Recap: p - prime

$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ with operations $+_p$: addition mod p

$\times_p$: mult. mod p

Properties:

- $+_p$, $\times_p$ are commutative, associative
- $(a +_p b) \times_p c = a \times_p c +_p b \times_p c$
- $\forall\, a \in \mathbb{Z}_p, \quad \exists\, b \in \mathbb{Z}_p$ s.t. $a +_p b = 0$ — additive inverse exists
- $\forall\, a \in \mathbb{Z}_p \setminus \{0\}, \quad \exists\, b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $a \times_p b = 1$ — mult. inverse exists

Several useful properties can be concluded from the above.

- $a, b \in \mathbb{Z}_p$, $a \times_p b = 0 \Rightarrow (a = 0) \vee (b = 0)$
- $a, b, c \in \mathbb{Z}_p$, $a \times_p b = a \times_p c \neq 0 \Rightarrow b = c$
- Any non zero deg. d polynomial $f(x) \in \mathbb{Z}_p[x]$ has at most d distinct roots.
- For any $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ s.t. x_is are all distinct, there exists at most one non-zero deg. d poly. $f(x) \in \mathbb{Z}_p[x]$ s.t. $\forall i \in [d+1]$, $f(x_i) = y_i$.

Lecture 10 :

Thm 10.1 • For any $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$ s.t. x_is are all distinct, there exists ~~at most~~ exactly one non-zero deg. d poly. $f(x) \in \mathbb{Z}_p[x]$ s.t. $\forall i \in [d+1]$, $f(x_i) = y_i$.

Proof By explicit construction :

(Lagrange Interpolation)

$$f(x) = y_1 \times_p (x -_p x_2) \times_p (x -_p x_3) \times_p \cdots \times_p (x -_p x_{d+1})$$
$$+_p y_2 \times_p (x -_p x_1) \times_p (x -_p x_3) \times_p \cdots \times_p (x -_p x_{d+1})$$
$$+_p \cdots +_p y_{d+1} \times_p (x -_p x_1) \times_p (x -_p x_2) \times_p \cdots \times_p (x -_p x_d)$$

Check that deg. of $f(x) \le d$.

Check that $\forall i \in [d+1]$, $f(x_i) = y_i$.

∎

APPLICATION : (t, n) Secret Sharing

Dist $(s \in \mathbb{Z}_p)$: Sample $a_1, a_2, \dots, a_{t-1} \leftarrow \mathbb{Z}_p$

$a_0 = s$. $f(x) = a_0 +_p a_1 \times_p x +_p \cdots +_p a_{t-1} \times_p x^{t-1}$

Person i gets $s_i = f(i)$

Note : $f(0) = s$.

Reconst $\left((i_1, s_{i_1}), (i_2, s_{i_2}), \ldots, (i_t, s_{i_t})\right)$:

Lagrange interpolation.

Use Thm 10.1 to construct $f(x)$ s.t.

$f(i_j) = s_{i_j}$ for all $j \in [t]$.

$s = f(0)$.

Correctness: For any t-size subset $\{i_1, i_2, \ldots, i_t\} \subseteq [n]$,

for any $s \in \mathbb{Z}_p$,

if Share$(s) \to (s_1, s_2, \ldots, s_n)$

then Reconst$\left((i_1, s_{i_1}), \ldots, (i_t, s_{i_t})\right) = s$.

[This part is not in syllabus]

Hiding: Before defining 'hiding property' formally, let us consider the two solutions for (n, n) secret sharing. Suppose $n = 50$ and we want to share a 100-bit secret.

$(50, 50)$ sec. sharing

Proposal 1:

Dist: Give first 2 bits to person 1
Give next 2 bits to person 2
⋮
Give last 2 bits to person 50

Proposal 2

Sample 49 uniformly random 100-bit strings $s_1, s_2, \ldots, s_{49}$.
Give s_i to person i.
Give $s \oplus (\oplus s_i)$ to person 50.

Intuitively, Proposal 2 'feels better' as compared to Proposal 1. If 49 people get together, in Proposal 1, they can learn 98 bits. But in Proposal 2, they "dont learn any info about s". How do we formally capture that they dont learn any info about s?

Informally, we want the following: suppose there are $t-1$ 'colluders'. Before receiving their shares, they know that the secret s comes from some known probability distribution $\mathcal{D}$. Even after receiving their shares, the distribution of the secret, CONDITIONED ON THE COLLUDERS' SHARES,

should remain $\mathcal{D}$.

