Fast Fourier Transform

cs208

by wwy

*https://www.youtube.com/watch?v=h7apO7q16V0&feature=emb_logo

Polynomial Multiplication

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

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

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

$C(x) = (x^2 + 3x + 2) \cdot (2x^2 + 1)$

$C(x) = x^2(2x^2 + 1) + 3x(2x^2 + 1) + 2(2x^2 + 1)$

$C(x) = 2x^4 + x^2 + 6x^3 + 3x + 4x^2 + 2$

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

How to storage

Polynomial Multiplication

$A(x) = x^2 + 3x + 2$ $\qquad A = [1,3,2]$

$B(x) = 2x^2 + 1$ $\qquad B = [1,0,2]$

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

$C(x) = (x^2 + 3x + 2) \cdot (2x^2 + 1)$

$C(x) = x^2(2x^2 + 1) + 3x(2x^2 + 1) + 2(2x^2 + 1)$

$C(x) = 2x^4 + x^2 + 6x^3 + 3x + 4x^2 + 2$

$C(x) = 2x^4 + 6x^3 + 5x^2 + 3x + 2$ $\qquad C = [2,3,5,6,2]$

Coefficient Representation

Polynomial Multiplication

$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$

$B(x) = b_0 + b_1x + b_2x^2 + \cdots + b_dx^d$

$C(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{2d}x^{2d}$

O(d^2)

Polynomial Multiplication

- (d+1) points uniquely define a degree d ploynomial

$$P(x) = p_0 + p_1 x + p_2 x^2 + \ldots + p_n x^d$$

$$\{(x_0, P(x_0)), (x_1, P(x_1)), \ldots, (x_d, P(x_d))\}$$

Value Representation

Polynomial Multiplication

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

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

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

d=4

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

$\{(-2,0), (-1,0), (0,2), (1,6), (2,12)\}$

5 points

$\{(-2,9), (-1,3), (0,1), (1,3), (2,9)\}$

$\{(-2,0), (-1,0), (0,2), (1,18), (2,108)\}$

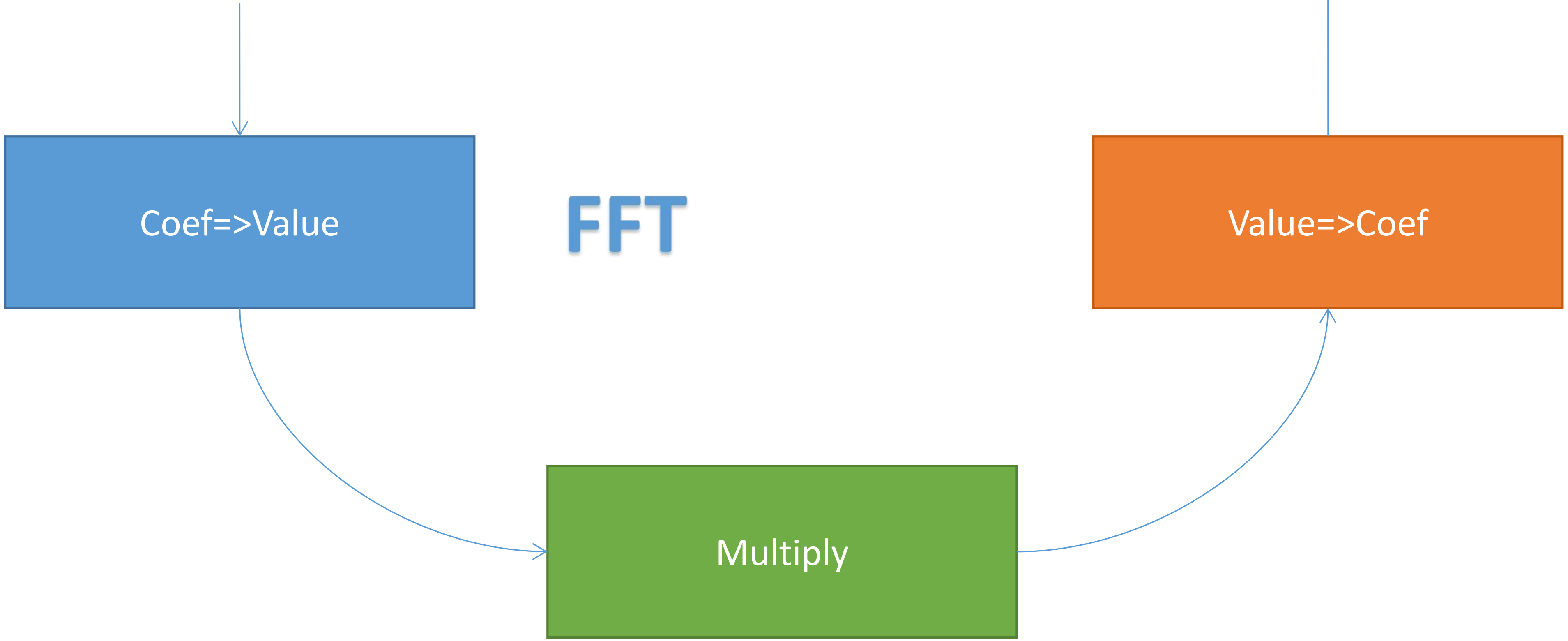
O(d)

