Бінарний алгоритм піднесення до степеню

Котенко А.
ФВЕ

Суть алгоритму

Піднесення до степеню “в лоб”:

$a^n = a*a*...*a$ складність ~O(n)

Очевидно, можна використовувати вже пораховані степені.

Наприклад, порахувати x^{16} можна наступним чином:

$x*x=x^2$

$x^2*x^2=x^4$

$x^4*x^4=x^8$

$x^8*x^8=x^{16}$

Види алгоритму

- "Зліва направо":

Степінь представляється в бінарному вигляді:

$n=(m_k m_{k-1}\ldots m_1 m_0)_2$

$n=2^k*m_k+2^{k-1}*m_{k-1}+\ldots+2^1*m_1+2^0*m_0$

$x^n=x\hat{}(\ (\ (2*m_k +m_{k-1})*2 + m_{k-2})*2 +\ldots)*2 + m_1)*2 + m_0)$

Наприклад:

$3^{13}=3^{1101_2}=3^{8*1+4*1+2*0+1*1}=3^8 * 3^4 * 3^1=$

$=3^{(\ (\ (\ (2*1)+1\ )*2+0)*2+1)}=$

$=(\ (\ (3^1)^2 *3^1)^2 *3^0)^2 *3^1$

Види алгоритму

- “Справа наліво”:

Біти степені читаються за остачею від ділення на 2, і відповідно до значення:

- **Змінна підноситься до квадрату, якщо остача нульова**
- **Змінна підноситься до квадрату та множиться на х**

Складність ~ [ln(n)] + g(n) = O(ln(n))

Види алгоритму

- "Справа наліво":

Наприклад: 3^{13}

Позначимо змінну як z, тоді

$13\%2 = 1 \rightarrow z=(3^2)*3=27$

$6\%2 = 0 \rightarrow z=27^2=729$

$3\%2 = 1 \rightarrow z=(729^2)*3=1594323$

$1\%2 = 1 \rightarrow z=(1594323^2)*3$

Обережно

АЛГОРИТМ НЕ Є НАЙШВИДШИМ!!!!! 11!!!1!!

Контр-приклад: x^{15}

Алгоритм дає $(((x)^2 * x)^2 * x)^2 * x$ - 6 дій

Але можна здогадатися
$(x*x*x)*((x*x*x)^2)^2$ - 5 дій

Застосування (1)

- Розрахування x^n mod m

Оскільки
(a*b) mod m = ((a mod m)*(b mod m)) mod m

то можна застосовувати алгоритм, лише замінивши всі операції множення на множення остач від m

Застосування (2)

- Геометричні перетворення точок:

$$\begin{pmatrix} x & y & z & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} = \begin{pmatrix} x' & y' & z' & 1 \end{pmatrix}$$

Зсув:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 5 & 7 & 9 & 1 \end{pmatrix}$$

Поворот:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta & 0 \\ 0 & \sin\theta & \cos\theta & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Скейл:

$$\begin{pmatrix} 10 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Застосування

Тобто алгоритм можна використовати в задачах, де необхідно багато раз повторити одну дію.

Але немає гарантії, що він буде оптимальним.