Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 4
Version 07.05.2020

Exercise 1.
Name the elements of $\mathbb{Z}_{12}$ which are invertible w.r.t. multiplication. Determine their inverses with the aid of the Euclidean algorithm.

Exercise 2.
In the residue class ring $(\mathbb{Z}_{16}, +, \cdot)$

(a) find all **zero-divisor** and

(b) solve the following system of equations:

$$\begin{array}{rrrrcl} 3x + & 5y & + & 7z & = & 3 \\ x + & 4y & + & 13z & = & 5 \\ 2x + & 7y & + & 3z & = & 4. \end{array}$$

Exercise 3.
Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n$ be fixed. Show that $ax = b \; mod \; n$ has a unique solution $x \in \mathbb{Z}_n$ for every $b \in \mathbb{Z}_n$ if and only if $gcd(a, n) = 1$.

Exercise 4.
Let $p > 2$ be prime and $b \in \mathbb{Z}_p^*$. Show that $x^2 \equiv b \; mod \; p$ either has no or two solutions in $\mathbb{Z}_p$.

Exercise 5.
Compute the smallest natural number which solves the subsequently stated system of congruences:

$$\begin{array}{ll} x \equiv 1 & \mod 25 \\ x \equiv 2 & \mod 7 \\ x \equiv 4 & \mod 9 \\ x \equiv 7 & \mod 38. \end{array}$$

Exercise 6.
Prove the Corollary 2.58 in the lecture with the aid of the Chinese Reminder Theorem.