Polynomial multiplication:

Given vectors $a=(a_0,a_1,\ldots,a_{n-1})$ & $b=(b_0,b_1,\ldots,b_{n-1})$

Compute $c=a*b=(c_0,c_1,\ldots,c_{2n-2})$

where $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$

View a & b as coefficients to polynomials:

$$A(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1} \quad \& \quad B(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}$$

then $C(x)=A(x)B(x)=c_0+c_1+c_2x^2+\cdots+c_{2n-2}x^{2n-2}$

Terminology: $c=a*b$ is called the convolution of a & b

denoted as $*$

Example: $A(x)=1+2x+3x^2$, $B(x)=2-x+4x^2$

Then $C(x)=A(x)B(x)=2+3x+8x^2+5x^3+12x^4$

In this case, $a=(1,2,3)$, $b=(2,-1,4)$

& $c=a*b=(2,3,8,5,12)$

Naive approach: $O(k)$ time for $c_k \Rightarrow O(n^2)$ total time

Today: Using FFT = fast Fourier transform

can do in $O(n\log n)$ time.

<u>Linear filtering:</u> Replace a datapoint by a linear combination of neighboring points

Applications: reducing noise, adding effects, etc.

<u>Examples:</u>

<u>Mean filter:</u> data $y=(y_1,\dots,y_n)$

replace y_j by $\hat{y}_j = \frac{1}{2M+1}\sum_{i=-M}^{M} y_{j+i}$

$$\hat{y} = y * f \quad \text{where} \quad f = \frac{1}{2M+1}\underbrace{(1,1,\dots,1)}_{\substack{2M+1\\ \text{coordinates}}} = \left(\frac{1}{2M+1},\dots,\frac{1}{2M+1}\right)$$

<u>Gaussian filter:</u>

replace y_j by $\hat{y}_j = \frac{1}{Z}\sum_{i=-M}^{M} e^{-i^2} y_{j+i}$

where $Z = \sum_{i=-M}^{M} e^{-i^2}$

$$\hat{y} = y * f \quad \text{where} \quad f = \frac{1}{Z}\left(e^{-M^2}, e^{-(M-1)^2}, \dots, e^{-1}, 1, e^{-1}, \dots, e^{-M^2}\right)$$

<u>Gaussian blur:</u> 2-dimensional Gaussian filter applied to an image to blur it.

Back to multiplying polynomials:

For polynomial $A(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$

Two representations:

1) Coefficients $a_0, a_1, \ldots, a_{n-1}$

or 2) values: $A(x_0), A(x_1), \ldots, A(x_{n-1})$

<u>Lemma</u>: Poly. of degree $n-1$ is uniquely characterized by its values at any n distinct points

<u>Example</u>: line is defined by two points on the line.
deg. 1

<u>Proof idea</u>: Take the n points, plug into $A(x)$ and you get n independent equations in n variables.

<u>Key idea</u>: Multiplying polynomials is easy in values representation.

Given $A(x_0), A(x_1), \ldots, A(x_{2n})$, & $B(x_0), \ldots, B(x_{2n})$

then for $i = 0 \to 2n$,

$$C(x_i) = A(x_i) B(x_i)$$

$O(1)$ time for each i, so $O(n)$ total time.

<u>FFT</u>: converts between coefficients $\longleftrightarrow$ values for well-chosen set of points.

Given $a = (a_0, \dots, a_{n-1})$ for poly $A(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$

we want to compute $A(x_1), \dots, A(x_{2n})$

for $2n$ points $x_1, \dots, x_{2n}$ $\underbrace{\text{that we choose}}_{\text{HOW?}}$

<u>Key idea</u>: Suppose $x_1, \dots, x_n$ are opposites of $x_{n+1}, \dots, x_{2n}$

So: $x_{n+1} = -x_1,\ x_{n+2} = -x_2,\ \dots,\ x_{2n} = -x_n$

Look at $A(x_i)$ & $A(x_{n+i}) = A(-x_i)$

- Same on even terms $a_{2k} x^{2k}$
- opposite on odd terms $a_{2k+1} x^{2k+1}$ or $-a_{2k+1} x^{2k+1}$

This split $A(x)$ into even & odd terms

Let $a_{even} = (a_0, a_2, a_4, \dots, a_{n-2})$ & $a_{odd} = (a_1, a_3, a_5, \dots, a_{n-1})$

Thus, $A_{even}(y) = a_0 + a_2 y + a_4 y^2 + \dots + a_{n-2} y^{\frac{n-2}{2}}$ deg. $\frac{n}{2} - 1$

$A_{odd}(y) = a_1 + a_3 y + a_5 y^2 + \dots + a_{n-1} y^{\frac{n-2}{2}}$

<u>Note</u>: $A(x) = A_{even}(x^2) + x A_{odd}(x^2)$

<u>Thus:</u> $A(x_i) = A_{even}(x_i^2) + x_i A_{odd}(x_i^2)$

& $A(x_{n+i}) = A(-x_i) = A_{even}(x_i^2) - x_i A_{odd}(x_i^2)$

So given $A_{even}(y_1), \ldots, A_{even}(y_n)$ & $A_{odd}(y_1), \ldots, A_{odd}(y_n)$

for $y_1 = x_1^2, \ldots, y_n = x_n^2$

then in $O(n)$ time we get:

$A(x_1), \ldots, A(x_n), A(x_{n+1}), \ldots, A(x_{2n})$

<u>Punchline:</u> to get $A(x)$ of deg. $\leq n-1$ at $2n$ points

we need $A_{even}(y)$ & $A_{odd}(y)$ of deg. $\leq \frac{n}{2}-1$ at n points

then $O(n)$ time to merge.

