Number Theory Motivation:

Shamir's Secret Sharing

02/12 Prof. Forrest

Warm-up

1. Discuss with your neighbors the place you would live, if you could live anywhere

2. Use a direct proof to show that the product of two odd numbers is odd.

$p \to q$

p is true

show that q is true

p, q are odd integers $\to$ pq is odd

$p := 2k+1$ $\quad q : 2l+1$

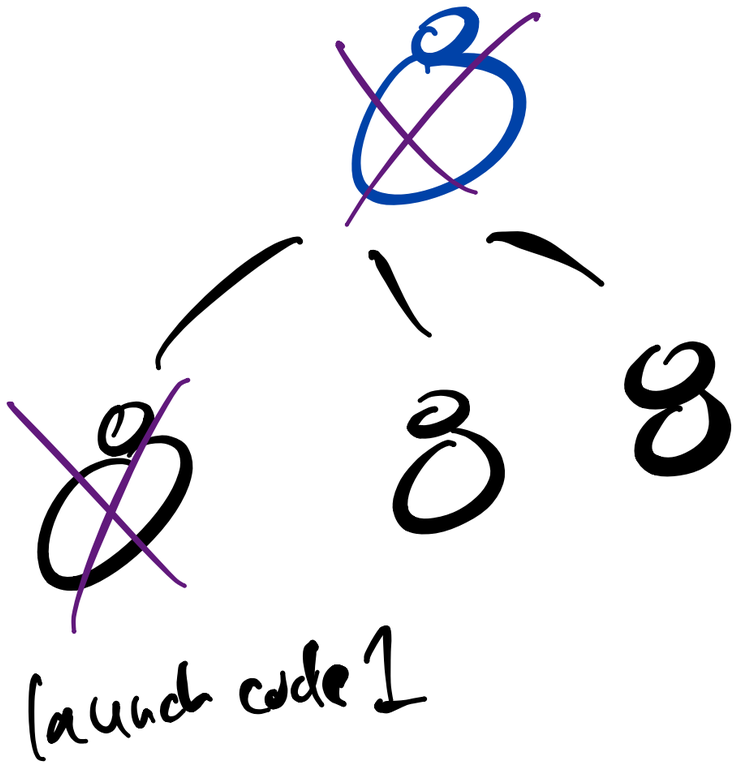
$$p \cdot q = (2k+1)(2l+1) = (4kl + 2k + 2l) + 1$$
$$2(2kl + k + l) + 1$$

