Musterlösung zur Serie 4
Algebra und Zahlentheorie und ihre Didaktik

Dr. Daniel Skodlerack

25. Mai 2017

Bitte beachten Sie Folgendes:

1. Beginnen Sie **jede** Aufgabe auf einem neuen Blatt.
2. Beschriften Sie **jedes** abzugebende Blatt mit Namen, Matrikelnummer und Übungsgruppe.
3. Begründen Sie Ihre Lösungen, wenn nicht anders lautend, **nur** mit der Vorlesung, der Übung und vorhergehender Übungsaufgaben.

Aufgabe 1 (5+5 Punkte)**.** (Äquivalenzrelationen)

1. Es sei R die folgende binäre Relation auf $\mathbb{Z} \times \mathbb{Z}$.

$$(z_1, z_2)R(z_1', z_2') \Leftrightarrow_{Def} ((z_1 z_1' > 0 \wedge z_2 z_2' > 0) \vee (z_1 = z_1' \wedge z_2 = z_2')).$$

   Zeigen Sie, dass R eine Äquivalenzrelation ist. Berechnen Sie alle Äquivalenzklassen von R und skizzieren Sie diese im Koordinatensystem der euklidischen Ebene.

2. Wir nennen zwei Äquivalenzrelationen (M, R_1) und (M, R_2) *kommensurabel*, falls jedes Element von $M/R_1 \cup M/R_2$ nur endlich viele Elemente aus $M/R_1 \cup M/R_2$ nichtleer schneidet. Zeigen Sie, dass Kommensurabilität eine Äquivalenzrelation auf der Menge der Äquivalenzrelationenen von M ist, und finden Sie eine zu R, aus Aufgabeteil 1, kommensurable Äquivalenzrelation S, so dass jede Äquivalenzklasse von S genau zwei Elemente aus $(\mathbb{Z} \times \mathbb{Z})/R$ nichtleer schneidet.

Lösung:

1. Wir zeigen zuerst, dass R eine Äquivalenzrelation ist. Die Reflexivität folgt direkt aus der Definition von R, und R ist symmetrisch, da die Multiplikation in $\mathbb{Z}$ kommutativ und die Gleichheitsrelation symmetrisch ist. Es bleibt also die Transitivität zu zeigen. Es sei $(z_1, z_2)R(z_1', z_2')R(z_1'', z_2'')$. Wenn zwei von den drei Paaren übereinstimmen, folgt $(z_1, z_2)R(z_1'', z_2'')$. Wir betrachten nun den Fall, dass die drei Paare paarweise verschieden sind. Also folgt nach Definition von R:

$$z_1 z_1' > 0 \wedge z_2 z_2' > 0 \wedge z_1' z_1'' > 0 \wedge z_2' z_2'' > 0.$$

   Daraus folgt aus S.2.1.2 $z_1 z_1'' z_1'^2 = z_1 z_1' z_1' z_1'' > 0$. Aus $z_1'^2 = |z_1'|^2 = |z_1'^2| > 0$ folgt nun durch Bemerkung 26: $z_1 z_1'' \in \mathbb{N}$, also ist es positiv. Analog zeigt man $z_2 z_2'' > 0$, und damit erhalten wir insgesamt: $(z_1, z_2)R(z_1'', z_2'')$. Damit ist gezeigt, dass R transitiv ist.

   Berechnung der Äquivalenzklassen:

   - $[(1,1)]_R = \{(z_1, z_2) \in \mathbb{Z}^2 | (z_1, z_2)R(1,1)\} = \{(z_1, z_2) \in \mathbb{Z}^2 | z_1 > 0 \wedge z_2 > 0\}$. (1. Quadrant)
   - $[(-1,1)]_R = \{(z_1, z_2) \in \mathbb{Z}^2 | (z_1, z_2)R(-1,1)\} = \{(z_1, z_2) \in \mathbb{Z}^2 | z_1 < 0 \wedge z_2 > 0\}$. (2. Quadrant)
   - $[(-1,-1)]_R = \{(z_1, z_2) \in \mathbb{Z}^2 | (z_1, z_2)R(-1,-1)\} = \{(z_1, z_2) \in \mathbb{Z}^2 | z_1 < 0 \wedge z_2 < 0\}$. (3. Quadrant)

