**Albert–Ludwigs–Universität Freiburg**
**Institut für Mathematik**
**Abteilung für Reine Mathematik**
PD Dr. K. Halupczok
Dipl.–Math. S. Feiler

Übungen zur Vorlesung

# Elementare Zahlentheorie

Sommersemester 2009

## 4. Übungsblatt

11. Mai 2009

**Abgabe** der Lösungen bis zum **18. Mai 2009 um 14.$\underline{15}$ Uhr**

**Aufgabe 13** (Ordnung und Repetiereinsen)
Seien $p \in \mathbb{P}$, $q \in \mathbb{P}$ mit $p \neq 2 \neq q$ und $a \in \mathbb{Z}$.
Sei $R : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & R_n := \sum_{j=0}^{n-1} 10^j \end{array} \right\}$. $(R_n)_{n\in\mathbb{N}} = \left(\underbrace{1\cdots 1}_{n \text{ mal}}\right)_{n\in\mathbb{N}}$ ist die Folge der „**Repetiereinsen**“ (siehe auch Anwesenheitsaufgabe 4).

**a)** Zeigen Sie, dass $\left(q|\,(a-1) \text{ oder } \exists\, k \in \mathbb{N} \text{ mit } q = 2kp+1\right)$ aus $q|\,(a^p-1)$ folgt!

**b)** Zeigen Sie, dass entweder $q = 3$ gilt oder es ein $k \in \mathbb{Z}$ mit $q = 2kp+1$ gibt, falls $q$ ein Teiler von $R_p$ ist.

**c)** Zeigen Sie $\min\{\, n \in \mathbb{N}\,; p|R_n\}|\,(p-1)$ im Falle $3 \neq p \neq 5$.

**Aufgabe 14** (Primitivwurzeln modulo 25 und modulo 50) 3 Punkte
Geben Sie sämtliche Primitivwurzeln modulo 25 und modulo 50 an!
Gehen Sie dabei wie im Beweis zum Satz von Euler 2.13 vor!

**Aufgabe 15** (Verallgemeinerung von Lemma 2.14 (5))
Nach Lemma 2.14 (5) folgt für $m \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $(a,m) = 1$ und $b \in \mathbb{Z}$ mit $(b,m) = 1$ aus $(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$, dass $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$ ist.
Sie sollen nun beobachten, was passiert, wenn die Teilerfremdheit der Ordnungen nicht gegeben ist. Seien $m \in \mathbb{N}$, $k \in \mathbb{N}$ und $a_j \in \mathbb{Z}$ mit $(a_j, m) = 1$ für alle $j \in \mathbb{N}$ mit $j \leq k$.

**a)** Zeigen Sie, dass $\mathrm{ord}_m(a_1 \cdot \ldots \cdot a_k)$ ein Teiler von $[\mathrm{ord}_m(a_1), \ldots, \mathrm{ord}_m(a_k)]$ ist!

**b)** Zeigen Sie, dass im Allgemeinen $\mathrm{ord}_m(a_1 \cdot \ldots \cdot a_k) \neq [\mathrm{ord}_m(a_1), \ldots, \mathrm{ord}_m(a_k)]$ gilt!

**c)** Zeigen Sie, dass es ein $b \in \mathbb{Z}$ mit $(b,m) = 1$ und $\mathrm{ord}_m(b) = [\mathrm{ord}_m(a_1), \ldots, \mathrm{ord}_m(a_k)]$ gibt!

(Tipp: Induktion nach $k$)

bitte wenden

**Aufgabe 16** (FERMAT–Zahlen) 5 Punkte

Sei $F: \left\{ \begin{array}{ccc} \mathbb{N}_0 & \to & \mathbb{N} \\ n & \mapsto & F_n := 2^{2^n} + 1 \end{array} \right\}$ die Folge der FERMAT–Zahlen.

**a)** Zeigen Sie, dass $F_n$ für alle $n \in \mathbb{N} \setminus \{1\}$ im Zehnersystem mit der Ziffer 7 endet!

**b)** Zeigen Sie $\{ F_n \in \mathbb{N} \,; n \in \mathbb{N}_0 \} \cap \{ k^2 \in \mathbb{N} \,; k \in \mathbb{N} \} = \emptyset$!

**c)** Zeigen Sie $2^{F_n} \equiv 2 \bmod F_n$ für alle $n \in \mathbb{N}_0$!

**d)** Bestimmen Sie $\mathrm{ord}_{F_n}(2)$ für alle $n \in \mathbb{N}_0$!

**e)** Zeigen Sie $\# \left\{ p \in \mathbb{P} \,; p \middle| \left(2^{2^n} - 1\right) \right\} \geq n$ für alle $n \in \mathbb{N}_0$!

(Tipp: Es ist $2^{2^n} - 1 = \prod_{j=0}^{n-1} F_j$ für alle $n \in \mathbb{N}$.)