Homework 1 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

25.10.2013

Exercise 1. Let $a, b, c, d \in \mathbb{Z}$. a is said to divide b if (and only if) there exists some $k \in \mathbb{Z}$ such that $a \cdot k = b$. Notation: $a \mid b$. Prove the following implications:

(a) $a \mid b$ and $b \mid c \quad \Rightarrow \quad a \mid c$.

(b) $a \mid b$ and $c \mid d \quad \Rightarrow \quad (ac) \mid (bd)$.

(c) $a \mid b$ and $a \mid c \quad \Rightarrow \quad a \mid (xb + yc) \;\; \forall\, x, y \in \mathbb{Z}$.

Exercise 2. Show the following properties for the greatest common divisor.

(a) Prove that: $a \in \mathbb{Z}_m$ invertible $\Leftrightarrow \gcd(a, m) = 1$.

(b) Let $a, b \in \mathbb{Z}$ with $b \neq 0$ and $q, r \in \mathbb{Z}$ and $a = bq + r$ and $0 \leq r < b$.
Prove that: $\gcd(a, b) = \gcd(b, r)$.

(c) Show that $\mathbb{Z}_m^* = \{b \in \mathbb{Z}_m \mid \gcd(b, m) = 1\}$ is a multiplicative group.

(d) Is 221 invertible modulo 2310?

Hint: For any $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

Exercise 3. Let M be a finite set. A permutation π over M is a bijective function $\pi : M \to M$.

(a) How many permutations exist for $M = \{1, 2, \ldots, n\}$?

(b) Show that the set of permutations over M forms a group together with the composition of functions. Is this group commutative, i.e., is the order of the composition of importance?