- $[(1,-1)]_R = \{(z_1,z_2) \in \mathbb{Z}^2 | (z_1,z_2)R(1,-1)\} = \{(z_1,z_2) \in \mathbb{Z}^2 | z_1 > 0 \wedge z_2 < 0\}$. (4. Quadrant)
- $[(z,0)]_R = \{(z_1,z_2) \in \mathbb{Z}^2 | (z_1,z_2)R(z,0)\} = \{(z,0)\}$, $z \in \mathbb{Z}$.
- $[(0,z)]_R = \{(z_1,z_2) \in \mathbb{Z}^2 | (z_1,z_2)R(0,z)\} = \{(0,z)\}$, $z \in \mathbb{Z} \setminus \{0\}$.

Dies sind alle Äquivalenzklassen, da diese ganz $\mathbb{Z}^2$ überdecken, d.h. die Vereinigung der oben angegebenen Mengen ist gleich $\mathbb{Z}^2$. Hier müsste jetzt eine Skizze folgen.

2. Wir zeigen zuerst, dass Kommensurabilität eine Äquivalenzrelation ist. Die Reflexivität folgt daher, dass die Faktormenge einer Äquivalenzrelation auf M nach Satz 32 eine Partition ist. Die Symmetrie folgt direkt aus der Definition, da die Struktur, die zwei Mengen die Vereinigung dieser zuordnet kommutativ ist. Es bleibt die Transitivität zu zeigen. Es seien nun R kommensurabel zu R' und R' kommensurabel zu R'', und es sei c ein Element aus $M/R \cup M/R''$. Aus Symmetriegründen können wir ohne Einschränkung $c \in M/R$ annehmen. In M/R gibt es nur ein Element, das c nichtleer schneidet, da M/R eine Partition und c ein Element aus M/R ist. Es bleibt zu zeigen, dass c nur endlich viele Elemente aus M/R'' schneidet. Da R und R' zueinander kommensurabel sind, schneiden nur endlich viele Elemente aus M/R' die Menge c nichtleer, etwa $c'_1, \ldots, c'_l$. Da M/R' eine Partition von M ist, also insbesondere ganz M überdeckt, folgt daraus $c \subseteq \bigcup_{i=1}^{l} c'_i$. Indem wir die Kommensurabilität von R' mit R'' nutzen erhalten wir analog, dass für jedes $i \in \mathbb{N}^{\leq l}$ nur endlich viele Elemente aus M/R'' existieren, die c'_i nichtleer schneiden. Also schneiden nur endlich viele Elemente aus M/R'' die Menge c nichtleer, da jede Menge, die c nichtleer schneidet,irgendein c'_i nichtleer schneiden muss. Damit ist die Transitivität gezeigt.

   Wir defnieren die folgende Partition P als die Vereinigung der folgenden zwei Mengen:

   - $\{[(z_1,z_2)]_R \cup [(-z_1,z_2)]_R | z_1 \in \mathbb{Z} \setminus \{0\}, z_2 \in \mathbb{Z}\}$,
   - $\{[(0,z)]_R \cup [(0,z+1)]_R | z \in [0]_2\}$.

   Jedes Element von P ist die Vereinigung von exakt zwei Äquivalenzklassen von R, da M/R invariant unter der Spiegelung an der y-Achse ist, und nur die Äquivalenzklassen, die in der y-Achse enthalten sind, von dieser Spiegelung fixiert werden. Also erfüllt die durch

$$(z_1,z_2)S(z'_1,z'_2) \Leftrightarrow_{Def.} \exists_{c \in P} : \ (z_1,z_2),(z'_1,z'_2) \in c$$

   definierte Äquivalenzrelation S die gewünschte Bedingung.

