FAST MULTIPLICATION

$a = (a_{n-1}, a_{n-2}, \ldots, a_1, a_0)_B$

$b = (b_{n-1}, b_{n-2}, \ldots, b_1, b_0)_B$

Add/subtract a, b : $O(n)$ built-in integer additions

Multiply a, b (schoolbook method): $O(n^2)$ built-in integer multiplications

Karatsuba-Ofman [1962]

$$a = a_{n-1} B^{n-1} + a_{n-2} B^{n-2} + \ldots + a_1 B + a_0$$
$$= A_1 B^{n/2} + A_0$$

$$b = b_{n-1} B^{n-1} + b_{n-2} B^{n-2} + \ldots + b_1 B + b_0$$
$$= B_1 B^{n/2} + B_0$$

Assume n is even

$$ab = (A_1 B + A_0)(B_1 B + B_0)$$

$$= \underline{A_1 B_1} B^2 + (\underline{A_1 B_0} + \underline{A_0 B_1}) B + \underline{A_0 B_0}$$

A_1, B_1, A_0, B_0 : $\frac{n}{2}$-digit integers

$\boxed{A_1 B_1, (A_1 B_0 + A_0 B_1), A_0 B_0 \text{ : can be computed using only } 3 \ \tfrac{n}{2}\text{-digit integer multiplications}}$

$$A_1 B_1, \quad A_0 B_0, \quad \underbrace{(A_1 + A_0)(B_1 + B_0)}_{U} \quad \underbrace{(A_1 - A_0)(B_1 - B_0)}_{V}$$

$$ab = A_1 B_1 B^2 + \underline{(U - A_0 B_0 - A_1 B_1)} B + A_0 B_0$$

$$(-V + A_0 B_0 + A_1 B_1)$$

$T(n)$: time required to compute a, b

$$T(n) = 3T\left(\frac{n}{2}\right) + O(n)$$

$$T(n) = \Theta\left(n^{1.585}\right)$$

Toom-Cook Multiplication (Toom-2)

$a = A_1 X + A_0$ $\qquad b = B_1 X + B_0$ $\qquad X$: indeterminate

$c = ab = C_2 X^2 + C_1 X + C_0$

$c(k) = a(k)\, b(k)$

$k = \infty, 0, 1$

$p(x)$: polynomial in variable x

$p(\infty) = \lim_{x \to \infty} \frac{p(x)}{x^{\deg p(x)}}$

= leading coeff of $p(x)$

Karatsuba of/main version 1

$$\begin{cases} c(\infty) = a(\infty)b(\infty) = A_1 B_1 = C_2 \\ c(0) = a(0)\, b(0) = A_0 B_0 = C_0 \\ c(1) = a(1)\, b(1) = (A_1 + A_0)(B_1 + B_0) = C_2 + C_1 + C_0 \end{cases}$$

Suppose I choose $k = \infty, 0, -1$

K-O version 2

$$c(-1) = a(-1) b(-1) = (A_0 - A_1)(B_0 - B_1) = C_2 - C_1 + C_0$$

Toom-3

$$R = B^m \qquad m = \left\lceil \frac{n}{3} \right\rceil$$

$$a = A_2 R^2 + A_1 R + A_0$$

$$b = B_2 R^2 + B_1 R + B_0$$

$$c = ab = C_4 R^4 + C_3 R^3 + C_2 R^2 + C_1 R + C_0$$

$$C_4 \to A_2 B_2$$

$$C_3 \to A_2 B_1 + A_1 B_2$$

$$C_2 \to A_2 B_0 + A_1 B_1 + A_0 B_2$$

$$C_1 \to A_1 B_0 + A_0 B_1$$

$$C_0 \to A_0 B_0$$

School-book → 9 products of $\frac{n}{3}$-digit integers

Toom-3 → 5 $\frac{n}{3}$-digit multiplications!

