Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Homework Sheet 3
Version 11.05.2020

Homework 1.

Show the following calculus rule for Euler's φ-function:

$$\forall m, n \in \mathbb{N}: \quad \varphi(m \cdot n) \cdot \varphi(\gcd(m, n)) = \varphi(m) \cdot \varphi(n) \cdot \gcd(m, n).$$

Hint: Write down the prime factorizations of m and n abstractly while distinguishing between individual and common prime factors.

Homework 2.

Fix $m = 26$.

i) Determine the number of primitive elements modulo 26.

ii) Knowing that 11 is a primitive element modulo 26, compute all the other primitive elements modulo 26.

iii) Determine $\log_{11} 15$ in $\mathbb{Z}_{26}^*$ with the aid of Shanks' algorithm.

Homework 3.

Determine all values $a, b \in \mathbb{Z}_6$ such that the matrix

$$\begin{pmatrix} a & 2 \\ 2 & b \end{pmatrix}$$

is invertible in $\mathbb{Z}_6$ and state the corresponding inverses.