

Cryptography

Prof. Dr. Klaus Meer, Ameen Naif

Exercise Sheet 5
Version 14.06.2019

Exercise 1.

Let $p > 2$ be prime and $b \in \mathbb{Z}_p^*$. Show that $x^2 \equiv b \pmod p$ either has no or two solutions in \mathbb{Z}_p .

Exercise 2.

Let $l_1, \dots, l_s \in \mathbb{N}$, $s > 2$.

- Give a formal definition of $\gcd(l_1, \dots, l_s)$.
- For $x, y, z \in \mathbb{N}$ show that $\gcd(x, y, z) = \gcd(x, \gcd(y, z))$.
- Suppose $\gcd(l_1, \dots, l_s) = 1$, i.e. all l_1, \dots, l_s are pairwise relatively prime. Use (b) and an induction proof to show: There exist $x_1, \dots, x_s \in \mathbb{Z}$ s.t. $1 = \sum_{i=1}^s x_i \cdot l_i$.

Exercise 3.

Let $p \in \mathbb{N}$ be a prime, $g \in \mathbb{Z}_p^*$ a generator of (\mathbb{Z}_p^*, \cdot) . Prove that the map

$$\begin{aligned} \log_g : \mathbb{Z}_p^* &\rightarrow \mathbb{Z}_{p-1} \\ h &\rightarrow \log_g(h) \pmod{p-1} \end{aligned}$$

is bijective and isomorphic, i.e. the following two conditions hold:

- $\forall a, b \in \mathbb{Z}_p^* : \log_g(a \cdot b) = (\log_g(a) + \log_g(b)) \pmod{p-1}$ and
- the map \log_g is bijective.

Exercise 4.

Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $a \equiv b \pmod n$ and $c \equiv d \pmod n$. Show that the following identities holds:

- Addition: $a + c \equiv b + d \pmod n$
- Subtraction: $a - c \equiv b - d \pmod n$
- Multiplication: $a \cdot c \equiv b \cdot d \pmod n$ and
- Exponentiation: $a^m \equiv b^m \pmod n$, where m is a positive integer.