Cryptography

Prof. Dr. Klaus Meer, Ameen Naif

Exercise Sheet 2
Version 26.04.2019

Exercise 1.

The recursive version of the **Euclidean Algorithm** is given below:

```
**Data**: $a, b \in \mathbb{N}_0$ and $b \leq a$.
**Result**: $gcd(a, b)$
**if** $b = 0$ **then**
  | **return** $a$ and **stop**
**else**
  | $gcd(b, a \ mod \ b)$
**end**
```

For this version prove the following:

(a) Correctness of the algorithm.

(b) Suppose the algorithm calls itself k times (i.e., it runs k times into the else-part before it stops). Show that then $a \geq F_{k+2}$ and $b \geq F_{k+1}$. Here, F_k denotes the k-th **Fibonacci number**, defined via:
$F_0 = 0$, $F_1 = 1$ and $F_k := F_{k-1} + F_{k-2}$ for $k \geq 2$.

(c) The time complexity of the algorithm is $O(log(b))$.

Exercise 2.

Let $\phi : \mathbb{N} \to \mathbb{N}$ denote the Euler function, i.e. $\phi(n) := |\mathbb{Z}_n^*|$. Prove the following:

(a) If p is a prime and e is a positive integer, then $\phi(p^e) = p^e - p^{e-1}$.

(b) If $m = p \cdot q$ with different primes $p \neq q$, then $\phi(m) = (p-1) \cdot (q-1)$.

(c) If n and l are relatively prime and $m = n \cdot l$, then $\phi(m) = \phi(n) \cdot \phi(l)$.

(d) Let m have prime factor decomposition $m = \prod_{i=1}^{s} p_i^{e_i}$, where the p_i are distinct primes and $e_i \geq 1$. Then $\phi(m) = \prod_{i=1}^{s} (p_i^{e_i} - p_i^{e_i - 1})$.

Exercise 3.

Prove that for all $a, b \in \mathbb{Z}$ the following is true:

(a) If $gcd(a, m) = 1$ and $gcd(b, m) = 1$, then $gcd(a \cdot b, m) = 1$.

(b) Let $d, m \in \mathbb{N}$ where $d|m$ und $a \equiv b \ mod \ m$, then $a \equiv b \ mod \ d$.

Exercise 4.

Solve in $\mathbb{Z}_{16}$ the following system of equations:

$$\begin{aligned} 3x + 5y + 7z &= 3 \\ x + 4y + 13z &= 5 \\ 2x + 7y + 3z &= 4. \end{aligned}$$

Exercise 5.

Show that for integers a and n the following are equivalent:

(a) there is a solution x in $\mathbb{Z}$ to $ax = 1 \; mod \; n$,

(b) there are solutions x and y in $\mathbb{Z}$ to $ax + ny = 1$ and

(c) a and n are relatively prime.

Exercise 6.

Find in $\mathbb{Z}_{11}$ the inverse of the matrix

$$M := \begin{pmatrix} 3 & 5 & 1 \\ 0 & 0 & 2 \\ 0 & 7 & 7 \end{pmatrix}.$$