Polynomials

$$p(x) = 3x^7 + 5x^6 + 3x + 1$$

$$A(x) = \sum_{j=0}^{n-1} a_j x^j$$

coefficients

Polynomial addition:

$$
\begin{array}{rcccccccc}
P(x) = & 3x^7 & + 5x^6 & + 0x^5 & + 0x^4 & + 0x^3 & + 0x^2 & + 3x & + 1 \\
Q(x) = & & 6x^6 & + 1x^5 & + 0x^4 & + 0x^3 & + 1x^2 & + 10x & + 0 \\
\hline
& 3x^7 & + 11x^6 & + 1x^5 & + 0x^4 & + 0x^3 & + 1x^2 & + 13x & + 1
\end{array}
$$

$$A(x) = \sum_{j=0}^{n-1} a_j x^j, \qquad B(x) = \sum_{j=0}^{n-1} b_j x^j,$$

$$C(x) = A(x) + B(x) = \sum_{j=0}^{n-1} (a_j + b_j) x^j$$

Polynomial multiplication:

$$A(x) = 6x^3 + 7x^2 - 10x + 9$$

$$B(x) = -2x^3 + 4x - 5$$

$$
\begin{array}{rrrrrrr}
 & & & 6x^3 & +7x^2 & -10x & +9 \\
 & & & -2x^3 & & +4x & -5 \\
\hline
 & & & -30x^3 & -35x^2 & +50x & -45 \\
 & & 24x^4 & +28x^3 & -40x^2 & +36x & \\
-12x^6 & -14x^5 & +20x^4 & -18x^3 & & & \\
\hline
-12x^6 & -14x^5 & +44x^4 & -20x^3 & -75x^2 & +86x & -45
\end{array}
$$

$$C(x) = \sum_{j=0}^{2n-2} c_j x^j, \quad C(x) = A(x) \cdot B(x)$$

$$c_j = \sum_{k=0}^{j} a_k b_{j-k}, \quad \text{degree}(C) = \text{degree}(A) + \text{degree}(B)$$

Convolution

$$c_j = a_0 b_j + a_1 b_{j-1} + a_2 b_{j-2} + \cdots + a_{j-1} b_1 + a_j \cdot b_0$$

Point-value representation of polynomials:

$A(x)$: a polynomial of degree-bound n (i.e. degree $< n$)

$\{(x_0, y_0), (x_1, y_1), \cdots, (x_{n-1}, y_{n-1})\}$ is called the point-value representation of $A(x)$ if

$y_k = A(x_k)$ and all of the x_k are distinct.

$$A(x) = \sum_{j=0}^{n-1} a_j x^j$$

$$A(x_0) = a_0 + a_1 x_0 + a_2 x_0^2 + a_3 x_0^3 + \cdots + a_{n-1} x_0^{n-1} \quad O(n^2) \text{ time}$$

$$= a_0 + x_0 (a_1 + a_2 x_0 + a_3 x_0^2 + \cdots + a_{n-1} x_0^{n-2})$$

$$= a_0 + x_0 (a_1 + x_0 (a_2 + a_3 x_0 + \cdots + a_{n-1} x_0^{n-3}))$$

$$= a_0 + x_0 (a_1 + x_0 (a_2 + x_0 (a_3 + \cdots + x_0 (a_{n-2} + x_0 a_{n-1}))))$$

Horner's rule. $\quad \underline{O(n) \text{ time}}$

$$P(x) = 5 + 6x + 3x^2 + 4x^3$$

$$= 5 + x(6 + x(3 + x \cdot 4))$$

Interpolation :

Given $\{(x_0, y_0), \cdots, (x_{n-1}, y_{n-1})\}$, calculate

$a_0, a_1, \cdots, a_{n-1}$ where $A(x) = \sum_{j=0}^{n-1} a_j x^j$ and $y_k = A(x_k)$.

Theorem 30.1 (Uniqueness of an interpolating polynomial)

For any set $\{(x_0, y_0), \cdots, (x_{n-1}, y_{n-1})\}$ such that

x_k are distinct, there is a unique polynomial $A(x)$

of degree $< n$ such that $y_k = A(x_k)$ for $0 \le k < n$.

