LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MATHEMATISCHES INSTITUT

Dr. Ralf Gerkmann

Wintersemester 2023/24
12.02.2024

Zahlentheorie

(Wiederholungsklausur alte Studienordnung)

Klausur

Nachname: _____ Vorname: _____

Matrikelnr.: _____

Studiengang:
- ❑ Lehramt Gymnasium
- ❑ Master Wirtschaftspädagogik

Ihr Klausurergebnis können Sie auf der Vorlesungshomepage mit Hilfe eines Benutzernamens, eines Passworts und einer vierstelligen Identifikationsnummer abrufen, die Ihnen persönlich zugeordnet ist. Sie erhalten diese Daten während der Klausur.

Aufgabe	1	2	3	4	5	6	7	8	$\sum$
Punkte									

Hinweise:

(a) Bitte überprüfen Sie, ob Sie **neun Blätter** (Deckblatt + 8 Aufgaben) erhalten haben.

(b) Für die Klausur sind **keine Hilfsmittel** (z.B. Skripten, handschriftliche Notizen, Taschenrechner) zugelassen.

(c) Schreiben Sie keine Lösungen zu unterschiedlichen Aufgaben auf dasselbe Blatt.

(d) Füllen Sie das Deckblatt bitte in Blockschrift aus. Schreiben Sie auf **jedes Blatt** Ihren **Vor- und Nachnamen**.

(e) Bitte denken Sie daran, jeden Schritt Ihrer Lösung zu begründen und explizit darauf hinzuweisen, wenn Sie Ergebnisse aus der Vorlesung verwenden. Die Verwendung von Ergebnissen aus Übungsaufgaben ist **nicht** zulässig.

(f) Bitte achten Sie darauf, dass Sie zu jeder Aufgabe nur eine Lösung abgeben; streichen Sie deutlich durch, was nicht gewertet werden soll.

(g) Bei Bedarf kann zusätzliches Schreibpapier angefordert werden. Bitte verwenden Sie keine eigenen Blätter.

Bearbeitungszeit: 120 Minuten

Viel Erfolg!

Name: _____

Aufgabe 1. (4+4+2 Punkte)

Wir betrachten im Körper $\mathbb{R}$ der reellen Zahlen die Teilmenge

$$S \quad = \quad \left\{ \frac{a}{7^b} \mid a \in \mathbb{Z} \ , \ b \in \mathbb{N}_0 \right\}.$$

(a) Zeigen Sie, dass S ein Teilring von $\mathbb{R}$ mit $S \supset \mathbb{Z} \cup \{\frac{5}{7}\}$ ist.

(b) Zeigen Sie, dass S mit dem Teilring $\mathbb{Z}[\frac{5}{7}]$ von $\mathbb{R}$ übereinstimmt.

(c) Geben Sie die Menge der Einheiten von S an. Ein Nachweis ist *nicht* erforderlich.

Lösung:

zu (a) Wir zeigen zunächst, dass S ein Teilring von $\mathbb{R}$ ist. Wegen $1 = \frac{1}{7^0}$ (und $1 \in \mathbb{Z}$, $0 \in \mathbb{N}_0$) gilt $1 \in S$. Seien nun $\alpha, \beta \in S$ vorgegeben. Dann gibt es $a, c \in \mathbb{Z}$ und $b, d \in \mathbb{N}_0$ mit $\alpha = \frac{a}{7^b}$ und $\beta = \frac{c}{7^d}$. Wegen

$$\alpha - \beta \quad = \quad \frac{a}{7^b} - \frac{c}{7^d} \quad = \quad \frac{7^d a - 7^b c}{7^{b+d}}$$

und $7^d a - 7^b c \in \mathbb{Z}$ und $b + d \in \mathbb{N}_0$ folgt $\alpha - \beta \in S$. Wegen $\alpha\beta = \frac{a}{7^b} \cdot \frac{c}{7^d} = \frac{ac}{7^{b+d}}$ und $ac \in \mathbb{Z}$, $b + d \in \mathbb{N}_0$ folgt $\alpha\beta \in S$. Jedes $a \in \mathbb{Z}$ kann in der Form $a = \frac{a}{7^0}$ dargestellt werden; dies zeigt (wegen $a \in \mathbb{Z}$, $0 \in \mathbb{N}_0$), dass a in S liegt. Wegen $\frac{5}{7} = \frac{5}{7^1}$ (und $5 \in \mathbb{Z}$, $1 \in \mathbb{N}_0$) gilt auch $\frac{5}{7} \in S$.

