Question of the day:

- Someone gives a gift to Yining, Khalid and Amin.
- The gift is in a locked chest with a long password.
- How should we share some information about the password with the instructors, such that at least two of the three instructors need to share their information to figure out the password?
Secret sharing

Share secret among N people.

Secrecy: Any K-1 knows nothing.
Robustness: Any K knows the secret
Efficient: Minimize storage

solution? Polynomials!

The idea:

Two Points make a unique.

This lecture:

d+1 Points make a unique degree d Polynomial.

Polynomials:

\[ P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0 \]

\( P(a) \) is a degree d Polynomial which is specified by coefficients \( a_0, a_1, \ldots, a_d \).

\( P(x) \) contains \( (x_i, y_i) \) if and only if \( P(x_i) = y_i \).
Polynomials over reals: \( a_0, \ldots, a_d \in \mathbb{R} \)

Polynomial Examples: \( \mathbb{R} \)

\[
\begin{align*}
\text{d} &= 1 \\
P(x) &= 2x - 1 \\
P(x) &= -0.5x \\
\text{d} &= 2 \\
P(x) &= x^2 + 2 \\
P(x) &= -x^2 + 8x - 14
\end{align*}
\]

Properties of Polynomials:

**Property 1:** A non-zero polynomial of degree \( d \) has at most \( d \) roots (zeros).

- \( x_i \) is a root if and only if \( P(x_i) = 0 \)

**Property 2:** Given \( d+1 \) pairs \( (x_1, y_1), \ldots, (x_{d+1}, y_{d+1}) \) with all the \( x_i \) distinct, there is a unique polynomial of degree at most \( d \) such that \( P(x_i) = y_i \) for \( i \in \{1, \ldots, d+1\} \).

**Proof of Property 1:**

First we need to review polynomial division.
If we have a polynomial degree \( d \), we can divide by a polynomial of degree \( \leq d \) using long division.

\[
p(x) = q'(x) q(x) + r(x)
\]

\( q'(x) \): the quotient \( r(x) \): the remainder

The degree for \( r(x) \) is less than the degree of \( q'(x) \).

**Examples:** Divide \( 4x^2 - 3x + 2 \) by \( (x-3) \)

\[
\begin{array}{c|cc}
  & 4x & +9 \\
\hline
  (x-3) & 4x^2 & -3x & +2 \\
  & - (4x^2 & -12x) \\
  & & 9x & +2 \\
  & & - (9x & -27) \\
  & & & 29 \\
\end{array}
\]

\[
p(x) = 4x^2 - 3x + 2 = (4x+9)(x-3) + 29
\]

Now we can prove Property 1.

**Property 1:** A non-zero polynomial of degree \( d \) has at most \( d \) roots.
Lemma 1: \( P(x) \) has root \( a \) iff
\[ P(x)/ (x-a) \text{ has remainder } 0 : p(x) = (x-a) Q(x) + 0 \]

Proof: we know \( P(x) = (x-a) Q(x) + r(x) \)

\[ P(x) = (x-a) Q(x) + c \]

If \( P(a) = 0 \) \( \implies 0 + c \implies c = 0 \implies r = 0 \)

If \( r = 0 \) \( \implies P(x) = (x-a) Q(x) \implies P(a) = 0 \).

Lemma 2: \( P(x) \) of degree \( d \) with distinct roots \( a_1, a_2, \ldots, a_d \) can be written as
\[ P(x) = c (x-a_1)(x-a_2) \ldots (x-a_d) \]

Proof: by induction on \( d \)

- Base case: \( d=0 \) \( \implies P(x) = c \)

- IH: for some \( d \geq 0 \) \( P(x) = c (x-a_1) \ldots (x-a_d) \)

- Induction step: \( P(x) \) of degree \( d+1 \) with roots \( a_1, a_2, \ldots, a_d, a_{d+1} \).

