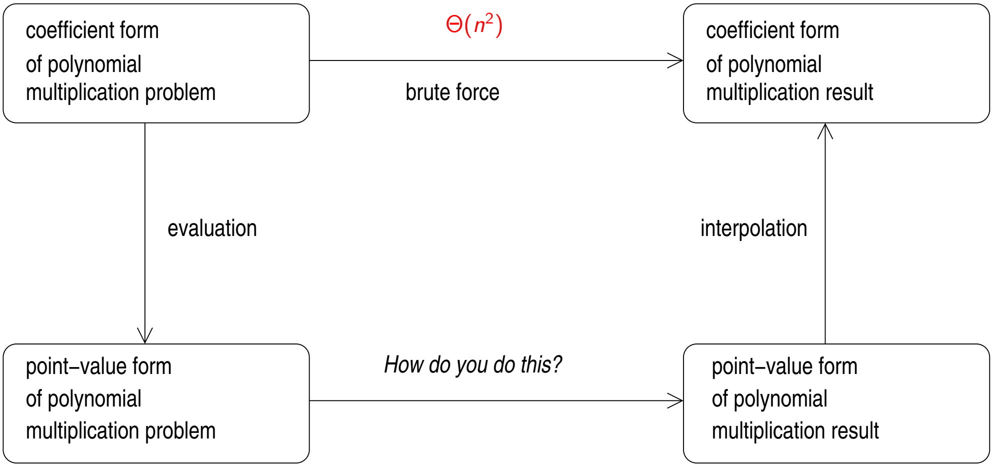
II. Topics / A. Fast Fourier transform

- Intoduction to premise and problem (Wednesday)
- The complex roots of unity (**Today**)
- FFT algorithm details (next week Friday, Oct 25)

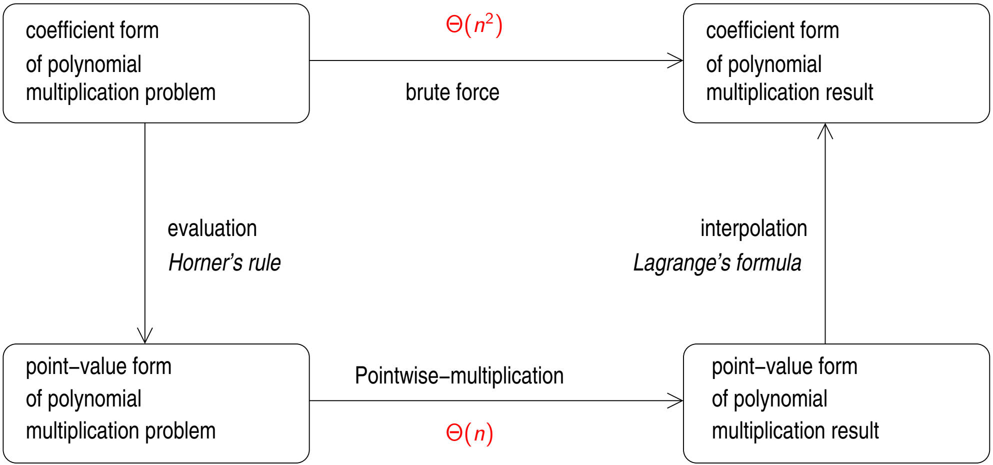
Today:

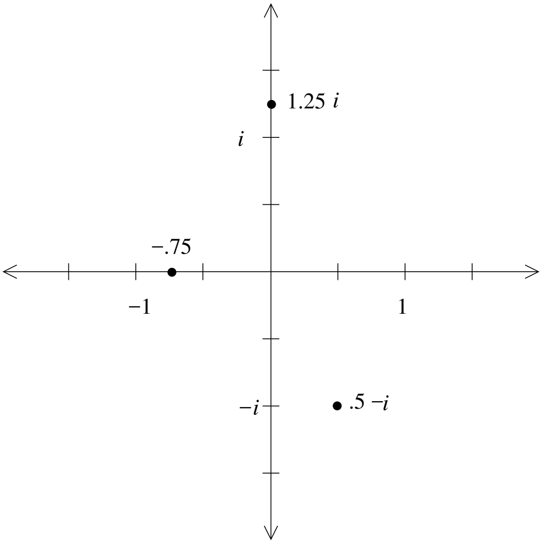
- Review of problem and goals
- Divide-and-conquer polynomial evaluation
- The complex roots of unity


coefficient form
of polynomial
multiplication problem
$\Theta(n^2)$
brute force
coefficient form
of polynomial
multiplication result
evaluation
interpolation
point–value form
of polynomial
multiplication problem
How do you do this?
point–value form
of polynomial
multiplication result