zu (b) Laut Vorlesung muss zusätzlich zu dem Ergebnis von Teil (a) noch gezeigt werden: Ist R ein beliebiger Teilring von $\mathbb{R}$ mit $R \supseteq \mathbb{Z} \cup \{\frac{5}{7}\}$, dann folgt $R \supseteq S$. Sei also R ein solcher Ring und $\alpha \in S$; zu zeigen ist dann $\alpha \in R$. Wegen $\alpha \in S$ gibt es Elemente $a \in \mathbb{Z}$ und $b \in \mathbb{N}_0$ mit $\alpha = \frac{a}{7^b}$. Wegen $\mathbb{Z} \subseteq R$, $\frac{5}{7} \in R$ und der Teilring-Eigenschaft ist auch $3 - 4 \cdot \frac{5}{7} = \frac{21}{7} - \frac{20}{7} = \frac{1}{7}$ in R enthalten. Wegen $\mathbb{Z} \subseteq R$ gilt $a \in R$, und wiederum auf Grund der Teilring-Eigenschaft damit auch $\alpha = a \cdot (\frac{1}{7})^b \in R$.

zu (c) Die Einheitengruppe von S ist gegeben durch $S^\times = \{\varepsilon 7^b \mid \varepsilon \in \{\pm 1\}, b \in \mathbb{N}_0\}$.

Name: _____

Aufgabe 2. (3+4+3 Punkte)

Wir betrachten die Menge $R = \mathbb{Q} \times \mathbb{Q}$ mit den durch komponentenweise Addition und Multiplikation gegebenen Verknüpfungen, d.h. wir definieren die Verknüpfungen $+$ und $\cdot$ auf R durch

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{und} \quad (a, b) \cdot (c, d) = (ac, bd)$$

für alle $(a, b), (c, d) \in R$. Ohne Beweis darf verwendet werden, dass $(R, +, \cdot)$ ein Ring ist.

(a) Bestimmen Sie die Menge der Nullteiler von R (mit Nachweis).

(b) Bestimmen Sie die Menge der Einheiten von R (mit Nachweis).

(c) Ist R ein Integritätsbereich? Ist R ein Körper? Bitte begründen Sie jeweils Ihre Antwort.

Lösung:

zu (a) Die Menge N der Nullteiler von R ist gegeben durch $N = \{(a, b) \in R \mid (a = 0) \vee (b = 0)\}$. Für jedes $a \in \mathbb{Z}$ gilt nämlich $(a, 0) \cdot (0, 1) = (0, 0) = 0_R$, und für jedes $b \in \mathbb{Z}$ gilt $(0, b) \cdot (1, 0) = (0, 0) = 0_R$. Wegen $(0, 1) \neq 0_R$ und $(1, 0) \neq 0_R$ zeigt dies, dass jedes Element aus N ein Nullteiler ist. Setzen wir umgekehrt voraus, dass $(a, b) \in R$ ein Nullteiler ist. Dann existiert ein $(c, d) \in R$ mit $(c, d) \neq 0_R$ und $(a, b) \cdot (c, d) = 0_R$, also $(ac, bd) = (0, 0)$ und somit $ac = 0$ und $bd = 0$. Wegen $(c, d) \neq 0_R$ ist $c \neq 0$ oder $d \neq 0$. Im Fall $c \neq 0$ folgt aus $ac = 0$, dass $a = 0$ gilt. Im Fall $d \neq 0$ folgt aus $bd = 0$, dass $b = 0$ gilt. In beiden Fällen folgt $(a, b) \in N$.

