Last Lecture :

(t, n) Secret Sharing : Distribute a secret s among n people s.t.

- Correctness - any t-size subset can recover the secret
- Hiding - any $(t-1)$ size subset learns nothing about s

Formally, a (t, n) secret sharing scheme with domain $\mathcal{D}$, share space S, consists of two algorithms :

- $\text{Dist}(s \in \mathcal{D}) \to (s_1, s_2, \ldots, s_n)$, each $s_i \in S$
- $\text{Reconst}(s_{i_1}, s_{i_2}, \ldots, s_{i_t}) \to s$

Correctness : $\forall\ s \in \mathcal{D}$, $\forall$ t-size subsets $\{i_1, i_2, \ldots, i_t\} \subseteq [n]$, if $\text{Dist}(s) \to (s_1, s_2, \ldots, s_n)$, then $\text{Reconst}(s_{i_1}, s_{i_2}, \ldots, s_{i_t}) \to s$.

Hiding : We will define this formally later. Intuitively, if we consider any $(t-1)$ subset of people, their shares should reveal no information about secret s.

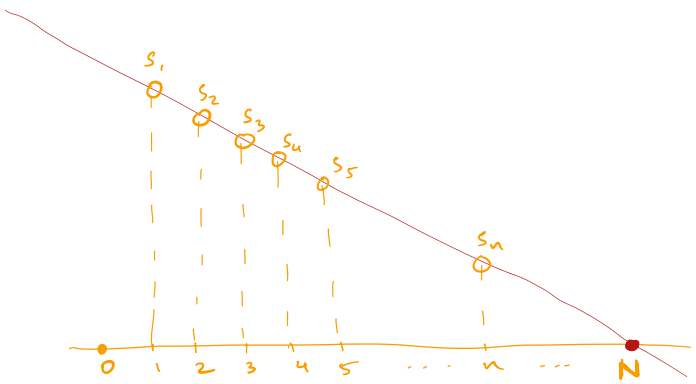
Secret sharing is at the core of several fundamental results in computer science. For us, it is an 'excuse' to study two important discrete structures : $\mathbb{Z}_n$, and polynomials over $\mathbb{Z}_n$.

Before seeing the formal solution, let us build some intuition using the following geometric solution. We consider $(2, n)$ secret sharing. Any two people should be able to reconstruct the secret, but a single person should learn nothing about the secret.

The solution can be summarised in one line, using the following geometric fact: given two points, there's a unique line passing through them.

Without loss of generality, let us assume the secret S is a natural number in the range $[1, N]$.

$(2, n)$ secret sharing



Dist (N):

1. Pick a random line L through $(N, 0)$. L is of the form $y = ax + b$

2. $s_i : a \cdot i + b \quad \forall\, i \in [n]$

Reconst (s_i, s_j):

1. Draw line passing through s_i & s_j

2. Wherever it intersects x axis is the secret.

It should be clear that this solution satisfies correctness. However, what does it mean to sample a "random line"? Which distribution do we use? How much precision should we use for storing the real / rational numbers?

It is much easier to answer these questions for finite sets. Therefore, we need finite sets which "behave like" $\mathbb{Q}$, $\mathbb{R}$. Finite sets where we can analogously claim that "bet." any two points, there is a unique line".

The set of numbers $\{0, 1, 2, \ldots, p-1\}$, (p: prime) together with appropriately defined addition and multiplication, behaves like $\mathbb{Q}$, $\mathbb{R}$ in many ways, and this allows us to transfer our $\mathbb{R}/\mathbb{Q}$-based intuition to these finite sets.

Before we discuss this set and the associated properties, let us review some basics of modular arithmetic.

BASICS OF MODULAR ARITHMETIC

Def 8.1 Let $n \in \mathbb{N}$ be a modulus. For any $a \in \mathbb{Z}$, $a \bmod n$ is the unique number $r \in \{0, 1, \ldots, n-1\}$ s.t. n divides $a - r$.

The following properties follow from def. of mod.

