Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 1

Friday, April 15, 2016

Problem 1. *(Multiplicative Inverses)* Take a look at the appendix of the lecture notes and solve the following tasks.

a) Compute $1234 \mod 357$ using the standard long division with a remainder.

b) Compute the greatest common divisor of 357 and 1234, i.e., $\gcd(357, 1234)$, using the Euclidean algorithm.

c) Compute the multiplicative inverse of 357 modulo 1234, i.e., $357^{-1} \mod 1234$ using the extended Euclidean algorithm. Check if $357 \cdot 357^{-1} \equiv 1 \mod 1234$ holds.

Consider polynomials with the indeterminate x and coefficients in $\mathbb{Z}_2 = \{0, 1\}$.

d) A polynomial $a(x)$ is a multiplicative inverse of $b(x)$ modulo $m(x)$ if the product yields $b(x) \cdot a(x) \equiv 1 \bmod m(x)$. Compute $\gcd(b(x), m(x))$ and the multiplicative inverse of $b(x) = x^3 + x + 1$ modulo $m(x) = x^5 + x^3 + 1$.

Hint: *Addition of the coefficients is taken modulo 2.*

Problem 2. *(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 $a \mid b$. 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 $a \mid c \quad \Rightarrow \quad a \mid (xb + yc) \;\; \forall\, x, y \in \mathbb{Z}.$