zu (b) Wir zeigen, dass $R^\times$ mit der Menge $E = \mathbb{Q}^\times \times \mathbb{Q}^\times$ übereinstimmt. Sei $(a, b) \in E$. Dann gilt $a \neq 0$ und $b \neq 0$, und die Gleichung $(a, b) \cdot (a^{-1}, b^{-1}) = (1, 1) = 1_R$ zeigt, dass (a, b) eine Einheit ist. Setzen wir umgekehrt $(a, b) \in R^\times$ voraus. Dann gibt es ein $(c, d) \in R$ mit $(ac, bd) = (a, b) \cdot (c, d) = 1_R = (1, 1)$, also $ac = 1$ und $bd = 1$. Daraus folgt $a \neq 0$ und $b \neq 0$, also $(a, b) \in E$.

zu (c) Nach Teil (a) existieren in R von 0_R verschiedene Nullteiler, zum Beispiel $(1, 0)$. Somit ist R kein Integritätsbereich. Laut Vorlesung ist jeder Körper ein Integritätsbereich. Also kann R auch kein Körper sein.

Name: _____

Aufgabe 3. (3+4+3 Punkte)

Wir betrachten in $\mathbb{C}$ den Teilring

$$R \quad = \quad \mathbb{Z}[\sqrt{-5}] \quad = \quad \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

(a) Bestimmen Sie die Einheiten des Rings R (mit Nachweis).

(b) Entscheiden Sie, welche der Elemente 15, 29, $2 + 3\sqrt{-5}$, $4 + 3\sqrt{-5}$ in R irreduzibel sind, und begründen Sie jeweils Ihre Entscheidung.

(c) Zeigen Sie mit Hilfe der Gleichungen $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$, dass 3 im Ring R zwar irreduzibel, aber kein Primelement ist.

Lösung:

zu (a) Sei $N : R \to \mathbb{N}_0$ die aus der Vorlesung bekannte Normabbildung, gegeben durch $N(a+b\sqrt{-5}) = a^2+5b^2$ für alle $a, b \in \mathbb{Z}$. Sei $\alpha = a + b\sqrt{-5} \in R$ mit $a, b \in \mathbb{Z}$. Laut Vorlesung ist $\alpha \in R^\times$ genau dann, wenn $N(\alpha) = 1$ ist. Weil $\pm(1, 0)$ die einzigen Lösungen der Gleichung $x^2 + 5y^2 = 1$ in R sind, gilt die Äquivalenz

$$\begin{aligned} \alpha \in R^\times \quad &\Leftrightarrow \quad N(\alpha) = 1 \quad \Leftrightarrow \quad a^2 + 5b^2 = 1 \quad \Leftrightarrow \quad (a, b) \in \{\pm(1, 0)\} \\ &\Leftrightarrow \quad a + b\sqrt{-5} \in \{(\pm 1) \cdot 1 + 0 \cdot \sqrt{-5}\} \quad \Leftrightarrow \quad \alpha \in \{\pm 1\}. \end{aligned}$$

Daraus folgt $R^\times = \{\pm 1\}$.

zu (b) Es ist $15 = 3 \cdot 5$, und wegen $N(3) = 9 > 1$ und $N(5) = 25 > 1$ sind 3 und 5 beides keine Einheiten. Dies zeigt, dass 15 in R reduzibel ist. Ebenso folgt aus $29 = 3^2 + 5 \cdot 2^2 = (3 + 2\sqrt{-5}) \cdot (3 - 2\sqrt{-5})$ und $N(3+2\sqrt{-5}) = N(3-2\sqrt{-5}) = 29 > 1$, dass 29 in R reduzibel ist. Die Norm $N(2+3\sqrt{-5}) = 2^2+5\cdot 3^2 = 49 = 7^2$ ist ein Primzahlquadrat, und die Gleichung $x^2 + 5y^2 = 7$ besitzt in $\mathbb{Z}^2$ keine Lösung (weil $7 - 5 \cdot 0^2 = 7$ und $7 - 5 \cdot 1^2 = 2$ keine Quadrate in $\mathbb{Z}$ sind). Laut Vorlesung ist $2 + 3\sqrt{-5}$ damit irreduzibel in R. Die Norm $N(4 + 3\sqrt{-5}) = 4^2 + 5 \cdot 3^2 = 16 + 45 = 61$ ist eine Primzahl. Laut Vorlesung ist $4 + 3\sqrt{-5}$ damit ebenfalls irreduzibel in R.