Evaluate $c(k) = a(k)\,b(k)$ at $k = \infty, 0, 1, -1, -2$

$$
\begin{aligned}
c(\infty) &= C_4 &&= A_2 B_2 \\
c(0) &= C_0 &&= A_0 B_0 \\
c(1) &= C_4 + C_3 + C_2 + C_1 + C_0 &&= (A_2 + A_1 + A_0)(B_2 + B_1 + B_0) \\
c(-1) &= C_4 - C_3 + C_2 - C_1 + C_0 &&= (A_2 - A_1 + A_0)(B_2 - B_1 + B_0) \\
c(-2) &= 16C_4 - 8C_3 + 4C_2 - 2C_1 + C_0 &&= (4A_2 - 2A_1 + A_0)(4B_2 - 2B_1 + B_0)
\end{aligned}
$$

5 $\frac{n}{3}$-digit number multiplications.

$$
\begin{bmatrix} c(\infty) \\ c(0) \\ c(1) \\ c(-1) \\ c(-2) \end{bmatrix}
=
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 \\
16 & -8 & 4 & -2 & 1
\end{bmatrix}
\begin{bmatrix} C_4 \\ C_3 \\ C_2 \\ C_1 \\ C_0 \end{bmatrix}
$$

All C_i's will evaluate to integer values

$$
\begin{bmatrix} C_4 \\ C_3 \\ C_2 \\ C_1 \\ C_0 \end{bmatrix}
=
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
2 & -\frac{1}{2} & \frac{1}{6} & \frac{1}{2} & -\frac{1}{6} \\
-1 & -1 & \frac{1}{2} & \frac{1}{2} & 0 \\
-2 & \frac{1}{2} & \frac{1}{3} & -1 & \frac{1}{6} \\
0 & 1 & 0 & 0 & 0
\end{bmatrix}
\begin{bmatrix} c(\infty) \\ c(0) \\ c(1) \\ c(-1) \\ c(-2) \end{bmatrix}
$$

involves multiplications & divisions by single-digit integers $O(n)$-time

Sub-products may also be computed recursively using Toom-3

Running time:

$$T(n) = 5T\left(\frac{n}{3}\right) + O(n)$$

$$= \Theta\left(n^{\log_3 5}\right) = \Theta\left(n^{1.465}\right)$$

<u>Toom-k</u>

$$O\left(d(k)\, n^{\log(2k-1)/\log k}\right)$$

Schönhage-Strassen: $O(n \log n \log \log n)$

FFT-based Multiplication

a, b : n-digit base-B integers

$$2^{t-1} < n \leq 2^{t} \qquad N = 2^{t+1}$$

Pad a, b with leading 0's to make them N-digit long.

$$a = (a_{N-1}, a_{N-2}, \dots, a_1, a_0)_B \qquad b = (b_{N-1}, b_{N-2}, \dots, b_1, b_0)_B$$

Cyclic convolution of the 2 sequences a, b

$$c = (c_{N-1}, c_{N-2}, \dots, c_1, c_0)$$

$$c_k = \sum_{\substack{0 \leq i, j \leq N-1 \\ i+j = k \bmod N}} a_i b_j \quad \text{for } k \in \{0, 1, \dots, N-1\}$$

$$c_k = \sum_{\substack{0 \le i,j \le N-1 \\ i+j=k \text{ or } i+j=k+N}} a_i b_j$$

$k \in \{0,1,\dots,N-1\}$

$a_i = b_j = 0$ for $\frac{N}{2} \le i,j < N$

$$c_k = \boxed{\sum_{\substack{0 \le i,j \le k \\ i+j=k}} a_i b_j}$$

k^{th} B-ary digit (from right) of $ab = c$

$$\sum_{\substack{0 \le i,j \le N-1 \\ i+j=k \text{ or } i+j=k+N}} a_i b_j$$

$$= a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0 + \underbrace{(a_{N-1} b_{k+1} + a_{N-2} b_{k+2} + \dots + a_{k+1} b_{N-1})}_{0}$$

$$\Rightarrow \quad ab = c_{N-1} B^{N-1} + c_{N-2} B^{N-2} + \dots + c_1 B + c_0$$

ω_N : primitive N^{th} root of unity (defined based on the field in which we work)

In $\mathbb{C}$, $\omega_N = e^{i2\pi/N}$, $i \in \sqrt{-1}$

Discrete Fourier Transform (DFT) of seq $(a_{N-1}, \ldots, a_1, a_0)$ is given by $(A_{N-1}, A_{N-2}, \ldots, A_1, A_0)$

$$A_k = \sum_{0 \le j \le N} (\omega_N^k)^j a_i$$ → polynomial a evaluated at ω_N^k