Polynomial Multiplication

$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$

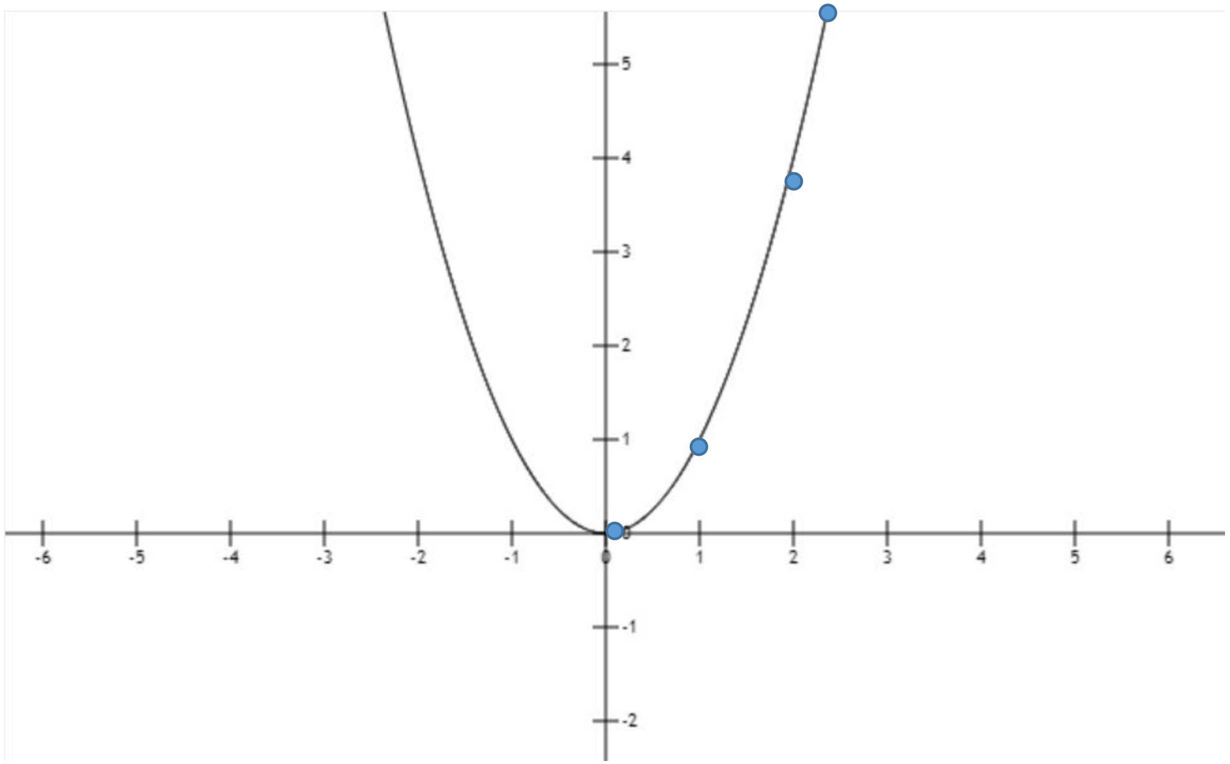
$C(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{2d} x^{2d}$

$B(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_d x^d$



Polynomial Multiplication

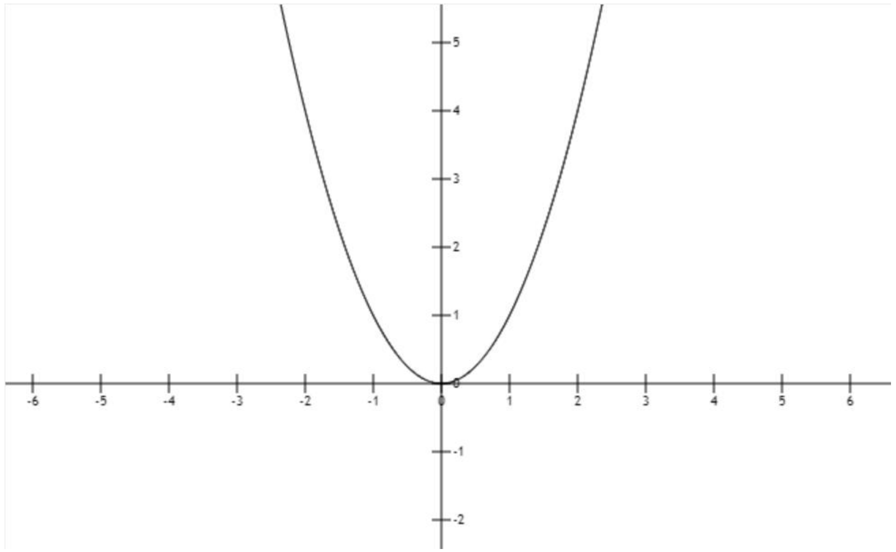
$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ $B(x) = b_0 + b_1x + b_2x^2 + \cdots + b_dx^d$



