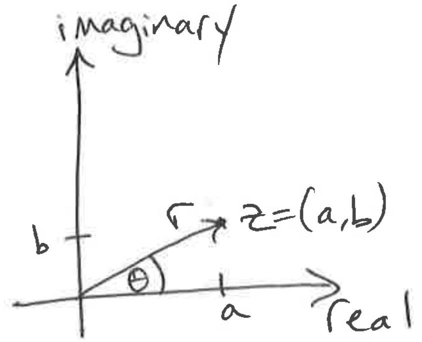
Review of complex numbers:

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

(can prove by taking Taylor'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 if $r = 1$, for $z = (1, \theta)$

then $z^n = (1, n\theta)$

another basic fact:

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

thus if $z = (r, \theta)$

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

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

They are numbers $z = (r, \theta)$ where $z^n = (1, 2\pi)$

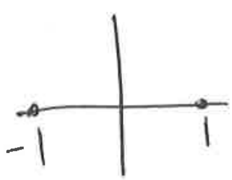
Thus, $r = 1$ & $n\theta = 2\pi j$ for integer j

Therefore, $\theta = \frac{2\pi}{n} j$ for $j = 0, 1, \ldots, n-1$ (this gets all distinct values)

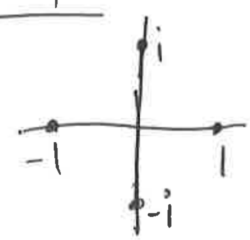
Let $\omega_n = \left(1, \frac{2\pi}{n}\right) = e^{2\pi i/n}$

The n^{th} roots of unity are $\underset{\substack{\shortparallel \\ 1}}{\omega_n^0}, \omega_n, \omega_n^2, \omega_n^3, \ldots, \omega_n^{n-1}$

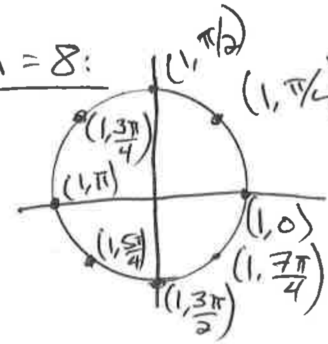
For $n=2$:



$n=4$:



$n=8$:



Key properties:

1) For even n: They satisfy the desired $\pm$ property — The 1^{st} $\frac{n}{2}$ are the opposite of the 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 it: for $\omega_n^j = \left(1, \frac{2\pi}{n} j\right)$

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

2) For n which is a power of 2:

What is the square of the n^{th} roots?

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

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

So the square of the n^{th} roots are the $\frac{n}{2}^{th}$ roots.

Recap from last lecture:

Take polynomial $A(x)$ of Deg. $\leq n-1$ (so $A(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$) where n is a power of 2.

We want to choose n points $x_0, x_1, \ldots, x_{n-1}$ to evaluate $A(x)$ at. (where $x_j = -x_{\frac{n}{2}+j}$ for $j = 0, \ldots, \frac{n}{2}-1$)

We will set $x_j = \omega_n^j$ for $j = 0, 1, \ldots, n-1$.

(so the n points are n^{th} roots of unity)

We then define $A_{even}(y)$ & $A_{odd}(y)$

where: $A_{even}(y) = a_0 + a_2 y + a_4 y^2 + \cdots + a_{n-2} y^{\frac{n}{2}-1}$

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

(these are both of degree $\leq \frac{n}{2} - 1$.)

Recursively we compute $A_{even}(y)$ & $A_{odd}(y)$ at:

$$y_0 = x_0^2 = x_{\frac{n}{2}}^2, \; y_1 = x_1^2 = x_{\frac{n}{2}+1}^2, \; \ldots, \; y_{\frac{n}{2}-1}^2 = x_{\frac{n}{2}-1}^2 = x_{n-1}^2$$

and these are the $\frac{n}{2}^{th}$ roots of unity by property 2.

