Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 9

Friday, June 21, 2019

Problem 1. *(Chinese Remainder Theorem Example)* There is the following system of linear congruences:

$$\begin{aligned} x &\equiv 3 \pmod{11} \\ x &\equiv 5 \pmod{13} \\ x &\equiv 7 \pmod{15} \\ x &\equiv 9 \pmod{17}. \end{aligned}$$

a) Compute the smallest positive solution using the Chinese Remainder Theorem.

Problem 2. *(Proof of Theorem 7.2b)* Let $n \in \mathbb{N}$. If there exists a primitive element modulo n, then there exist $\varphi(\varphi(n))$ many.

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?

Problem 4. *(Proof of Proposition 7.5)* Prove Proposition 7.5 from the lecture, which gives a possibility to generate a primitive element modulo n:

Let $p > 3$ be prime, $p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ the prime factorization of $p - 1$. Then,

$$a \in \mathbb{Z}_p^* \text{ is a primitive element modulo } p \Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p} \text{ for all } i \in \{1, \dots, k\}.$$