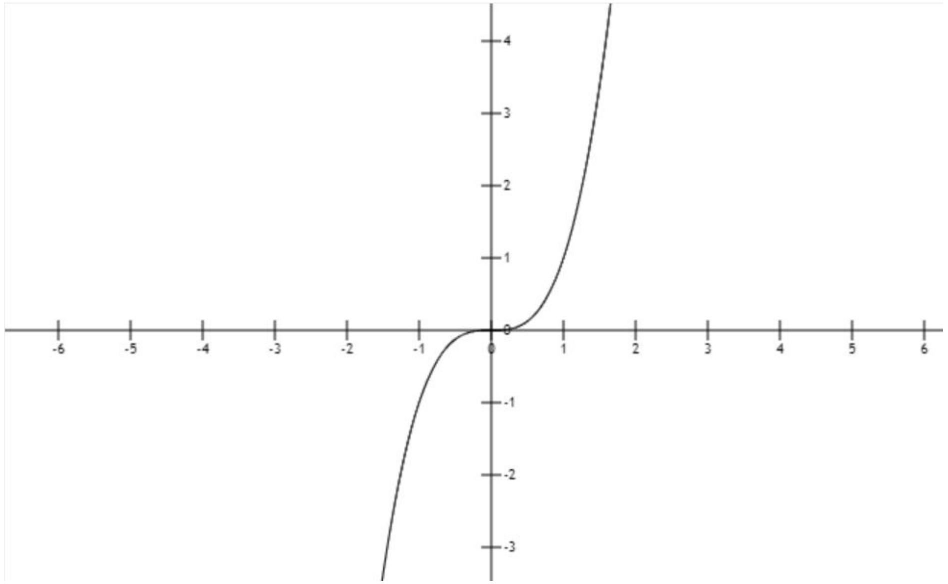
Polynomial Multiplication

$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$

$B(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_d x^d$



even



odd

Polynomial Multiplication

$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$

$B(x) = b_0 + b_1x + b_2x^2 + \cdots + b_dx^d$

eg

$A(x) = 3x^5 + 2x^4 + x^3 + 7x^2 + 5x + 1$

O(nlogn)

$$A(x) = \underbrace{(2x^4 + 7x^2 + 1)}_{A_e(x^2)} + x\underbrace{(3x^4 + x^2 + 5)}_{A_o(x^2)}$$

$A_e(x^2) = A_e(y) = 2y^2 + 7y + 1$

$A_o(x^2) = A_o(y) = 3y^2 + y + 5$

$$A(x) = A_e(x^2) + xA_o(x^2)$$

$$\begin{cases} A(x_i) = A_e(x_i^2) + x_iA_o(x_i^2) \\ A(-x_i) = A_e(x_i^2) - x_iA_o(x_i^2) \end{cases}$$

4th power->square

Recursion?Merge conquer?

Polynomial Multiplication

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

$$B(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_d x^d$$

eg

$$A(x) = 3x^5 + 2x^4 + x^3 + 7x^2 + 5x + 1$$

$$A(x) = \underbrace{(2x^4 + 7x^2 + 1)}_{A_e(x^2)} + x\underbrace{(3x^4 + x^2 + 5)}_{A_o(x^2)}$$

$$A_e(x^2) = A_e(y) = 2y^2 + 7y + 1$$

$$A_o(x^2) = A_o(y) = 3y^2 + y + 5$$

$$A(x) = A_e(x^2) + xA_o(x^2)$$

$$\begin{cases} A(x_i) = A_e(x_i^2) + x_i A_o(x_i^2) \\ A(-x_i) = A_e(x_i^2) - x_i A_o(x_i^2) \end{cases}$$

Recursion?Merge conquer?

Polynomial Multiplication

$$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$$

$$B(x) = b_0 + b_1x + b_2x^2 + \cdots + b_dx^d$$

eg

$$A(x) = 3x^5 + 2x^4 + x^3 + 7x^2 + 5x + 1$$

$$A(x) = \underbrace{(2x^4 + 7x^2 + 1)}_{A_e(x^2)} + x\underbrace{(3x^4 + x^2 + 5)}_{A_o(x^2)}$$

$$A(x) = A_e(x^2) + xA_o(x^2)$$

$$\left\{\begin{aligned} A(x_i) &= A_e(x_i^2) + x_iA_o(x_i^2) \\ A(-x_i) &= A_e(x_i^2) - x_iA_o(x_i^2) \end{aligned}\right.$$