Aufgabe 2 (2+3+5 Punkte)**.** (Restklassen) Wir definieren auf $\mathbb{Z}/_{\equiv_m}$ wie folgt eine Addition und eine Multiplikation:

$$[a]_m + [b]_m := [a+b]_m, \ [a]_m \cdot [b]_m := [ab]_m.$$

1. Zeigen Sie, dass die Abbildung $\cdot : \mathbb{Z}/_{\equiv_m} \times \mathbb{Z}/_{\equiv_m} \to \mathbb{Z}/_{\equiv_m}$ wohldefiniert ist.

2. Es sei n eine ganze Zahl. Zeigen Sie, dass n^3+4 nicht die Summe von zwei dritten Potenzen ganzer Zahlen ist, d.h. dass nicht zwei ganze Zahlen z_1, z_2 existieren, so dass $z_1^3 + z_2^3 = n^3 + 4$ ist. Hinweis: Rechnen Sie mod m für einen geeigneten Modul m. Der Exponent könnte beim Finden des Moduls behilflich sein.

3. Zeigen Sie, dass es unendlich viele Primzahlen in $[3]_4$ gibt. Hinweis: Finden Sie einen Beweis, ähnlich zum Beweis vom Satz von Euklid (Satz 29), und rechnen Sie modulo 4.

Lösung:

1. Es seien $[a]_m = [a']_m$ und $[b]_m = [b']_m$. Daraus folgen $m|a-a'$ und $m|b-b'$. Also $m|(a-a')b$ und $m|a'(b-b')$, und somit teilt m die Summe $(a-a')b + a'(b-b')$, also auch $ab - a'b'$. Also sind ab und $a'b'$ kongruent zueinander modulo m, somit $ab \in [a'b']_m$ und deshalb $[ab]_m \cap [a'b']_m \neq \emptyset$. Somit stimmen nach Satz 32.1) die Restklassen $[ab]_m$ und $[a'b']_m$ überein.

2. Wir betrachten den Modul $m = 9$. Die dritte Pontenz einer ganzen Zahl ist kongruent zu -1,1 oder 0 modulo 9, da für $k \in \mathbb{Z}$ und $\epsilon \in \{1, -1, 0\}$ das Folgende gilt:

$$(3k + \epsilon)^3 \equiv_9 (3k)^3 + 3(3k)^2\epsilon + 3(3k)\epsilon^2 + \epsilon^3 \equiv_9 \epsilon.$$

Die Summe $z_1^3 + z_2^3 + (-n)^3$ kann somit modulo 9 nur die Reste $-3, -2, -1, 0, 1, 2, 3$ annehmen. Folglich gibt es keine ganzzahlige Lösung für $z_1^3 + z_2^3 + (-n)^3 = 4$.

3. Angenommen, es gibt nur endlich viele Primzahlen in $[3]_4$, etwa $p_1, \ldots, p_l$. Wir definieren $n = 2p_1 \cdot \ldots \cdot p_l + 1$. Behauptung: n ist ein Element von $[3]_4$. Beweis: $n \equiv_4 2(-1)^l + 1 \equiv_4 2 + 1 \equiv_4 3$. q.e.d. Wir betrachten die Primfaktorzerlegung $n = q_1 \cdot \ldots \cdot q_t$ von n. Wenn alle Primzahlen q_i kongruent zu 1 mod 4 sind, dann ist auch das Produkt, also n, kongruent zu 1 mod 4. Ein Widerspruch zur obigen Behauptung. Deshalb gibt es einen Index i_0, so dass q_{i_0} kongruent zu 3 modulo 4 ist. Also muss q_{i_0} eines der p_j sein, und folglich teilt q_{i_0} die Differenz $n - 2p_1 \cdot \ldots \cdot p_l$, d.h. $q_{i_0}|1$. Ein Widerspruch zu Bemerkung 26, da q_{i_0} als Primzahl größer als 1 sein muss.

