Ruhr-Universität Bochum
Fakultät für Mathematik Sommersemester 2005

Übungsaufgaben zur Zahlentheorie

(Holtkamp)

Sonderregelung: Zur vollständigen Lösung jeder Aufgabe gehört die Kennzeichnung der (maximal 4) Schritte, die als wichtigste Schritte eingeschätzt werden!

1: Man zeige: Durch

$$\Big(\big\{r \in \mathbb{Q} : r^2 \leq 3 \text{ oder } r < 0\big\}, \big\{r \in \mathbb{Q} : r > 0 \text{ und } r^2 > 3\big\}\Big)$$

wird ein Dedekindscher Schnitt in $\mathbb{Q}$ definiert, der nicht rational ist.
2: Es sei $z = (A, B) > 0$ ein (positiver) Dedekindscher Schnitt in $\mathbb{Q}$. Man zeige, dass durch $z' = (A', B')$ mit

$$B' = \big\{r^{-1} : r \in A, r > 0, r \neq \max A\big\}, A' = (B')^c$$

ein Schnitt definiert wird, der multiplikativ invers ist zu z.
3*: Eine Folge (I_n) von abgeschlossenen Intervallen $I_n = [r_n, s_n]$ in $\mathbb{Q}$ heißt rationale Intervallschachtelung, wenn

$$I_{n+1} \subseteq I_n \text{ (für alle } n) \text{ und } \lim(s_n - r_n) = 0.$$

(i) Man zeige, dass auf der Menge aller Intervallschachtelungen eine Äquivalenzrelation gegeben wird durch

$$(I_n) \approx (I'_n) \iff \text{ es existiert eine gemeinsame Verfeinerung } (J_n)$$

(Eine Schachtelung (J_n) heißt Verfeinerung von (I_n), falls $J_n \subseteq I_n$ für alle n.)
Für die Menge R der Äquivalenzklassen beweise man, dass durch $r \mapsto ([r, r])$ eine Inklusion $\mathbb{Q} \subseteq R$ definiert wird.

(ii) Man zeige: Ist $([r_n, s_n])$ rationale Intervallschachtelung, so sind $(r_n), (s_n)$ rationale Cauchy-Folgen und durch $([r_n, s_n]) \mapsto (r_n)$ wird eine Abbildung $R \to F/N = \mathbb{R}$ gegeben. Existiert eine Umkehrabbildung?

4: Man zeige: $I = \{0, \pm 12, \pm 24, \pm 36, \ldots\}$ ist ein Ideal im Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen, und der zugehörige Restklassenring $\mathbb{Z}/I$ kann nicht zu einem Körper gemacht werden.

5:

(i) Sei x eine Menge (von Mengen). Man betrachte die Menge $\{x\}$, die x als einziges Element besitzt, und folgere aus dem Fundierungsaxiom, dass $x \notin x$ gilt.

(ii) Sei $(5, 7, 2)$ bzw. $(21, 9, 17)$, die Ausgangsstellung eines NIM-Spiels, bei dem Sie entscheiden dürfen, ob Sie beginnen oder nicht. Was tun Sie?

6: Es sei $\frac{1}{2} := (\{0\}, \{1\})$.

(i) Man zeige: $\frac{1}{2}$ ist eine Conway-Zahl und $0 \leq \frac{1}{2}$, $1 \not\leq \frac{1}{2}$.

(ii) Man berechne $1 + \frac{1}{2}$.

(iii) Man zeige: $1 \leq \frac{1}{2} + \frac{1}{2}$.

(iv) Man zeige, dass $\frac{1}{2} + \frac{1}{2} \leq 1$ und folgere, dass $\frac{1}{2} + \frac{1}{2} = 1$.

7: Für $2 \leq m \in \mathbb{N}$ sei E_m die Menge der zu m teilerfremden Zahlen k mit $1 \leq k \leq m$.
Man zeige: Für jedes $e \in E_m$ besitzt die Restklasse $\bar{e}$ in $\mathbb{Z}/m\mathbb{Z}$ ein multiplikatives Inverses.
Man berechne $\bar{e}^{-1}$ für jedes $e \in E_{12}$.

8:

(i) Man berechne den ggT$(1929, 1623)$ mittels euklidischem Algorithmus.

(ii) Man gebe alle ganzzahligen Lösungen der Gleichung

$$1929X - 1623Y = 6$$

an.

9: Man berechne alle ganzzahligen Lösungen der Gleichung

$$-15X_1 + 10X_2 - 6X_3 = 7.$$

10:

(i) Man zeige: Der Polynomring $\mathbb{Q}[x, y]$ in zwei Variablen über $\mathbb{Q}$ ist kein Hauptidealring.

