DIS 5A

POLYNOMIALS

a **polynomial p** of **degree d**

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0$$

can be uniquely defined by either

1. its d+1 coefficients $(a_d, a_{d-1}, \ldots a_0)$
2. d+1 points (x_i, y_i) with distinct x_i's

and has at most **d** roots

---

we can work with polynomials in a **finite field**:

GF(p) means we work mod p (for prime p)

LAGRANGE INTERPOLATION

given: $d+1$ points $(x_1, y_1) \dots (x_{d+1}, y_{d+1})$

goal: find degree d polynomial that passes through all of these points

method: example with $d=2$

given (x_1, y_1) (x_2, y_2) (x_3, y_3)

construct $\Delta_i(x) = \underbrace{\prod_{j \neq i} (x - x_j)}_{=0 \text{ when } x \neq x_i} \underbrace{\left(\prod_{j \neq i} (x_i - x_j) \right)^{-1}}_{=1 \text{ when } x = x_i}$

$\Delta_1(x) = (x-x_2)(x-x_3)((x_1-x_2)(x_1-x_3))^{-1}$

$\Delta_2(x) = \dots$

$\Delta_3(x) = \dots$

similar to CRT!

$P(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) + y_3 \Delta_3(x)$

SECRET SHARING

in the traditional secret sharing scheme:

we want at least k people to collaborate to access the secret.

→ use a degree $k-1$ polynomial $f(x)$
(and work in $GF(p)$ where $p \geq k+1$)

→ let $f(0) =$ secret (not distributed)

→ each person is given one (distinct) point on the polynomial

↓

any group of k people can come together to construct f (Lagrange interpolation) and retrieve $f(0)$.