Polynomial multiplication:

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

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

where $c_k = a_0 b_k + a_1 b_{k-1} + ... + a_{k-1} b_1$

View $a$ & $b$ as coefficients to polynomials:

$A(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1}$ & $B(x) = b_0 + b_1 x + ... + b_{n-1} x^{n-1}$

Then $C(x) = A(x) B(x) = c_0 + c_1 x + c_2 x^2 + ... + c_{2n-2} x^{2n-2}$

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

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

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

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

Today: Using FFT = fast Fourier transform can do in $O(n \log n)$ time.
Linear filtering: Replace a data point by a linear combination of neighboring points.

Applications: reducing noise, adding effects, etc.

Examples:

Mean filter: data \( y = (y_1, \ldots, y_n) \)
replace \( y_j \) by \( \hat{y}_j = \frac{1}{2m+1} \sum_{i=-m}^{m} y_{j+i} \)

\( \hat{y} = y * f \) where \( f = \frac{1}{2m+1} \begin{bmatrix} 1 & 1 & \ldots & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2m+1} & \ldots & \frac{1}{2m+1} \end{bmatrix} \)

Gaussian filter:
replace \( y_j \) by \( \hat{y}_j = \frac{1}{Z} \sum_{i=-m}^{m} e^{-i^2} y_{j+i} \)
where \( Z = \sum_{i=-m}^{m} e^{-i^2} \)

\( \hat{y} = y * f \) where \( f = \frac{1}{Z} \begin{bmatrix} e^{-m^2} & e^{-(m-1)^2} & \ldots & e^{-1} & e^{0} & \ldots & e^{m^2} \end{bmatrix} \)

Gaussian blur: 2-dimensional Gaussian filter applied to an image to blur it.
Back to multiplying polynomials:

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

Two representations:

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

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

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

Example: line is defined by two points on the line.

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

Key idea: 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 $i = 0 \Rightarrow 2n$,

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

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

FFT: converts between coefficients $\leftrightarrow$ values for well-chosen set of points.
Given \( a = (a_0, \ldots, a_{n-1}) \) for poly \( A(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \), we want to compute \( A(x_1), \ldots, A(x_{2n}) \) for \( 2n \) points \( x_1, \ldots, x_{2n} \) that we choose. How?

**Key idea:** Suppose \( x_1, \ldots, x_n \) are opposites of \( x_{n+1}, \ldots, x_{2n} \).

So: \( x_{n+1} = -x_1, x_{n+2} = -x_2, \ldots, x_{2n} = -x_n \)

Look at \( A(x_i) \) & \( A(x_{n+1}) = A(-x_i) \)

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

Thus, \( A_{\text{even}}(y) = a_0 + a_2 y + a_4 y^2 + \cdots + a_{n-2} y^{\frac{n-2}{2}} \) \( \deg \frac{n-2}{2} \)

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

**Note:** \( A(x) = A_{\text{even}}(x^2) + xA_{\text{odd}}(x^2) \)
Thus: \[ A(x_i) = \text{Aeven}(x_i^2) + x_i \text{Aodd}(x_i^2) \]
& \[ A(x_{n+1}) = A(-x_i) = \text{Aeven}(x_i^2) - x_i \text{Aodd}(x_i^2) \]

So given \( \text{Aeven}(y_1), \ldots, \text{Aeven}(y_n), \text{Aodd}(y_1), \ldots, \text{Aodd}(y_n) \)
for \( y_i = x_i^2, \ldots, y_n = x_n^2 \)

then in \( O(n) \) time we get:
\[ A(x_1), \ldots, A(x_n), A(x_{n+1}), \ldots, A(x_{2n}) \]

Punchline: to get \( A(x) \) of \( \text{deg} \leq n - 1 \) at \( 2n \) points
we need \( \text{Aeven}(y) \) of \( \text{deg} \leq \frac{n}{2} - 1 \) at \( n \) points
then \( O(n) \) time to merge.

\[ T(n) = 2T\left(\frac{n}{2}\right) + O(n) = O(n \log n) \]

But next level of recursion has \( y_i = x_i^2, \ldots, y_n = x_n^2 \)
we want that:
\[ y_1 = -y_{\frac{n}{2}+1} \iff x_1^2 = -x_{\frac{n}{2}+1}^2 \]
\[ \vdots \]
\[ y_{\frac{n}{2}} = -y_n \iff x_{\frac{n}{2}}^2 = -x_n^2 \]

This is impossible unless we use complex numbers.
Review of complex numbers:

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

$z = (a, b) \text{ where: } (a, b) = (r \cos \theta, r \sin \theta)$

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

Euler's formula
(Prove by taking Euler's expression)

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 $-z = (r, \theta + \pi)$
The $n^{th}$ 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 $r = 1$ and $n\theta = 2\pi j$ so $\theta = \frac{2\pi j}{n}$.

Let $w_n = (1, \frac{2\pi}{n}) = e^{2\pi j/n}$.

Then $n^{th}$ roots of unity are $w_n^0, w_n^1, w_n^2, \ldots, w_n^{n-1}$.

Note: $w_n^j = (1, \frac{2\pi j}{n})$ and $(w_n^j)^n = (1, 2\pi j) = 1$. ✓

For $n = 2$:

- $1 = w_2^0$
- $-1 = w_2^1$

For $n = 4$:

- $1 = w_4^0$
- $i = w_4^1$
- $-1 = w_4^2$
- $-i = w_4^3$

Take unit circle & subdivide into $n$ equally spaced points starting at 1.
Key Properties:

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

\[
\begin{align*}
1 + \frac{n}{2} & \text{ are opposite } 1 - \frac{n}{2} \\
\omega_n^0 &= -\omega_n^{n/2} \\
\omega_n^1 &= -\omega_n^{n/2 + 1} \\
& \quad \vdots \\
\omega_n^{n-1} &= -\omega_n^{n-1}
\end{align*}
\]

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

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

2) For \( n \) which is a power of 2:

What are the squares of the \( n^{th} \) roots?

\[
(\omega_n^j)^2 = (1, \frac{2\pi j}{n})^2 = (1, \frac{2\pi j}{n/2}) = \omega_n^{2j}
\]
\[
2(\omega_n^{n/2})^2 = (-\omega_n^j)^2 = \omega_n^{j^2} = \omega_n^{j/2}
\]

So \((n^{th} \text{ roots})^2 = (\frac{n}{2})^{48} \text{ roots}\).