$\boxed{\text{21 Feb}}$ Multiplying polynomials and convolution.

Example. $(2x+1)(4x-3) = 8x^2 - 2x - 3$

$$\left.\begin{array}{r} 2x + 1 \\ 4x - 3 \\ \hline -6x - 3 \\ 8x^2 + 4x \quad \\ \hline 8x^2 - 2x - 3 \end{array}\right\}$$

Quadratic time
$O(\text{degree}^2)$
arithmetic operations

If $\quad A(x) = A_1 x + A_0$

$\quad B(x) = B_1 x + B_0$

and $\quad C(x) = A(x)\, B(x)$

then $\quad C(x) = A_1 B_1 x^2 + [A_0 B_1 + A_1 B_0]x + A_0 B_0$

$\quad = P_1 x^2 + (P_2 - P_1 - P_0)x + P_0$

where $\quad P_0 = A_0 B_0$

$\quad P_1 = A_1 B_1$

$\quad P_2 = (A_0 + A_1)(B_0 + B_1)$

This is the basis of an $O(n^{\log_2 3})$ algorithm for multiplying degree n polynomials, similar to Karatsuba's.

Why multiplying polynomials matters...

1. Basic operation in algebra.

2. Underpinning of integer multiplication (crypto)

   A binary number of n bits is just a degree $n-1$ polynomial evaluated at $x=2$, with $\{0,1\}$ coefficients.

3. Polynomials can represent signals (sequences of numbers).

   Multiplication represents convolution.

   Ex. Take the sequence

   0 2 4 3 4 1

   $\ldots, 0, 0, 4, 8, 2, 0, 0, \ldots$

   and replace every element with the average of the preceding and following ones.

$$
\begin{array}{r}
(4x^3 + 8x^2 + 2x + 0) \\
\frac{1}{2}x^2 \qquad\qquad + \frac{1}{2} \\
\hline
2x^3 + 4x^2 + x + 0 \\
2x^5 + 4x^4 + x^3 + 0 \qquad\qquad\qquad \\
\hline
2x^5 + 4x^4 + 3x^3 + 4x^2 + x + 0
\end{array}
$$

2 4 3 4 1 0

If $a_0, a_1, a_2, \ldots, a_n$

$b_0, b_1, b_2, \ldots, b_m$

are two sequences, their convolution is the sequence $c_0, c_1, c_2, \ldots, c_{m+n}$ where

$$\boxed{c_k = \sum_{i+j=k} a_i b_j}$$

e.g.

$$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0.$$

Often (a_i) is a "signal" / "image"

(b_j) is a "mask" / "weights"

If the sequences (a_i), (b_j) are encoded as polynomials

$$A(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

$$B(x) = b_0 + b_1 x + \ldots + b_m x^m$$

then their product $A \cdot B$ is a polynomial whose coeffs are the convolution of (a_i) and (b_j).

3. Multiplying polynomials encodes summing independent random variables.

Ex. if one rolls two standard dice what is the probability of every possible sum?

outcome :	1	2	3	4	5	6
probability :	1/6	1/6	1/6	1/6	1/6	1/6

$$\frac{1}{6}\left(x+x^2+x^3 \cdots + x^6\right)$$

"Prob. generating function"

$$\sum_i \Pr(i)\, x^i$$

If two indep rand. vars. have prob. gen. func's A and B

$$A(x) = \sum a_i x^i = \sum \Pr(\text{"variable A"} = i) \cdot x^i$$

$$B(x) \quad \text{---} \quad \text{---} \quad \text{``}$$

then $A(x) \cdot B(x)$ is the PGF of their sum.

Ex. $$\frac{1}{36}\left(x+x^2+x^3+x^4+x^5+x^6\right)^2$$

$$= \frac{1}{36}x^2 + \frac{2}{36}x^3 + \frac{3}{36}x^4 \cdots + \frac{2}{36}x^{11} + \frac{1}{36}x^{12}$$