(ii) Im Polynomring $(\mathbb{Z}/3\mathbb{Z})[x]$ in einer Variablen über dem Körper $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ seien die Elemente

$$f = x^7 + 2x^4 + x^3 + x, \quad g = 2x^3 + x + 2$$

gegeben.
Man finde Polynome q, r in $(\mathbb{Z}/3\mathbb{Z})[x]$, so dass gilt:

$$f = qg + r$$

mit $\text{grad}(r) < \text{grad}\ (g)$.

11: Man bestimme alle irreduziblen Polynome vom Grad ≤ 5 im Polynomring $(\mathbb{Z}/2\mathbb{Z})[x]$ in einer Variablen über dem Körper $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$.
12*: Seien a und $b \neq 0$ komplexe Zahlen. Man zeige:
Sind a und b algebraisch, so sind auch $a \cdot b$ und b^{-1} algebraisch.
13: Für jede der folgenden algebraischen Zahlen a bestimme man das Minimalpolynom $\mu_a \in \mathbb{Q}[x]$

(i)
$$a = -1 + i\sqrt{3}$$

(ii)
$$a = \sqrt{2} + \sqrt{3}$$

(iii)
$$a = \sqrt{2} - \sqrt{3}$$

(iv)
$$a = \sqrt{2} - i\sqrt{3}$$

Hierbei ist $i = \sqrt{-1}$.
14: Man entscheide für jede der folgenden komplexen Zahlen ob sie ganzalgebraisch ist oder nicht:

$$2,\ \frac{1}{2},\ \frac{1}{\sqrt[17]{2}},\ 3 + 5\sqrt{7},\ 6 - \frac{2}{7}\sqrt{-1},\ \frac{\sqrt{5} - 1}{2},\ \frac{\sqrt{-5} - 1}{2},$$
$$\frac{\sqrt{-3} - 1}{2},\ \frac{\sqrt[3]{-108}}{3},\ \frac{3 + 2\sqrt{6}}{1 - \sqrt{6}},\ \frac{3 + 2\sqrt{6}}{2 - \sqrt{6}},\ \frac{\sqrt{3} + \sqrt{7}}{2}$$

15: Sei $m \in \mathbb{Z}$ quadratfrei, $m \leq -2$. Man bestimme die Einheiten von O_m.
16*: Man zeige: Für $m \in \{2, 3, 5\}$ ist O_m euklidisch.
17: Sei $d = -5$ und O_d der Ganzheitsring des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-5})$. Für $a \in O_d$ sei $N(a)$ die Norm bzgl. $\mathbb{Q}(\sqrt{-5})$.

(i) Man berechne $N(3), N(2 + \sqrt{-5}), N(2 - \sqrt{-5})$.

(ii) Man zeige, dass $\{a \in O_d : 2 \leq N(a) \leq 3\} = \emptyset$ gilt und folgere, dass $2 + \sqrt{-5}$, $2 - \sqrt{-5}$ und 3 irreduzibel in O_d sind.

(iii) Welche der Zahlen $2 + \sqrt{-5}$, $2 - \sqrt{-5}$ und 3 sind prim in O_d?

(iv) Man gebe ein Beispiel an für nicht (bis auf Vorzeichen und Reihenfolge der Faktoren) eindeutige Darstellungen eines $a \in O_d$ als Produkt irreduzibler Elemente.

18: Man bestimme die Menge $\{(x, y) \in \mathbb{N} \times \mathbb{N} : x^2 + y^2 = 5 \cdot 13 \cdot 17\}$.
19*: Sei $\varphi : \mathbb{N} \to \mathbb{N}$ die Eulersche Phifunktion. Man zeige:

(i) Ist $n = p^\alpha$, p prim und $\alpha \in \mathbb{N}$, so ist $\varphi(n) = p^\alpha - p^{\alpha-1}$.

(ii) Sind m, n teilerfremd, so ist $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

20: Man bestimme eine Primitivwurzel modulo 5^4.
21*:

(i) Gibt es zwei Einheiten a, b in $(\mathbb{Z}/70\mathbb{Z})^*$, die die Einheitengruppe $(\mathbb{Z}/70\mathbb{Z})^*$ erzeugen (d.h. $\{a^i b^j : i, j \in \mathbb{N}\} = (\mathbb{Z}/70\mathbb{Z})^*$)?

(ii) Gibt es drei Einheiten a, b, c in $(\mathbb{Z}/120\mathbb{Z})^*$, die die Einheitengruppe $(\mathbb{Z}/120\mathbb{Z})^*$ erzeugen (d.h. $\{a^i b^j c^k : i, j, k \in \mathbb{N}\} = (\mathbb{Z}/120\mathbb{Z})^*$)?

