Prof. Dr. Peter Bürgisser
Jesko Hüttenhain

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Sekretariat MA 3-2

Übungen zur Vorlesung Algebra 1

Wintersemester 2016/2017

Aufgabenzettel 9

Für $n \in \mathbb{Z}$ sei $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ und für $a, b \in \mathbb{Z}$ schreiben wir $a \equiv_n b$, wenn $a - b \in n\mathbb{Z}$. Wir bezeichnen mit $\varphi(n) := |\mathbb{Z}_n^\times|$ die *Eulersche Phi-Funktion*.

Aufgabe 1 (8 Punkte). Bestimme alle $x \in \mathbb{Z}$ mit: $x \equiv_7 2$, $x \equiv_{13} 6$ und $x \equiv_3 1$. Gib auch die kleinste positive Lösung an.

Aufgabe 2 (10 Punkte). Zeige, dass für verschiedene Primzahlen $p, q \in \mathbb{Z}$ die folgenden Formeln gelten:

$$\varphi(p^k) = p^{k-1}(p-1), \tag{1}$$

$$\varphi(p \cdot q) = (p-1)(q-1). \tag{2}$$

Aufgabe 3 (10 Punkte).

(1) Sei $n \in \mathbb{Z}$ und $k := \varphi(n)$. Zeige, dass für jede zu n teilerfremde Zahl $a \in \mathbb{Z}$ die Gleichung $a^k \equiv_n 1$ erfüllt ist.

Sei nun $n = p \cdot q$ für zwei verschiedene Primzahlen p und q. Sei außerdem $e \in \mathbb{Z}$ teilerfremd zu k.

(2) Zeige, dass es ein $d \in \mathbb{Z}$ gibt, so dass $ed \equiv_k 1$.

(3) Zeige, dass $m^{ed} \equiv_n m$ für alle $m \in \mathbb{Z}$.

Bemerkung. Es ist keine effiziente Methode bekannt, um die Zahl d aus dem Tupel (n, e) zu berechnen. Auf diesem Problem basiert das RSA-Kryptosystem.

Aufgabe 4 (12 Punkte). Sei $\mathbb{K}$ ein Körper. Zeige:

(1) Es gibt in $\mathbb{K}[X]$ unendlich viele normierte, irreduzible Polynome.

(2) Falls jedes nicht-konstante Polynom aus $\mathbb{K}[X]$ eine Nullstelle hat, so enthält $\mathbb{K}$ unendlich viele Elemente.

Auf der nächsten Seite geht es weiter.

Die Abgabe erfolgt bis **Dienstag**, den **3.1.2017**, vor der Übung. Gutes Gelingen!

Prof. Dr. Peter Bürgisser
Jesko Hüttenhain

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Sekretariat MA 3-2

Weihnachtsaufgaben

Auf diesem Übungszettel sind insgesamt 70 Punkte erreichbar, für die Gesamtwertung zählt der Zettel jedoch mit den üblichen 40 Punkten, d.h. es können Bonuspunkte erzielt werden, welche für die Gesamtwertung und die Zulassung zählen. Wenn ihr diese Bonusaufgaben bearbeitet, gebt sie bitte auf einem **separaten Zettel** ab.

Wir wünschen frohe Weihnachten!

Aufgabe 5 (10 Weihnachtspunkte). Sei $f \in \mathbb{Z}_2[X]$ und $R := \mathbb{Z}_2[X]/(f)$. Bezeichne mit x das Bild von X unter der kanonischen Abbildung $\mathbb{Z}_2[X] \to R$.

(1) Sei $f = X^5 + X^2 + 1$. Zeige, dass das Inverse von $x + x^2 + x^4$ in R gleich x^3 ist.

(2) Sei $f = X^4 + X^3 + 1$. Zeige, dass $x + 1 \in R^\times$ und berechne $(x+1)^{-1}$.

Aufgabe 6 (20 Weihnachtspunkte).

(1) Sei G eine endliche, abelsche Gruppe und $m := \max\{\operatorname{ord}(g) \mid g \in G\}$. Zeige, dass $\forall g \in G\colon\ \operatorname{ord}(g) \mid m$.

(2) Sei $\mathbb{K}$ ein beliebiger Körper. Man zeige, dass es zu jeder natürlichen Zahl $n > 1$ höchstens $n - 1$ Elemente der Ordnung n in $\mathbb{K}^\times$ gibt.

(3) Sei $\mathbb{K}$ ein endlicher Körper. Zeige, dass $\mathbb{K}^\times$ zyklisch ist. Verwende dazu die Aufgabenteile 1 und 2.

(4) Was ist die Anzahl der primitiven Elemente in $\mathbb{Z}_p^\times$? Ein primitives Element ist ein $x \in \mathbb{Z}_p^\times$, so dass x ganz $\mathbb{Z}_p^\times$ als Gruppe erzeugt.

Die Abgabe erfolgt bis **Dienstag**, den **3.1.2017**, vor der Übung. Gutes Gelingen!