UNIVERSITÄT DES SAARLANDES
Fachrichtung 6.1 - Mathematik
Christian Bopp

Übungen zur Elementaren Zahlentheorie

Sommersemester 2018

Die Lösungen des Übungsblattes sind bis spätestens 14.00 Uhr, am 30.05.2018, in die Briefkästen vor dem Zeichensaal in Geb. E2 5, einzuwerfen.
Alle Übungsblätter und Informationen zur Vorlesung werden auf der Seite unserer Arbeitsgruppe unter *Teaching* zu finden sein: www.math.uni-sb.de/ag-schreyer/

Blatt 7 — 23.05.2018

Aufgabe 1. Für $a, n \in \mathbb{N}$ definieren wir $A_n = a^{2^n} - 1$. Zeigen Sie, dass $A_n \big| (A_m - 2)$, falls $m > n$. Berechnen Sie $\mathrm{ggT}(A_m, A_n)$ und folgern Sie, dass es unendlich viele Primzahlen gibt.

Aufgabe 2. Beweisen oder widerlegen Sie:

(a) Ist $a \equiv b \bmod m$, so ist $a^2 \equiv b^2 \bmod m$
(b) Ist $a^2 \equiv b^2 \bmod m$, so ist $a \equiv b \bmod m$
(c) Ist $a^2 \equiv b^2 \bmod m$, dann gilt $a \equiv b \bmod m$ oder $a \equiv -b \bmod m$
(d) Ist $a \equiv b \bmod m$, so ist $a^2 \equiv b^2 \bmod m^2$

Aufgabe 3. Sei $m \in \mathbb{N}_{\geq 2}$. Zeigen Sie, dass $\mathbb{Z}/m\mathbb{Z}$ bezüglich der in Bemerkung 4.5 definierten Verknüpfungen ein kommutativer Ring mit Einselement ist.

Aufgabe 4. (a) Bestimmen Sie die Additions- und Multiplikationstabelle von $\mathbb{Z}/8\mathbb{Z}$.
(b) Haben die Elemente $[10], [13] \in \mathbb{Z}/600\mathbb{Z}$ ein multiplikatives Inverses? Wenn ja, bestimmen Sie dieses.
(c) Sei $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie, dass $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist.