Fakultät für Mathematik
Universität Bielefeld
Joa Weber

WS 2010/11

3. Februar 2011

Elementare Zahlentheorie

Musterlösung zur Klausur I

Aufgabe 1. Sei $g \in \mathbb{N}$ mit $g \geq 2$. Bestimmen Sie die (g-adischen) Ziffern der Zahl in der rechten unteren Ecke des kleinen Einmaleins für das g-adische Ziffernsystem.

Lösung Aufgabe 1. Die gesuchte Zahl ist offenbar $(g-1)^2$. Es bleibt das Problem ihre g-adischen Ziffern zu bestimmen: Es gilt

$$(g-1)^2 = g^2 - 2g + 1 = 1 + (g-2) \cdot g = c_0 + c_1 \cdot g,$$

mit $c_0 := 1$ und $c_1 := g - 2$. Also ist

$$((g-2)\ 1)_g$$

die gesuchte g-adische Zifferndarstellung.

Aufgabe 2. Bestimmen Sie $\mathrm{ggT}(270, 115)$ und $\mathrm{ggT}(163148, 163153)$.

Lösung Aufgabe 2. Es gilt $\mathrm{ggT}(270, 115) = \mathrm{ggT}(2 \cdot 3^3 \cdot 5, 5 \cdot 23) = 2^0 \cdot 3^0 \cdot 5^1 \cdot 23^0 = 5$ und

$$\mathrm{ggT}(163148, 163153) = \mathrm{ggT}(163148, 163148 + 5) = \mathrm{ggT}(163148, 5) = 1.$$

Hier gilt die zweite Gleichheit, da sich der ggT endlich vieler ganzer Zahlen nicht ändert, wenn man zu einer Zahl eine ganzzahlige Linearkombination der anderen Zahlen addiert. Die letzte Gleichheit gilt, da 5 eine Primzahl ist und die letzte Ziffer eines Vielfachen von 5 entweder 0 oder 5 ist.

Aufgabe 3. Bestimmen Sie eine Lösung der diophantischen Gleichung

$$270r + 115s = 5.$$

Lösung Aufgabe 3. Es gilt $5 = \mathrm{ggT}(270, 115)$. Mit dem Euklidischen Algorithmus ergibt sich

$$\begin{aligned} 270 &= 2 \cdot 115 + 40 \\ 115 &= 2 \cdot 40 + 35 \\ 40 &= 1 \cdot 35 + 5 \\ 35 &= 7 \cdot 5 + 0. \end{aligned}$$

Hieraus folgt durch wiederholtes Einsetzen von unten nach oben

$$\begin{aligned} 5 &= 40 - 35 \\ &= 40 - (115 - 2 \cdot 40) \\ &= -115 + 3\,(270 - 2 \cdot 115) \\ &= 3 \cdot 270 - 7 \cdot 115. \end{aligned}$$

Somit ist $(r, s) = (3, -7)$ die gesuchte Lösung.

Aufgabe 4. Bestimmen Sie, falls existent, alle Lösungen der diophantischen Gleichung

$$270x + 115y = 0.$$

Bestimmen Sie, falls existent, eine Lösung der diophantischen Gleichung

$$270x + 115y = 185.$$

Lösung Aufgabe 4. Nach Aufgabe 2 ist $d := \mathrm{ggT}(270, 115) = 5$. Setzen wir $a := 270 = ed$ und $b := 115 = fd$, so folgt $e = 54$ und $f = 23$. Nach Aufgabe 3 ist $(r, s) = (3, -7)$ eine Lösung der Gleichung $270r + 115s = 5$.

