Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Qinwei He

Exercise 1

Friday, April 21, 2017

Problem 1. *(Dividers)* Let $a, b, c, d \in \mathbb{Z}$. The integer a divides b if and only if there exists a $k \in \mathbb{Z}$ such that $a \cdot k = b$. This property is denoted by $a \,|\, b$. Prove the following implications:

a) $a \,|\, b$ and $b \,|\, c \quad \Rightarrow \quad a \,|\, c$.

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

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

Problem 2. *(Permutation Cipher)* The plaintext is an English sentence. A permutation cipher with blocklength 8 revealed the following ciphertext

REXETSIH ONSICESI UCIFTFID REHTLIET

a) Decrypt the ciphertext and explain your approach.

b) Determine the corresponding permutations π and π^{-1}.

Problem 3. *(GCD Multiplicativity)* Let $a, b, m \in \mathbb{Z}$. Show that if $\gcd(a, b) = 1$, then $\gcd(ab, m) = \gcd(a, m)\gcd(b, m)$.