Karatsuba 法

基数を R で表すとき、長さ $2n$ の 2 つの多倍長整数 A, B は次のように表される。

$$A = a_{2n-1}R^{2n-1} + a_{2n-2}R^{2n-2} + \cdots + a_1R + a_0$$
$$B = b_{2n-1}R^{2n-1} + b_{2n-2}R^{2n-2} + \cdots + b_1R + b_0$$

通常の筆算法で積 AB を計算する場合、各桁同士それぞれ乗算が必要になるので、トータルで $(2n)^2$ 回の乗算が必要になる。（これを計算量 $O((2n)^2)$ と表す）

そこで、以下のように A, B それぞれを左右（上位と下位）の 2 つに分解して考えてみる。

$$\begin{aligned} A &= (a_{2n-1}R^{n-1} + \cdots + a_n)R^n + (a_{n-1}R^{n-1} + \cdots + a_0) \\ &= A_1R^n + A_0 \\ B &= (b_{2n-1}R^{n-1} + \cdots + b_n)R^n + (b_{n-1}R^{n-1} + \cdots + b_0) \\ &= B_1R^n + B_0 \end{aligned}$$

（ただし、$A_1 = a_{2n-1}R^{n-1} + \cdots + a_n,\ A_0 = a_{n-1}R^{n-1} + \cdots + a_0,$
$B_1 = b_{2n-1}R^{n-1} + \cdots + b_n,\ B_0 = b_{n-1}R^{n-1} + \cdots + b_0$ ）

となり、基数 R^n の 2 桁同士の乗算と考えることができる。

しかし、これでも筆算法では $2^2(=4)$ 回の乗算が必要なるので、以下のように変形する。

$$\begin{aligned} AB &= (A_1R^n + A_0)(B_1R^n + B_0) \\ &= A_1B_1R^{2n} + (A_1B_0 + A_0B_1)R^n + A_0B_0 \\ &= A_1B_1R^{2n} + \{(A_1 + A_0)(B_1 + B_0) - A_1B_1 - A_0B_0\}R^n + A_0B_0 \\ &= A_1B_1R^{2n} + (VW - A_1B_1 - A_0B_0)R^n + A_0B_0 \\ &\quad (\text{ただし、} V = A_1 + A_0, W = B_1 + B_0) \end{aligned}$$

これで、乗算は A_1B_1, A_0B_0, VW の 3 回になる。

通常はこのアルゴリズムを再帰的に使用する。そして、n 桁同士の乗算の計算量は一般的に、

$$O(3^{\log_2 n}) = O(n^{\log_2 3}) \simeq O(n^{1.585})$$

となる。