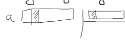
Деление многочленов

$O(\deg A \cdot \deg B) \to Q, R$ $\quad A = B \cdot Q + R$, $\deg R < \deg B$, $\deg Q = \deg A - \deg B$



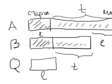
```
F a[n]   //deg=n-1
F b[m]
F q[n-m+1]
for (i = n-m; i >= 0; --i)
    q[i] = a[i+m] / b[m]
    for (j = 0; j <= m; j++)
        a[i+j] -= b[j] * q[i]
```

$O(m \cdot (n-m))$

q, $r = a$

Утв. $\deg A = n$, $\deg B = m$, $l = n-m+1 = \mathrm{len}(Q) = \deg + 1$

Тогда Q зависит только от
- l старш. коэфф. A
- $\min(l, \deg B + 1)$ старш. коэфф. B



Д-во 1). $(A + t) = BQ + (R + t)$

$\mathrm{len}(t) \le n + 1 - l = m$

$\deg t < m = \deg B$

2) • $\mathrm{len}(B) < l$

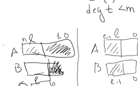
• $\mathrm{len}(B) \ge l$ $\quad \mathrm{len}(t) = m + 1 - l$, $\deg(t) \le m - l = 2m - n - 1$

$m + 1 \ge n - m + 1$, $2m \ge n$, $m \ge \frac{n}{2}$

$A = (B + t)Q + (R - (Qt))$

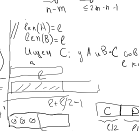
$\deg Qt = \deg Q + \deg t \le n - m + 2m - n - 1 = m - 1 = \deg B$ — ост?

$\deg Q = n - m$, $\deg t \le 2m - n - 1$



```
int* Div(int l, int* A, int* B) {      // len(A)=l
    C = Div(l/2, A[l/2:], B[l/2:])      // len(B)=l
    A' = A - (C*B)[l]                   // Ищем C: у A и B·C совп. первые l коэфф.
    D = Div(l/2, A', B[l/2:])
    return C·x^(l/2) + D
```

$l = 2^k$

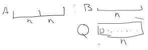


$T(l) = 2 \cdot T(l/2) + \mathrm{Mult} = 2 \cdot T(l/2) + O(l \log l) = O(l \log^2 l)$

Деление чисел

n — длина числа, k, $Base = 10^k$

$\frac{n}{k} = \#$ „цифр"

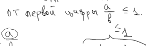


① Двоичное деление: $O(n^2/k)$

② Бинпоиск по Q, $\log Q = n$

$n \cdot \mathrm{Mult} \nearrow n^2 \log n$ FFT $\searrow n^3/k^2$

③ $\frac{n^2}{k^2}$



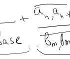
Узнать первую „большую цифру" частного.

$1 \le A < base$, $\quad a_n a_{n-1} \dots a_0$, $\quad x = \frac{a_n \cdot base + a_{n-1}}{b_m \cdot base + b_{m-1}}$ $\quad \overline{a_n a_{n-1}}$

$1 \le B < base$, $\quad b_m b_{m-1} \dots b_0$

Утв: x отл. от первой цифры $\frac{a}{b}$ ≤ 1.

$L = \frac{\overline{a_n a_{n-1}}}{\overline{b_m b_{m-1}} + 1/base} \le x$ $\quad L \le \frac{a}{b}$



$R = \frac{\overline{a_n, a_{n-1}} + 1/base}{\overline{b_m, b_{m-1}}} \ge x$ $\quad R \ge \frac{a}{b}$

$R - L = \frac{\overline{a_n, a_{n-1}}}{\overline{b_m b_{m-1}} + \frac{1}{base}} + \frac{1}{(\overline{b_m, b_{m-1}}) \cdot base} + \frac{\overline{a_n, a_{n-1}}}{\overline{b_m b_{m-1}}} =$

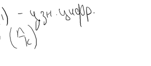
$= \overline{a_n a_{n-1}} \left(\frac{-\overline{b_m b_{m-1}} + \overline{b_m b_{m-1}} + \frac{1}{base}}{\overline{b_m b_{m-1}} \left(\overline{b_m, b_{m-1}} + \frac{1}{base} \right)} \right) + \frac{1}{\overline{b_m b_{m-1}}\, base} =$

$= \frac{\overline{a_n a_{n-1}}}{\overline{b_m b_{m-1}} \cdot base} \left(\frac{base}{\overline{b_m b_{m-1}} + \frac{1}{base}} + 1 \right) \le \frac{base^2 - 1}{base^2} \left(\frac{base}{base + 1} + 1 \right)$

(×base: $\overline{a_n a_{n-1}} \le base^2 - 1$; ×base: $\overline{b_m b_{m-1}} \ge base$, $\ge base^2$; $\overline{b_m b_{m-1}} + \frac{1}{base} \ge base + 1$)

$= \frac{base - 1}{base^2} \left(base + base + 1 \right) \le 2$

a : b



x−1, x, x+1

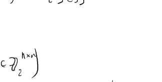
n/k шагов, ∀ шаг O(1) − узн. цифр. $O\left(\frac{n}{k}\right)$

$O\left(\frac{n^2}{k^2}\right)$

Зам. Можно доделать до $n \log^2 n$

Метод 4 русских

$A \cdot B = C$ — матр. $n \times n$



① $A, B, C \in \mathbb{Z}_2^{n \times n}$

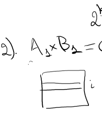
```
for (i = 0; i < n; ++i)
    for (int j = 0; j < n; ++j) if a[i][j] == 1:
        c[i] ^= b[j]
```

$O(n^3/w)$ (bitset)

② $A, B, C \in \mathbb{R}^{n \times n}$ $\quad (A \in \mathbb{Z}_2^{n \times n})$

$\forall A_{ij} \in \{0, 1\}$

$A \times B = \sum_{i=1}^{n/k} A_i \cdot B_i$



2^k

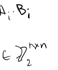
1). Переберем все возможные 2^k пот. строк матрицы A_1

$\vec{a} \times B_1 = $ строка $\vec{c}$

$f[mask] = \begin{cases} \vec{0 \dots 0} & mask = 00\dots0 \\ f[mask \wedge (1 \ll b)] + B_1[b], & mask \text{ содерж. } 1 \ll b \end{cases}$

$2^k \cdot n$

2). $A_1 \times B_1 = C_1$



$f[(A_1)_i] =: (C_1)_i$

$O(n^2)$

$\sum_{i=1}^{n/k} A_i \cdot B_i$ $\quad \frac{n}{k}(2^k \cdot n + n^2) = \frac{n}{\log n} n^2 = \frac{n^3}{\log n}$

$k = \log n$

③ $A, B, C \in \mathbb{Z}_2^{n \times n}$ $\quad \frac{n^3}{\log n \cdot w}$