$$A_e(x^2) = A_e(y) = 2y^2 + 7y + 1$$

$$A_o(x^2) = A_o(y) = 3y^2 + y + 5$$

Recursion， Merge conquer

real number->complex num

Polynomial Multiplication

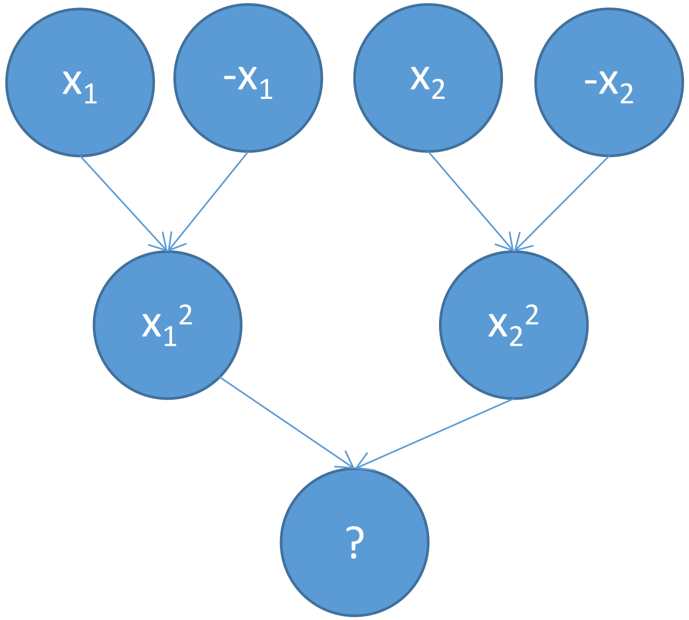
$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

