Klausur zur Elementaren Zahlentheorie (SS 2018)

PD Dr. Jürgen Müller

Lösungshinweise

(0.1) Aufgabe 1: Ringe. **(2 + 2 + 3 Punkte)**
Es sei $R := \{\frac{a}{b} \in \mathbb{Q};\, a, b \in \mathbb{Z},\, 2 \nmid b\}$. Man zeige:

a) Die Menge R wird mit der üblichen Addition und Multiplikation von Brüchen zu einem kommutativen Ring. Ist R ein Integritätsbereich?

Es sind $\frac{0}{1}, \frac{1}{1} \in R$. Weil das Produkt zweier ungerader Zahlen wieder ungerade ist, hat man außerdem für alle $\frac{a}{b}, \frac{a'}{b'} \in R$:

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'} \in R \quad \text{und} \quad \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'} \in R.$$

Somit ist R ein Unterring von $\mathbb{Q}$. Insbesondere ist R kommutativ und ein Integritätsbereich.

b) Die Einheitengruppe von R ist $R^* = \{\frac{a}{b} \in R;\, 2 \nmid a\}$. Ist R ein Körper?

$\supseteq$: Sei $\frac{a}{b} \in R$ mit $2 \nmid a$. Dann ist $\frac{b}{a} \in R$, also $\frac{a}{b} \in R^*$. $\subseteq$: Ist $\frac{a}{b} \in R^*$, dann existiert ein $\frac{a'}{b'} \in R$ mit $\frac{aa'}{bb'} = 1$. Also ist $aa' = bb'$ ungerade. Insbesondere gilt $2 \nmid a$.

R ist kein Körper, z.B. ist $0 \neq \frac{2}{1} \notin R^*$

c) Das Element $2 \in R$ ist (bis auf Assoziierte) das einzige unzerlegbare Element.

Wegen unserer Beschreibung von R^* ist jedes Element aus $R - \{0\}$ assoziiert zu einem Element der Form 2^n, für ein $n \in \mathbb{N}_0$. 2^n ist zerlegbar, falls $n \geq 2$. Außerdem ist $2 \in R - R^*$. Angenommen, 2 wäre zerlegbar. Dann hätte man $\frac{a}{b}, \frac{a'}{b'} \in R - R^*$ mit $2 = \frac{aa'}{bb'}$, also $aa' = 2bb'$. Ohne Einschränkung folgern wir nun, dass $2 \mid a$, also $2 \nmid a'$. Dies ist ein Widerspruch zu $\frac{a'}{b'} \notin R^*$.

(0.2) Aufgabe 2: Quadratische Zahlringe. **(2 + 3 + 2 Punkte)**
Man betrachte den Ring $R := \mathbb{Z}[\sqrt{-5}]$.

a) Man zeige: Das Element $2 \in R$ ist unzerlegbar, aber nicht prim.

Betrachte die Normabbildung $N(a + \sqrt{-5}) = a^2 + 5b^2$. Diese ist multiplikativ. Nun ist $N(2) = 4$ und $N^{-1}(\{2\}) = \emptyset$, also ist 2 unzerlegbar. Betrachte nun die Gleichungen $2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Wegen $2 \nmid 1 \pm \sqrt{-5}$ kann 2 somit nicht prim sein.

b) Man zeige: Das Element $\sqrt{-5} \in R$ ist prim. Ist es unzerlegbar?

Die Vielfachen von $\sqrt{-5}$ sind der Form $a + b\sqrt{-5}$ mit $5 \mid a$. Gelte nun

$$\sqrt{-5} \mid (a + b\sqrt{-5}) \cdot (a' + b'\sqrt{-5}).$$

Dies ist äquivalent zu $5 \mid aa' - 5bb'$, also zu $5 \mid a$ oder $5 \mid a'$. Also teilt $\sqrt{-5}$ einen der beiden Faktoren, ist somit prim. Insbesondere ist $\sqrt{-5}$ unzerlegbar.

c) Man bestimme alle Teiler des Elements $10 \in R$.

Wegen $100 = N(10)$ suchen wir zunächst Elemente mit Norm $\in \{1, 2, 4, 5, 10\}$. Wir erhalten dafür $\{\pm 2, \pm\sqrt{-5}\}$. Die Teilermenge von 10 ist somit

$$\{\pm 1, \pm 2, \pm\sqrt{-5}, \pm 10, \pm 5, \pm 2 \cdot \sqrt{-5}\}.$$

(0.3) Aufgabe 3: Gaußsche Zahlen. (3 Punkte)
Im Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen gilt

$$2 \cdot 5 = 10 = (3 + i) \cdot (3 - i).$$

Ist dies ein Beispiel einer "nicht-eindeutigen Faktorisierung"?