Then we get $A(x)$ at the n points, by:

$$A(x) = A_{even}(x^2) + x\, A_{odd}(x^2)$$

This gives the FFT algorithm.
We present it in a more general form where given ω which is a $n^{\underline{th}}$ root of unity then we evaluate $A(x)$ at $x_0=\omega^0, x_1=\omega^1, \ldots, x_{n-1}=\omega^{n-1}$!
By setting $\omega=\omega_n=e^{2\pi i/n}$ we get the earlier outline.
But later we'll use the same algorithm with a different ω.

Here is the algorithm:

FFT(a,ω):

input: coefficients $a=(a_0,a_1,\ldots,a_{n-1})$ for polynomial $A(x)$ where n is a power of 2, & ω which is a $n^{\underline{th}}$ root of unity.

output: $A(\omega^0), A(\omega^1), A(\omega^2), \ldots, A(\omega^{n-1})$.

if $n=1$, return$(A(1))$

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

Call FFT(a_{even},ω^2) to get:

$$A_{even}(\omega^0), A_{even}(\omega^2), A_{even}(\omega^4), \ldots, A_{even}(\omega^{2(\frac{n}{2}-1)})$$

Call FFT(a_{odd},ω^2) to get:

$$A_{odd}(\omega^0), A_{odd}(\omega^2), \ldots, A_{odd}(\omega^{2(\frac{n}{2}-1)})$$

For $j=0 \to \frac{n}{2}-1$:

$$A(\omega^j)=A_{even}(\omega^{2j})+\omega^j A_{odd}(\omega^{2j})$$
$$A(\omega^{\frac{n}{2}+j})=A_{even}(\omega^{2j})+\omega^{\frac{n}{2}+j}A_{odd}(\omega^{2j})$$

Return$(A(\omega^0), A(\omega), A(\omega^2), \ldots, A(\omega^{n-1}))$.

This can be written more compactly as:

FFT(a, ω):

if $n=1$, return$(A(1))$
Let $a_{even} = (a_0, a_2, \ldots, a_{n-2})$ & $a_{odd} = (a_1, a_3, \ldots, a_{n-1})$
$(s_0, s_1, \ldots, s_{\frac{n}{2}-1}) = FFT(a_{even}, \omega^2)$
$(t_0, t_1, \ldots, t_{\frac{n}{2}-1}) = FFT(a_{odd}, \omega^2)$
For $j = 0 \to \frac{n}{2} - 1$:
$r_j = s_j + \omega^j t_j$
$r_{\frac{n}{2}+j} = s_j - \omega^j t_j$
Return$(r_0, r_1, \ldots, r_{n-1})$

Running time: $T(n) = 2T(\frac{n}{2}) + O(n) = O(n \log n)$.

To multiply $A(x)$ & $B(x)$ we first get $A(x)$ & $B(x)$ at the $2n^{th}$ roots of unity. Then we compute $C(x)$ at these $2n$ points. Finally we need to convert back to get the coefficients for $C(x)$ — How to do this last step (interpolate)?

For a polynomial $A(x)$ when we apply $FFT(a, \omega_n)$ we get
$A(\omega_n^0), A(\omega_n), \dots, A(\omega_n^{n-1})$.

In general for points $x_0, x_1, \dots, x_{n-1}$ we have that:

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ & & \vdots & & \\ 1 & x_n & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

For our case above we have $x_j = \omega_n^j$, thus:

$$\underbrace{\begin{bmatrix} A(1) \\ A(\omega_n) \\ A(\omega_n^2) \\ \vdots \\ A(\omega_n^{n-1}) \end{bmatrix}}_{\text{Call this vector } A} = \underbrace{\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_n & \omega_n^2 & \cdots & \omega_n^{n-1} \\ 1 & \omega_n^2 & \omega_n^4 & \cdots & \omega_n^{2(n-1)} \\ & & \vdots & & \\ 1 & \omega_n^{n-1} & \omega_n^{2(n-1)} & \cdots & \omega_n^{(n-1)(n-1)} \end{bmatrix}}_{= M_n(\omega_n)} \underbrace{\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix}}_{= a}$$

So: $A = M_n(\omega_n) a$

What's $M_n^{-1}(\omega_n)$?