As an example, let us consider Proposal 1.

Suppose there are 49 colluders, persons $1, \ldots, 49$.

Before receiving their shares, suppose they know that the secret comes from the uniform dist^n.

After receiving their shares $s_1, s_2, \ldots, s_{49}$, they know that the secret is one of 4 possible strings:

$s_1\ s_2 \ldots s_{49}\ 00$ $\quad$ $s_1\ s_2 \ldots s_{49}\ 01$

$s_1\ s_2 \ldots s_{49}\ 10$ $\quad$ $s_1\ s_2 \ldots s_{49}\ 11$

Hence, the distribution, conditioned on $s_1, s_2, \ldots, s_{49}$, is no longer the uniform dist^n on $\{0,1\}^{100}$.

Below, I don't want to talk in terms of dist^n $\mathcal{D}$, hence have provided a different looking, but equivalent definition.

Formally defing "$\{i_1, i_2, \ldots, i_{t-1}\}$ dont learn any info about secret"

i_j has share s_{i_j}.

Def 10.1 We say that $\{i_1, \ldots, i_{t-1}\}$ dont learn any info about the secret if, <u>for all secrets s</u>,

for all shares $s_{i_1}, s_{i_2}, \ldots, s_{i_{t-1}}$,

$$\Pr\left[\text{Dist}(s) \text{ outputs share } s_{i_j} \text{ for } i_j, \text{ for all } j \in [t-1]\right]$$

is the same (for all secrets s).

Let us consider Proposal 1. Here Dist is a deterministic algorithm.

Suppose you have shares $s_1, s_2, \ldots, s_{49}$.

There are only 4 secrets that agree with $s_1 \ldots s_{49}$.

As a result, other than $s \in \left\{ \begin{array}{l} s_1\ s_2 \ldots s_{49}\ 00 \\ s_1\ s_2 \ldots s_{49}\ 01 \\ s_1\ s_2 \ldots s_{49}\ 10 \\ s_1\ s_2 \ldots s_{49}\ 11 \end{array} \right\}$, for all other secrets, the probability is 0.

Now, let us consider proposal 2.

Suppose you have the shares $s_1, s_2, \ldots, s_{49}$.

Take any secret s.

$$\Pr\left[\begin{array}{l} \text{Dist}(s) \text{ gives } s_1 \text{ to person 1} \\ \quad\quad\ \ " \quad\ s_2 \text{ to person 2} \\ \quad\quad\ \ \vdots \\ \quad\quad\ \ s_{49} \text{ to person 49} \end{array}\right] = \left(\frac{1}{2^{100}}\right)^{49}$$

This probability is independent of s.

Therefore, we say that $s_1 \ldots s_{49}$ reveal no info. about s.

Thm 10.2 Consider our polynomial-based approach for (t, n) secret sharing.

For any $\{i_1, i_2, \ldots, i_{t-1}\}$, $s_{i_1}, s_{i_2}, \ldots, s_{i_{t-1}}$ do not reveal any information about s. (using Def 10.1).

Pf: Take any secret s.

$$\Pr\left[\text{Dist}(s) \text{ gives } s_{i_j} \text{ to person } i_j \ \forall j \in [t-1]\right]:$$

Dist(s) samples $a_1 \ldots a_{t-1}$ unif. at. rand. from $\mathbb{Z}_p$.

$$f(x) = s +_p a_1 \times_p x +_p a_2 \times_p x^2 +_p \cdots +_p a_{t-1} \times_p x^{t-1}$$

For how many choices of $a_1 \ldots a_{t-1}$ do we have that $f(i_j) = s_{i_j}$? Exactly one choice of $a_1, \ldots, a_{t-1}$ is such that $f(i_j) = s_{i_j}$ for all $j \in [t-1]$. This is because we have t pairs $(0, s), (i_1, s_{i_1}), \ldots, (i_{t-1}, s_{i_{t-1}})$, and there is exactly one non zero poly. of deg. $\leq t-1$ that passes through all these t pts.

Hence, the probability is $\underbrace{1/p^{t-1}}_{\uparrow \text{ indep. of } s}$. ∎

End of Secret Sharing

Another useful property of $\mathbb{Z}_p$:

We know that every non-zero element in $\mathbb{Z}_p$ has an inverse. And this can be computed efficiently using Extd. Euclid's algorithm. Is there a clean, closed form expression for the mult. inv. of a?

