Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein  Dipl.-Math. Jochen Schröder

# Einführung in Algebra und Zahlentheorie – Übungsblatt 11

**Aufgabe 1** (4 Punkte)
Sei $R$ ein kommutativer Ring, $d, g \in R$ mit $d|g-1$. Weiterhin sei $x \in R$ $g$-adisch dargestellt durch

$$x = \sum_{i=0}^{n} a_i g^i \text{ mit } n \in \mathbb{N}_0, a_i \in R.$$

Zeige, dass $d$ genau dann ein Teiler von $x$ ist, wenn es die Summe $\sum_{i=0}^{n} a_i$ der Koeffizienten teilt.[1]

**Aufgabe 2** (4 Punkte)

a) Ist $2^n - 1$ für $n \in \mathbb{N}$ eine Primzahl, so ist bereits $n$ prim.

b) Ist $2^n + 1$ für $n \in \mathbb{N}$ eine Primzahl, so ist $n$ eine Zweierpotenz $n = 2^k$ für ein $k \in \mathbb{N}_0$.

c) Zeige, dass für $F_k = 2^{(2^k)} + 1$, $k \in \mathbb{N}_0$ die folgende Rekursion gilt: $F_k = \prod_{i=0}^{k-1} F_i + 2$.

d) Folgere aus c), dass es unendlich viele Primzahlen gibt.

*Bemerkung:* Die Umkehrungen von a) und b) wurden lange Zeit vermutet, sind aber jeweils falsch. Die kleinsten Gegenbeispiele sind $2^{11} - 1 = 23 \cdot 89$ und $2^{(2^5)} + 1 = 641 \cdot 6700417$.
Eine (Prim-)Zahl der Form $2^n - 1$ heißt *Mersenne-(Prim-)Zahl.* Diese spielen heute bei der Suche nach großen Primzahlen eine wichtige Rolle. Eine (Prim-)Zahl der Form $2^{(2^k)} + 1$ heißt *Fermat-(Prim-)Zahl.*

**Aufgabe 3** (4 Punkte)
Seien $n \in \mathbb{N}$ quadratfrei, $a \in \mathbb{Z}$ beliebig. $\varphi$ sei die eulersche $\varphi$-Funktion. Zeige folgende Aussagen:

a) Für alle $k \in \mathbb{N}_0$ ist $a^{k \cdot \varphi(n)+1} \equiv a$ (modulo $n$).

b) Für $e \in \mathbb{N}$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$ ist die Abbildung $a \mapsto a^e$ eine Bijektion auf $\mathbb{Z}/n\mathbb{Z}$.

*Bemerkung*: Das RSA-Verfahren basiert auf einem Spezialfall dieser Aussage.

**Aufgabe 4** (4 Punkte) (**Aufgabenteil c) umformuliert**)
Seien $a, b \in \mathbb{N}$ und $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Desweiteren seien $g = \mathrm{ggt}(a, b)$, $k = \mathrm{kgV}(a, b)$.

a) Finde einen Isomorphismus zwischen $\mathbb{Z}^2/A\mathbb{Z}^2$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

b) Finde $S, T \in \mathrm{SL}_2(\mathbb{Z})$ mit $S$ von der Form $\begin{pmatrix} 1 & 1 \\ * & * \end{pmatrix}$, so dass $SAT = \begin{pmatrix} g & 0 \\ 0 & k \end{pmatrix}$.

c) Zeige $\mathbb{Z}^2/A\mathbb{Z}^2 \cong \mathbb{Z}^2/SAT\mathbb{Z}^2$ oder $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ und folgere anschließend die jeweils andere Aussage daraus.

**Abgabe** bis Dienstag, 3. Juli, 9:40 Uhr im Abgabekasten, direkt vor der großen Übung um 9:45 Uhr oder auch vorher direkt bei deinem Übungsleiter.

[1] Erinnere dich daran, dass du das für $R = \mathbb{Z}$, $g = 10$, $d = 3$ (oder auch $d = 9$) bereits aus der Schule kennst.