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

<u>But:</u> next level of recursion has $y_1 = x_1^2, \ldots, y_n = x_n^2$

we want that:

$$y_1 = -y_{\frac{n}{2}+1} \Longleftrightarrow x_1^2 = -x_{\frac{n}{2}+1}^2$$

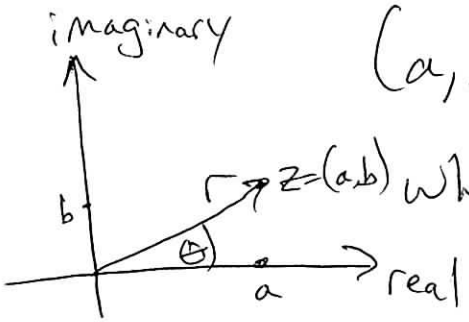
$$\vdots$$

$$y_{\frac{n}{2}} = -y_n \Longleftrightarrow x_{\frac{n}{2}}^2 = -x_n^2$$

this is impossible unless we use complex numbers.

Review of complex numbers:

Number $z = a + bi$ represented in the complex plane as (a, b) or in polar coordinates (r, θ)



where: $(a, b) = (r\cos\theta, r\sin\theta)$

Thus, $z = r(\cos\theta + i\sin\theta) = re^{i\theta}$

Euler's formula
(prove by taking Euler's expansions)

- Polar coordinates are convenient for multiplying:

$$(r_1, \theta_1) \times (r_2, \theta_2) = (r_1 r_2, \theta_1 + \theta_2)$$

So for $r = 1$, then $z = (1, \theta)$ & $z^n = (1, n\theta)$

also: $-1 = (1, \pi)$

thus for $z = (r, \theta)$ then $-z = (r, \theta + \pi)$

n^{th} complex roots of unity are solutions to $z^n = 1$

These are z where $z^n = 1 = (1, 2\pi j)$ for integer j.

for $z = (r, \theta)$ need that $r^n = 1$ so $r = 1$

& $n\theta = 2\pi j$ so $\theta = \frac{2\pi j}{n}$

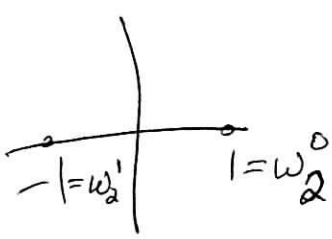
Let $\omega_n = \left(1, \frac{2\pi}{n}\right) = e^{2\pi i/n}$

Then n^{th} roots of unity are

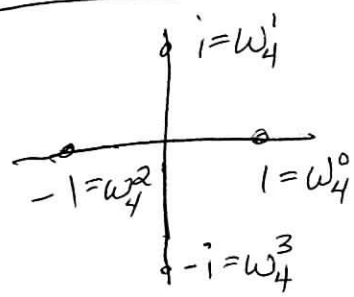
$$\omega_n^0, \omega_n^1, \omega_n^2, \ldots, \omega_n^{n-1}$$

note: $\omega_n^j = \left(1, \frac{2\pi j}{n}\right)$ & $(\omega_n^j)^n = (1, 2\pi j)$
$= 1.$ ✓

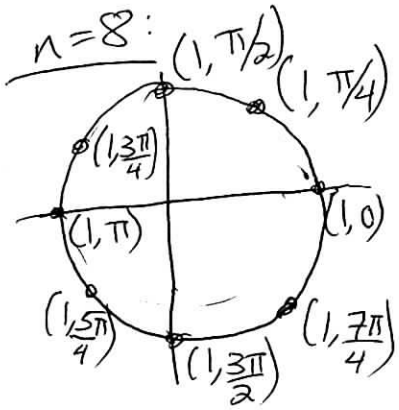
For $n=2$:



$n=4$:



$n=8$:



— Take unit circle & subdivide into n equally spaced points starting at 1.

Key properties:

1) For even n: satisfy $\pm$ property

$1^{st}\ \frac{n}{2}$ are opposite last $\frac{n}{2}$

$$\omega_n^0 = -\omega_n^{n/2}$$
$$\omega_n^1 = -\omega_n^{n/2+1}$$
$$\vdots$$
$$\omega_n^{\frac{n}{2}-1} = -\omega_n^{n-1}$$

to see this: $\omega_n^j = \left(1, \frac{2\pi}{n} j\right)$

then $\omega_n^{\frac{n}{2}+j} = \left(1, \frac{2\pi}{n}\left(\frac{n}{2}+j\right)\right) = \left(1, \pi + \frac{2\pi}{n} j\right)$

$$= -\left(1, \frac{2\pi}{n} j\right) = -\omega_n^j$$

2) For n which is a power of 2:

What are the squares of the nth roots?

$$\left(\omega_n^j\right)^2 = \left(1, \frac{2\pi j}{n}\right)^2 = \left(1, \frac{2\pi j}{n/2}\right) = \omega_{n/2}^j$$

$$\& \left(\omega_n^{j+\frac{n}{2}}\right)^2 = \left(-\omega_n^j\right)^2 = \omega_{n/2}^j$$

So $\left(n^{th}\text{ roots}\right)^2 = \left(\frac{n}{2}\right)^{th}$ roots.