Logisitics

Proof Assignment 1 due Monday

Lab 2 due Friday

Midterm Exam 1 has been shifted to March 5



launch code 1

launch code = 1 2 4 6 | 3 2 7 1

shared

person 1

shared

person 2

launch = $10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10$

$$\frac{10 \cdot 10 \cdot 10 \cdot 10}{}$$

$$10^2$$

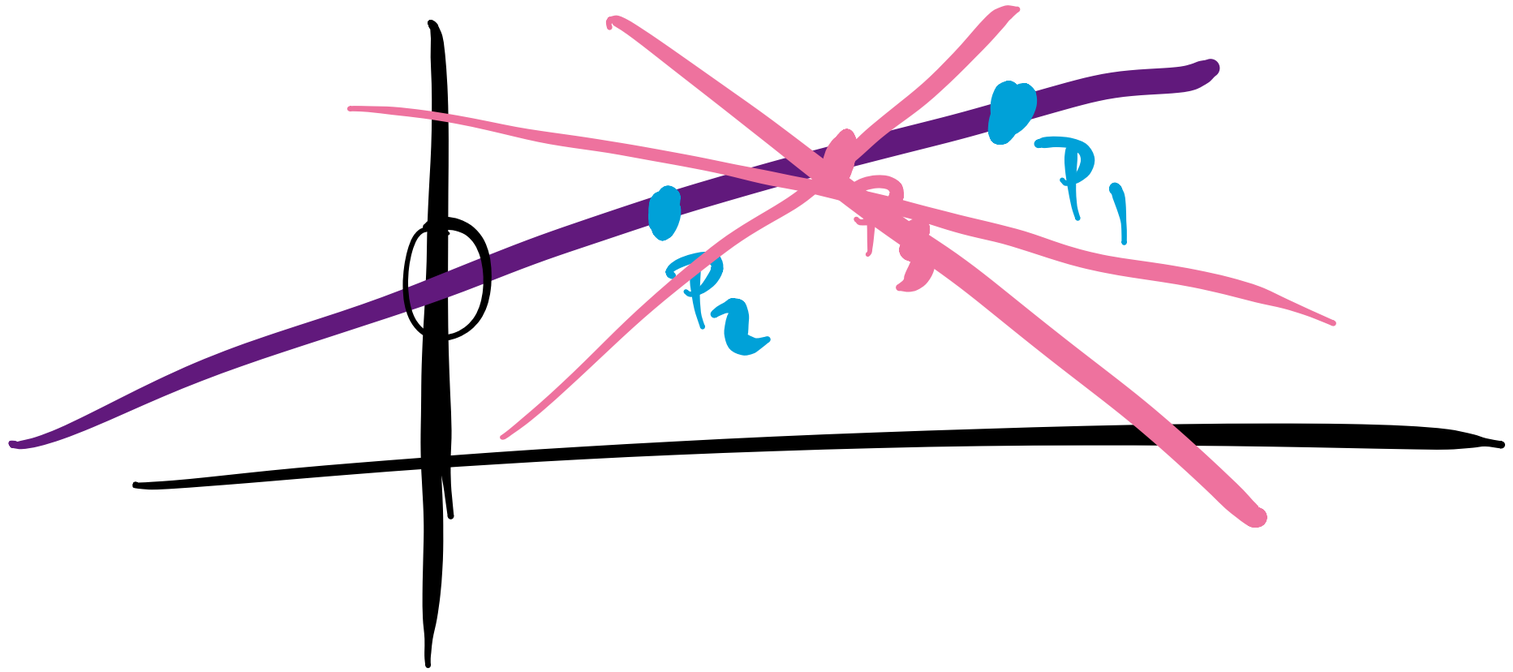
$$1000$$

$$10,000$$

Goals

1. You need a specific # of people to agree (≥) any ≤ people

2. any group ≤ ≤ to have not learned anything



$$a_1 x + b = y$$

degrees of freedom

a line has
2 degrees of freedom

a $\bigvee$ has
3 degrees of freedom

⋮

- Secret code
- have a secret Polynomial
- secure channel where I share some info

Secret = 22

$k = 2$

$a_1 \in \mathbb{Z}$

$f(x) = b + a_1 x$

b ↗ secret

$a_1 = 7$

$f(x) = 22 + a_i x = 22 + 7x$

known to me

Note that $f(0)$ is our secret.

$f(1) = 29$

$f(2) = 36$

$f(3) = 43$

$f(n) = \dots$

$f(1) = 29$

$f(2) = 36$

$29 = \text{secret} + a(1)$

$36 = \text{secret} + a(2)$

$29 - \text{secret} = a$

$36 = \text{secret} + a(2)$

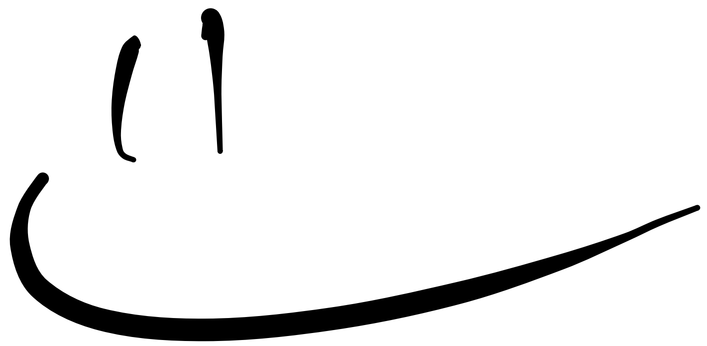
$= \text{secret} + (29 - \text{secret})(2)$

$36 = \text{secret} + \cancel{29(2)}^{58} - 2(\text{secret})$

$36 = \text{secret} + 58 - 2(\text{secret})$

$\text{secret} = 58 - 36$

$= 22$



Lagrange basis polynomial

$L(x)$ this L is unique

for some degree of freedom

Lagrange interpolating polynomial Definition

Given a set of $k+1$ points $\{x_0, x_1, \ldots, x_k\}$ which are all distinct ($x_j \neq x_m$ for indices $j \neq m$) $\{1, 2, 0, 1\}$ ($x_0 = x_3$ and $0 \neq 3$)

the Lagrange basis for polynomials of degree $\leq k$ for those points is the set of polynomials $\{l_0(x), l_1(x), \ldots, l_k(x)\}$ each of degree k which take values $l_j(x_m) = 0$ if $m \neq j$ and $l_j(x_j) = 1$.

