Polynomial Multiplication via FFT

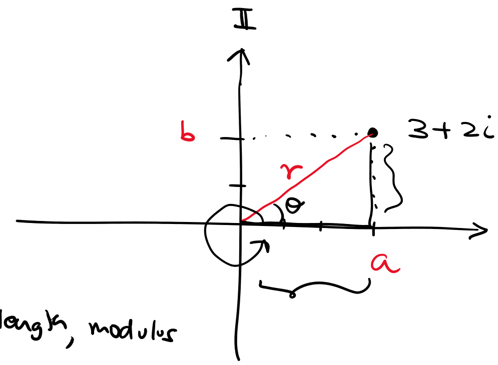
Complex Numbers : $a + ib = z$ ← $a, b \in \mathbb{R}$

a: real, $i = \sqrt{-1}$, b: imaginary

$z \in \mathbb{C}$

angle:

mod 2π



$a = 3$
$b = 2$

Cartesian coordinates

$z = 3 + 2i$

⇓

Polar co-ordinates

$r \equiv$ absolute value, length, modulus

$r = |z|$

$r = \sqrt{a^2 + b^2}$

$$\boxed{\begin{aligned} \cos\theta &= \frac{a}{r} \\ \sin\theta &= \frac{b}{r} \end{aligned}}$$

$z = (r, \theta)$

$z = \underbrace{r\cos\theta}_{a} + \underbrace{r\sin\theta}_{b}\, i$

Multiply two complex numbers

$z = a + ib$
$x = c + id$

$$z \cdot x = (a + ib) \cdot (c + id)$$
$$= \underbrace{(ac - bd)} + i\,\underbrace{(ad + bc)}$$

$i^2 = -1$

$i = \sqrt{-1}$

Multiplication in polar coordinate

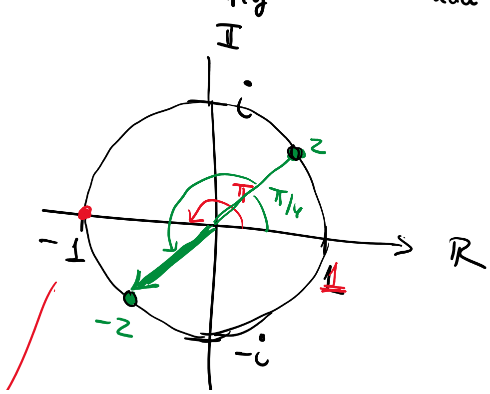
$z = (r, \theta)$
$X = (R, \alpha)$

$$\boxed{z \cdot x = (r \cdot R\, ,\ \theta + \alpha)}$$

lengths multiply

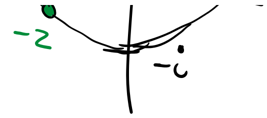
angle add

multiplication



$r = 1$

all complex numbers with absolute value 1 or radius 1



n-1 complex numbers with absolute value 1 or radius 1

$$-1 = -1 + 0i \equiv (1, \pi)$$

$$z = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i \equiv \left(1, \frac{\pi}{4}\right)$$

angle in radians

$\pi \Rightarrow 180°$

$$|z| = \sqrt{\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2} = \sqrt{\frac{1}{2} + \frac{1}{2}} = \sqrt{1} = 1$$

$$-z = -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} i \quad \text{negation}$$

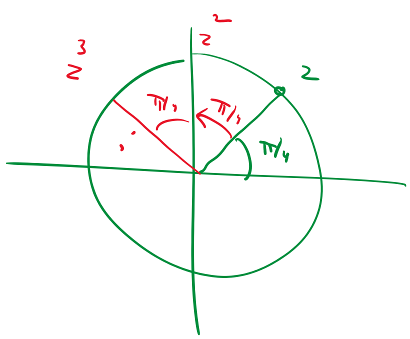
$$-z \equiv \left(1, \pi + \frac{\pi}{4}\right)$$

exponentiation

$$z = \frac{1}{\sqrt{2}}(1+i) \equiv \left(1, \frac{\pi}{4}\right)$$

$$z^2 = z \cdot z \equiv \left(1, \frac{\pi}{4}\right)\left(1, \frac{\pi}{4}\right) = \left(1 \cdot 1, \frac{\pi}{4} + \frac{\pi}{4}\right) = \left(1, \frac{\pi}{2}\right)$$

$$z^n = \left(1, \frac{\pi}{4} \cdot n\right)$$



Polynomial multiplication

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{d-1} x^{d-1} + 0x^d + 0x^{d+1} \cdots + 0 \cdot x^{n-1}$$

$$B(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{d-1} x^{d-1} + 0x^d + 0x^{d+1} + \cdots + 0 \cdot x^{n-1}$$

exactly $n = 2^k$ terms

zero padding

$$C(x) = A(x) \cdot B(x)$$

$$= c_0 + c_1 x + \cdots + c_{2(d-1)} x^{2(d-1)} + \cdots + c_{n-1} x^{n-1}$$

$$= \underbrace{c_0 + c_1 x + \dots + c_{2(n-1)} x^{n-1} + \dots + c_{n-1} x^{n-1}}_{n\text{ - terms in the result}}$$

