

$$w_i \equiv W \pmod{m_i} \qquad (*)$$

] Известен вычет $X \pmod{m_0 m_1 m_2 m_3}$

представ. X по mod $m_0 m_1$ и $m_2 m_3$:

$X \equiv X_{01} \pmod{m_0 m_1}$; $X \equiv X_{23} \pmod{m_2 m_3}$

↓ ↓

$X_{01} \equiv X_0 \pmod{m_0}$ $X_{23} \equiv X_2 \pmod{m_2}$

$X_{01} \equiv X_1 \pmod{m_1}$ $X_{23} \equiv X_3 \pmod{m_3}$

Ускорение:

$w_i M_i N_i$ для разных i сум. много общ. множит. $\Rightarrow$ $m_0 m_1 \dots m_{\frac{k}{2}-1} \mid w_i M_i N_i$, $\frac{k}{2} \le i \le k-1$

$m_{\frac{k}{2}} m_{\frac{k}{2}+1} \dots m_{k-1} \mid w_i M_i N_i$, $0 \le i < \frac{k}{2}$

$\exists\ k = 2^t$

$$(*) \Rightarrow W \equiv \left(\sum_{i=0}^{\frac{k}{2}-1} w_i M_i N_i \right) \prod_{r=\frac{k}{2}}^{k-1} m_r \ \oplus \left(\sum_{i=\frac{k}{2}}^{k-1} w_i M_i N_i \right) \prod_{s=0}^{\frac{k}{2}-1} m_s \pmod M$$

Находим: $m_0 m_1$; $m_2 m_3$; …; $m_{k-2} m_{k-1}$

$m_0 m_1 m_2 m_3$; …; $m_{k-4} m_{k-3} m_{k-2} m_{k-1}$

$\exists\ x_{i,j} = \prod_{r=i}^{i+2^j-1} m_r$ – произвед. 2^j подряд идущих модулей, начиная с m_i.

Находим $y_{ij} = \sum_{r=i}^{i+2^j-1} \frac{x_{ij} N_r w_r}{m_r}$

↓

для ускорения вычисл

$y_{i0} = N_i w_i$

$y_{ij} = y_{i,j-1} \cdot x_{i+2^{j-1},j-1} + y_{i+2^{j-1},j-1} x_{i,j-1} \; ; \; j \geq 1$

$k = 2^t$

$y_{0t} = W$

$O(k \log k)$

Пример: $U = 31$; $V = 57$

$m_0 = 5$
$m_1 = 6$
$m_2 = 7$
$m_3 = 11$

$M = 2310$

Вычислим x_{ij} ; N_i

$x_{00} = 5$ $x_{01} = 30$ $N_0 = 3$
$x_{10} = 6$ $x_{21} = 77$ $N_1 = 1$
$x_{20} = 7$ $x_{02} = 2310$ $N_2 = 1$
$x_{30} = 11$ $N_3 = 1$

$U = (1, 1, 3, 9)$

$V = (2, 3, 1, 2)$

m_0 m_1 m_2 m_3

$\Rightarrow W = (2; 3; 3; 7)$

w_0 w_1 w_2 w_3

$y_{00} = w_0 N_0 = 6$

$y_{10} = w_1 N_0 = 3$

$y_{20} = w_2 N_2 = 3$

$y_{30} = w_3 N_3 = 7$

$y_{01} = 51$

$y_{21} = 82$

$y_{02} = 6387 \Rightarrow W \pmod M$

$W = 1767$