Lagrange's formula for interpolation:
Given n points, $(x_0, y_0), \ldots (x_{n-1}, y_{n-1})$,

$$A(x) = \sum_{k=0}^{n-1} y_k \frac{\prod_{j \neq k}(x - x_j)}{\prod_{j \neq k}(x_k - x_j)}$$


coefficient form
of polynomial
multiplication problem
$\Theta(n^2)$
brute force
coefficient form
of polynomial
multiplication result
evaluation
Horner's rule
interpolation
Lagrange's formula
point–value form
of polynomial
multiplication problem
Pointwise–multiplication
$\Theta(n)$
point–value form
of polynomial
multiplication result



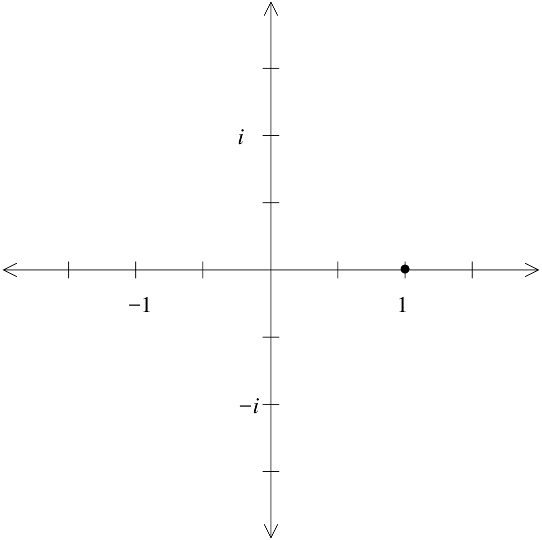
$i = \sqrt{-1}$

$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$

$\mathbb{C}$ can be represented as $\mathbb{R} \times \mathbb{R}$.

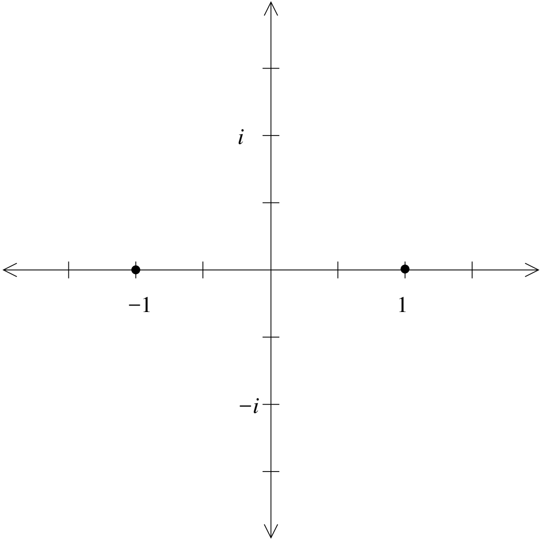
$e^{\pi i} = -1$

An nth *complex root of unity* is $\omega \in \mathbb{C}$ such that $\omega^n = 1$.



