Toom-Cook 法

基数を R で表すとき、d 分割した多倍長整数 A, B と積 $C(=AB)$ は次のように表される。

$$\begin{aligned} A &= a_{d-1}R^{d-1} + a_{d-2}R^{d-2} + \cdots + a_1R + a_0 \\ B &= b_{d-1}R^{d-1} + b_{d-2}R^{d-2} + \cdots + b_1R + b_0 \\ AB = C &= c_{2d-2}R^{2d-2} + c_{2d-3}R^{2d-3} + \cdots + c_1R + c_0 \end{aligned}$$

基数 R を多項式の変数 x、A, B を関数 $a(x), b(x)$ と考えると、

$$\begin{aligned} a(x) &= a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1x + a_0 \\ b(x) &= b_{d-1}x^{d-1} + b_{d-2}x^{d-2} + \cdots + b_1x + b_0 \\ c(x) &= c_{2d-2}x^{2d-2} + c_{2d-3}x^{2d-3} + \cdots + c_1x + c_0 \end{aligned}$$

となる。Karatsuba 法 $(d=2)$ の場合は、

$$\begin{aligned} c(x) &= c_2x^2 + c_1x + c_0 \\ (\text{ 但し、} c_2 &= a_1b_1 \\ c_1 &= a_1b_0 + a_0b1 = (a_1+a_0)(b_1+b_0) - a_1b_1 - a_0b_0 \\ c_0 &= a_0b_0 \ ) \end{aligned}$$

となり、c_2, c_1, c_0 が求まれば $C(=AB)$ が求まった。（乗算回数は 3 回）

次に、$d=3$ の場合で考えてみる。$a(x), b(x)$ は、

$$a(x) = a_2x^2 + a_1x + a_0$$
$$b(x) = b_2x^2 + b_1x + b_0$$

となり、$a(x), b(x)$ の積 $c(x)$ は、

$$c(x) = a(x)b(x) = (a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0) \quad (1)$$
$$= c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 \quad (2)$$

(但し、$c_4 = a_2b_2$
$c_3 = a_2b_1 + a_1b_2$
$c_2 = a_2b_0 + a_1b_1 + a_0b_2$
$c_1 = a_1b_0 + a_0b_1$
$c_0 = a_0b_0$)

となる。c_4, c_3, c_2, c_1, c_0 が求まれば AB が求まるわけだが、単純に計算すると 9 回の乗算が必要となり標準（筆算）法と変わらない。そこで、別の方法で c_4, c_3, c_2, c_1, c_0 を求めることにする。

まず、(2) の式に $-2, -1, 0, 1, 2$ を代入する。

$$c(-2) = 16c_4 - 8c_3 + 4c_2 - 2c_1 + c_0 \quad (3)$$
$$c(-1) = c_4 - c_3 + c_2 - c_1 + c_0 \quad (4)$$
$$c(0) = c_0 \quad (5)$$
$$c(1) = c_4 + c_3 + c_2 + c_1 + c_0 \quad (6)$$
$$c(2) = 16c_4 + 8c_3 + 4c_2 + 2c_1 + c_0 \quad (7)$$

この (3)〜(7) の連立 5 元 1 次方程式を解いて、c_4, c_3, c_2, c_1, c_0 が求まれば、(2) すなわち、A と B の積が求まることになる。

実際に、(3)〜(7) の連立 5 元 1 次方程式を解てみると、

$$c_4 = (c(-2) - 4c(-1) + 6c(0) - 4c(1) + c(2)) \ / \ 24 \quad (8)$$
$$c_3 = (-c(-2) + 2c(-1) - 2c(1) + c(2)) \ / \ 12 \quad (9)$$
$$c_2 = (-c(-2) + 16c(-1) - 30c(0) + 16c(1) - c(2)) \ / \ 24 \quad (10)$$
$$c_1 = (c(-2) - 8c(-1) + 8c(1) - c(2)) \ / \ 12 \quad (11)$$
$$c_0 = c(0) \quad (12)$$

となる。

$c(-2), c(-1), c(0), c(1), c(2)$ は、(1) の式より

$$c(-2) = a(-2)b(-2) = (4a_2 - 2a_1 + a_0)(4b_2 - 2b_1 + b_0) \quad (13)$$
$$c(-1) = a(-1)b(-1) = (a_2 - a_1 + a_0)(b_2 - b_1 + b_0) \quad (14)$$
$$c(0) = a(0)b(0) = a_0b_0 \quad (15)$$
$$c(1) = a(1)b(1) = (a_2 + a_1 + a_0)(b_2 + b_1 + b_0) \quad (16)$$
$$c(2) = a(2)b(2) = (4a_2 + 2a_1 + a_0)(4b_2 + 2b_1 + b_0) \quad (17)$$

と求まる。（ここでの加減算回数は 16 回、乗算回数は 5 回）

(13)〜(17) の値を (8)〜(12) に代入すれば、c_4, c_3, c_2, c_1, c_0 が求まり、(2) すなわち、A と B の積が求まったことになる。

加減算は乗算より計算コストは小さいものの、もう少し演算回数を減らすことを考えてみる。

$c(2)$ の代わりに $c(\infty)$ を考える。

$$a'(x) = \frac{a(x)}{x^2},\ b'(x) = \frac{b(x)}{x^2}$$

とし、それぞれを $x \to \infty$ としたものを $a(\infty), b(\infty)$ とすることにする。すなわち、

$$a(\infty) = \lim_{x\to\infty} a' = \lim_{x\to\infty} \frac{a(x)}{x^2} = \lim_{x\to\infty} \frac{a_2x^2 + a_1x + a_0}{x^2} = a_2$$
$$b(\infty) = \lim_{x\to\infty} b' = \lim_{x\to\infty} \frac{b(x)}{x^2} = \lim_{x\to\infty} \frac{b_2x^2 + b_1x + b_0}{x^2} = b_2$$

よって、

$$c(-2) = a(-2)b(-2) = (4a_2 - 2a_1 + a_0)(4b_2 - 2b_1 + b_0) \tag{18}$$
$$c(-1) = a(-1)b(-1) = (a_2 - a_1 + a_0)(b_2 - b_1 + b_0) \tag{19}$$
$$c(0) = a(0)b(0) = a_0b_0 \tag{20}$$
$$c(1) = a(1)b(1) = (a_2 + a_1 + a_0)(b_2 + b_1 + b_0) \tag{21}$$
$$c(\infty) = a(\infty)b(\infty) = a_2b_2 \tag{22}$$

となる。（ここでの加減算回数は 12 回、乗算回数は 5 回）