



Übungen zur Vorlesung Mathematik für Informatiker 1

Wintersemester 2013/14

Die Lösungen des Übungsblattes sind am 20.11.2013 **vor der Vorlesung** abzugeben.

**Blatt 5**

13. November 2013

**Aufgabe 1** (Zur Qualität von Primzahltests mit Hilfe des kleinen Satzes von Fermat). Nach dem kleinen Satz von Fermat gilt:

$$p \text{ ist Primzahl} \implies a^{p-1} \equiv 1 \pmod{p} \quad \forall a \text{ mit } \text{ggT}(a, p) = 1.$$

Verwenden Sie MAPLE, um zu zeigen, dass die Umkehrung nicht gilt, d.h. finden Sie eine zusammengesetzte Zahl  $n$ , für die  $a^{n-1} \equiv 1 \pmod{n}$  für alle  $a$  mit  $\text{ggT}(a, n) = 1$  gilt.

**Aufgabe 2** (Endliche Körper).

- (a) Zeigen Sie, dass es einen Körper mit genau 4 Elementen gibt, indem Sie die Verknüpfungstafeln herleiten.
- (b) Zeigen Sie, dass es keinen Körper mit genau 6 Elementen gibt.

**Aufgabe 3** (Irrationale Zahlen). Zeigen Sie:

- (a)  $\sqrt{3}$ ,  $\sqrt{15}$ ,  $\sqrt{45}$  sind irrational,
- (b)  $\sqrt[3]{2}$  ist irrational,
- (c)  $\sqrt{p}$  ist irrational für jede Primzahl  $p$ .

**Aufgabe 4.** Zeigen Sie, dass  $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$  zusammen mit den Verknüpfungen

$$+ : \mathbb{Q}[\sqrt{2}] \times \mathbb{Q}[\sqrt{2}] \longrightarrow \mathbb{Q}[\sqrt{2}], \quad (a + b\sqrt{2}, c + d\sqrt{2}) \mapsto (a + c) + (b + d)\sqrt{2},$$

$$\cdot : \mathbb{Q}[\sqrt{2}] \times \mathbb{Q}[\sqrt{2}] \longrightarrow \mathbb{Q}[\sqrt{2}], \quad (a + b\sqrt{2}, c + d\sqrt{2}) \mapsto (ac + 2bd) + (ad + bc)\sqrt{2},$$

ein Körper ist. (Hinweis: Zur Bestimmung des Inversen, denken Sie an die dritte binomische Formel sowie das Erweitern von Brüchen.)