Im Fall $c := 0 = nd$, folgt $n = 0$ und wir erhalten nach der in der Vorlesung in II §6 entwickelten Lösungstheorie die Lösungsgesamtheit

$$\left\{ \begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} nr + fk \\ ns - ek \end{pmatrix} = \begin{pmatrix} 23k \\ -54k \end{pmatrix} \;\middle|\; k \in \mathbb{Z} \right\}.$$

Im Fall $c := 185$ erhält man wegen $185 = 37 \cdot 5$ mittels Aufgabe 3 z.B. die Lösung

$$(x, y) = (3 \cdot 37, -7 \cdot 37).$$

Eine andere Möglichkeit ist obige Lösungstheorie heranzuziehen. Mit $c = 185 = nd = 37 \cdot 5$ ergibt sich die Lösungsgesamtheit

$$\left\{ \begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} 37 \cdot 3 + 23k \\ 37 \cdot (-7) - 54k \end{pmatrix} \;\middle|\; k \in \mathbb{Z} \right\}.$$

Aufgabe 5. Es seien $a, b \in \{0, 1, 2, 3, 4\}$. Beweisen Sie, daß $(abab)_5$ durch 2 und durch 13 teilbar ist.

Lösung Aufgabe 5. Es gilt

$$(abab)_5 = b + a{\cdot}5 + b{\cdot}5^2 + a{\cdot}5^3 = b\left(1 + 5^2\right) + a5\left(1 + 5^2\right) = (b + a5){\cdot}26 = (b + a5){\cdot}2{\cdot}13.$$

Aufgabe 6. Gegeben ganze Zahlen a, m, x mit $x^2 \equiv a(m)$ und $m \geq 2$. Zeigen Sie:

$$a, m \text{ teilerfremd} \qquad \Rightarrow \qquad x, m \text{ teilerfremd}.$$

Lösung Aufgabe 6. Nach Voraussetzung existiert ein $q \in \mathbb{Z}$ mit $x^2 - a = qm$. Widerspruchs-annahme: x, m nicht teilerfremd. Also besitzen sie einen gemeinsamen Teiler $d > 1$. Wegen $a = x^2 - qm$ teilt d auch a, aber das ist ein Widerspruch zur Teilerfremdheit von a und m.

Aufgabe 7. Die Zahl $n = 8549$ ist das Produkt zweier Primzahlen $p < q$. Die prime Restklassengruppe $\mathbb{Z}_n^*$ hat die Ordnung $\varphi(n) = 8364$. Bestimmen Sie p und q (wie immer mit Angabe des Lösungsweges).

(Erinnerung: Die Lösungen der quadratischen Gleichung $ax^2 + bx + c = 0$ sind gegeben durch $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.)

Lösung Aufgabe 7. Es gilt

$$8364 = \varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1) = pq - p - q + 1 = 8550 - p - q$$

und daraus folgt

$$p = 186 - q.$$

Also gilt

$$8549 = pq = (186 - q)q \qquad \Leftrightarrow \qquad q^2 - 186q + 8549 = 0.$$

Hieraus erhält man die Lösungen

$$q_{1,2} = \frac{186 \pm \sqrt{186^2 - 4 \cdot 8549}}{2} = 93 \pm \frac{\sqrt{34596 - 34196}}{2} = 93 \pm \frac{\sqrt{400}}{2} = 93 \pm 10.$$

Für $q_1 = 83$ ergibt sich $p_1 = 186 - 83 = 103$ und für $q_2 = 103$ natürlich $p_2 = 186 - 103 = 83$. Also sind $p = 83$ und $q = 103$ die gesuchten Größen.

Aufgabe 8. (i) Gegeben zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ in einem K1-Ring R, beweisen Sie, daß die Summe $\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a},\, b \in \mathfrak{b}\}$ ein Ideal in R ist. Geben Sie in jedem Schritt die verwendeten Ringaxiome an.

