Cryptography

Prof. Dr. Klaus Meer, Ameen Naif

Exercise Sheet 5
Version 14.06.2018

Exercise 1.
Let $p > 2$ be prime and $b \in \mathbb{Z}_p^*$. Show that $x^2 \equiv b \ mod \ p$ either has no or two solustions in $\mathbb{Z}_p$.

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

(a) Give a formal definition of $gcd(l_1, ..., l_s)$.

(b) For $x, y, z \in \mathbb{N}$ show that $gcd(x, y, z) = gcd(x, gcd(y, z))$.

(c) Suppose $gcd(l_1, ..., l_s) = 1$, i.e. all $l_1, ..., l_s$ are pairwise relatively prime. Use (b) and an induction proof to show: There exist $x_1, ..., x_s \in \mathbb{Z}$ 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

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

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

i) $\forall a, b \in \mathbb{Z}_p^*$: $log_g(a \cdot b) = (log_g(a) + log_g(b)) \ mod \ p-1$ and

ii) the map log_g is bijective.

Exercise 4.
Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $a \equiv b \ mod \ n$ and $c \equiv d \ mod \ n$. Show that the following identities holds:

(a) Addition: $a + c \equiv b + d \ mod \ n$

(b) Subtraction: $a - c \equiv b - d \ mod \ n$

(c) Multiplication: $a \cdot c \equiv b \cdot d \ mod \ n$ and

(d) Exponentiation: $a^m \equiv b^m \ mod \ n$, where m is a positive integer.