If it's defined then: $M_n(\omega_n)^{-1} A = a$

So we can go from A to a

Lemma: $M_n(\omega_n)^{-1} = \frac{1}{n} M_n(\omega_n^{-1})$

What's ω_n^{-1}? $\omega_n^{-1} = \omega_n^{n-1}$ because:

$\omega_n^{n-1} \times \omega_n = \omega_n^n = 1$ since ω_n is a n^{th} root of unity.

Then to compute $M_n(\omega_n)^{-1} A$ we apply FFT.

In particular, $FFT(A, \omega_n^{n-1})$ gives

$M_n(\omega_n^{-1}) A = M_n(\omega_n)^{-1} A = na$.

To prove the lemma we need the following property of ω:

First notice that:

$$(z-1)(z^{n-1} + z^{n-2} + \cdots + z + 1) = z^n - 1$$

Set $z = \omega$ where ω is a n^{th} root of unity & $\omega \neq 1$:

$$(\omega-1)(\omega^{n-1} + \omega^{n-2} + \cdots + \omega + 1) = \omega^n - 1 = 0$$

Since $\omega^n = 1$ (because ω is a n^{th} root)

Thus, $(\omega-1)(\omega^{n-1} + \omega^{n-2} + \cdots + \omega + 1) = 0$

So $\omega - 1 = 0$ or $\underbrace{\omega^{n-1} + \omega^{n-2} + \cdots + 1 = 0}$

assuming $\omega \neq 1$ so it must be

Thus, for $\omega \neq 1$ which is a n^{th} root of unity, we know that:

$$\omega^{n-1} + \omega^{n-2} + \cdots + \omega + 1 = 0. \quad (*)$$

Now let's prove the lemma.
We need to show that:

$$\frac{1}{n} M_n(\omega_n^{-1}) M_n(\omega_n)^{-1} = I$$

I is the identity matrix $= \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$

Look at the diagonal entry of $M_n(\omega_n) M_n(\omega_n)^{-1}$

take row k of $M_n(\omega_n) = (1, \omega_n^k, \omega_n^{2k}, \ldots, \omega_n^{(n-1)k})$

& column k of $M_n(\omega_n^{-1}) = \begin{pmatrix} 1 \\ (\omega_n^{-1})^k \\ (\omega_n^{-1})^{2k} \\ \vdots \\ (\omega_n^{-1})^{(n-1)k} \end{pmatrix}$

Then entry (k,k) of $\frac{1}{n} M_n(\omega_n) M_n(\omega_n^{-1})$

$$= \frac{1}{n}\left(1, \omega_n^k, \omega_n^{2k}, \ldots, \omega_n^{(n-1)k}\right) \cdot \left(1, (\omega_n^{-1})^k, (\omega_n^{-1})^{2k}, \ldots, (\omega_n^{-1})^{(n-1)k}\right)$$

$$= \frac{1}{n}(1 + 1 + \cdots + 1)$$

$$= 1$$

So the diagonals are correct.

For the off-diagonal's, take row k of $M_n(\omega_n)$

& column j of $M_n(\omega_n^{-1})$

for $k \neq j$.

Then we have:

$$\frac{1}{n}\left(1, \omega_n^{k}, \omega_n^{2k}, \ldots, \omega_n^{(n-1)k}\right) \cdot \left(1, (\omega_n^{-1})^{j}, (\omega_n^{-1})^{2j}, \ldots, (\omega_n^{-1})^{(n-1)j}\right)$$

$$= \frac{1}{n}\left(1 + \omega_n^{k-j} + \left(\omega_n^{k-j}\right)^2 + \left(\omega_n^{k-j}\right)^3 + \cdots + \left(\omega_n^{k-j}\right)^{n-1}\right)$$

Since $k \neq j$ then $k - j \neq 0$

and since ω_n is a n^{th} root of unity

then ω_n^{l} for integer l is also a n^{th} root.

Finally, $\omega_n \neq 1$ for $n > 1$,

So $\omega_n^{k-j} \neq 1$ since $k - j \neq 0$

thus we know that for $\omega = \omega_n^{k-j}$, by $(*)$,

$$\omega^{n-1} + \omega^{n-2} + \cdots + \omega + 1 = 0$$

thus ______

$= 0$

therefore the off-diagonals are also correct.

This proves the lemma.