(ii) Sei R ein Integritätsring und $a, b, d \in R$. Beweisen Sie:

$$Ra + Rb = Rd \qquad \Rightarrow \qquad d \in \mathrm{ggT}(a, b).$$

Lösung Aufgabe 8. (i) Da $\mathfrak{a}$ bzw. $\mathfrak{b}$ wenigstens ein Element a_0 bzw. b_0 enthält, ist auch die Menge $\mathfrak{a}+\mathfrak{b}$ nicht leer: Es gilt $a_0 + b_0 \in \mathfrak{a}+\mathfrak{b}$. Es bleibt zu zeigen, daß $\mathfrak{a}+\mathfrak{b}$ invariant unter Differenzenbildung ist sowie unter Multiplikation mit Elementen von R. Seien nun $c, c' \in \mathfrak{a}+\mathfrak{b}$ und $r \in R$. Nach Definition von $\mathfrak{a}+\mathfrak{b}$ gilt $c = a+b$ und $c' = a' + b'$ mit $a, a' \in \mathfrak{a}$ und $b, b' \in \mathfrak{b}$. Aus dem Assoziativ- und dem Kommutativgesetz der Addition folgt

$$(a + b) - (a' + b') = (a - a') + (b - b') \in \mathfrak{a} + \mathfrak{b},$$

da $a - a' \in \mathfrak{a}$ und $(b - b') \in \mathfrak{b}$ wegen der Idealeigenschaft von $\mathfrak{a}$ und $\mathfrak{b}$, respektive. Aus dem Distributivgesetz folgt

$$r(a + b) = ra + rb \in \mathfrak{a} + \mathfrak{b},$$

da $ra \in \mathfrak{a}$ und $rb \in \mathfrak{b}$ wegen der Idealeigenschaft von $\mathfrak{a}$ und $\mathfrak{b}$, respektive.

(ii) Da $a \in Ra \subset Rd$ ist a ein Vielfaches von d, also $d \mid a$. Analog folgt $d \mid b$ und das erste Axiom eines ggT ist für d bewiesen. Sei nun t irgendein gemeinsamer Teiler von a und b, d.h. $a = ut$ und $b = vt$ mit $u, v \in R$. Aus $d \in Rd = Ra + rb$ folgt $d = ra + sb$ mit $r, s \in R$. Daher gilt

$$d = ra + sb = rut + svt = (ru + sv)t$$

und dies beweist das zweite Axiom: Jeder gemeinsame Teiler von a und b teilt d.

Aufgabe 9. Bestimmen Sie die prime Restklassengruppe modulo $m = 18$. Wieviele *verschiedene* Primitivwurzeln zu 18 gibt es, d.h. wieviele paarweise inkongruente Primitivwurzeln $c \in \mathbb{Z}$ zu 18 gibt es? Wieviele Primitivwurzeln zu 18 gibt es (insgesamt)? Wieviele Primitivwurzeln zu 16 gibt es? Begründen Sie jeweils Ihre Antwort.

Lösung Aufgabe 9. Die prime Restklassengruppe $\mathbb{Z}_{18}^*$ besteht aus den Restklassen aller zu 18 teilerfremden ganzen Zahlen

$$\mathbb{Z}_{18}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\} \subset Z_{18}.$$

Probe: Die Ordnung von $\mathbb{Z}_{18}^*$ ist $\varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2)\varphi(3^2) = 1 \cdot (3 - 1)3^1 = 6$. Nach dem Theorem von Gauss ist $\mathbb{Z}_{2 \cdot 3^2}^*$ zyklisch. Also gibt es nach IV §2 Korollar 13 genau

$$\varphi(\operatorname{ord} \mathbb{Z}_{18}^*) = \varphi(6) = \varphi(2 \cdot 3) = \varphi(2)\varphi(3) = (2 - 1)(3 - 1) = 2$$

Erzeuger (Elemente der Ordnung sechs) und somit zwei verschiedene Primitivwurzeln zu 18. Nach Definition ist jeder Repräsentant eines der beiden Elemente eine Primitivwurzel zu 18, also gibt es unendlich viele. Nach dem Theorem von Gauss ist $\mathbb{Z}_{16}^* = \mathbb{Z}_{2^4}^*$ nicht zyklisch, also gibt es kein erzeugendes Element und somit auch keine Primitivwurzel zu 16.