Let $a, b \in \mathbb{Z}$.

$$(a + b) \bmod n = \Big((a \bmod n) + (b \bmod n)\Big) \bmod n$$

$$(a \cdot b) \bmod n = \Big((a \bmod n) \cdot (b \bmod n)\Big) \bmod n$$

$$b > 0, \quad (a^b) \bmod n = (a \bmod n)^b \bmod n.$$

$$\forall c, \Big((a \bmod n = b \bmod n) \Rightarrow (a \cdot c \bmod n = b \cdot c \bmod n)\Big)$$

A common mistake: the converse is not true.

$$\forall c \neq 0 \Big((a \cdot c \bmod n = b \cdot c \bmod n) \Rightarrow (a \bmod n = b \bmod n)\Big) ?$$

No.

When can we 'divide both sides by c' and conclude that $a \bmod n = b \bmod n$?

Claim 9.1: If $\gcd(c, n) = 1$, then

$$a \cdot c \bmod n = b \cdot c \bmod n \Rightarrow a \bmod n = b \bmod n.$$

Proof: Using Bézout's identity, we know that

$$\exists\ s, t \in \mathbb{Z} \text{ s.t. } 1 = \gcd(c, n) = s \cdot c + t \cdot n$$

$$a \cdot c \bmod n = b \cdot c \bmod n$$
$$\Leftrightarrow (a-b) \cdot c = k \cdot n \text{ for some } k \in \mathbb{Z}.$$

multiply by s , multiply by t then add the two equations

$$\Rightarrow (a-b) \cdot c \cdot s + (a-b) \cdot t \cdot n = (k \cdot s + t) \cdot n$$
$$\Rightarrow (a-b)[c \cdot s + t \cdot n] = (k \cdot s + t) \cdot n$$
$$\Rightarrow a - b = (k \cdot s + t) \cdot n$$
$$\Rightarrow a \bmod n = b \bmod n.$$

∎

$$\forall n \in \mathbb{N},\ \forall c \text{ s.t. } \gcd(c, n) = 1,$$
$$\left((a \cdot c \bmod n = b \cdot c \bmod n) \Rightarrow (a \bmod n = b \bmod n)\right)$$

Our motivation for discussing modular arithmetic is to study the subset of numbers $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

$\mathbb{Z}_p$ when p is a prime:

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$$

we can define $+_p$ and $\times_p$ on $\mathbb{Z}_p$.

$$a +_p b = (a + b) \bmod p$$

$$a \times_p b = (a \times b) \bmod p.$$

Some immediate properties:

1. $+_p$, $\times_p$ are associative and commutative

$$(a +_p b) +_p c = a +_p (b +_p c)$$

Suppose $a = k_1 p + a_0$, $b = k_2 p + b_0$, $c = k_3 p + c_0$.
Then both LHS and RHS are equal to
$(a_0 + b_0 + c_0) \bmod p$.

$$(a \times_p b) \times_p c = a \times_p (b \times_p c)$$

Same argument. Both LHS and RHS are equal to $(a \cdot b \cdot c) \bmod p$.

2. Distributive: $a \times_p (b +_p c) = a \times_p b +_p a \times_p c$

Same argument. Both LHS and RHS equal to
$a_0 b_0 + a_0 c_0$.

3. $\forall\ a \in \mathbb{Z}_p,\quad 0 +_p a = a,$

4. $\forall\ a \in \mathbb{Z}_p,\quad \exists\ b \in \mathbb{Z}_p$ s.t. $a +_p b = 0$

$b = (p - a) \bmod p$ ↑ additive inverse of a

5. $\forall\ a \in \mathbb{Z}_p,\quad 1 \times_p a = a,\quad 0 \times_p a = 0$

6. $\forall\ a \in \mathbb{Z}_p,\ a \neq 0,\quad \exists\ b \in \mathbb{Z}_p$ s.t. $a \times_p b = 1$

↑ mult. inverse of a.

Uniqueness Proof: follows from Claim 9.1

The set $\mathbb{Z}_p$, together with operations $+_p$ and $\times_p$ behaves a lot like $\mathbb{R}$, $\mathbb{Q}$, with operations $+$ and $\times$.

