Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 1
Version 16.04.2020

Exercise 1.

Prove the following using the definition of divisibility:

(a) $\forall a \in \mathbb{N}\colon 1|a$.

(b) $\forall a, b \in \mathbb{N}_0\colon a|b \wedge b|a \Longrightarrow a = b$.

(c) $\forall a, b, c, d \in \mathbb{N}_0\colon a|b \wedge c|d \Longrightarrow (ac)|(bd)$.

Exercise 2.

Prove that for all $a, b, m \in \mathbb{N}$ the following is true:
If $gcd(a, m) = 1$ and $gcd(b, m) = 1$, then $gcd(a \cdot b, m) = 1$.

Exercise 3.

For the pairs of integers a, b given below use the Euclidean Algorithm to find the $gcd(a, b)$:

i) $a = 13$, $b = 32$ and

ii) $a = 40$, $b = 148$.

Exercise 4.

Using the Fermat factorization method, factor each of the following positive integers: a) 73 and b) 46009.

Exercise 5.

For $n \in \mathbb{N}$, the number of the form $M_n = 2^n - 1$ is called the n-th **Mersenne number**.

(a) Prove that M_r is a divisor of $M_{r \cdot s}$, wehre $r, s \in \mathbb{N}$.

(b) Show that: If M_n is prime, then n must be prime. (Or if n is composite, then M_n is also composite).

(c) Find using a) the prime factorization of M_6.