Weil $\mathbb{Z}[i]$ als euklidischer Ring faktoriell ist, kann dies nicht sein. Die involvierten Elemente sind alle zerlegbar: Z.B. hat man die Faktorisierungen

$$2 = (1+i)(1-i), 5 = (2+i)(2-i), (3+i) = (1+i)(2-i), (3-i) = (1-i)(2+i).$$

(0.4) Aufgabe 4: Gaußsche Primzahlen. (4 + 2 Punkte)
Ziel ist die Faktorisierung des Elements $41 \in \mathbb{Z}[i]$. Dazu gehe man wie folgt vor:

a) Man bestimme eine Lösung $x \in \mathbb{Z}$ der Kongruenz $X^2 \equiv -1 \pmod{41}$, und berechne $\mathrm{ggT}(41, x + i) \subseteq \mathbb{Z}[i]$.

Eine Lösung der Kongruenz ist $x = 9$. Mittels des Euklidischen Algorithmus findet man, dass $\pi = 5 - 4i$ ein größter gemeinsamer Teiler von 41 und $9 + i$ ist.

b) Man bestimme alle Primteiler und die Faktorisierung des Elements $41 \in \mathbb{Z}[i]$.

Es ist 41 prim in $\mathbb{Z}$ und $\equiv 1 \pmod{4}$. π hat Norm 41, ist somit prim. Also ist eine Faktorisierung von 41 in $\mathbb{Z}[i]$ gegeben durch $41 = \pi \cdot \kappa(\pi)$. Die Menge aller Primteiler von 41 ist $\{\pm\pi, \pm\kappa(\pi)\}$.

(0.5) Aufgabe 5: Dezimaldarstellung. (4 Punkte)
Man bestimme alle positiven ganzen Zahlen x, so daß die Dezimaldarstellung von $123 \cdot x$ mit den Ziffern 999 endet.

Zu lösen ist die Kongruenz $123X = 999 \equiv -1 \pmod{1000}$. Man erhält aus dem erweiterten euklidischen Algorithmus, daß $\overline{123}^{-1} = \overline{187} \in (\mathbb{Z}/1000\mathbb{Z})^*$. Wir schließen, daß $X \equiv -187 \pmod{1000}$. Die Lösungsmenge dieser Kongruenz ist $\{813 + k \cdot 1000 \mid k \in \mathbb{N}_0\}$.

(0.6) Aufgabe 6: Binärdarstellung. (4 Punkte)
Man bestimme jeweils die letzten fünf Ziffern der Binärdarstellung von

i) 5^{5^5}, **ii)** 6^{6^6}.

zu **(i)**: Reduziere zunächst modulo 32 und benutze den Satz von Euler. Es ist $\phi(32) = 16$ und $5^5 \equiv 5 \pmod{16}$. Man erhält $5^{5^5} \equiv 5^5 \equiv 21 \pmod{32}$. Die letzten fünf Stellen in der Binärdarstellung sind somit $[21]_2 = 10101$.

zu **(ii)**: Wegen $2^5 \mid 6^{6^6}$ sind die letzten fünf Binärstellen $[0]_2 = 00000$.

(0.7) Aufgabe 7: Eulersche φ-Funktion. **(4 Punkte)**
Es seien $m, n \in \mathbb{N}$. Man zeige: Für die übliche Eulersche Funktion gilt

$$\varphi(mn) = \varphi\big(\mathrm{kgV}_+(m,n)\big) \cdot \mathrm{ggT}_+(m,n).$$

Schreibe $m = \prod_{i=1}^r p_i^{a_i}, n = \prod_{i=1}^r p_i^{b_i}$ mit paarweise verschiedenen Primzahlen p_i, und $a_i, b_j \in \mathbb{N}_0$, $a_i + b_i \geq 1$. Dann ist

$$\varphi(mn) = \varphi(\prod_{i=1}^r p_i^{a_i+b_i}) = \prod_{i=1}^r \varphi(p_i^{a_i+b_i})$$

$$= \prod_{i=1}^r p_i^{a_i+b_i-1} \cdot (p_i - 1) = \prod_{i=1}^r p_i^{\max(a_i,b_i)-1} \cdot (p_i - 1) \cdot p_i^{\min(a_i,b_i)}$$

$$= \prod_{i=1}^r \varphi(p_i^{\max(a_i,b_i)}) \cdot p_i^{\min(a_i,b_i)} = \varphi\big(\mathrm{kgV}_+(m,n)\big) \cdot \mathrm{ggT}_+(m,n).$$

(0.8) Aufgabe 8: Simultane Kongruenzen. **(4 Punkte)**
Im 'Handbuch der Arithmetik' des Chinesen SUN-TSU heißt es:

Wir haben eine gewisse Anzahl von Dingen, wissen aber nicht genau wieviele. Wenn wir sie zu je drei zählen, bleibt eines übrig. Wenn wir sie zu je fünf zählen, bleiben vier übrig. Wenn wir sie zu je sieben zählen, bleiben zwei übrig.