$n = 1$

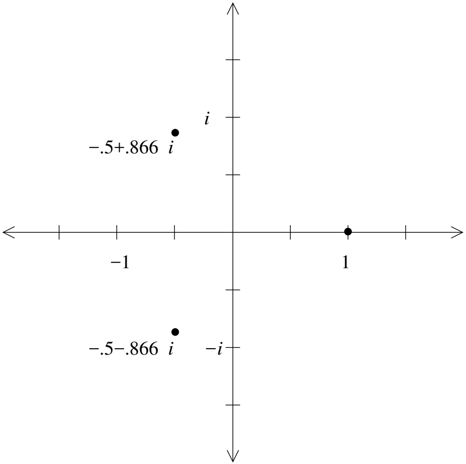
$1^1 = 1$



$n = 2$

$1^2 = 1$

$(-1)^2 = 1$



$n = 3$

$1^3 = 1$

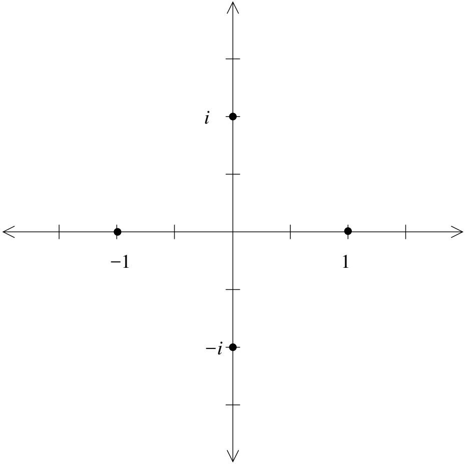
$(e^{\frac{2\pi i}{3}})^3 = (e^{\pi i})^2 = (-1)^2 = 1$

$(e^{\frac{4\pi i}{3}})^3 = (e^{2\pi i})^2 = (1)^2 = 1$

Moreover...

$e^{\frac{2\pi i}{3}} = \cos(\frac{2}{3}\pi) + i\sin(\frac{2}{3}\pi) = -.5 + .866i$

$e^{\frac{4\pi i}{3}} = \cos(\frac{4}{3}\pi) + i\sin(\frac{4}{3}\pi) = -.5 - .866i$



$n = 4$

$1^4 = 1$

$i^4 = (i^2)^2 = (-1)^2 = 1$

$(-1)^4 = 1$

$(-i)^4 = (i^2)^2 = 1$

In general, the *principal nth root of unity* is $\omega_n = e^{\frac{2\pi i}{n}}$

The n complex nth roots of unity are $\omega_n^0, \omega_n^1, \ldots, \omega_n^{n-1}$.

Note that $\omega_n = \omega_n^1$ and $\omega_n^0 = \omega_n^n = 1$.

Note also that $\omega_n^k = e^{\frac{2\pi i}{n}k} = e^{\frac{2k\pi i}{n}} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$

Cancellation lemma. (30.3)
For any integers $n \geq 0$, $k \geq 0$, and $d > 0$, $\omega_{dn}^{dk} = \omega_n^k$.

Proof. $\omega_{dn}^{dk} = (\omega_{dn})^{dk} = (e^{\frac{2\pi i}{dn}})^{dk} = (e^{\frac{2\pi i}{n}})^k = \omega_n^k$. $\square$

Corollary to above. (30.4)
For any even integer $n > 0$, $\omega_n^{\frac{n}{2}} = \omega_2 = -1$

In general, the *principal nth root of unity* is $\omega_n = e^{\frac{2\pi i}{n}}$

The n complex nth roots of unity are $\omega_n^0, \omega_n^1, \ldots, \omega_n^{n-1}$.

Note that $\omega_n = \omega_n^1$ and $\omega_n^0 = \omega_n^n = 1$.

Note also that $\omega_n^k = e^{\frac{2\pi i}{n}k} = e^{\frac{2k\pi i}{n}} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$

Cancellation lemma. (30.3)
For any integers $n \geq 0$, $k \geq 0$, and $d > 0$, $\omega_{dn}^{dk} = \omega_n^k$.

Proof. $\omega_{dn}^{dk} = (\omega_{dn})^{dk} = (e^{\frac{2\pi i}{dn}})^{dk} = (e^{\frac{2\pi i}{n}})^k = \omega_n^k$. $\square$

Corollary to above. (30.4)
For any even integer $n > 0$, $\omega_n^{\frac{n}{2}} = \omega_2 = -1$

Proof. Let m be such that $n = 2m$. Then $\omega_n^{\frac{n}{2}} = \omega_{2m}^m = \omega_2 = -1$. $\square$

Cancellation lemma rewritten.
If d is a common divisor of n and k, then $\omega_n^k = \omega_{\frac{n}{d}}^{\frac{k}{d}}$.