Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 5
Version 14.05.2020

Exercise 1.

a) Determine all natural numbers $n \in \mathbb{N}$ such that $\varphi(n) = 2$.

b) Determine all natural numbers $n \in \mathbb{N}$ such that $\varphi(n) = 4$.

Exercise 2.

Determine the inverse of the matrix

$$\begin{pmatrix} 9 & 1 & 15 \\ 21 & 0 & 9 \\ 19 & 3 & 20 \end{pmatrix}$$

in $\mathbb{Z}_{26}$ with the aid of

i) Lemma 2.73,

ii) Gaussian elimination.

Exercise 3.

Compute the number of primitive elements *modulo* 29. Given the primitive element 3 *modulo* 29, compute all other primitive elements *modulo* 29. Finally, compute $log_3 13$ in $\mathbb{Z}_{29}^*$.

Exercise 4.

Let $p \in \mathbb{N}$ be a prime, $g \in \mathbb{Z}_p^*$ a generator of $(\mathbb{Z}_p^*, \odot)$. Prove that the map

$$\begin{aligned} log_g : \; & \mathbb{Z}_p^* \to \mathbb{Z}_{p-1} \\ & h \to log_g(h) \; mod \; p-1 \end{aligned}$$

is bijective and isomorphic, i.e. the following two conditions hold:

i) $\forall a, b \in \mathbb{Z}_p^*$: $log_g(a \odot b) = (log_g(a) \oplus log_g(b))$ and

ii) the map log_g is bijective.