By lemma: \( P(x) = (x-a_{d+1}) Q(x) \)

\[ P(ai) = (ai-a_{d+1}) Q(ai) = 0 \quad \forall a_i \mid i \neq d+1 \]
\[ Q(a_i) = 0 \quad \forall i \neq d+1 \]

From IH \( Q(a) = C(x-a_1) \cdots (x-a_d) \)

\[ \Rightarrow Q(x) = C(x-a_1) \cdots (x-a_d)(x-a_{d+1}) \]

Use Lemma 1 and 2 to prove Property 1.

For \( P(x) \) of degree \( d \)

\[ P(x) = C(x-a_1) \cdots (x-a_d) \]

\( \forall a \neq a_i, i=1, \ldots, d, \Rightarrow P(a) \neq 0 \)

\[ \Rightarrow P(x) \text{ of degree } d \text{ has at most } d \text{ roots.} \]

Proof of Property 2:

Property 2: Given \( d+1 \) pairs \((x_1, y_1), \ldots, (x_{d+1}, y_{d+1})\) with all the \( x_i \) distinct, there is a unique polynomial of degree at most \( d \) such that \( P(x_i) = y_i \) for \( i \in \{1, 2, \ldots, d+1\} \).

Two steps: 1. Existence, 2. Uniqueness
1. **Existence**

2 **Points** $\Rightarrow$ **a unique line**

Find the unique $P(x)$ for $(1, 3), (2, 4)$

$$P(x) = a_1 x + a_0$$

$$P(1) = 3 \Rightarrow \left\{ \begin{array}{l} a_1 + a_0 = 3 \\ 2a_1 + a_0 = 4 \end{array} \right. \Rightarrow a_1 = 1, a_0 = 2$$

$$P(x) = x + 2$$

3 **Points** $\Rightarrow$ **a unique quadratic function**

Find the unique $P(x)$ for $(1, 7), (2, 13), (3, 27)$

$$P(x) = a_2 x^2 + a_1 x + a_0$$

$$P(1) = 2 \Rightarrow \left\{ \begin{array}{l} a_2 + a_1 + a_0 = 7 \\ 4a_2 + 2a_1 + a_0 = 13 \Rightarrow a_2 = 2, a_1 = 1 \\ 9a_2 + 2a_1 + a_0 = 27 \Rightarrow a_0 = 4 \end{array} \right.$$ 

In General

$d+1$ Points: $(x_1, y_1); (x_2, y_2); \ldots; (x_{d+1}, y_{d+1})$

$$P(x) = a_d x^d + \ldots + a_0$$

Solve

$$\left\{ \begin{array}{l} a_d x_1^d + \ldots + a_0 = y_1 \\ \vdots \\ a_d x_{d+1}^d + \ldots + a_0 = y_{d+1} \end{array} \right.$$
Does the solution exist?

To prove the existence, use Lagrange interpolation:

**Delta Polynomial**: for set of values \( x_1, \ldots, x_{d+1} \)

\[
\Delta_i(x) = \begin{cases} 
1 & \text{if } x = x_i \\
0 & \text{if } x = x_j \text{ and } x_j \neq x_i 
\end{cases}
\]

Why is it useful to interpolate a polynomial passing \((x_1, y_1), \ldots, (x_{d+1}, y_{d+1})\)?

- \( y_1 \Delta_1(x) \) contains \((x_1, y_1)\)
- \( y_2 \Delta_2(x) \) contains \((x_2, y_2)\)
  
\[
P(x) = y_1 \Delta_1(x) + \cdots + y_{d+1} \Delta_{d+1}(x)
\]

