Числовые алгоритмы

Число N, то оно задаётся $n = \log_2 N$ битов.

Сложение: $O(n)$

Умножение: $O(n^2)$, $O(n^{\log_2 3})$, $O(n \log n)$

```
Mult(a, b):
    if (b == 0)
        return 0
    z = Mult(a, ⌊b/2⌋)
    if (b mod 2 == 1)
        return 2z + a
    else
        return 2z
```

123	15
61	30
30	60
15	120
7	240
3	480
1	960

z

```
Div(a, b)
    if (a < b)
        return (0, a)
(q, z) = Div(⌊a/2⌋, b)
    q = 2·q
    z = 2·z
    if a mod 2 == 1:
        z = z + 1
    if z ≥ b:
        z = z − b
        q = q + 1
    return (q, z)
```

$O(n^2)$

```
Pow(a, k):
  if k = 0:
    return 1
  y = Pow(a, ⌊k/2⌋)
  if k mod 2 == 1
    return y^2 · a
  return y^2
```

В лоб $O(n^2 k)$

$n = \log_2 a$

$O(\log k)$ итераций

Сложность: $O((kn)^2 \log k)$

Модульная арифметика

Сложение: $O(n)$ $\quad n = \log_2 M$

$a + b \bmod M$

```
if (a+b) > M
  return a+b-M
```

Умножение: $O(n^2)$ (умножить и поделить)

Возведение в степень:

$O(n^2 \log k)$

$O(n^3)$

Деление:

Расширенный алгоритм Евклида

$d = НОД(a, b) = НОД(b, a \bmod b)$

$d = ax + by = bx' + (a \bmod b)\, y'$

$a \vdots d \quad b \vdots d$

$ax + by = bx' + \left(a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b\right) y'$

$ax + by = ay' + b\left(x' - \left\lfloor \frac{a}{b} \right\rfloor y'\right)$

```
E.Euclid (a, b)
  if b == 0
    return (1, 0, a)        // ax + by = d
  (x', y', d) ← E.Euclid (b, a mod b)
  return (y', x' - ⌊a/b⌋ y', d)
```

Если нужно a / b в кольце mod M:

$a \cdot b^{-1}$

b^{-1} существует $\Leftrightarrow$ НОД$(b, M) = 1$

E.Euclid $(b, M) \longrightarrow (b^{-1}, y, 1)$

Время работы алг. Евклида

Утв: если $a > b$, то $(a \bmod b) \le a/2$.

- $b \le a/2$

  $(a \bmod b) < b \le a/2$

- $b > a/2$

  $(a \bmod b) = a - b < a - a/2 = a/2$

$\Rightarrow$ # итераций в алг. Евклида $= O(n)$

Сложность $O(n \cdot n^2)$

$\Rightarrow$ Деление работает за $O(n^3)$

Числа Фибоначчи по модулю

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^N$$ за $O(\log N)$ арифм. операций

За $O(n^3)$ против $O(n\,N)$

2^n