Universität Bielefeld

Peter Zeiner
Fakultät für Mathematik

Bielefeld, 17.10.2013

Wintersemester 2013/14

Elementare Zahlentheorie

Übungszettel 1

Aufgabe 5: (a) Zeigen Sie, dass $\mathrm{ggT}(ak, bk) = k\,\mathrm{ggT}(a, b)$ für $k \in \mathbb{N}$ gilt.

(b) Zeigen Sie, dass $ab = \mathrm{ggT}(a, b)\,\mathrm{kgV}(a, b)$ für $a, b \in \mathbb{N}$ gilt.
Hinweis: Beachten Sie, dass sowohl $\frac{ab}{\mathrm{ggT}(a,b)}$ als auch ab ein Vielfaches von $\mathrm{kgV}(a, b)$ ist, d.h. es existiert ein $c \in \mathbb{N}$ so, dass $ab = c\,\mathrm{kgV}(a, b)$. Wodurch ist die rechte Seite teilbar? **(2+2 Punkte)**

Aufgabe 6: Betrachten Sie den euklidischen Algorithmus $r_{-1} = a$, $r_0 = b$, $r_{k-2} = q_k r_{k-1} + r_k$ für zwei ganze Zahlen a, b mit $|b| < |a|$ wie in der Vorlesung in zwei verschiedenen Varianten.

(a) Betrachten Sie zuerst die Variante mit $-\frac{|r_{k-1}|}{2} < r_k \leq \frac{|r_{k-1}|}{2}$. Zeigen Sie, dass der euklidische Algorithmus nach spätestens $[\log_2 |b|] + 1$ Schritten terminiert, d.h. es existiert ein $k \leq [\log_2 |b|] + 1$ so, dass $r_k = 0$ gilt.

(b) Betrachten Sie im Folgenden die Variante mit $0 \leq r_k < r_{k-1}$. Zeigen Sie, dass hier nicht mehr als $2[\log_2 |b|] + 1$ Schritte notwendig sind.
Hinweis: Vergleichen Sie die einzelnen Schritte der beiden Varianten.

(c) Die Fibonacci-Zahlen sind definiert durch $f_{n+1} = f_n + f_{n-1}, f_1 = f_2 = 1$. Geben Sie den Euklidischen Algorithmus für $a = f_{m+1}, b = f_m$ explizit an, d.h. geben Sie q_k und r_k für alle k an.

(d) Geben Sie das kleinste Paar (lexikographische Ordnung) zweier Zahlen an, für das der euklidische Algorithmus nach 5 Schritten stoppt. **(1+2+2+1 Punkte)**

Aufgabe 7: (a) Sei $I \subseteq \mathbb{Z}$ ein Unterring von $\mathbb{Z}$. Zeigen Sie, dass I von der Form $a\mathbb{Z} := \{an \mid n \in \mathbb{Z}\}$ ist.

(b) Ein Ring, dessen Ideale alle Hauptideale sind, heißt Hauptidealring. Begründen Sie, warum $\mathbb{Z}$ ein Hauptidealring ist. Zur Erinnerung: Ein Hauptideal ist ein Ideal der Form $aR := \{ab \mid b \in R\}$ für ein festes $a \in R$ **(2+1 Punkte)**

Aufgabe 8: Zur Erinnerung: Ein Unterring $I \subseteq R$ eines kommutativen Rings heißt Ideal, falls $ab \in I$ für alle $a \in I, b \in R$. Die Summe zweier Ideale I und J ist definiert durch $I + J := \{a + b \mid a \in I, b \in J\}$. Das Produkt $I \cdot J = IJ$ ist die Menge aller endlichen Summen der Form $\sum_i a_i b_i$ mit $a_i \in I, b_i \in J$.

(a) Zeigen Sie, dass $R := \mathbb{Z}[i\sqrt{5}] := \{m + in\sqrt{5} \mid m, n \in \mathbb{Z}\}$ mit der üblichen Addition und Multiplikation ein Ring mit 1 ist (i ist die imaginäre Einheit).

(b) Berechnen Sie $I = 2R + (1 + i\sqrt{5})R$, d.h., charakterisieren Sie die Elemente von I auf eine geeignete, einfache Weise. *Hinweis:* Die Elemente von I sind von der Form $m + in\sqrt{5}$, wobei $m + n$ eine einfache Bedingung erfüllt.

(c) Gilt $I = R$ oder $I = (3 + i\sqrt{5})R$?

(d) Sei $J = 2R + (1 - i\sqrt{5})R$. Berechnen Sie $I \cdot J$. **(2+2+2+2 Punkte)**

Abgabe bis zum 24.10.2013!