zu (c) Die Norm $N(3) = 9 = 3^2$ ist ein Primzahlquadrat, die Gleichung $x^2 + 5y^2 = 3$ in $\mathbb{Z}^2$ aber unlösbar. Dies zeigt, dass 3 in R irreduzibel ist. Die Gleichung aus der Aufgabenstellung zeigt, dass 3 ein Teiler des Produkts $(1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ ist. Wäre 3 in R ein Primelelement, dann müsste 3 eines der Elemente $1 \pm 2\sqrt{-5}$ teilen. Es gäbe also in $\gamma \in R$ mit $3\gamma = 1 \pm 2\sqrt{-5}$, was zu $\gamma = \frac{1}{3} \pm \frac{2}{3}\sqrt{-5}$ äquivalent ist. Aber dies ist unmöglich, denn die Zahlen $\frac{1}{3} \pm \frac{2}{3}\sqrt{-5}$ haben keinen ganzzahligen Realteil und liegen somit nicht in R.

Name: _____

Aufgabe 4. (2+6+2 Punkte)

(a) Sei $n \in \mathbb{N}$, und seien $a, u, v \in \mathbb{Z}$ mit $ua + vn = \mathrm{ggT}(a, n) = 1$. Zeigen Sie, dass im Restklassenring die Gleichung $u + n\mathbb{Z} = (a + n\mathbb{Z})^{-1}$ erfüllt ist.

(b) Bestimmen Sie die multiplikativen Inversen der Elemente $\bar{3}$, $\bar{9}$, $\overline{27}$ im Körper $\mathbb{F}_{43}$.

(c) Sei $R = \mathbb{Z}[i]/(5)$ und $\alpha = i + (5) \in R$. Bestimmen Sie das Inverse α^{-1} von α in R.

Lösung:

zu (a) Wegen $(ua+vn)-ua = vn \in n\mathbb{Z}$ gilt $(u+n\mathbb{Z})\cdot(a+n\mathbb{Z}) = ua+n\mathbb{Z} = ua+vn+n\mathbb{Z} = 1+n\mathbb{Z} = 1_{\mathbb{Z}/n\mathbb{Z}}$. Daraus folgt $(a + n\mathbb{Z})^{-1} = u + n\mathbb{Z}$.

zu (b) Die Gleichung $3u + 43v = 1$ besitzt die Lösung $(u, v) = (-14, 1)$. Nach Teil (a) folgt daraus $\bar{3}^{-1} = (3 + 43\mathbb{Z})^{-1} = (-14) + 43\mathbb{Z} = 29 + 43\mathbb{Z}$. Aus $\bar{9} = \bar{3}^2$ folgt $\bar{9}^{-1} = (\bar{3}^{-1})^2 = (-\overline{14})^2 = \overline{196} = -\overline{19} = \overline{24}$ und $\overline{27}^{-1} = \bar{3}^{-1} \cdot \bar{9}^{-1} = (-\overline{14}) \cdot \overline{24} = -\overline{336} = \overline{94} = \bar{8}$.

zu (c) Es gilt $\alpha\cdot((-i)+(5)) = (i+(5))\cdot((-i)+(5)) = i\cdot(-i)+(5) = 1+(5) = 1_R$ und somit $\alpha^{-1} = (-i)+(5)$.

Name: _____

Aufgabe 5. (2+4+4 Punkte)

(a) Formulieren Sie das Eisenstein-Kriterium.

(b) Bestimmen Sie alle irreduziblen, normierten Polynome vom Grad 2 in $\mathbb{F}_3[x]$.

(c) Beweisen Sie mit Hilfe des Reduktionskriteriums, dass das Polynom $f = x^4 - 3x^3 + 6x^2 + 7x - 10$ in $\mathbb{Q}[x]$ irreduzibel ist.