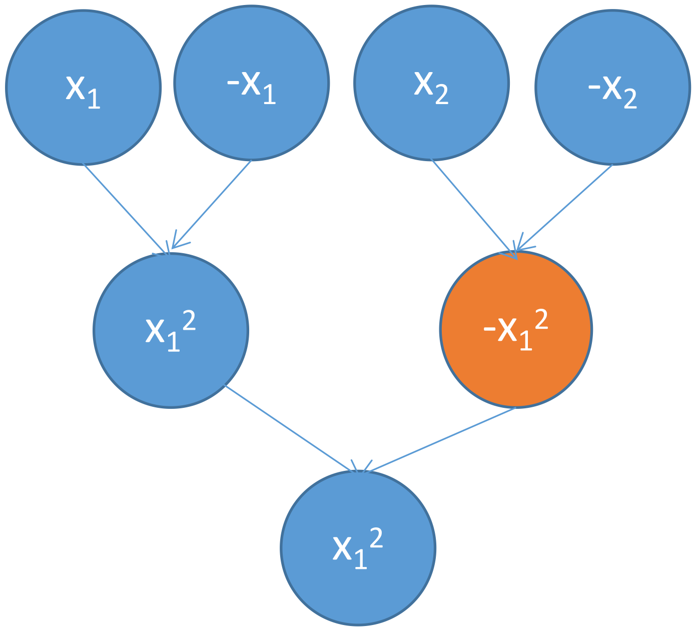
$$\Big\downarrow \text{eg}$$

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

Recursion， Merge conquer

real number->complex num



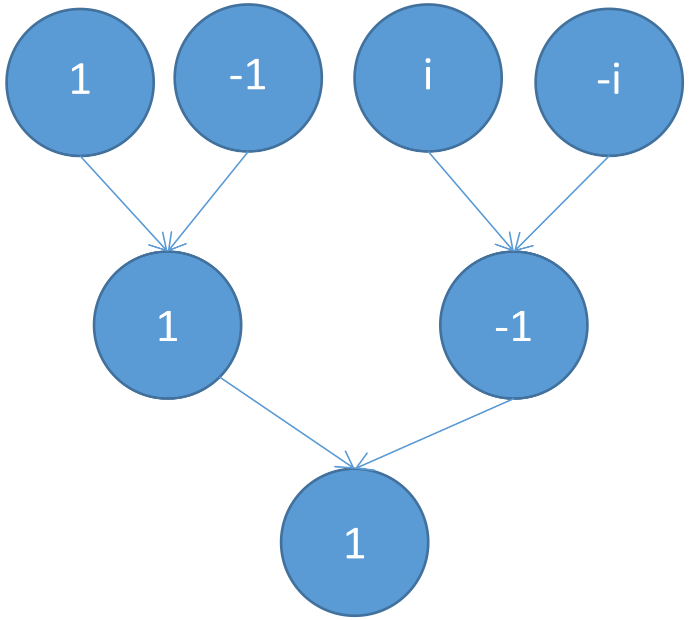


Polynomial Multiplication

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

eg

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



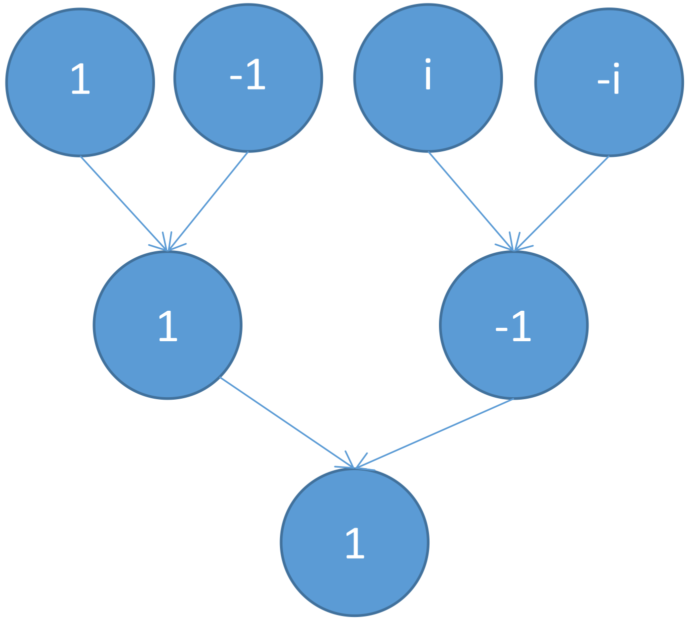
Polynomial Multiplication

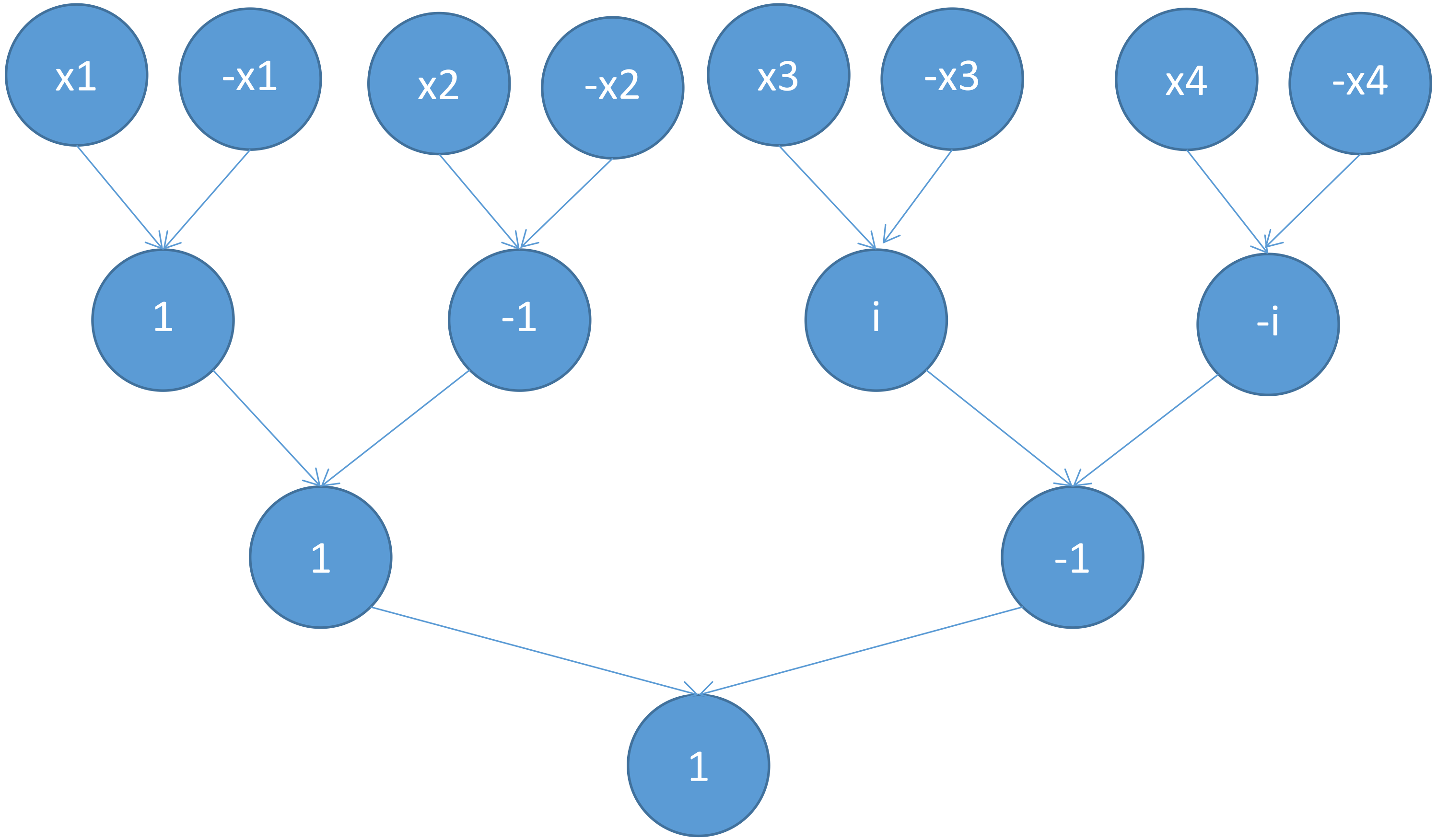
6 points->8 pts(2^3)