22: Man bestimme für alle $c \in \mathbb{N}$, $c \leq 12$ das Legendre-Symbol $\left(\frac{c}{13}\right)$, die Anzahl $\mu_{13}(c)$ und für alle Primitivwurzeln a modulo 13 den Index $\mathrm{ind}_a(c)$.
23*: Seien $\alpha, n, c \in \mathbb{N}$, c ungerade, $\alpha > 2$. Weiterhin sei u fest gewählt mit $u \equiv \pm 3 \mod 8$. Man zeige:

(i) c ist genau dann n-ter Potenzrest modulo 2^α, wenn gilt:
Die Gleichungen $nX \equiv i \mod 2$ und $nY \equiv j \mod 2^{\alpha-2}$ sind lösbar (in $\mathbb{Z}$), wobei i, j definiert sind durch $c \equiv (-1)^i u^j \mod 2^\alpha$.

(ii) Ist n ungerade, so ist c ein n-ter Potenzrest modulo 2^α. Ist n gerade und $c \not\equiv 1 \mod 8$, so ist c kein n-ter Potenzrest modulo 2^α.

(iii) Ist $c \equiv 1 \mod 8$, so sind i, j gerade und es gilt für alle geraden n:
c ist ein n-ter Potenzrest modulo 2^α genau dann, wenn j durch $\mathrm{ggT}(n, 2^{\alpha-2})$ teilbar ist.

24:

(i) Ist 521 quadratischer Rest modulo 572?

(ii) Ist 1042 quadratischer Rest modulo 572?

(iii) Ist 103 quadratischer Rest modulo 828?

(iv) Ist 57 quadratischer Rest modulo 828?

25:

(i) Sei $p = 10k \pm 1$ eine Primzahl, $k \in \mathbb{N}$. Dann ist $\left(\frac{5}{p}\right) = 1$.

(ii) Sei $p = 10k \pm 3$ eine Primzahl, $k \in \mathbb{N}$. Dann ist $\left(\frac{5}{p}\right) = -1$.

26:

(i) Man bestimme die 12-adische Darstellung von 165 533 996 616.

(ii) Man zeige: 7 teilt $\sum_{i=0}^{k} a_i 10^i$ genau dann, wenn

$$\sum_{j\geq 0}(-1)^j(a_{3j} + 3a_{3j+1} + 2a_{3j+2})$$

durch 7 geteilt wird.

(iii) Man wende das in (ii) gegebene Kriterium auf die Zahlen 165 533 996 600 und 165 533 996 616 an.

27*:

(i) Man bestimme $|\ |_3$ von $999, 156, \frac{1}{30}, \frac{1}{9}, 0, -6$. Welche zwei dieser Zahlen haben den kleinsten 3-adischen Abstand voneinander?

(ii) Man zeige (für p prim, $x, y \in \mathbb{Z}_p$): $|xy|_p = |x|_p|y|_p$ und $|x + y|_p \leq \max(|x|_p, |y|_p)$

(iii) Man zeige (für p prim, $x, y, z \in \mathbb{Z}_p$): $|x, y|_p \leq \max(|x, z|_p, |z, y|_p)$, und $|x, y|_p = 0$ genau dann, wenn $x = y$

28*: Man zeige: Es gibt $i \in \mathbb{Z}_5$ mit $i^2 = -1$ und $j \in \mathbb{Z}_{13}$ mit $j^2 = -1$.
Man bestimme die zugehörige Restklasse von i bzw. j in $\mathbb{Z}/p^5\mathbb{Z}$ ($p = 5$ bzw. 13).

29*: Es sei p Primzahl, $a = \sum_{i=-m}^{\infty} a_i p^i \in \mathbb{Q}_p$. Man zeige:

(i) Ist $a = \frac{k}{n}, n \in \mathbb{N}, k = a \cdot n \in \mathbb{Z}$ so gibt es $s, t \in \mathbb{N}$ mit $a_i = a_{i+s}$ für alle $i \geq t$.

(ii) Gibt es $s, t \in \mathbb{N}$ mit $a_i = a_{i+s}$ für alle $i \geq t$, so existiert $n \in \mathbb{N}$ mit $na \in \mathbb{Z}$.

30*: Man finde alle Grundeinheiten von $O_d \subset \mathbb{Q}(\sqrt{d})$ für $d = 3, 7, 11, 15$.
Man bestimme $q \in \mathbb{Q}$ mit $|q - \sqrt{7}| < \frac{1}{10^5}$.