Goethe-Universität Frankfurt
Institut für Mathematik
Summer term 2019
21. April 2020

Elementare Zahlentheorie
Prof. Dr. Martin Möller
Dr. Jonathan Zachhuber
M.Sc. Riccardo Zuffetti

Übungsblatt 1

Aufgabe 1

The *Fermat numbers* are defined as

$$F_n = 2^{2^n} + 1, \quad \text{for every } n \in \mathbb{N}.$$

(i) Prove that $\prod_{k=0}^{n-1} F_k = F_n - 2$ for every $n \geq 1$.

(ii) Prove that the Fermat numbers are pairwise coprime, i.e.

$$\gcd(F_n, F_m) = 1, \quad \text{for every } n \neq m.$$

The *Fibonacci sequence* $\{L_n\}_{n\in\mathbb{N}}$ is the sequence of positive integers defined recursively as

$$L_0 = 1, \quad L_1 = 1 \quad \text{and} \quad L_{n+2} = L_{n+1} + L_n \quad \text{for every } n \in \mathbb{N}.$$

(a) Compute $\gcd(L_{n+1}, L_n)$ for every $n \in \mathbb{N}$.

(b) How many divisions with remainder are necessary to compute $\gcd(L_{n+1}, L_n)$ via the Euclidean algorithm?

Aufgabe 2

Let $a_1, \dots, a_n, r$ be integers, with $n > 0$. Prove that the Diophantine equation

$$a_1X_1 + \cdots + a_nX_n = r$$

admits a solution if and only if $\gcd(a_1, \dots, a_n)$ divides r.

Aufgabe 3

Find the solutions of the following Diophantine equations.

(i) $105X + 234Y = 9$.

(ii) $315X + 420Y + 234Z = 9$.

Aufgabe 4

Let $f(a, b)$ be the number of iterations the Euclidean algorithm needs to compute $\gcd(a, b)$, where $0 \leq a \leq b$. Prove that

$$f(a, b) = O(\log_2 a), \quad \text{when } a \to \infty.$$

Hint. The request of the exercise can be rewritten without the *big O notation* as follows. Prove that there exist a positive constant C and $n_0 \in \mathbb{N}$ such that

$$f(a, b) \leq C \cdot \log_2 a \quad \text{for every } a \geq n_0 \text{ and for every } b \geq a.$$

Please, upload your solutions on the Olat page of this course, by **14:00** on **Wednesday, 29.4.2020**.