Lösung:

zu (a) Sei R ein faktorieller Ring, p ein Primelement in R und $f = a_n x^n + ... + a_1 x + a_0 \in R[x]$ ein primitives Polynom mit $p \nmid a_n$, $p \mid a_k$ für $0 \leq k < n$ und $p^2 \nmid a_0$. Dann ist f in $R[x]$ irreduzibel.

zu (b) Die normierten, irreduziblen Polynom in $\mathbb{F}_3[x]$ vom Grad 2 haben die Form $x^2 + ax + b$ mit $a, b \in \mathbb{F}_3$. Die Polynome mit $b = \bar{0}$ haben $\bar{0} \in \mathbb{F}_3$ als Nullstelle und sind als Polynome vom Grad 2 somit reduzibel. Die Polynome $x^2 + \bar{2}$, $x^2 + x + \bar{1}$ und $x^2 + \bar{2}x + \bar{1}$ haben $\bar{1} \in \mathbb{F}_3$ als Nullstelle und somit ebenfalls reduzibel. Dagegen besitzen $x^2 + \bar{1}$, $x^2 + x + \bar{2}$ und $x^2 + \bar{2}x + \bar{2}$ keine Nullstelle in $\mathbb{F}_3$ und somit somit als Polynome vom Grad 2 irreduzibel. Es gibt also genau drei normierte, irreduzible Polynome vom Grad 2 in $\mathbb{F}_3[x]$.

zu (c) Auf Grund des Reduktionskriteriums genügt es zu überprüfen, dass $\bar{f} = x^4 + x + \bar{2}$, das Bild von f in $\mathbb{F}_3[x]$, im Polynomring $\mathbb{F}_3[x]$ irreduzibel ist. Dieses Polynom hat in $\mathbb{F}_3$ keine Nullstelle (wegen $\bar{f}(\bar{0}) = \bar{2}$, $\bar{f}(\bar{1}) = \bar{4} = \bar{1}$ und $f(\bar{2}) = \overline{20} = \bar{2}$). Als normiertes Polynom vom Grad 4 kann es also nur dann reduzibel sein, wenn es als Produkt zweier irreduzibler Polynome vom Grad 2 darstellbar ist. Es müsste also als Produkt $\bar{f} = gh$ mit $g, h \in \{x^2 + \bar{1}, x^2 + x + \bar{2}, x^2 + \bar{2}x + \bar{2}\}$ darstellbar sein. Wäre $\bar{f}$ ein Quadrat eines dieser Polynome, dann wäre der konstante Term von $\bar{f}$ wegen $\bar{1}^2 = \bar{2}^2 = \bar{1}$ gleich $\bar{1}$. Die einzigen beiden möglichen Produkte mit konstantem Term $\bar{2}$ sind

$$(x^2 + \bar{1}) \cdot (x^2 + x + \bar{2}) = x^4 + x^3 + x + \bar{2} \quad \text{und} \quad (x^2 + \bar{1}) \cdot (x^2 + \bar{2}x + \bar{2}) = x^4 + \bar{2}x^3 + \bar{2}x + \bar{2}.$$

Weil keines dieser Produkte mit $\bar{f}$ übereinstimmt, ist $\bar{f}$ in $\mathbb{F}_3[x]$ irreduzibel.

Name: _____

Aufgabe 6. (2+2+4+4 Punkte)

(a) Geben Sie alle Primideale und alle maximalen Ideale des Rings $\mathbb{Z}$ an.

(b) Geben Sie alle Primideale und alle maximalen Ideale des Rings $\mathbb{Q}$ an.

(c) Zeigen Sie, dass $I = (2+i, 3)$ im Ring $\mathbb{Z}[i]$ der Gauß'schen Zahlen mit dem Einheitsideal übereinstimmt.

(d) Weisen Sie nach, dass $J = (7, 1+2\sqrt{-5})$ im Ring $\mathbb{Z}[\sqrt{-5}]$ kein Hauptideal ist. Dabei darf ohne Nachweis verwendet werden, dass $J \subsetneq (1)$ gilt.

In Teil (a) und (b) ist *kein* Nachweis erforderlich.