Definition of each Lagrange basis polynomial

$$l_j(x) = \prod_{\substack{0 \leq m \leq k \\ m \neq j}} \frac{x - x_m}{x_j - x_m}$$

$$= \frac{x - x_0}{x_j - x_0} \cdots \frac{x - x_{j-1}}{x_j - x_{j-1}} \frac{x - x_{j+1}}{x_j - x_{j+1}} \cdots \frac{x - x_k}{x_j - x_k}$$

the lagrange interpolating polynomial for those points through the corresponding values $\{y_0, y_1, \ldots, y_k\}$ is the linear combination

$$L(x) = \sum_{j=0}^{k} y_j l_j(x)$$

An example of Lagrange interpolation polynomials

Say I want to write the $L(x)$ when my true polynomial is x^2. I need 3 points

my points

$x_0 = 1$ $\quad y_0 = f(x_0) = 1$

$x_1 = 2$ $\quad y_1 = f(x_1) = 4$

$x_2 = 3$ $\quad y_2 = f(x_2) = 9$

---

the lagrange interpolating polynomial for these points through the corresponding values $\{y_0, y_1, \dots, y_k\}$ is the linear combination

$$L(x) = \sum_{j=0}^{k} y_j \ell_j(x)$$

$$L(x) = \sum_{j=0}^{3} y_j \ell_i(x)$$

$$= y_0 \ell_0(x) + y_1 \ell_1(x) + y_2 \ell_2(x)$$

$$= 1 \cdot \left[\frac{x-2}{1-2}\frac{x-3}{1-3}\right] + 4\left[\frac{x-1}{2-1}\frac{x-3}{2-3}\right] + 9\left[\frac{x-1}{3-1}\frac{x-2}{3-2}\right]$$

$$= 1 \cdot \left[\tfrac{1}{2}x^2 - \tfrac{5}{2}x + 3\right] + 4\left[-x^2 + 4x - 3\right] + 9\left[\tfrac{1}{2}x^2 - \tfrac{3}{2}x + 1\right]$$

$$= \tfrac{1}{2}x^2 - 4x^2 + \tfrac{9}{2}x^2 + \left(-\tfrac{5}{2}x\right) + 16x + \left(-\tfrac{27}{2}x\right) + 3 + (-12) + 9$$

$$L(x) = x^2$$

$\Rightarrow L(x) = x^2$ which was our o.g. function

Definition of each lagrange basis polynomial

$$\ell_j(x) = \prod_{\substack{0 \le m \le k \\ m \neq j}} \frac{x - x_m}{x_j - x_m}$$

$$= \frac{x-x_0}{x_j - x_0} \cdots \frac{x - x_{j-1}}{x_j - x_{j-1}} \frac{x - x_{j+1}}{x_j - x_{j+1}} \cdots \frac{x - x_k}{x_j - x_k}$$

$$\ell_0(x) = \prod_{\substack{0 \le m \le k \\ m \neq j}} \frac{x - x_m}{x_j - x_m}$$

$$= \frac{x - x_1}{x_0 - x_1} \frac{x - x_2}{x_0 - x_2}$$

(Skipped $\frac{x-x_0}{x_0-x_0}$ because $j=0$ & $m=0$)

$$= \frac{x-2}{1-2} \frac{x-3}{1-3}$$

$$\ell_1(x) = \frac{x-1}{2-1} \frac{x-3}{2-3}$$

$$\ell_2(x) = \frac{x-1}{3-1} \frac{x-2}{3-2}$$

Find my secret

$k=3$

$f(3)=162$

$f(7)=298$

$f(8)=347$

$$l_1(x) = \frac{x-7}{3-7}\frac{x-8}{3-8} \qquad l_2(x) = \frac{x-3}{7-3}\frac{x-8}{7-8} \qquad l_3(x) = \frac{x-3}{8-3}\frac{x-7}{8-7}$$

$$L(x) = 142 \cdot l_1(x) + 298\, l_2(x) + 347\, l_3(x)$$

$$L(0) = 123$$

1. $f(1000)$ = very large

10,000 ~ ----.

~~overflow~~

2. $\frac{X-8}{3-8}$ = 1.33333333

1.66667

floating precision

We need some way to practically implement secret sharing technique

Mod p

$$f(x) = \left(m + \sum_{i=1}^{k-1} a_i x^i\right) \bmod p$$

m: secret

k^{th} degree polynomial

p: prime

General form of Shamir's Secret Sharing (1979)

Say $k = 4$

$$f(x) = m + \sum_{i=1}^{4-1} a_i x^i$$

$$= m + a_1 x + a_2 x^2 + a_3 x^3$$

We need

1. Mod
2. **Mod** arthmetic
3- Mod division
4. primes