分治:乘法运算

原创 李伟杰 LOA算法学习笔记 2021-01-29 16:10

01 问题描述

给定两个整数 x,y，计算乘积x×y。

02 解决方案

2.1 小学乘法

Divide:$x = x_h \times 10^{\frac{n}{2}} + x_l, y = y_h \times 10^{\frac{n}{2}} + y_l$

Conquer:计算$x_h y_h, x_l y_h, x_h y_l, x_l y_l$

Combine:$xy = \left(x_h \times 10^{\frac{n}{2}} + x_l\right)\left(y_h \times 10^{\frac{n}{2}} + y_l\right) = x_h y_h 10^n + (x_l y_h + x_h y_l)10^{\frac{n}{2}} + x_l y_l$

- 例子：x=12,y=34

$$x = 12 = 1 \times 10 + 2，\ y = 34 = 3 \times 10 + 4$$

$$x \times y = (1 \times 3) \times 10^2 + \big((1 \times 4) + (2 \times 3)\big) \times 10 + 2 \times 4 = 408$$

其中，有 4 个子问题，3 次加法，2 次移位。
算法复杂度为：

$$T(n) = 4T\left(\frac{n}{2}\right) + O(n) = O(n^2)$$

2.2 Karatsuba乘法

Divide:$x = x_h \times 10^{\frac{n}{2}} + x_l, y = y_h \times 10^{\frac{n}{2}} + y_l$

Conquer:计算$x_h y_h, x_l y_l, P = (x_h + x_l)(y_h + y_l)$

Combine:$xy = \left(x_h \times 10^{\frac{n}{2}} + x_l\right)\left(y_h \times 10^{\frac{n}{2}} + y_l\right) = x_h y_h 10^n + (P - x_h y_h - x_l y_l)10^{\frac{n}{2}} + x_l y_l$

- 例子：x=12,y=34

其中，有 3 个子问题，6 次加法，2 次移位。
算法复杂度为：

2.3 Toom-Cook乘法

Toom-Cook的原理是，对于给定的两个大整数a和b，将a和b分成k个较小的部分，每个部分长度为l，并对这些子部分执行运算，其复杂度为 $O(n^{\frac{log2k-1}{logk}})$ 。

- 例子：以Toom-3算法为例,即k=3时,取m=123,n=456,基数B=10

1) 拆分

$$m_2 = 1, m_1 = 2, m_0 = 3, n_2 = 4, n_1 = 5, n_0 = 6$$

$$p(x) = x^2 + 2x + 3, q(x) = 4x^2 + 5x + 6$$

2) 求值：取最简单的 5 个点0,−1,1,−2, ∞

$$p(0) = 3, p(-1) = 2, p(1) = 6, p(-2) = 3, p(\infty) = m_2 = 1$$

$$q(0) = 6, q(-1) = 5, q(1) = 15, q(-2) = 12, q(\infty) = n_2 = 4$$

3) 点乘

$$r(0) = 18, r(-1) = 10, r(1) = 90, r(-2) = 36, r(\infty) = 4$$

4) 插值

$$\begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix} = \begin{pmatrix} 0^0 & 0^1 & 0^2 & 0^3 & 0^4 \\ 1^0 & 1^1 & 1^2 & 1^3 & 1^4 \\ (-1)^0 & (-1)^1 & (-1)^2 & (-1)^3 & (-1)^4 \\ (-2)^0 & (-2)^1 & (-2)^2 & (-2)^3 & (-2)^4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} r(0) \\ r(1) \\ r(-1) \\ r(-2) \\ r(\infty) \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{3} & -1 & \frac{1}{6} & -2 \\ -1 & \frac{1}{2} & \frac{1}{2} & 0 & -1 \\ -\frac{1}{2} & \frac{1}{6} & \frac{1}{2} & -\frac{1}{6} & 2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} r(0) \\ r(1) \\ r(-1) \\ r(-2) \\ r(\infty) \end{pmatrix}$$

有以下计算步骤，

$$r_0 \leftarrow r(0) = 18, r_4 \leftarrow r(\infty) = 4$$

$$r_3 \leftarrow \frac{r(-2) - r(1)}{3} = -18, r_1 \leftarrow \frac{r(1) - r(-1)}{2} = 40, r_2 \leftarrow r(-1) - r(0) = -8$$

$$r_3 \leftarrow \frac{r_2 - r_3}{2} + 2r(\infty) = 13$$

$$r_2 \leftarrow r_2 + r_1 - r_4 = 28$$

$$r_1 \leftarrow r_1 - r_3 = 27$$

$$\therefore r(x) = 4x^4 + 13x^3 + 28x^2 + 27x + 18$$

5) 重组

$$r(B) = r(10) = 40000 + 13000 + 2800 + 270 + 18 = 56088$$

∴123×456=56088，验证正确

03 总结

Toom-Cook乘法采用的是分治的思想，把大整数分解成k个部分进行求解。Karatsuba算法实际是Toom-Cook算法k=2的特例，而长乘法是k=1时的特例。在密码方案的实现中，乘法往往采用Toom-4和Karatsuba算法相结合的方式进行运算。