Exercises I

Note: We discuss solutions to the exercises together in the class on the **26th November 2025**.

Exercise 1. *Insecure Secret Sharing*

Let us consider the following secret sharing scheme over $\mathbb{Z}/8\mathbb{Z}$ for three parties:

- Share(α): decompose $\alpha \in \{0, \dots, 7\}$ into a sequence of three bits $a\,b\,c$ and give bit a to party 1, b to party 2 and c to party 3;
- Reconstruct(a, b, c): compute $\alpha = 4a + 2b + c$.

1. Argue that the above scheme is correct as a 3-out-of-3 secret sharing scheme, but not secure.
2. Would reconstruction still work if only 2 out of the 3 parties participate?

Exercise 2. *3-out-of-3 Secret Sharing*

During the lecture we have seen the 2-out-of-2 additive secret sharing over $\mathbb{Z}/q\mathbb{Z}$ for prime q, which works as follows:

- Share(α): sample $r \leftarrow U(\mathbb{Z}/q\mathbb{Z})$ uniformly at random, set $s_1 = r$ and $s_2 = \alpha - r$;
- Reconstruct(s_1, s_2): $\alpha = s_1 + s_2$.

We have proven it to be correct and secure.

1. Provide a generalization of this scheme to build a 3-out-of-3 additive secret sharing using the same idea.
2. Can you see a pattern? Use it to further generalize the idea to N-out-of-N additive secret sharing for any integer N.

Exercise 3. *Concrete Shamir Secret Sharing*

We want to give a concrete example for Shamir's secret sharing in the case of $q = 17$, $N = 5$ and $t = 3$.

1. Provide a concrete execution of the Share algorithm for $\alpha = 5$.
2. Using the secret shares $s_1 = 15$ of Party 1, $s_3 = 10$ of Party 3 and $s_5 = 6$ of Party 5, recover the secret α' (possibly different to α) using the Reconstruct algorithm.

Exercise 4. *Packed Shamir*

We want to give a concrete example for **packed** Shamir's secret sharing in the case of $q = 17$, $N = 5$, $\ell = 2$ and $t = 3$.

1. Provide a concrete execution of the Share algorithm for $\alpha_0 = 5$ and $\alpha_1 = 3$.
2. Assume $t \geq \ell - 1$. What happens if one picks $q(x)$ of degree $t - \ell$ (instead of $t - 1 - \ell$)?