Wieviele Dinge sind es mindestens?

Wir erhalten das System von Kongruenzen

$$X \equiv 1 \pmod 3, \quad X \equiv 4 \pmod 5, \quad X \equiv 2 \pmod 7.$$

Die gesamte Lösungsmenge ist dann $79 + \mathbb{Z} \cdot 105$. Es sind also mindestens 79 Dinge.

(0.9) Aufgabe 9: Lineare Kongruenzen. **(6 Punkte)**
Man gebe diejenigen Parameter $b \in \mathbb{Z}_8$ an, so daß das folgende System von Kongruenzen ganzzahlig lösbar ist, und bestimme gegebenenfalls alle Lösungen:

$$2X \equiv b \pmod 8 \qquad \text{und} \qquad 3X \equiv 1 \pmod{10}.$$

Die zweite Kongruenz ist äquivalent zu $X \equiv 1 \pmod 2$ und $X \equiv 2 \pmod 5$. Die erste Kongruenz ist lösbar genau dann, wenn $2 \mid b$. Dies nehmen wir ab

sofort an, und setzen $b' = \frac{b}{2}$. Wir erhalten, daß das System von Kongruenzen genau dann lösbar ist, falls $2 \mid b$ und $2 \nmid b'$. Dies ist äquivalent zu

$$b \in \{2, 6\}.$$

Falls $b = 2$ ist, erhalten wir die Lösungsmenge

$$(17 + \mathbb{Z} \cdot 40) \cup (37 + \mathbb{Z} \cdot 40).$$

Falls $b = 6$ ist, erhalten wir die Lösungsmenge

$$(7 + \mathbb{Z} \cdot 40) \cup (27 + \mathbb{Z} \cdot 40).$$

(0.10) Aufgabe 10: Quadratische Kongruenzen. _____ (6 Punkte)
Man bestimme jeweils alle Lösungen der folgenden Kongruenzen:

i) $X^2 \equiv 34 \pmod{45}$, **ii)** $X^2 \equiv 11 \pmod{45}$.

zu **(i):** Die Kongruenz ist äquivalent zu

$$X \equiv \pm 4 \pmod 9 \quad X \equiv \pm 2 \pmod 5.$$

Die Lösungsmenge ist dann

$$\{\pm 22, \pm 13\} \pmod{45}.$$

zu **(ii):** Die Kongruenz ist nicht lösbar. Für eine Lösung x gölte $x^2 \equiv 2 \pmod 9$, also auch $x^2 \equiv 2 \pmod 3$. Aber 2 ist kein Quadrat modulo 3.

(0.11) Aufgabe 11: Polynomielle Kongruenzen. _____ (10 Punkte)
Man bestimme jeweils alle Lösungen der Kongruenz

$$X^2 + 3 \equiv 0 \pmod{p^k}$$

in den Fällen

i) $p = 2$ und $k \in \{1, 2, 3\}$, **ii)** $p = 3$ und $k \in \{1, 2, 3\}$,
iii) $p = 5$ und $k \in \{1, 2, 3\}$, **iv)** $p = 7$ und $k \in \{1, 2, 3\}$.

Gleichung	Lösung
$X^2 \equiv -3 \pmod 2$	$x \equiv 1 \pmod 2$
$X^2 \equiv -3 \pmod 4$	$x \equiv \pm 1 \pmod 4$
$X^2 \equiv -3 \pmod 8$	$\emptyset$
$X^2 \equiv -3 \pmod 3$	$x \equiv 0 \pmod 3$
$X^2 \equiv -3 \pmod 9$	$\emptyset$
$X^2 \equiv -3 \pmod{27}$	$\emptyset$
$X^2 \equiv -3 \pmod 5$	$\emptyset$
$X^2 \equiv -3 \pmod{25}$	$\emptyset$
$X^2 \equiv -3 \pmod{125}$	$\emptyset$
$X^2 \equiv -3 \pmod 7$	$x \equiv \pm 2 \pmod 7$
$X^2 \equiv -3 \pmod{49}$	$x \equiv \pm 37 \pmod{49}$
$X^2 \equiv -3 \pmod{343}$	$x \equiv \pm 37 \pmod{343}$

Mit Ausnahme der letzten beiden Gleichungen wird das Hensel-Lemma nicht benötigt. Die Lösungen der vorletzten Gleichung sind der Form $\pm 2 + k \cdot 7 \pmod{49}$, mit $\pm 3 \cdot k \equiv 1 \pmod 7$. Daraus ergibt sich $k \equiv 5 \pmod 7$ oder $k \equiv 2 \pmod 7$, und somit $\pm 37 \pmod{49}$. Dies ergibt auch die Lösungen der letzten Gleichung.

