Prof. Dr. M. Lesch
P. Holy

Abgabe wegen dies academicus am 02.12.
auch noch am 03.12. vor 09:15 morgens möglich

Übungen zur Vorlesung Elemente der Mathematik

ÜBUNGSBLATT 6

Aufgabe 1: (3 Punkte) Zeigen Sie, dass es unendlich viele Primzahlen p gibt so dass

$$p \equiv 2 \ (3).$$

Tipp: Nehmen Sie für einen Widerspruch an es gäbe nur endlich viele solche Primzahlen $p_1, \ldots, p_n$. Betrachten Sie ähnlich wie im Beweis des Satzes von Euklid in der Vorlesung deren Produkt und unterscheiden Sie die Fälle dass n gerade oder ungerade ist.

Aufgabe 2: (6 Punkte) Sei $F_0 = 0$, $F_1 = 1$ und für $n \geq 1$ sei $F_{n+1} = F_n + F_{n-1}$, $\langle F_n \mid n \in \mathbb{N} \rangle$ bezeichne also die Folge der *Fibonacci-Zahlen*.

(a) Bestimmen Sie die Lösungen x_+ und x_- der Gleichung $x^2 - x - 1 = 0$, dabei soll x_+ die positive und x_- die negative Lösung bezeichnen.

(b) Zeigen Sie mit vollständiger Induktion, dass für alle $n \in \mathbb{N}$ gilt:

$$F_n = \frac{1}{\sqrt{5}} (x_+^n - x_-^n).$$

(c) Für $x \in \mathbb{R}$ bezeichne $[x]$ die größte Zahl $y \in \mathbb{Z}$ so dass $y \leq x$. Zeigen Sie, dass für alle $n \in \mathbb{N}$ gilt:

$$F_n = \left[\frac{1}{\sqrt{5}} x_+^n + \frac{1}{2} \right].$$

(d) Zeigen Sie, dass für alle $n \geq 1$ gilt:

$$x_+^n \leq F_n \cdot \sqrt{5} + \frac{1}{2}.$$

Sei $a > b > 0$ für $a, b \in \mathbb{N}$. Wir notieren eine Berechnung von (a, b) mit Hilfe des Euklidischen Algorithmus wie folgt. Sei $r_0 = a$ und sei $r_1 = b$.

$$\begin{aligned} r_0 &= q_0 r_1 + r_2 \\ r_1 &= q_1 r_2 + r_3 \\ &\ldots \\ r_{n-2} &= q_{n-2} r_{n-1} + r_n \\ r_{n-1} &= q_{n-1} r_n + 0 \end{aligned}$$

Dabei ist also $r_n = (a, b)$. Wir sagen in obigem Fall, dass die Berechnung des ggT von a und b genau n Schritte benötigt (das entspricht der Anzahl der Zeilen in obiger Berechnung).

Aufgabe 3: (3 Punkte) Zeigen Sie

(a) Für alle $k \leq n$ gilt $r_k \geq 1$ und für alle $k < n$ gilt $q_k \geq 1$.

(b) Wenn die Berechnung von (a, b) genau n Schritte benötigt, dann ist $a \geq F_{n+1}$ und $b \geq F_n$.

(c) Bezeichnet $K(a)$ die maximale Anzahl der nötigen Schritte in der Berechnung von (a, b) für beliebiges $b < a$, so gilt

$$K(a) \leq \frac{\log(a \cdot \sqrt{5} + \frac{1}{2})}{\log x_+} - 1.$$

Bemerkung: Damit ist also der Berechnungsaufwand für die Ermittlung von (a, b) logarithmisch in a.

Aufgabe 4: (6 Punkte) Sei p eine Primzahl.

(a) Zeigen Sie: $(\mathbb{Z}/p\mathbb{Z}, +)$ ist eine kommutative Gruppe mit neutralem Element $[0]$.

(b) Zeigen Sie: $(\mathbb{Z}/p\mathbb{Z}, \cdot)$ ist nullteilerfrei – sind $[a], [b]$ beide in $\mathbb{Z}/p\mathbb{Z}$ und ist $[a] \cdot [b] = [0]$, so ist $[a] = [0]$ oder $[b] = [0]$.

(c) Sei $(\mathbb{Z}/p\mathbb{Z})^{\neq 0} := (\mathbb{Z}/p\mathbb{Z}) \setminus \{[0]\}$. Zeigen Sie: Wenn wir $[b] \in (\mathbb{Z}/p\mathbb{Z})^{\neq 0}$ fest wählen, so ist die Multiplikation mit $[b]$ eine injektive Operation auf $(\mathbb{Z}/p\mathbb{Z})^{\neq 0}$, das soll heißen sind $[a_0] \neq [a_1]$ beide in $(\mathbb{Z}/p\mathbb{Z})^{\neq 0}$, so ist $[a_0] \cdot [b] \neq [a_1] \cdot [b]$.

(d) Zeigen Sie mit Hilfe von (b) und (c): Ist $[a] \in (\mathbb{Z}/p\mathbb{Z})^{\neq 0}$, so gibt es $[b] \in (\mathbb{Z}/p\mathbb{Z})$ mit $[a] \cdot [b] = [1]$.

(e) Zeigen Sie: $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist ein Körper.

(f) Welche der zu zeigenden Aussagen in (a)-(e) gelten noch, wenn wir nicht voraussetzen, dass p Primzahl ist (jedoch soll $p > 1$ sein)?