$$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d \xrightarrow{\text{eg}} A(x) = 3x^5 + 2x^4 + x^3 + 7x^2 + 5x + 1$$

eg

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





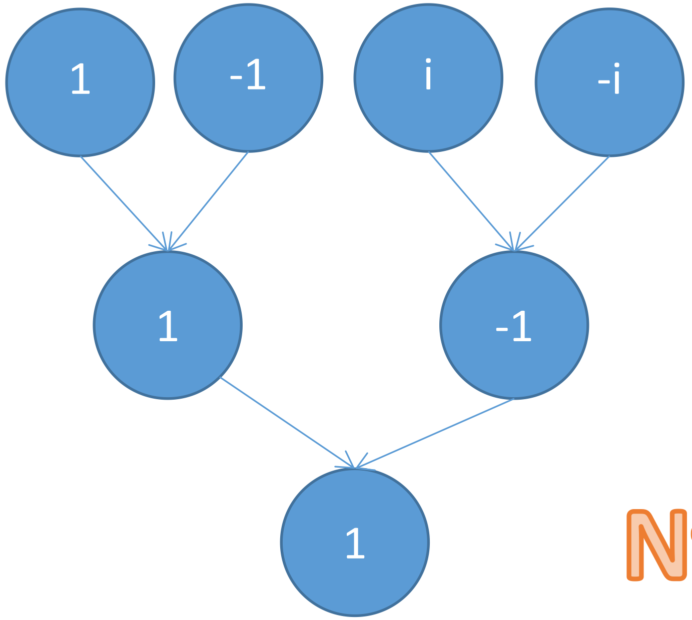
Polynomial Multiplication

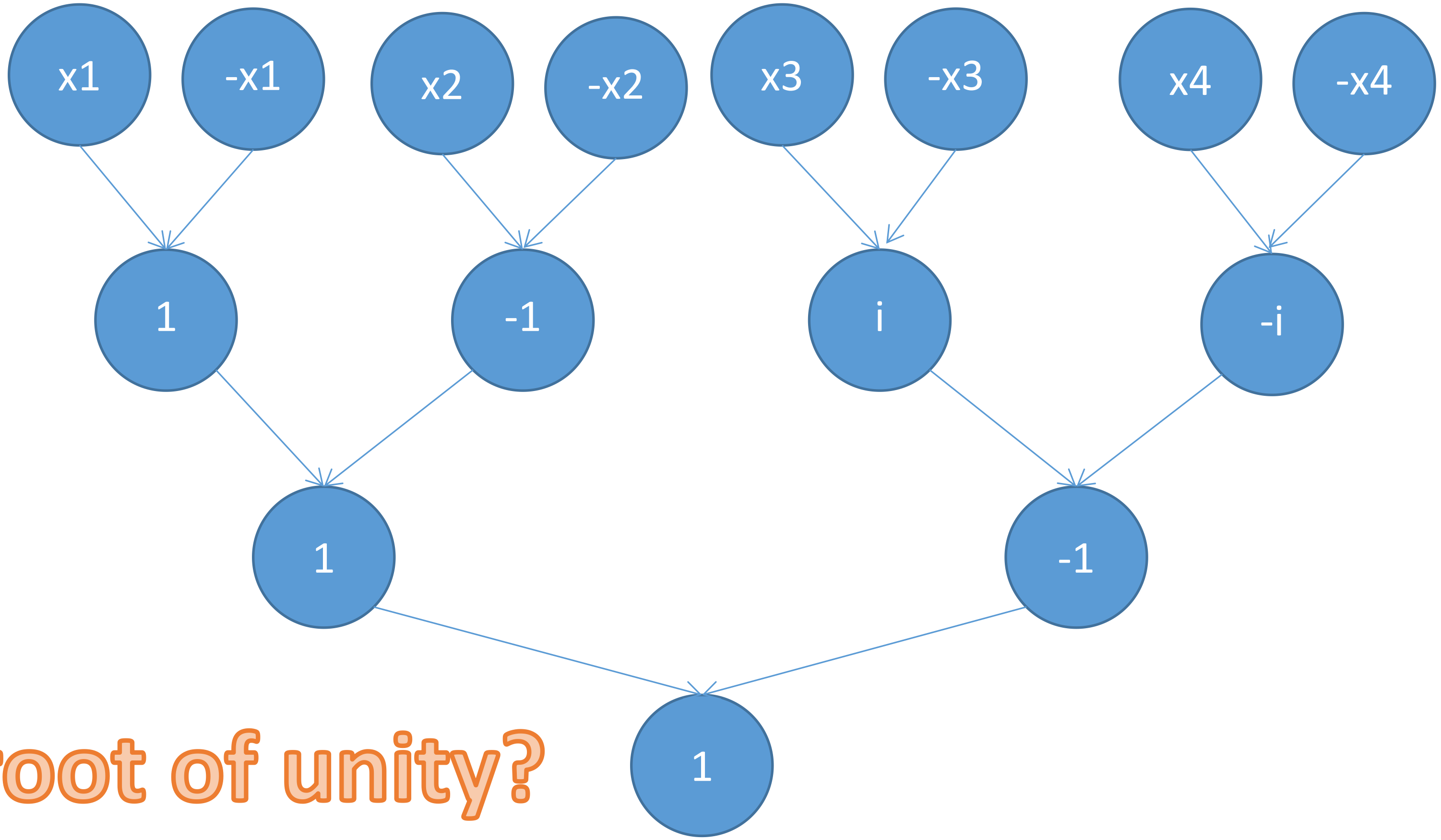
6 points->8 pts(2^3)

