Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Homework Sheet 1
Version 23.04.2020

Homework 1.

a) Apply the Euclidean algorithm in order to compute the greatest common divisor of

i) 14345 and 16289,

ii) 142241 and 153049.

b) For $a := 101$ and $b = 37$, compute integers $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Homework 2.

Compute the prime factors of

a) 809009 and 200583 with the aid of Fermat's factorization method.

b) 11!. Justify your arguments.

c) 1001^{11}.

Homework 3.

Let $n \in \mathbb{N}$ be a natural number with $n \geq 2$ and set $S := \{m \in \mathbb{N} : m \,|\, n\}$. Furthermore, define

$$\forall a, b \in S: \quad a * b := \gcd(a, b).$$

Show that $(S, *)$ is a commutative monoid. Is it a group?

Homework 4.

Let $S := \{1, \mathrm{i}, -1, -\mathrm{i}\} \subset \mathbb{C}$ be fixed (i denotes the imaginary unit). Show with the aid of a Cayley-table that $(S, \cdot)$, where $\cdot$ denotes the common multiplication in the complex numbers, is a group. Determine all its subgroups.

Homework 5.

Prove Lemma 2.30 of the lecture.