Übungen zur Vorlesung Elementare Zahlentheorie (SS 18)

PD Dr. Jürgen Müller

(3.1) Aufgabe: Primzahlen.
Es seien $1 \neq a \in \mathbb{N}$ und $k \in \mathbb{N}$. Man zeige:

a) Ist $a^k - 1$ prim, so ist $a = 2$ und k prim. Ist umgekehrt $2^p - 1 \in \mathbb{Z}$ prim, wenn $p \in \mathcal{P}$ prim ist?
Bemerkung: Primzahlen der Form $2^p - 1$ heißen **Mersenne-Primzahlen**.

b) Ist $2^k + 1$ prim, so ist $k = 2^n$ für ein $n \in \mathbb{N}_0$. Ist umgekehrt $2^{2^n} + 1 \in \mathbb{Z}$ stets prim?
Bemerkung: Primzahlen der Form $2^{2^n} + 1$ heißen **Fermat-Primzahlen**.

(3.2) Aufgabe: Monotonie der Gradabbildung.
Es sei R ein Integritätsring und $\delta' : R \setminus \{0\} \to \mathbb{N}_0$ eine Abbildung, welche die Bedingung **i)** aus der in der Vorlesung gegebenen Definition eines euklidischen Rings erfüllt. Zeigen Sie, daß die Abbildung

$$\delta : R \setminus \{0\} \to \mathbb{N}_0, \quad a \mapsto \min\{\delta'(b) \mid b \in R \setminus \{0\} \quad \text{und} \quad a \mid b\}$$

beide Bedingungen aus dieser Definition erfüllt.

(3.3) Aufgabe: Laufzeit des erweiterten euklidischen Algorithmus.
Die Fibonacci-Folge $\{\mathrm{F}_n \mid n \in \mathbb{N}\}$ ist die Folge mit $\mathrm{F}_1 = \mathrm{F}_2 = 1$ und $\mathrm{F}_n = \mathrm{F}_{n-1} + \mathrm{F}_{n-2}$, für alle $n \geq 3$.

a) Zeigen Sie, daß

$$\mathrm{F}_n = \frac{\tau^n - (\tau')^n}{\sqrt{5}} = \lfloor \frac{\tau^n}{\sqrt{5}} + \frac{1}{2} \rfloor,$$

wobei $\tau = \frac{1+\sqrt{5}}{2}, \tau' = \frac{1-\sqrt{5}}{2}$ und $\lfloor x \rfloor$ der ganzzahlige Teil von $x \in \mathbb{R}$ ist.

b) Seien nun $a, b \in \mathbb{N}$ mit $a > b$, so daß der erweiterte euklidische Algorithmus $l - 1$ Divisionen benötigt. Zeigen Sie, daß $a_1 \geq \mathrm{F}_l$ ist.

c) Folgern Sie, daß $l \leq \log_\tau((a_1 + \frac{1}{2}) \cdot \sqrt{5})$.

(3.4) Aufgabe: Erweiterter euklidischer Algorithmus.
Bestimmen Sie $x, y \in \mathbb{Z}$, so daß $xa + yb = \mathrm{ggT}_+(a, b)$, für

a) $(a, b) = (2^{10} - 1, 2^4 - 1)$.

b) $(a, b) = (2^{16} + 1, 2^8 + 1)$.

Abgabe: 3.05.2018 (Donnerstag), bis 10:00 Uhr.