Aufgabe 3 (5+5 Punkte)**.** (Chinesischer Restsatz) Berechnen Sie alle Lösungen für die folgenden Kongruenzssysteme mit nachvollziehbarem Lösungsweg und Probe.

1. $X \equiv_8 2,\ X \equiv_{21} 16,\ X \equiv_{22} 14,\ X \equiv_{12} 10.$
2. $3X + 7 \equiv_{17} 0,\ 5X - 4 \equiv_{11} 0,\ 7X + 2 \equiv_9 6.$

Lösung:

1. Unter Anwendung des chinesischen Restsatzes erhält man, dass $X \equiv_{21} 16$ äquivalent zu ($X \equiv_3 16 \wedge X \equiv_7 16$), $X \equiv_{22} 14$ äquivalent zu ($X \equiv_{11} 14 \wedge X \equiv_2 14$) und $X \equiv_{12} 10$ äquivalent zu ($X \equiv_3 10 \wedge X \equiv_4 10$) ist. Folglich ist das Kongruenzsystem der Teilaufgabe, welches wir mit (I) bezeichnen, äquivalent zu:

$$X \equiv_8 2 \wedge X \equiv_3 1 \wedge X \equiv_7 2 \wedge X \equiv_{11} 3 \wedge X \equiv_2 0 \wedge X \equiv_3 1 \wedge X \equiv_4 2.$$

Nach Wegefall der Redundanz erhalten wir

$$X \equiv_8 2 \wedge X \equiv_3 1 \wedge X \equiv_7 2 \wedge X \equiv_{11} 3,$$

und nach dem chinesischen Restsatz:

$$X \equiv_{56} 2 \wedge X \equiv_3 1 \wedge X \equiv_{11} 3.$$

Es ist $58 \in [1]_3$, und deshalb ist nach dem chinesischen Restsatz ($X \equiv_{56} 58 \wedge X \equiv_3 58$) äquivalent zu $X \equiv_{168} 58$. Also ist (I) äquivalent zu (II):

$$X \equiv_{168} 58 \wedge X \equiv_{11} 3.$$

Ansatz: $x = 168s + 58$. Wir setzen x in die zweite Kongruenz ein und erhalten $3s + 3 \equiv_{11} 3$, und somit $3s \equiv_{11} 0$. Da 3 und 11 teilerfremd sind, folgt $11|s$. Wir wählen $s = 0$ und erhalten $x = 58$. Da 58, wie eine leichte Probe zeigt, (II) erfüllt, ist nach dem chinesischen Restsatz die Menge $[58]_{1848}$ die Lösungsmenge von (II), und da (I) äquivalent zu (II) ist, ist es auch die Lösungsmenge von (I).

Probe: $1848 = 11 * 168 = 11 * 21 * 8$ ist das kgV der Moduln von (I), und die Differenz zweier Lösungen muss durch das kgV teilbar sein. Also reicht es 58 zu testen.

$$58 \equiv_8 64 - 6 \equiv_8 2,\ 58 \equiv_{21} 63 - 5 \equiv_{21} 16,\ 58 \equiv_{22} 66 - 8 \equiv_{22} 14,\ 58 \equiv_{12} 60 - 2 \equiv_{12} 10.$$

2. Wir bezeichnen das Kongruenzsystem der 2. Teilaufgabe mit (I). Wir multiplizieren die erste Kongruenz mit 6, die zweite Kongruenz mit 2 und die dritte Kongruenz mit 4, und erhalten:

$$X \equiv_{17} -42 \wedge -X \equiv_{11} 8 \wedge X \equiv_9 16,$$

und somit

$$X \equiv_{17} 9 \wedge X \equiv_{11} 3 \wedge X \equiv_9 -2.$$

Ansatz: $x = 17s+9$. Wir setzen x in die zweite Kongruenz ein und erhalten $6s \equiv_{11} -6$. Multiplikation mit 2 ergibt: $s \equiv_{11} -1$. Ansatz: $s = 11r-1$, also $x = 187r-8$. Einsetzen in die dritte Kongruenz ergibt: $7r+1 \equiv_9 -2$, und somit $-2r \equiv_9 -3$. Wir multiplizieren mit -5 und erhalten $r \equiv_9 15 \equiv_9 -3$. Wir setzen $r = -3$ und erhalten $x = -569$.

Probe: $3*(-569)+7 \equiv_{17} 3*(-8)+7 \equiv_{17} 3*9+7 \equiv_{17} 34 \equiv_{17} 0$, $5*(-569)-4 \equiv_{11} 5*(-19)-4 \equiv_{11} 5*3-4 \equiv_{11} 0$ und $7*(-569) \equiv_9 7*(-29) \equiv_9 (-2)*(-2) \equiv_9 4$.

Für die Differenz Δ von zwei Lösungen aus (I) muss $17|3\Delta \wedge 11|5\Delta \wedge 9|7\Delta$ gelten, d.h. $17*11*9$ muss Δ teilen. Es kann also höchstens eine Lösung modulo $17*11*9 = 1683$ geben. Andererseits, wenn man eine Lösung hat, dann ist dessen Restklasse modulo $17*11*9$ eine Teilmenge der Lösungsmenge. Somit ist $[-569]_{1683}$ die Lösungsmenge des Kongruenzsystems.

Aufgabe 4 (5+5+5*)**.** (Diophantische Gleichungen) Es seien $\mathbb{P}$ die Menge der Primzahlen, und $z = \epsilon \prod_{p\in\mathbb{P}} p^{\nu_p(z)}$ die nach der Vorlesung und Übung bis auf Reihenfolge der Faktoren eindeutige Primfaktorzerlegung von $z \in \mathbb{Z} \setminus \{0\}$ wobei ϵ ein Element aus $\{1,-1\}$ ist. Wir setzen $\nu_p(0) := \infty$ für jede Primzahl p.

1. Zeigen Sie, dass $\nu_p : \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ für alle ganzen Zahlen z_1 und z_2 das Folgende erfüllt:
   - $\nu_p(z_1+z_2) \geq \min\{\nu_p(z_1), \nu_p(z_2)\}$ und
   - $\nu_p(z_1+z_2) = \min\{\nu_p(z_1), \nu_p(z_2)\}$, falls $\nu_p(z_1) \neq \nu_p(z_2)$,

   wobei wir $n < \infty$ für alle $n \in \mathbb{Z}$ setzen.
2. Zeigen Sie, dass für $n \in \{0,1,2\}$ die Gleichung $X^3 - Y^3 = XY^n$ keine ganzzahlige Lösung (x,y) mit $y \neq 0$ besitzt. Hierbei dürfen Sie den großen Satz von Fermat verwenden.
3.* Finden Sie alle ganzzahligen Lösungen von $X^3 - Y^3 = XY^3$.

Lösung:

1. Wir haben
$$z_1 + z_2 = \prod_{p\in\mathbb{P}} p^{\min\{\nu_p(z_1),\nu_p(z_2)\}}(z_1' + z_2'),$$
wobei z_i' der Komplementärteiler von z_i bzgl. $\prod_{p\in\mathbb{P}} p^{\min\{\nu_p(z_1),\nu_p(z_2)\}}$ ist. Also folgt
$$\nu_p(z_1+z_2) = \nu_p(z_1'+z_2') + \min\{\nu_p(z_1),\nu_p(z_2)\} \geq \min\{\nu_p(z_1),\nu_p(z_2)\}.$$
Es sei nun $\nu_p(z_1) \neq \nu_p(z_2)$ und ohne Einschränkung $\nu_p(z_1) < \nu_p(z_2)$. Dann gilt $\nu_p(-z_2) = \nu_p(z_2) + \nu_p(-1) = \nu_p(z_2) + 0$ nach der Übung, und es gilt somit mit der ersten Ungleichung:
$$\nu_p(z_1) = \nu_p(z_2+z_1-z_2) \geq \min\{\nu_p(z_1+z_2), \nu_p(-z_2)\} = \min\{\nu_p(z_1+z_2), \nu_p(z_2)\} = \nu_p(z_1+z_2),$$
wobei die letzte Gleichung aus $\nu_p(z_1) < \nu_p(z_2)$ folgt. Also haben wir
$$\nu_p(z_1) \geq \nu_p(z_1+z_2) \geq \min\{\nu_p(z_1),\nu_p(z_2)\} = \nu_p(z_1).$$
2. Angenommen die Gleichung hat eine ganzahlige Lösung (x,y) mit $y \neq 0$. Dann ist auch x ungleich Null aufgrund der Gleichung. Wir zeigen, dass xy^n eine dritte Potenz ist.