Lagrange's formula :

$$A(x) = \sum_{k=0}^{n-1} y_k \cdot \frac{\prod_{j \ne k} (x - x_j)}{\prod_{j \ne k} (x_k - x_j)}$$

coefficient representation $\Longleftrightarrow$ point-value representation

$$A(x) = \sum_{j=0}^{n-1} a_j x^j \qquad (x_k, y_k) \quad 0 \le k < n$$

$$y_k = A(x_k)$$

Polynomial operations through point-value representations

① addition : $C(x) = A(x) + B(x) \Rightarrow C(x_k) = A(x_k) + B(x_k)$

$A(x) : \{(x_0, y_0), (x_1, y_1), \cdots, (x_{n-1}, y_{n-1})\}$

$B(x) : \{(x_0, y_0'), (x_1, y_1'), \cdots, (x_{n-1}, y_{n-1}')\}$

$\Rightarrow C(x) : \{(x_0, y_0 + y_0'), (x_1, y_1 + y_1'), \cdots, (x_{n-1}, y_{n-1} + y_{n-1}')\}$

O(n) time

② multiplication

$$\underset{<2n}{C(x)} = \underset{<n}{A(x)} \cdot \underset{<n}{B(x)} \Rightarrow C(x_k) = A(x_k) \cdot B(x_k)$$

$A(x)$: $(x_0, y_0), (x_1, y_1), \cdots, (x_{2n-1}, y_{2n-1})$

$B(x)$: $(x_0, y_0'), (x_1, y_1'), \cdots, (x_{2n-1}, y_{2n-1}')$

$\Rightarrow C(x)$: $(x_0, y_0 y_0'), (x_1, y_1 y_1'), \cdots, (x_{2n-1}, y_{2n-1} \cdot y_{2n-1}')$

$O(n)$ time

Summary:

$$
\begin{array}{ccc}
\begin{matrix} a_0, a_1, \cdots, a_{n-1} \\ b_0, b_1, \cdots, b_{n-1} \end{matrix} & \xrightarrow[\text{time} = \Theta(n^2)]{\text{Ordinary multiplication}} & c_0, c_1, \cdots, c_{2n-2} \\
\Big\downarrow \begin{matrix} \text{Evaluation (DFT)} \\ \Theta(n \lg n) \end{matrix} & & \Big\uparrow \begin{matrix} \text{Interpolation} \\ \Theta(n \lg n) \\ \text{(IDFT)} \end{matrix} \\
\begin{matrix} A(\omega_{2n}^0), & B(\omega_{2n}^0) \\ A(\omega_{2n}^1), & B(\omega_{2n}^1) \\ \vdots & \\ A(\omega_{2n}^{2n-1}), & B(\omega_{2n}^{2n-1}) \end{matrix} & \xrightarrow[\text{time} = \Theta(n)]{\text{Pointwise multiplication}} & \begin{matrix} C(\omega_{2n}^0) \\ C(\omega_{2n}^1) \\ \vdots \\ C(\omega_{2n}^{2n-1}) \end{matrix}
\end{array}
$$

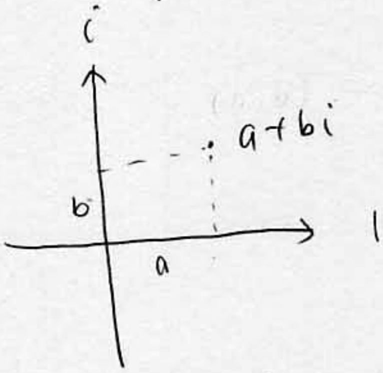
$x_k = \omega_{2n}^k$

Complex number

① $i = \sqrt{-1}$, $i^2 = -1$

$$(a+bi)\cdot(c+di) = (ac-bd) + (ad+bc)i$$

② Gaussian plane



③ $$a+bi = \sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}}i\right)$$

$$= \rho\cdot(\cos\theta + i\sin\theta), \quad \cos^2\theta + \sin^2\theta = 1$$

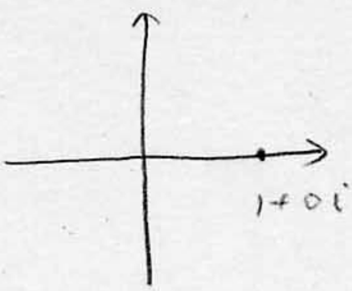
④ $$e^{i\theta} = \cos\theta + i\sin\theta$$

$$e^{i\phi} = \cos\phi + i\sin\phi$$

$$\Rightarrow e^{i\theta}\, e^{i\phi} = \cos(\theta+\phi) + i\sin(\theta+\phi) = e^{i(\theta+\phi)}$$

Complex roots of unity :

$x^n = 1$ has exactly n roots

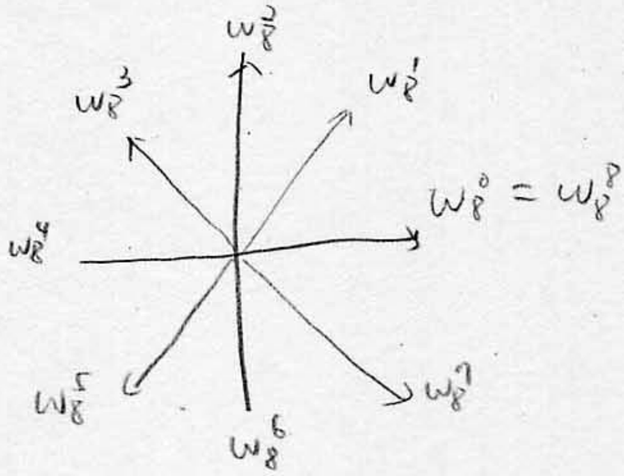


$$1 = \cos 0 + i\sin 0$$
$$= \cos 2\pi + i\sin 2\pi$$
$$= \cos 4\pi + i\sin 4\pi$$
$$= \cos 6\pi + i\sin 6\pi$$