↳ this should be a power of 2

Evaluate at $\underbrace{\tfrac{n}{2} \text{ pairs of } (+,-) \text{ points}}_{\text{total of } n \text{ points}}$, allowing for -ve square ⇒ complex numbers

A(x) & B(x) @ these n points via FFT

$n = 8$ ← result is with degree 8

$A(x) = 2 + 5x + 1x^2 + 2x^3$

$B(x) = 1 - 2x - x^2 + x^3$

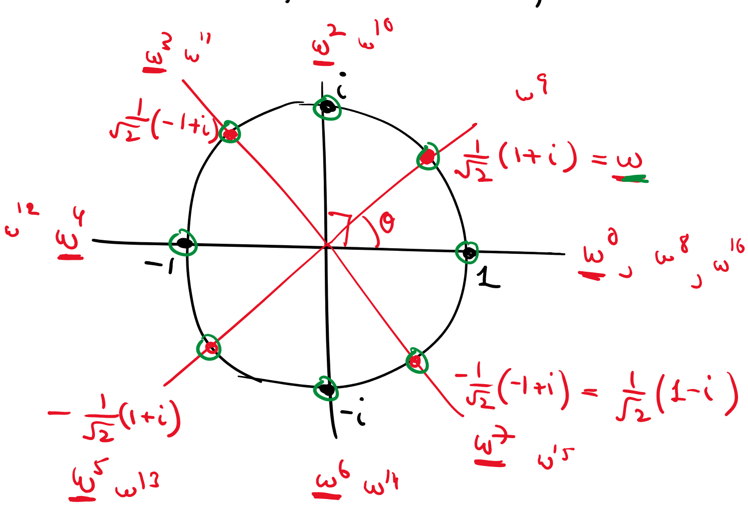
$C(x) =$

we need 8 distinct points (+, −) paired

$\boxed{z^n = 1}$

Our n points all solutions to this equation

$\boxed{\omega = \left(1, \frac{2\pi}{n}\right)}$



$\boxed{z^8 = 1}$

Solutions to this equation

ω : primitive 8th root of unity

$\theta = \frac{2\pi}{8}$

$\omega = \left(1, \frac{2\pi}{8}\right) = \left(1, \frac{\pi}{4}\right)$

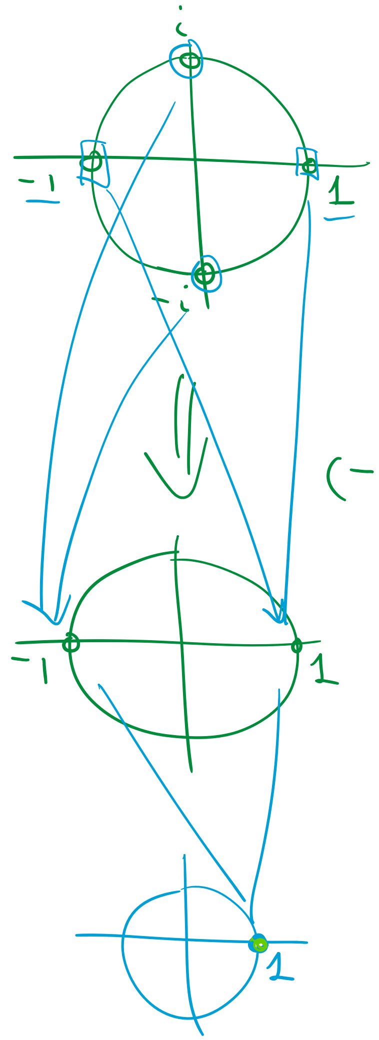
$\omega^2 = \left(1, \frac{2\pi}{4}\right) = \left(1, \frac{\pi}{2}\right)$

all the n solutions are given as powers of ω from ...