$$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d \xrightarrow{\text{eg}} A(x) = 3x^5 + 2x^4 + x^3 + 7x^2 + 5x + 1$$

eg

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





Nth root of unity?

Polynomial Multiplication

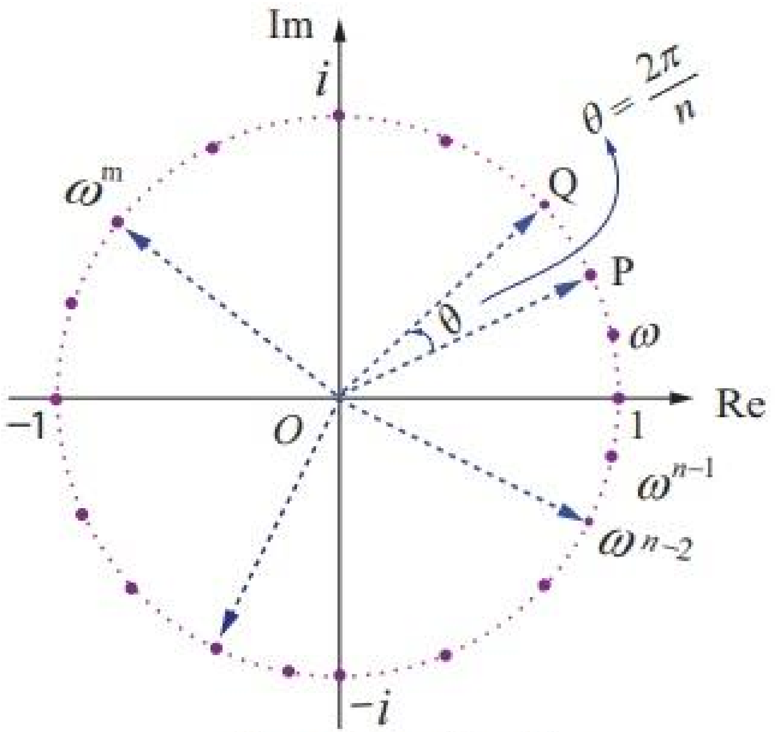
$$\omega = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi i}{n} + i\sin\frac{2\pi i}{n}$$

$$\Rightarrow \quad \omega^n = \left(e^{\frac{2\pi i}{n}}\right)^n = e^{2\pi i} = 1\,.$$

- Nth root of unity

$$e^{i\theta} = cos(\theta) + isin(\theta)$$

$$\omega^{j+n/2} = -\,\omega^j$$



n^{th} roots of unity

we wanna know A(x) at 1,w, w^2,...,w^{n-1} ($n=2^k$)

so you can do the Recursion!

*https://www.brainkart.com/article/The-nth--roots-of-unity_39108/

FFT

$P(x): [p_0, p_1, \ldots, p_{n-1}]$ $\quad \omega = e^{\frac{2\pi i}{n}}: [\omega^0, \omega^1, \ldots, \omega^{n-1}]$

$when\, n = 1, P(1): \; n = 2^k$

$P_e(x^2): [p_0, p_2, \ldots, p_{n-2}] \quad [\omega^0, \omega^2, \ldots, \omega^{n-2}]$

$y_e = [P_e(\omega^0), P_e(\omega^2), \ldots, P_e(\omega^{n-2})]$

$P_o(x): [p_1, p_3, \ldots, p_{n-1}] \quad [\omega^0, \omega^2, \ldots, \omega^{n-2}]$

$y_o = [P_o(\omega^0), P_o(\omega^2), \ldots, P_o(\omega^{n-2})]$

$$P(x_j) = P_e(x_j^2) + x_j P_o(x_j^2)$$
$$P(-x_j) = P_e(x_j^2) - x_j P_o(x_j^2)$$
$$j \in \{0,1,\ldots,(\frac{n}{2} - 1)\}$$

