recap

Polynomials : $p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x^1 + a_0 x^0$

degree

d+1 terms

constant

Properties : ① nonzero polynomial of degree d has at most d roots

② a set of d+1 distinct coordinates (x_i, y_i) where all x_i are distinct uniquely characterizes a polynomial of degree (at most) d

GF(p) : all values are $\{0 \dots p-1\}$

finite field

$x^{p-1} \equiv 1$ GF(p) $\longrightarrow$ in GF(5), $x^7 \equiv x^3$

Secret Sharing :

- need d+1 people to unlock a secret
- hide secret at $x=0$ of a degree d polynomial
- give individual people one point each
- secret will only be revealed if a d+1 people agree to share their point

recap **Lagrange Interpolation**

goal: find degree d polynomial given $d+1$ (x,y) pairs.

(x_1, y_1)

(x_2, y_2)

(x_3, y_3)

find $\Delta_i(x)$ st $\Delta_i(x_i) = 1$, $\Delta_i(\text{anything else}) = 0$

basis polynomial

① start with the zeros. want x_2 and x_3 to be zeros of Δ_i.

$\Delta_1(x) = c_1(x - x_2)(x - x_3)$

② find c_1 st $\Delta_1(x_1) = 1$

→ if in $\mathbb{R}$: $c_1 = \dfrac{1}{(x_1 - x_2)(x_1 - x_3)}$

→ if in $GF(p)$: $c_1 = (x_1 - x_2)(x_1 - x_3)^{-1}$ mod p

find Δ_2, Δ_3 same way.

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

things to remember

- an odd degree polynomial must have at least 1 root
- fix the x values when looking @ # of possible points for the polynomial.
- secret at $p(0)$. make sure not to give out $p(0)$ to anyone when distributing points!

thanks for coming! help me help you → https://www.tinyurl.com/aishani-sp21-fb