all the n solutions are given as powers of ω, from 0 to n-1

$\omega^0, \omega^1, \omega^2, \ldots, \omega^{n-1}$

$$\boxed{\omega^i = \left(1, \frac{2\pi}{n} i\right)}$$



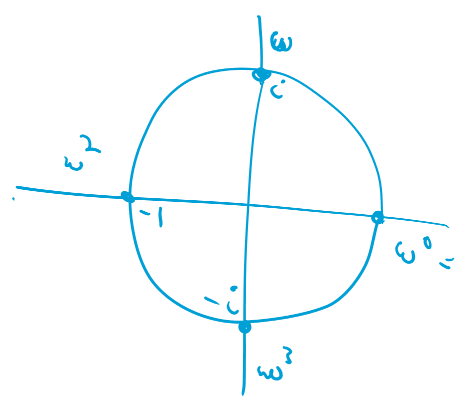
4 remaining in recursive call

$i^2 = -1 \qquad 1^2 = 1$

$(-i)^2 = -1 \qquad -1^2 = 1$

$$\boxed{A(x) = 2 + 3x - 5x^2 + 2x^3}$$

Evaluate $A(x)$ @ $\omega^0, \omega^1, \omega^2, \omega^3$



$$A(\omega^0) = 2(\omega^0) + 3(\omega^0)^1 - 5(\omega^0)^2 + 2(\omega^0)^3$$
$$A(\omega^1) = 2 + 3\omega^1 - 5(\omega^1)^2 + 2(\omega^1)^3$$
$$A(\omega^2) = 2 + 3\omega^2 - 5(\omega^2)^2 + 2(\omega^2)^3$$
$$A(\omega^3) = 2 + 3\omega^3 - 5(\omega^3)^2 + 2(\omega^3)^3$$

n

$\omega^0 = 1$

$$\begin{bmatrix} A(\omega^0) \\ A(\omega^1) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} \begin{matrix} \leftarrow a_0 \\ \leftarrow a_1 \end{matrix}$$

$$\begin{bmatrix} \vdots \\ A(\omega^1) \\ A(\omega^2) \\ A(\omega^3) \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix}}_{M} \begin{bmatrix} 2 \\ 3 \\ -5 \\ 2 \end{bmatrix} \begin{matrix} \leftarrow a_0 \\ \leftarrow a_1 \\ \leftarrow a_2 \\ \leftarrow a_3 \end{matrix}$$

?

Vandermonde matrix

given

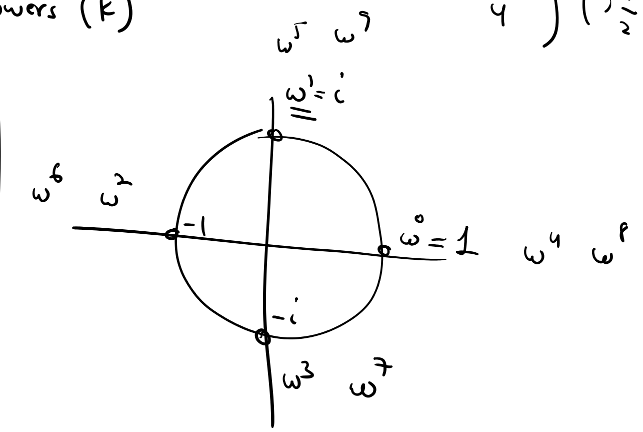
typical case $\underline{O(n^2)}$ time to multiply

FFT $O(n \log n)$

$n = 4$

$\omega = (1, \frac{2\pi}{4}) = (1, \frac{\pi}{2})$

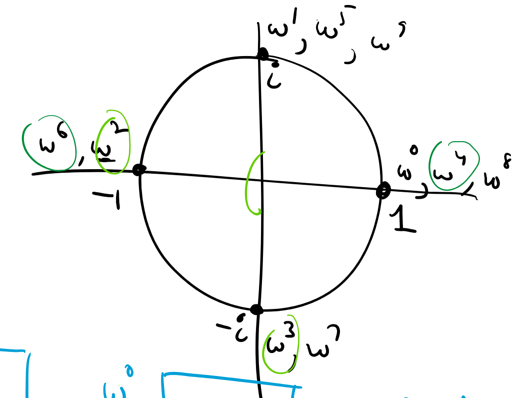
$$\begin{array}{c|c} & \begin{matrix} 0 & 1 & 2 & 3 \end{matrix} \leftarrow \text{powers } (k) \\ \begin{matrix} j & \to \omega^0 \\ & \to \omega^1 \\ & \to \omega^2 \\ n\text{-roots} & \to \omega^3 \end{matrix} & \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \end{array}$$



even-odd rearrangement

[any power can be taken modulo $n = 4$]

$$j \quad \begin{bmatrix} A(\omega^0) \\ A(\omega^1) \\ A(\omega^2) \\ A(\omega^3) \end{bmatrix} = \underbrace{\begin{array}{c} \begin{matrix} 0 & 2 & 1 & 3 \end{matrix} \\ \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & \omega^2 & \omega & \omega^3 \\ \hline 1 & \omega^4 & \omega^2 & \omega^6 \\ 1 & \omega^6 & \omega^3 & \omega^9 \end{array}\right] \end{array}}_{M(4)} \begin{bmatrix} a_0 \\ a_2 \\ a_1 \\ a_3 \end{bmatrix} \leftarrow \text{Coefficients}$$



$$M(2) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \begin{bmatrix} 1 & \omega^4 = 1 \\ 1 & \omega^6 \end{bmatrix} \quad \begin{matrix} \omega^0 \leftarrow \\ \omega^1 \end{matrix} \begin{bmatrix} 1 & 1 \\ \cdots & \cdots \end{bmatrix} = \begin{matrix} \omega^0 \\ \omega^1 \end{matrix} \boxed{M(2)}$$