$x_j = \omega^j$

$$P(\omega^j) = P_e(\omega^{2j}) + \omega^j P_o(\omega^{2j})$$
$$P(-\omega^j) = P_e(\omega^{2j}) - \omega^j P_o(\omega^{2j})$$
$$j \in \{0,1,\ldots,(\frac{n}{2} - 1)\}$$

$-\omega^j = \omega^{j+n/2}$

$$P(\omega^j) = P_e(\omega^{2j}) + \omega^j P_o(\omega^{2j})$$
$$P(\omega^{j+n/2}) = P_e(\omega^{2j}) - \omega^j P_o(\omega^{2j})$$
$$j \in \{0,1,\ldots,(\frac{n}{2} - 1)\}$$

$$y_e[j] = P_e(\omega^{2j})$$
$$y_o[j] = P_o(\omega^{2j})$$

$$P(\omega^j) = y_e[j] + \omega^j y_o[j]$$
$$P(\omega^{j+n/2}) = y_e[j] - \omega^j y_o[j]$$
$$j \in \{0,1,\ldots,(\frac{n}{2} - 1)\}$$

FFT

```
def FFT(P):
    # P - [p_0, p_1, ..., p_{n-1}] coeff representation
    n = len(P) # n is a power of 2
    if n == 1:
        return P
    ω = e^{2πi/n}
    P_e, P_o = [p_0, p_2, ..., p_{n-2}], [p_1, p_3, ..., p_{n-1}]
    y_e, y_o = FFT(P_e), FFT(P_o)
    y = [0] * n
    for j in range(n/2):
        y[j] = y_e[j] + ω^j y_o[j]
        y[j + n/2] = y_e[j] - ω^j y_o[j]
    return y
```

$$P(x) : [p_0, p_1, \ldots, p_{n-1}]$$

$$\omega = e^{\frac{2\pi i}{n}} : [\omega^0, \omega^1, \ldots, \omega^{n-1}]$$

$$when\ n = 1, P(1):\ n = 2^k$$

$$P_e(x^2) : [p_0, p_2, \ldots, p_{n-2}]$$

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

$$y_e = [P_e(\omega^0), P_e(\omega^2), \ldots, P_e(\omega^{n-2})]$$

$$P_o(x) : [p_1, p_3, \ldots, p_{n-1}]$$

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

$$y_o = [P_o(\omega^0), P_o(\omega^2), \ldots, P_o(\omega^{n-2})]$$

$$P(\omega^j) = y_e[j] + \omega^j y_o[j]$$

$$P(\omega^{j+n/2}) = y_e[j] - \omega^j y_o[j]$$

$$j \in \{0,1, \ldots, (\frac{n}{2} - 1)\}$$

$$y = [P(\omega^0), P(\omega^1), \ldots, P(\omega^{n-1})]$$

FFT vs IFFT

$$\text{IFFT}(\text{<values>}) \Leftrightarrow \text{FFT}(\text{<values>}) \text{ with } \omega = \frac{1}{n} e^{\frac{-2\pi i}{n}}$$

def $\text{FFT}(P)$:

$\quad$ # P - $[p_0, p_1, \ldots, p_{n-1}]$ coeff rep

$\quad$ $n = \text{len}(P)$ # n is a power of 2

$\quad$ if $n == 1$:

$\quad\quad$ return P

$\quad$ $\omega = e^{\frac{2\pi i}{n}}$

$\quad$ $P_e, P_o = P[::2], P[1::2]$

$\quad$ $y_e, y_o = \text{FFT}(P_e), \text{FFT}(P_o)$

$\quad$ $y = [0] * n$

$\quad$ for j in range$(n/2)$:

$\quad\quad$ $y[j] = y_e[j] + \omega^j y_o[j]$

$\quad\quad$ $y[j + n/2] = y_e[j] - \omega^j y_o[j]$

$\quad$ return y

def $\text{IFFT}(P)$:

$\quad$ # P - $[P(\omega^0), P(\omega^1), \ldots, P(\omega^{n-1})]$ value rep

$\quad$ $n = \text{len}(P)$ # n is a power of 2

$\quad$ if $n == 1$:

$\quad\quad$ return P

$\quad$ $\omega = (1/n) * e^{\frac{-2\pi i}{n}}$

$\quad$ $P_e, P_o = P[::2], P[1::2]$

$\quad$ $y_e, y_o = \text{IFFT}(P_e), \text{IFFT}(P_o)$

$\quad$ $y = [0] * n$

$\quad$ for j in range$(n/2)$:

$\quad\quad$ $y[j] = y_e[j] + \omega^j y_o[j]$

$\quad\quad$ $y[j + n/2] = y_e[j] - \omega^j y_o[j]$

$\quad$ return y

THX :-)