Lösung:

zu (a) Die maximalen Ideale von $\mathbb{Z}$ sind die Hauptideale (p), wobei p die Menge der Primzahlen durchläuft. Jedes maximale Ideal ist auch ein Primideale von $\mathbb{Z}$, und das einzige nicht-maximale Primideal ist das Nullideal (0).

zu (b) Das einzige Primideal von $\mathbb{Q}$, und zugleich das einzige maximale Ideal, ist das Nullideal.

zu (c) Jedes Ideal eines Rings ist im Einheitsideal enthalten, insbesondere gilt $I \subseteq (1)$. Umgekehrt sind mit $2+i$ und 3 auch die Elemente $5 = (2-i)\cdot(2+i)$ und $1 = 2\cdot 5 - 3\cdot 3$ in I enthalten. Aus $1 \in I$ folgt $(1) \subseteq I$, insgesamt $I = (1)$.

zu (d) Sei $R = \mathbb{Z}[\sqrt{-5}]$, und nehmen wir an, dass J ein Hauptideal ist, also $J = (\alpha)$ für ein $\alpha \in R$ erfüllt ist. Wegen $7 \in (\alpha)$ und $1 + 2\sqrt{-5} \in (\alpha)$ gibt es Elemente $\beta, \gamma \in R$ mit $7 = \alpha\beta$ und $1 + 2\sqrt{-5} = \alpha\gamma$. Mit der Normfunktion $N : R \to \mathbb{N}_0$, $a + b\sqrt{-5} \mapsto a^2 + 5b^2$ erhalten wir $49 = N(7) = N(\alpha)N(\beta)$ und $21 = N(1+2\sqrt{-5}) = N(\alpha)N(\gamma)$. Aus $N(\alpha) \mid 49$ und $N(\alpha) \mid 21$ folgt $N(\alpha) \mid 7$ (wegen $\mathrm{ggT}(49, 21) = 7$), also $N(\alpha) \in \{1, 7\}$. Im Fall $N(\alpha) = 1$ wäre α eine Einheit, und daraus würde $J = (\alpha) = (1)$ folgen, was laut Angabe ausgeschlossen ist. Also gilt $N(\alpha) = 7$. Schreiben wir $\alpha = a + b\sqrt{-5}$ mit $a, b \in \mathbb{Z}$, dann folgt $a^2 + 5b^2 = N(\alpha) = 7$. Aber das ist unmöglich, weil die Gleichung $x^2 + 5y^2 = 7$ in $\mathbb{Z}^2$ unlösbar ist.

Name: _____

Aufgabe 7. (4+3+3 Punkte)

(a) Bestimmen Sie ein $r \in \mathbb{N}$ und zyklische Gruppen $C_1, ..., C_r$, so dass die prime Restklassengruppe $(\mathbb{Z}/600\mathbb{Z})^\times$ isomorph zu $C_1 \times ... \times C_r$ ist.

(b) Begründen Sie, dass $(\mathbb{Z}/600\mathbb{Z})^\times$ keine zyklische Gruppe ist.

(c) Geben Sie die Anzahl der Elemente der Ordnung 2 in $(\mathbb{Z}/600\mathbb{Z})^\times$ an.
Ein Nachweis ist *nicht* erforderlich.

Lösung:

zu (a) Mit Hilfe der Primfaktorzerlegung $600 = 2^3 \cdot 3 \cdot 5^2$ und dem Chinesischen Restsatz erhalten wir zunächst

$$(\mathbb{Z}/600\mathbb{Z})^\times \quad \cong \quad (\mathbb{Z}/2^3\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5^2\mathbb{Z})^\times.$$

Laut Vorlesung gilt $(\mathbb{Z}/2^3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, und außerdem $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/5^2\mathbb{Z})^\times \cong \mathbb{Z}/20\mathbb{Z}$, weil 3^1 und 5^2 Potenzen ungerader Primzahlen sind. Setzen wir dies ein, so erhalten wir $(\mathbb{Z}/600\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/20\mathbb{Z}$.

zu (b) Wäre $(\mathbb{Z}/600\mathbb{Z})^\times$ zyklisch, dann müsste dasselbe auch für die isomorphe Gruppe $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/20\mathbb{Z}$ gelten. In der Gruppe würde dann ein Element der Ordnung $|(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/20\mathbb{Z}| = 2^3 \cdot 20 = 160$ existieren. Für alle $((a,b,c),d) \in (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/20\mathbb{Z}$ gilt aber $20 \cdot ((a,b,c),d) = ((20a, 20b, 20c), 20d) = ((\bar{0},\bar{0},\bar{0}),\bar{0})$, da 20 ein gemeinsames Vielfaches von 2 und 20 ist. Jede Ordnung eines Elements der Gruppe ist also Teiler von 20. Es gibt also keine Elemente der Ordnung 160 in der Gruppe, und folglich ist diese nicht zyklisch.