Let $w_n = e^{2\pi i \cdot \frac{1}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$

$w_n^0, w_n^1, \dots, w_n^{n-1}$ are the roots of $x^n = 1$

$n = 8$:



Lemma (Cancellation lemma)

For any integer $n \geq 0$, $k \geq 0$, $d > 0$,

$$w_{dn}^{dk} = w_n^k$$

Corollary: For any integer $n > 0$,

$$w_{2n}^n = w_2 = -1$$

Lemma (Halving lemma)

The squares of $w_{2n}^0, w_{2n}^1, \dots, w_{2n}^{2n-1}$ are the roots of $x^n = 1$. (That is, $w_n^0, w_n^1, \dots, w_n^{n-1}$)

Lemma (Summation lemma)

For any integer $n \geq 1$ and $n \nmid k$

$$\sum_{j=0}^{n-1} (w_n^k)^j = 0$$

DFT :

$$A(x) = \sum_{j=0}^{n-1} a_j x^j$$

Evaluate $\quad y_k = A(w_n^k) = \sum_{j=0}^{n-1} a_j w_n^{kj}$ for $0 \le k < n$

$(y_0, y_1, \dots, y_{n-1})$ is the DFT of $(a_0, a_1, \dots, a_{n-1})$.

FFT :

$$\begin{aligned} A(x) &= a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_{2n-1} x^{2n-1} \\ &= (a_0 + a_2 x^2 + a_4 x^4 + \cdots + a_{2n-2} x^{2n-2}) + \\ &\quad (a_1 x + a_3 x^3 + a_5 x^5 + \cdots + a_{2n-1} x^{2n-1}) \\ &= P(x^2) + x \cdot Q(x^2). \end{aligned}$$

where $P(y) = a_0 + a_2 y + a_4 y^2 + \cdots + a_{2n-2} x^{n-1}$

$\quad\quad\quad Q(y) = a_1 + a_3 y + a_5 y^2 + \cdots + a_{2n-1} x^{n-1}$.

$$A(w_{2n}^k) = P(w_{2n}^{2k}) + w_{2n}^k \cdot Q(w_{2n}^{2k})$$

$$\begin{aligned} A(w_{2n}^{k+n}) &= P(w_{2n}^{2k+2n}) + w_{2n}^{k+n} \cdot Q(w_{2n}^{2k+2n}) \\ &= P(w_{2n}^{2k}) - w_{2n}^k \cdot Q(w_{2n}^{2k}). \end{aligned}$$

$$w_{2n}^{2k} = w_n^k,$$

Therefore we can compute $A(w_{2n}^k)$ and $A(w_{2n}^{k+n})$

from the results of $P(w_n^k)$ and $Q(w_n^k)$.

Algorithm (FFT)

Input: $a_0, a_1, a_2, \cdots, a_{2n-1}$ where $A(x) = \sum_{j=0}^{2n-1} a_j x^j$

Output: $A(w_{2n}^0), A(w_{2n}^1), \cdots, A(w_{2n}^{2n-1})$.

① Let $P = (a_0, a_2, a_4, \cdots, a_{2n-2})$,

$Q = (a_1, a_3, a_5, \cdots, a_{2n-1})$.

Let $P(y) = \sum_{j=0}^{n-1} a_{2j} y^j$, $Q(y) = \sum_{j=0}^{n-1} a_{2j+1} y^j$

Then $A(x) = P(x^2) + x \cdot Q(x^2)$.

② Evaluate

$P(y)$ and $Q(y)$ for $y = w_n^0, w_n^1, w_n^2, \cdots, w_n^{n-1}$

recursively.

③ Let
$$\begin{cases} A(w_{2n}^k) = P(w_n^k) + w_{2n}^k \cdot Q(w_n^k) \\ A(w_{2n}^{k+n}) = P(w_n^k) - w_{2n}^k \cdot Q(w_n^k) \end{cases} \quad \text{for } 0 \le k < n$$

Return $A(w_{2n}^0), A(w_{2n}^1), \cdots, A(w_{2n}^n), A(w_{2n}^{n+1}), \cdots, A(w_{2n}^{2n-1})$.

Inverse DFT:

Given $y_0, y_1, y_2, \cdots, y_{n-1}$,

evaluate $a_j = \frac{1}{n} \sum_{k=0}^{n-1} y_k \cdot w_n^{-kj}$ $0 \le j < n$