Many properties of $\mathbb{R}$, $\mathbb{Q}$ also hold true for $\mathbb{Z}_p$. We will study one such property. In the quiz, you proved the following:

$\forall\ f(x) \in \mathbb{Q}[x]$ of deg $d \geq 1$,
α is rational root of f
$\Leftrightarrow (x - \alpha)$ divides $f(x)$.

This can be extended to prove the following:

$\forall f(x) \in \mathbb{Q}[x]$ of deg. $d \geq 1$, f can have at most d distinct rational roots.

Exercise: Prove (using induction) that any non-zero, deg. d polynomial $f(x) \in \mathbb{Q}[x]$ has at most d distinct roots.

Corollary: For any $d+1$ pairs $(x_1, y_1), \cdots, (x_{d+1}, y_{d+1})$ such that the x_is are all distinct, there exists at most one polynomial $f(x) \in \mathbb{Q}[x]$ of deg. at most d s.t. $f(x_i) = y_i$ for all $i \in [d+1]$.

Proof: Proof by contradiction.

Suppose $\exists$ $d+1$ pairs $(x_1, y_1), \cdots, (x_{d+1}, y_{d+1})$ s.t. the x_is are all distinct, and there exist two polynomials $f(x), g(x) \in \mathbb{Q}[x]$ of deg. $\leq d$ s.t. $\forall i \in [d+1]$, $f(x_i) = g(x_i) = y_i$.

Consider $h(x) = f(x) - g(x)$. Since $f(x) \neq g(x)$, $h(x)$ is not identically equal to 0.

Degree of $h(x) \leq \max(\text{deg. of } f(x), \text{deg. of } g(x))$
$\leq d$.

$\forall i \in [d+1]$, x_i is a root of $h(x)$. All x_is are distinct.
$\Rightarrow$ $h(x)$ has $d+1$ distinct rational roots. Contradiction ∎

ALL THE ABOVE RESULTS ALSO HOLD IF WE REPLACE $\mathbb{Q}$ WITH $\mathbb{Z}_p$.

In order to define polynomials over $\mathbb{Z}_p$, we need to define exponentiation

For any $d \in \mathbb{N}$, $x \in \mathbb{Z}_p$,

$$\exp_p(x, d) = \underbrace{x \times_p x \times_p \cdots \times_p x}_{d \text{ times}}$$

Def. 9.1:

$$\mathbb{Z}_p[x] = \left\{ f(x) : f(x) = a_0 +_p a_1 \times_p x +_p \cdots +_p a_d \times_p \exp(x, d) \right\}$$

$a_0, a_1, \ldots, a_d \in \mathbb{Z}_p$

$\alpha \in \mathbb{Z}_p$ is a root of $f(x) \in \mathbb{Z}_p[x]$ if $f(\alpha) = 0$

THEOREM 9.1 For any $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1}) \in \mathbb{Z}_p^2$ if all x_is are distinct, then there exists at most one non-zero deg. $\leq d$ polynomial $f(x) \in \mathbb{Z}_p[x]$ s.t. $\forall\, i \in [d+1]$, $f(x_i) = y_i$

We are now ready to solve our secret sharing puzzle. Suppose the secret s is a k-bit string, and we want (t, n) secret sharing.

Dist $(s \in \{0,1\}^n)$:

1. Pick a prime p s.t. $p > n$, $p > 2^k$.

2. Express s as a number in $\mathbb{Z}_p$. This is possible since $p > 2^k$.

3. Pick uniformly random numbers $a_1 \dots a_{t-1}$ from $\mathbb{Z}_p$. Set $a_0 = s$.

4. Consider the polynomial $f(x) = a_0 +_p a_1 \times_p x +_p \dots +_p a_{t-1} \times_p \exp(x, t-1)$ $f(x) \in \mathbb{Z}_p[x]$.

5. Set $s_i = f(i)$ for all $i \in [n]$. This is possible since $p > n$.

Reconst $((i_1, s_{i_1}), (i_2, s_{i_2}), \dots, (i_t, s_{i_t}))$:

We know that there exists a polynomial $f(x) \in \mathbb{Z}_p[x]$ s.t. $f(i_j) = s_{i_j}$ for all $j \in [t]$. How to find $f(x)$, or at least, the constant term of this polynomial?