$(B_{N-1}, \ldots, B_0)$: DFT of $(b_{N-1}, \ldots, b_1, b_0)$

$(C_{N-1}, \ldots, C_0)$: DFT of $(c_{N-1}, \ldots, c_1, c_0)$

$C_k = \underline{A_k B_k}$ for all $k = 0, 1, \ldots, N-1$

Computing $(c_{N-1}, \ldots, c_0)$ from $(C_{N-1}, \ldots, C_0)$

$$\underline{(\hat{C}_{N-1}, \ldots, \hat{C}_1, \hat{C}_0)} : \text{DFT of } (C_{N-1}, \ldots, C_0)$$

$$(c_{N-1}, \ldots, c_0) = \frac{1}{N}(\hat{C}_1, \hat{C}_2, \ldots, \hat{C}_{N-1}, \hat{C}_0)$$

Inverse DFT

$$(C_{N-1}, \ldots, C_0) : \text{DFT } (c_{N-1}, \ldots, c_0)$$

$$\underline{c_k} = \frac{1}{N}\sum_{j=0}^{N-1} C_j \omega_N^{-kj}$$

Naive method (i.e. computing all products $A_k B_k$)

$O(N^2)$ time

FAST FOURIER TRANSFORM

$$a = a^{(e)}(B^2) + B \times a^{(o)}(B^2)$$

$$a^{(e)} = a_{N-2} B^{N/2 - 1} + a_{N-4} B^{\frac{N}{2}-2} + \dots + a_2 B + a_0$$ → coefficient in even positions of a

$$a^{(o)} = a_{N-1} B^{\frac{N}{2}-1} + a_{N-3} B^{\frac{N}{2}-2} + \dots + a_3 B + a_1$$ → odd positions of a.

Recursively compute

FFT (DFT)

$$\left(A^{(e)}_{\frac{N}{2}-1}, A^{(e)}_{\frac{N}{2}-2}, \dots, A^{(e)}_1, A^{(e)}_0\right) \text{ of } a^{(e)}$$

$$\left(A^{(o)}_{\frac{N}{2}-1}, A^{(o)}_{\frac{N}{2}-2}, \dots, A^{(o)}_1, A^{(o)}_0\right) \text{ of } a^{(o)}$$

$\omega_{\frac{N}{2}} = \omega_N^2$ is a primitive $\frac{N}{2}$-th root of unity.

for $k = 0, 1, \ldots, \frac{N}{2} - 1$, we have

$$O(N) \text{ field operations } \left\{ \begin{array}{l} A_k = A_k^{(e)} + \omega_N^k A_k^{(o)} \\ \hline A_{\frac{N}{2}+k} = A_k^{(e)} - \omega_N^k A_k^{(o)} \end{array} \right.$$

$$A_k = \sum_{j=0}^{N-1} (\omega_N^k)^j a_j$$

$$= \sum_{\substack{j \text{ even} \\ 0 \le j \le N-1}} (\omega_N^k)^j a_j + \sum_{\substack{j \text{ odd} \\ 0 \le j \le N-1}} (\omega_N^k)^j a_j$$

$$= \sum_{j \text{ even}} (\omega_N^2)^{k\, j/2} a_j + \sum_{j \text{ even}} \omega_N^k (\omega_N^{kj}) a_{j+1}$$

$$= \underbrace{\sum_{0 \le \ell \le \frac{N}{2}-1} (\omega_{\frac{N}{2}})^{k\ell} a_\ell^{(e)}}_{} + \omega_N^k \underbrace{\sum_{0 \le \ell \le \frac{N}{2}-1} (\omega_{\frac{N}{2}})^{k\ell} a_\ell^{(o)}}_{}$$

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

$$= \Theta(N \log N) = \Theta(n \log n)$$

no. of field operations

Complex field : running time $O(n \log n \log\log n \log\log\log n \ldots)$

Schönhage-Strassen : running time $O(n \log n \log\log n)$

Only integer arithmetic suffices

Work in $\mathbb{Z}_{2^s+1}$ (for some suitable s)

Use 2 as the $2s$-th root of unity