[Fermat's Little Thm]

Thm 10.3 $\forall\, a \in \mathbb{Z}_p \setminus \{0\}$, $\exp_p(a, p-1) = 1$

Therefore, $b = \exp_p(a, p-2)$ is mult. inv. of a.

Try to prove this yourself. There are several approaches possible, including using induction. In the approach discussed below, carefully check which properties of $(\mathbb{Z}_p, +_p, \times_p)$ are being used.

Often a good idea to try out a few examples.

$p = 7$, $a = 4$. $4^1 = 4$ $4^2 = 2$ $4^3 = 1$ $4^4 = 4$ $4^5 = 2$ $4^6 = 1$

$p = 13$, $a = 6$ $6^1 = 6$ $6^2 = 10$ $6^3 = 8$ $6^4 = 9$ $6^5 = 2$ $6^6 = 12$

$6^7 = 7$ $6^8 = 3$ $6^9 = 5$ $6^{10} = 4$ $6^{11} = 11$ $6^{12} = 1$

Proof: Consider any $a \in \mathbb{Z}_p \setminus \{0\}$.

Let $S = \{ a \times_p 1,\ a \times_p 2,\ \ldots,\ a \times_p (p-1) \}$

Observation 1: S has exactly $p-1$ elements.

i.e. $S = \mathbb{Z}_p \setminus \{0\}$.

Proof : Proof by contradiction. Suppose S has less than $p-1$ elements. Then $\exists$ distinct $i, j \in \mathbb{Z}_p$ s.t. $a \times_p i = a \times_p j$.

$\Rightarrow i = j$ [using the mult. inverse of a]

Contradiction. ∎

Since $S = \mathbb{Z}_p \setminus \{0\}$, the product of all elements of S is equal to the product of all elements in $\mathbb{Z}_p \setminus \{0\}$.

$$\Rightarrow (a \times_p 1) \times_p (a \times_p 2) \times_p \dots \times_p (a \times_p (p-1)) \qquad (*)$$
$$= 1 \times_p 2 \times_p \dots \times_p (p-1)$$

$\times_p$ is associative and commutative.

Therefore, LHS of $(*)$ is equal to $\exp_p(a, p-1) \times_p \underbrace{(1 \times_p 2 \times_p \dots \times_p (p-1))}$

non-zero, therefore inverse exists

$$\Rightarrow \exp_p(a, p-1) = 1$$

∎

We can prove something stronger. Suppose z is the smallest positive integer s.t. $\exp_p(a, z) = 1$. Then z divides $(p-1)$.

$p = 7$, $a = 4$. $4^1 = 4$ $4^2 = 2$ $4^3 = 1$ $4^4 = 4$ $4^5 = 2$ $4^6 = 1$

Here, $z = 3$, and 3 divides $(p-1)$.

[Lagrange's Thm]

Thm 10.4: Take any $a \in \mathbb{Z}_p \setminus \{0\}$. Let z be the smallest positive number s.t. $\exp_p(a, z) = 1$. Then z divides $p-1$.

Different as can have different z. This number z is called the "order of a wrt p" $z = \text{ord}_p(a)$

Proof: Proof by contradiction. Suppose z does not div. $(p-1)$. Then $p-1 = z \cdot q + r$ for some $r \in \{1, \dots, z-1\}$

1. $\exp_p(a, p-1) = 1$ [using Fermat's Little Thm]

2. $$1 = \exp_p(a, p-1) = \exp_p(a, z \cdot q) \times_p \exp_p(a, r)$$
$$= \exp_p(\underbrace{\exp_p(a, z)}_{=1}, q) \times_p \exp_p(a, r)$$
$$= 1 \times_p \exp_p(a, r)$$

Contradiction, since we assumed z is the smallest positive integer s.t. $\exp_p(a, z) = 1$, and we have found a smaller positive integer r s.t. $\exp_p(a, r) = 1$.

∎

What properties of $\mathbb{Z}_p \setminus \{0\}$ did we use for Fermat's Little Theorem and Lagrange's Theorem?

1. if $a, b \in \mathbb{Z}_p$, then $a \times_p b$ is also in $\mathbb{Z}_p$.

2. Every element in $\mathbb{Z}_p \setminus \{0\}$ has a mult. inverse.

3. $\times_p$ is commutative and associative.

It is possible to prove Fermat's Little Theorem and Lagrange's theorem without using the comm. of $\times_p$. This is useful when you want to prove similar properties for sets with non-comm. operation.