Define \( \Delta_i(x) \) as:

\[
\Delta_i(x) = \prod_{j \neq i} \frac{x-x_j}{x_i-x_j}
\]

\[
P(x_1) = y_1 \]
\[
P(x_2) = y_2 \]
\[
P(x_{d+1}) = y_{d+1}
\]

\[
\begin{cases} 
\text{simplify} \Delta_i(x) \\
\prod_{j \neq i} (x-x_j)
\end{cases}
\]

\[
\Delta_i(x) = \begin{cases} 
1 & x = x_i \\
0 & x = x_j, x_j \neq x_i
\end{cases}
\]
\[ \Delta_i(x) = n \]

\[ \Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} \]

\[ \Delta_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)} \]

\[ \begin{cases} 
P(1) = 5 \\
P(2) = 6 \\
P(3) = 9 
\end{cases} \]
Uniqueness: At most one polynomial of degree $d$ hits $d+1$ points.

Remember property 1: Any non-zero polynomial of degree $d$ has at most $d$ roots.

Proof of uniqueness: Proof by contradiction

Assume two different polynomials $P(x)$, $Q(x)$ hit the $d+1$ points.

Define $R(x) = P(x) - Q(x)$

- $R(x)$ is degree $d$.
- $R(x_i) = P(x_i) - Q(x_i) = y_i - y_i = 0$ for all $i = 0, 1, \ldots, d+1$.
- $R$ has $d+1$ roots.
Polynomials on Finite Fields:

what if $x \in \mathbb{N}$ or $x \in \mathbb{Z}$

Does property 1 and 2 still hold?

For polynomial interpolation and proof of property 1 and 2 we can add, subtract, multiply and divide (except 0).

$x \in \mathbb{N}$: Subtracting two numbers may not be a natural number.

$x \in \mathbb{Z}$: Division of two numbers may not be an integer.

what if

Polynomials with arithmetic modulo $p$:

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

$a_d, \ldots, a_0 \in \{0, \ldots, p-1\}$

$x \in \{0, \ldots, p-1\}$, $p$ is prime number

Addition, subtraction and multiplication (mod $p$) are allowed.

Division? if $\gcd(x, p) = 1$, so the inverse of $x$ exist for all $p \in \{0, \ldots, p-1\}$
Hence, property 1 and 2 hold if the coefficient of $P(x)$ are $(\text{mod } P)$ for a prime $P$.

This is over a Finite Field, denoted by $\mathbb{F}_p$ or $\text{GF}(p)$ (Galois Field).

The field is set of elements with addition, subtraction, multiplication and inverses.

Note the result of operators on the elements of the field is an element in the field.

Examples: $P(x) \equiv (\text{mod } p)$

\[ P_1(x) = 3x + 2 \pmod{5} \]
\[ P_2(x) = x + 1 \pmod{5} \]

Intersection of $P_1(x)$ and $P_2(x)$?

\[ 3x + 2 = x + 1 \pmod{5} \]

\[ 3x - x + 2 - 1 = 0 \pmod{5} \]

\[ 2x \equiv 4 \pmod{5} \]

\[ x \equiv 2 \equiv 2 \pmod{5} \]

$\therefore x = 2$
If 2 points are given, there are five polynomials with degree 2 that pass through \( p_1 \) and \( p_2 \).

**Application: Secret Sharing**

Share Secret among \( n \) People.

- **Secrecy:** Any \( k-1 \) knows nothing.
- **Robustness:** Any \( k \) knows the secret.
- **Efficient:** Minimize Storage.

**Shamir’s \( k \) out of \( n \) scheme:**

1. Choose \( a_0 = s \) and random \( a_1, \ldots, a_{k-1} \).
2. Let \( P(x) = a_{k-1}x^{k-1} + \ldots + a_0 \) where \( a_0 = s \).
3. Share Points \( (i, P(x_i) \mod p) \text{ with } i \in \{1, \ldots, n\} \).
Result: Any \( K \) points gives the polynomial. The secret \( s = a_0 \)

\[ P(0) = a_0 \Rightarrow \text{secret} \]

So

- with \( K \) shares, reconstruct \( P(x) \)
- with \( K-1 \) shares, any of \( P \) values are possible for \( P(0) \)!