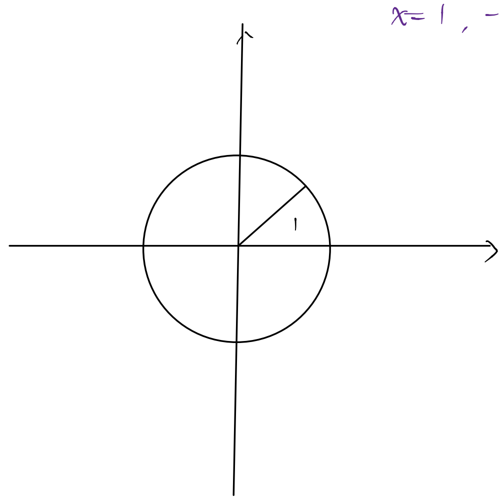
n^{th} roots of (unity $=1$) $n=2$ $\sqrt{1} = \{+1, -1\}$

$\{1, w, w^2 \dots w^{n-1}\}$ — n^{th} roots of 1

$x^n = 1$

4^{th} roots of unity. $\{x^4 = 1\}$

$x = 1, -1, i, -i$



n^{th} roots of unity

$=$ n equally spaced points on circle.

$w^k = (\cos 2\pi k/n + i \cdot \sin 2\pi k/n)$ t^{th} number.

$= e^{2\pi i/n \cdot t}$.

FOURIER TRANSFORM.

$a_0, \dots a_{n-1} \overset{FT.}{\Longrightarrow} A[1], \dots A[w^{n-1}]$

Time domain $\underset{IFT.}{\Leftarrow}$ Frequency domain.

$a_0, a_1 \dots a_{n-1}$

$\Downarrow$

$A[x] = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}$

$\Downarrow$.

$A[1], A[w] \dots A[w^{n-1}] \leftarrow$ evaluate at roots of unity.

$n = 4$ $\quad\quad (1, 2, 3, 4)$

$A[x] = 1 + 2x + 3x^2 + 4x^3$

$\Downarrow$.

evaluate $A[x]$ at 4^{th} roots of unity

$\{1, -1, i, -i\}$

$A[1] = 10$ $\quad\quad A[i] = -2 - 2i$

$A[-i] =$ $\quad\quad A[-1] =$

INPUT $a_0 \cdots a_{n-1}$

Goal: Compute $A[1] \cdots A[\omega^{n-1}]$

where $A[x] = a_0 + a_1 x + \cdots a_{n-1} x^{n-1}$

FFT $((a_1 \cdots a_n) \mid$ evaluate a degree n poly $A[x] = a_0 + \cdots + a_{n-1} x^{n-1}$ at n^{th} roots of unity $)$.

FFT$((\underbrace{\quad}_{\frac{n}{2}}))$

evaluate some $\deg \frac{n}{2}$ poly on $\frac{n}{2}^{th}$ roots of unity.

FFT$((\underbrace{\quad}_{\frac{n}{2}}))$.

$+ O(n)$ extra addition

$T[n] = n\log n.$

Prop 1 squaring nth roots of unity

gives you $n/2^{th}$ roots of unity.

$n=8.$

$A[x] = 0 + 1\cdot x + 2\cdot x^2 + 3x^3 + 4x^4 + 5\cdot x^5 + 6x^6 + 7x^7$

$A[1]$

$A[w]$

$A[w^2]$

$A[w^3]$

$A[w^4] = A[-1]$

$A[w^5] = A[-w]$

$A[w^6] = A[-w^2]$

$A[w^7] = A[-w^3]$

Compute A on 8^{th} roots of unity

$\Downarrow$

compute O, E, on squares of 8^{th} roots of unity.

$\parallel$

4^{th} roots of unity.

$A[t] = a_0 + a_1 t + a_2 t^2 + \cdots = (a_0 + a_2 t^2 + \cdots) + (a_1 t + a_3 t^3 + \cdots)$

$A[-t] = a_0 + a_1(-t) + a_2 t^2 + a_3(-t)^3 + \cdots$

$= a_0 - a_1 t + a_2 t^2 - a_3 t^3 + a_4 t^4 \cdots$

$x,$

$$= a_0 + a_2 t^2 + a_4 t^4 + a_6 t^6 - (a_1 t + a_3 t^3 + \cdots)$$

$$O(y) = a_1 + a_3 y + a_5 y^2 + \cdots$$

$$E(y) = a_0 + a_2 y + a_4 y^2 + \cdots$$

$$A[x] = E[x^2] + x O[x^2]$$

$$A[x] \to O(x^2)$$
$$E(x^2)$$

Application: Polynomial multiplication

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

$$= 2 + (2+1)\cdot x + (3+2+2)x^2 + (+)x^3 + 3x^4.$$

$$A(x) = a_0 + a_1 x + \cdots + a_n x^n$$

$$B(x) = b_0 + b_1 x + \cdots + b_n x^n.$$

want to find coefficients of $C(x) = A(x)\cdot B(x)$.

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

$c_0 = a_0 b_0$

$c_1 = a_0 b_1 + c_1 b_0$

$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2$

$\vdots$

$T(n) = 1 + 2 + 3 + \cdots = O(n^2)$

Inverse FFT

C is a polynomial of degree $N-1$, where N is a power of 2.

given $C(1), C(\omega), \dots C(\omega^{N-1})$

where $1, \omega, \dots \omega^{N-1}$ are N^{th} roots of unity

in $O(N \lg N)$ time find coefficients of C.

$\downarrow$

given $A(1), A(\omega) \dots A(\omega^{N-1})$

$B(1), B(\omega), \dots B(\omega^{N-1})$.

$\downarrow$

then in $O(N)$ time we can compute

$C(1) = A(1) \cdot B(1)$, $C(\omega) = A(\omega) B(\omega) \dots$

$C(\omega^{N-1}) = A(\omega^{N-1}) B(\omega^{N-1})$.

$\downarrow$

with FFT, given A, B.

compute $A(1) \cdots A(\omega^{N-1})$ in $O(N\log N)$ time

$B(1) \cdots B(\omega^{N-1})$

Input $A(x) = a_0 + \cdots + a_n x^n$

$B(x) = b_0 + \cdots + b_n x^n$.

Let N be a power of 2 $\geq 2n+1$ and $\leq 4n$.

$A(1), A(\omega) \cdots A(\omega^{N-1}) = FFT(A, N)$ $N\log N$.

$B(1), B(\omega) \cdots B(\omega^{N-1}) = FFT(B, N)$

$C(1) = A(1) \cdot B(1)$

$\vdots$ N.

$C(\omega^{N-1}) = A(\omega^{N-1}) B(\omega^{N-1})$

coefficient of $C = IFFT(C(1), \cdots C(\omega^{N-1}))$ $N\log N$