zu (c) In der Gruppe $(\mathbb{Z}/600\mathbb{Z})^\times$ gibt es genau 15 Elemente der Ordnung 2. (Die Elemente der Ordnung 2 in der isomorphen Gruppe $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/20\mathbb{Z}$ sind genau die Elemente $((a,b,c),d)$ mit $a,b,c \in \{\bar{0},\bar{1}\}$ und $d \in \{\bar{0},\overline{10}\}$, wobei das Neutralelement $((\bar{0},\bar{0},\bar{0}),\bar{0})$ ausgenommen ist.)

Name: _____

Aufgabe 8. (4+6 Punkte)

(a) Begründen Sie, dass die Lösungsmenge des Kongruenzsystems

$$x \equiv 2 \bmod 3 \ , \ x \equiv 3 \bmod 11 \ , \ x \equiv 7 \bmod 13$$

mit der Lösungsmenge des Kongruenzsystems $x \equiv 14 \bmod 33$, $x \equiv 7 \bmod 13$ übereinstimmt, und diese wiederum mit der Lösungsmenge der Kongruenz $x \equiv -19 \bmod 429$.

(b) Bestimmen Sie die Lösungsmenge des Kongruenzsystems $x \equiv 4 \bmod 23$, $x \equiv 6 \bmod 41$.

In Teil (b) ist kein Nachweis erforderlich, es genügt der Rechenweg.

Lösung:

zu (a) Sei $a \in \mathbb{Z}$ ein Element, dass $a \equiv 14 \bmod 33$ und $a \equiv 7 \bmod 13$ erfüllt. Wegen $3 \mid 33$ folgt $a \equiv 14 \equiv 2 \bmod 3$, und aus $a \equiv 14 \equiv 3 \bmod 11$. Dies zeigt, dass a auch eine Lösung des ersten Kongruenzsystems ist. Setzen wir dies umgekehrt voraus, dann folgt $a \equiv 2 \equiv 14 \bmod 3$ und $a \equiv 3 \equiv 14 \bmod 11$. Die Zahlen 3 und 11 sind also Teier von $a - 14$. Somit ist auch $\mathrm{kgV}(3, 11) = 33$ ein Teiler von $a - 14$, und es folgt $a \equiv 14 \bmod 33$. Somit ist a auch eine Lösung des Systems $x \equiv 14 \bmod 33$, $x \equiv 7 \bmod 13$.

Erfüllt $a \in \mathbb{Z}$ die Kongruenz $a \equiv -19 \bmod 429$, dann folgt wegen $429 = 33 \cdot 13$ auch $a \equiv -19 \equiv 14 \bmod 33$ und $a \equiv -19 \equiv 7 \bmod 13$. Setzen wir dies umgekehrt voraus, dann sind 33 und 13 Teiler von $a + 19$. Daraus folgt, dass auch $\mathrm{kgV}(33, 13) = 429$ ein Teiler von $a + 19$ ist, und es folgt $a \equiv 19 \bmod 429$.

zu (b) Wir wenden den Euklidischen Algorithmus auf die Zahlen 41 und 23 an.

q	a_n	x_n	y_n
–	41	1	0
–	23	0	1
–	18	1	-1
–	5	-1	2
–	3	4	-7
–	2	-5	9
–	1	9	-16

Es gilt also $(-16)\cdot 23 + 9 \cdot 41 = 1$. Die Zahl $1 + 16 \cdot 23 = 369$ erfüllt die Kongruenzen $369 \equiv 1 \bmod 23$, $369 \equiv 0 \bmod 41$, und $1 - 369 = -368$ erfüllt $-368 \equiv 0 \bmod 23$, $-368 \equiv 1 \bmod 41$. Die Zahl $a = 4 \cdot 369 + 6 \cdot (-368) = -732$ erfüllt somit $a \equiv 4 \bmod 23$, $a \equiv 6 \bmod 41$. Wegen $23 \cdot 41 = 943$ und $-732 \equiv 211 \bmod 943$ erhalten wir die Lösungsmenge $\mathscr{L} = -732 + 943\mathbb{Z} = 211 + 943\mathbb{Z}$.