(0.12) Aufgabe 12: Legendre-Symbole. _____ **(4 Punkte)**
Man berechne die folgenden Legendre-Symbole:

i) $\left(\frac{2}{23}\right)$, **ii)** $\left(\frac{3}{23}\right)$, **iii)** $\left(\frac{4}{23}\right)$, **iv)** $\left(\frac{5}{23}\right)$.

$\left(\frac{2}{23}\right) = 1$, weil $23 \equiv -1 \pmod 8$. $\left(\frac{3}{23}\right) = -\left(\frac{2}{3}\right) = 1$. $4 = 2^2$, also $\left(\frac{4}{23}\right) = 1$. $\left(\frac{5}{23}\right) = \left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1$.

(0.13) Aufgabe 13: Primitivwurzeln. _____ **(2 + 4 Punkte)**
a) Es seien $p \in \mathcal{P}$ und $\rho \in \mathbb{Z}$ eine Primitivwurzel modulo p. Für das zugehörige Legendre-Symbol zeige man: Es gilt $\left(\frac{\rho}{p}\right) = -1$.

Nach dem Satz von Euler wäre $\rho^{\frac{p-1}{2}} \equiv \left(\frac{\rho}{p}\right) \equiv 1 \pmod p$, aber $\mid (\mathbb{Z}/p\mathbb{Z})^* \mid = p - 1$.

b) Man bestimme die kleinste positive Primitivwurzel ρ modulo $p = 47$. Welche Potenzen von ρ sind ebenfalls Primitivwurzeln modulo p?

Wegen $\left(\frac{2}{47}\right) = \left(\frac{3}{47}\right) = \left(\frac{4}{47}\right) = 1, \left(\frac{5}{47}\right) = -1$ testen wir $\rho = 5$. Zu zeigen ist dann $\rho^2 \not\equiv 1 \pmod{47}$ und $\rho^{23} \not\equiv 1 \pmod{47}$. Letzteres gilt wegen des Satzes von Euler, weil $\left(\frac{\rho}{47}\right) = -1$. Ersteres gilt ebenso: $25 \not\equiv 1 \pmod{47}$. Somit ist 5 die kleinste positive Primitivwurzel modulo $p = 47$.

Sei $i \in \{1, \ldots, 46\}$. Dann ist 5^i Primitivwurzel modulo 47 genau dann, wenn i teilerfremd zu 46 ist. Also

$$i = 2j + 1, \quad j \neq 11, 0 \leq j \leq 22.$$

(0.14) Aufgabe 14: Fermat-Zahlen. _____ **(2 + 2 + 3 + 1 Punkte)**
Es seien $n \in \mathbb{N}_0$ und $F_n := 2^{2^n} + 1$ die n-te Fermat-Zahl.

a) Man bestimme die Ordnung von $\overline{2} \in (\mathbb{Z}/F_n\mathbb{Z})^*$.

Es ist $2^{2^n} \equiv -1 \pmod{F_n}$, also $\mathrm{ord}(\overline{2}) \mid 2^{n+1}$. Es gilt sogar Gleichheit, weil 2^n der einzige echte maximale Teiler von 2^{n+1} ist.

b) Es sei $p \in \mathcal{P}$ ein Primteiler von F_n. Man zeige: Es gilt $2^{n+1} \mid p - 1$.

Man erhält analog zu **a)**, daß 2 in $(\mathbb{Z}/p\mathbb{Z})^*$ die Ordnung 2^{n+1} hat. Der Satz von Euler gibt die Behauptung.

c) Nun sei $n \geq 2$. Man zeige: Es gilt sogar $2^{n+2} \mid p - 1$.

Wegen $n \geq 2$ ist $p \equiv 1 \pmod 8$. Dann existiert nach dem Ergänzungssatz zum QRG ein $a \in \mathbb{Z}$ mit $a^2 \equiv 2 \pmod p$. Man zeigt, daß a in $(\mathbb{Z}/p\mathbb{Z})^*$ die Ordnung 2^{n+2} hat. Der Satz von Euler gibt dann, daß $2^{n+2} \mid p-1$.

d) Wie kann man damit einen Primteiler von F_5 finden?

Man durchläuft $k \cdot 2^{n+2} + 1$, für $k = 1, 2, 3, \ldots$. Für $k = 5$ erhält man den Primteiler 641.