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

Exercise 9

Friday, June 24, 2016

Problem 1. *(Proof Chinese Remainder Theorem)*
Prove the Chinese Remainder Theorem: Suppose $m_1, \ldots, m_r$ are pairwise relatively prime, $a_1, \ldots, a_r \in \mathbb{N}$.

The system of r congruences

$$x \equiv a_i \pmod{m_i}, \qquad i = 1, \ldots, r,$$

has a unique solution modulo $M = \prod_{i=1}^{r} m_i$ given by

$$x \equiv \sum_{i=1}^{r} a_i \, M_i \, y_i \pmod{M},$$

where $M_i = M/m_i$, $y_i = M_i^{-1} \pmod{m_i}, i = 1, \ldots, r$.

Problem 2. *(proof existence of a primitive element modulo n)*
Let $n \in \mathbb{N}$. Show that there exists a primitive element modulo n in $\mathbb{Z}_n^*$ if and only if:

$$n \in M = \{2, 4, p^k, 2p^k \mid p \geq 3 \text{ prime}, \ k \in \mathbb{N}\}$$

holds (cf. Theorem 7.2 a) in lecture notes).

Hint 1: It has already been shown before that $n = \prod_i \varphi(p_i^{k_i}) = \prod_i p_i^{k_i - 1}(p_i - 1)$.

Hint 2: " $\Rightarrow$ " Show by induction that for each odd prime p, there exists a primitive element modulo p such that for all $k > 1$ it holds $g^{\varphi(p^{k-1})} \not\equiv 1 \mod p^k$.

Hint 3: " $\Leftarrow$ " Show for $n = 2^k$ with $k > 2$, that for all $a \in \mathbb{Z}_n^*$ it holds $a^{\varphi(n)/2} \equiv 1 \mod n$.

Problem 3. *(properties of the discrete logarithm)* We examine the properties of the discrete logarithm.

a) Compute the discrete logarithm of 18 and 1 in the group $\mathbb{Z}_{79}^*$ with generator 3 (by trial and error if necessary).

b) How many tryings would be necessary to determine the discrete logarithm in the worst case?