   Es sei p eine Primzahl. Wenn sich $\nu_p(x)$ und $\nu_p(y)$ unterscheiden, dann gilt nach Teil 1 für die linke Seite der Gleichung
   $$\nu_p(x^3 - y^3) = \min\{3\nu_p(x), 3\nu_p(y)\},$$
   und insbesondere ist $\nu_p(xy^n)$ durch 3 teilbar. Wenn sich $\nu_p(x)$ und $\nu_p(y)$ nicht unterscheiden, dann gilt im Falle $n = 2$, dass $\nu_p(xy^n)$ ein Vielfaches von 3 ist, und im Fall $0 \leq n \leq 1$ gilt nach Teil 1.
   $$0 \leq 3\nu_p(x) = \min\{3\nu_p(x), 3\nu_p(y)\} \leq \nu_p(x^3-y^3) = \nu_p(xy^n) = \nu_p(x)(1+n) \leq 2\nu_p(x),$$
   also $\nu_p(x) = \nu_p(y) = 0$.

   Wir erhalten also für jede Primzahl p: $3|\nu_p(xy^n)$. Also ist xy^n eine dritte Potenz, etwa z^3. Da x und y ungleich Null sind ist auch z ungleich Null, und damit $(x,-y,z)$ eine Lösung der Fermat-Gleichung zum Exponenten 3 mit $xyz \neq 0$. So eine Lösung existert nicht nach dem großen Satz von Fermat. Also haben wir einen Widerspruch.

3. Es sei (x, y) eine ganzzahlige Lösung der Gleichung. Wenn eine der beiden Koordeinaten verschwindet, dann verwchwindet auch die andere und wir erhalten $(x, y) = (0, 0)$. Wir können uns deshalb auf den Fall beschränken, dass beide Koordinaten nicht null sind. Umstellen der Gleichung ergibt: $(x + 1)y^3 = x^3$. Da x^3 teilerfremd zu $x + 1$ ist, muss x^3 die ganze Zahl y^3 teilen, etwa $y^3 = sx^3$, und wir erhalten $((x + 1)s - 1)x^3 = 0$, und aus der Nullteierfreiheit von $\mathbb{Z}$ folgt $(x+1)s = 1$, also $|x+1||s| = 1$. Daraus folgen $|x+1| = 1$ und $|s| = 1$. Wir erhalten damit die Fälle $x + 1 = \pm 1$, d.h. $x = 0$ (was ausgeschlossen wurde) oder $x = -2$. Aus $|s| = 1$ folgt $|x|^3 = |y|^3$ und $3\nu_p(x) = 3\nu_p(y)$ für alle Primzahlen p, und des Weiteren sind $|x|$ und $|y|$ positiv. Die ganzen Zahlen $|x|$ und $|y|$ müssen also übereinstimmen, da sie die gleiche Primfaktorzerlegung haben (Achtung: Das Vorzeichen gehört auch zur Primfaktorzerlegung!). Wir erhalten also insgesamt die Kandidaten $(0, 0), (-2, -2)$ und $(-2, 2)$. Einsetzen zeigt, dass nur $(0, 0)$ und $(-2, 2)$ Lösungen sind, das heißt, dass

$$\{(0, 0), (-2, 2)\}$$

die Lösungsmenge der Gleichung ist. Das war ein Beispiel, bei dem die Probe noch einen Kandidaten entfernt hat.