M(2) with each ...

$$M(2) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & \omega^4 = 1 \\ 1 & \omega^6 = -1 \end{bmatrix}$$

$$\begin{array}{c} \omega^0 \leftarrow \\ \omega^1 \leftarrow \end{array} \begin{bmatrix} 1 & 1 \\ 1 & \omega^2 = -1 \end{bmatrix} = \begin{array}{c} \omega^0 \\ \omega^1 \end{array} \begin{bmatrix} M(2) \end{bmatrix}$$

$M(2)$ with each row multiplied by corresponding ω^j

$$M(4) = \begin{bmatrix} M(2) & \\ M(2) & \end{bmatrix}$$

$$\begin{bmatrix} \omega^2 & \omega^6 \\ \omega^3 & \omega^9 \end{bmatrix} = \begin{array}{c} \omega^2 \\ \omega^3 \end{array} \begin{bmatrix} 1 & \omega^4 = 1 \\ 1 & \omega^6 = -1 \end{bmatrix}$$

$$= \begin{array}{c} \omega^2 \\ \omega^3 \end{array} \begin{bmatrix} M(2) \end{bmatrix} = \begin{array}{c} -\omega^0 \\ -\omega^1 \end{array} \begin{bmatrix} M(2) \end{bmatrix}$$

$$\begin{bmatrix} A(\omega^0) \\ A(\omega^1) \\ A(\omega^2) \\ A(\omega^3) \end{bmatrix} = \begin{array}{cc} \text{even} & \text{odd} \end{array} \begin{bmatrix} M(2) & \begin{array}{c} \omega^0 \\ \omega^1 \end{array} M(2) \\ M(2) & \begin{array}{c} -\omega^0 \\ -\omega^1 \end{array} M(2) \end{bmatrix} \begin{bmatrix} a_0 \\ a_2 \\ a_1 \\ a_3 \end{bmatrix}$$

Input: $\underbrace{[a_0 \; a_1 \; a_2 \; a_3]}_{\text{Coefficients}}, \; \omega$ (n^{th} primitive root)

$([a_0 \; a_2], \omega^2)$ even $\quad ([a_1 \; a_3], \omega^2)$ odd

FFT(n)

E: even: FFT$(n/2)$

O: odd: FFT$(n/2)$

result: $E + \boxed{\omega} \cdot O$

: $E - \boxed{\omega} \cdot O$

return $[A(\omega^0), A(\omega^1), A(\omega^2), A(\omega^3)]$

evaluation of A @ 4 distinct points!

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

$O(n \log n)$ time :)

$\underline{O(n \log n)}$ time :)

Polynomial Multiplication via FFT

$n \leftarrow$ power of 2 larger than or equal to $2(d-1)$

$\omega = \left(1, \frac{2\pi}{n}\right)$ ← polar

$= \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$

Cartesian

// $A(x)$, $B(x)$ of degree $d-1$ at most

// $C(x) \leftarrow$ return $C(x)$, degree $2(d-1)$ at most

// Evaluation step

coefficient space

$A_x = FFT([\underbrace{a_0, a_1, a_2, \ldots, a_{d-1}, 0, 0, \ldots 0}_{n}], \omega)$ $O(n \log n)$

$B_x = FFT([\underbrace{b_0, b_1, b_2, \ldots, b_{d-1}, 0, 0, \ldots, 0}_{n}], \omega)$ $O(n \log n)$

// Value space (@ n value)

$C_x = A_x \odot B_x$ ← $C(X) = \underline{A(X)} \cdot B(X)$

$O(n)$ elementwise multiplication

// Convert C_x back to C, recover $(\underbrace{c_0, c_1, c_2, \ldots, c_{2(d-1)}, 0 \ldots}_{n})$

// Interpolation

Interpolation

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{pmatrix} = \boxed{M(n)^{-1}} \begin{pmatrix} C(\omega^0) \\ C(\omega^1) \\ \vdots \\ C(\omega^{n-1}) \end{pmatrix}$$

Inverse

$$= \frac{1}{n} M(n, \omega^{-1})$$

Evaluation

$$A(x) = \underline{M(n)} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

orthogonal matrix

$$\underline{[c_0\ c_1 \cdots c_{n-1}]} = FFT(c_x\ ,\ \underline{\omega^{-1}}) \qquad O(n\log n)$$

$O(n\log n)$ total time