

Elementare Zahlentheorie

Klausur II

34=3+3+3+5+3+4+3+4+6 Punkte

Aufgabe 1. (3 Punkte) Sei $g > 2$ eine ungerade natürliche Zahl. Beweisen Sie, daß jede in g -adischer Zifferndarstellung in der Form $(abab)_g$ gegebene natürliche Zahl gerade ist.

Lösung 1. Es gilt (1 Punkt)

$$(abab)_g = b + a \cdot g + b \cdot g^2 + a \cdot g^3 = b(1 + g^2) + ag(1 + g^2) = (1 + g^2)(b + ag).$$

Nun ist $1 + g^2$ gerade, da g ungerade ist (1 Punkt). Das Produkt einer geraden mit einer beliebigen natürlichen Zahl ist gerade (1 Punkt).

Aufgabe 2. (3 Punkte) Für $a, b, c, d \in \mathbb{Z}$ und $n \in \mathbb{N}$ gelte

$$n \mid (5a - b), \quad n \mid (5c - d).$$

Beweisen Sie:

$$n \mid (ad - bc).$$

Lösung 2. Nach Voraussetzung existieren $k, \ell \in \mathbb{Z}$ mit (1 Punkt)

$$5a - b = kn, \quad 5c - d = \ell n$$

und daraus folgt (1 Punkt)

$$5ac - bc = knc, \quad 5ac - ad = \ell na$$

Also gilt (1 Punkt)

$$-bc + ad = (knc - 5ac) + (5ac - \ell na) = n(kc - \ell a).$$

Aufgabe 3. (3 Punkte) Für ganze Zahlen a, b mit $(a, b) \neq (0, 0)$ sind $u, v \in \mathbb{Z}$ festgelegt durch

$$a = u \cdot \text{ggT}(a, b), \quad b = v \cdot \text{ggT}(a, b).$$

Zeigen Sie, daß u, v teilerfremd sind.

Lösung 3. Es gilt (1 Punkt)

$$\text{ggT}(a, b) = \text{ggT}(u \cdot \text{ggT}(a, b), v \cdot \text{ggT}(a, b)) = \text{ggT}(a, b) \cdot \text{ggT}(u, v).$$

Weiter gilt $\text{ggT}(a, b) \neq 0$, da $(a, b) \neq (0, 0)$ (**1 Punkt**). Durch kürzen ergibt sich $\text{ggT}(u, v) = 1$ (**1 Punkt**).

Aufgabe 4. (5 Punkte) Sei p eine ungerade Primzahl und n eine ganze Zahl mit $0 \leq n \leq p-1$. Zeigen Sie:

$$\binom{p-1}{n} \equiv (-1)^n \pmod{p}.$$

Lösung 4. Nach Definition des Binomialkoeffizienten (siehe Präsenzübung 7) gilt (**1 Punkt**)

$$\binom{p-1}{n} = \frac{(p-1)(p-2)\dots(p-n)}{n!}.$$

Wir definieren

$$f(p) := (p-1)(p-2)\dots(p-n)$$

und schreiben dieses Polynom vom Grad n in der allgemeinen Form

$$f(p) = p^n + a_{n-1}p^{n-1} + \dots + a_1p + (-1)^n(n!)$$

mit $a_1, \dots, a_{n-1} \in \mathbb{Z}$. Mit $g(p) := p^{n-1} + a_{n-1}p^{n-2} + \dots + a_2p + a_1$ erhalten wir die Zerlegung (**1 Punkt**)

$$f = pg + (-1)^n(n!).$$

Damit ergibt sich

$$\binom{p-1}{n} = \frac{f}{n!} = \frac{pg + (-1)^n(n!)}{n!} = \frac{pg}{n!} + (-1)^n.$$

Insbesondere ist $\frac{pg}{n!} \in \mathbb{Z}$, d.h. $n!$ teilt pg (**1 Punkt**). Nun sind $n!$ und p teilerfremd (**1 Punkt**), da $p \in \mathbb{P}$ und $0 \leq n \leq p-1$, also gilt

$$n! \mid pg \quad \Rightarrow \quad n! \mid g.$$

Somit ist $g = \ell(n!)$ für ein $\ell \in \mathbb{Z}$ und wir erhalten (**1 Punkt**)

$$\binom{p-1}{n} = \frac{p\ell(n!)}{n!} + (-1)^n = p\ell + (-1)^n \equiv (-1)^n \pmod{p}.$$

Aufgabe 5. (3 Punkte) a) Erstellen Sie die Additions- und die Multiplikationstabelle der 4-adischen Ziffern. b) Bestimmen Sie die 5-adische Darstellung der 4-adischen Zahl $(123)_4$.

Lösung 5. a) Die Additionstabelle der 4-adischen Ziffern hat die (4-adischen) Einträge (**1 Punkt**)

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & (10)_4 \\ 2 & 3 & (10)_4 & (11)_4 \\ 3 & (10)_4 & (11)_4 & (12)_4 \end{pmatrix}.$$

Die Multiplikationstabelle der 4-adischen Ziffern hat die (4-adischen) Einträge (**1 Punkt**)

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & (10)_4 & (12)_4 \\ 0 & 3 & (12)_4 & (21)_4 \end{pmatrix}.$$

b) (1 Punkt) Es gilt

$$(123)_4 = 1 \cdot 4^2 + 2 \cdot 4 + 3 = 27 = 1 \cdot 5^2 + 0 \cdot 5 + 2 = (102)_5.$$

Aufgabe 6. (4 Punkte) Sei R ein Integritätsring mit ggT. Seien $a, m \in R$ mit $(a, m) \neq (0, 0)$ und sei $d \in \text{ggT}(a, m)$. Beweisen Sie:

$$x \in R \text{ löst } aX \equiv 0(m) \quad \Leftrightarrow \quad x = \frac{m}{d} \ell \text{ für ein } \ell \in R.$$

(Bemerkung: Es gilt $m = nd$ für ein $n \in R$ und $\frac{m}{d}$ steht symbolisch für n .)

Lösung 6. Wir schreiben $a = bd$ und $m = nd$ mit $b, n \in R$. Wegen $(a, m) \neq (0, 0)$ gilt $d \neq 0$ (1/2 Punkt). Wir zeigen b und n sind teilerfremd: Nach III §B Satz 8 und Rechenregel 9) gilt (1/2 Punkt)

$$d \in \{r \in R \mid r \sim d\} = \text{ggT}(a, m) = \text{ggT}(bd, nd) = d \cdot \text{ggT}(b, n).$$

Wegen $d \in d \cdot \text{ggT}(b, n)$ und $d \neq 0$ muß gelten $1 \in \text{ggT}(b, n)$ (1/2 Punkt), also gilt wieder mit Satz 8 (1/2 Punkt)

$$\text{ggT}(b, n) = \{r \in R \mid r \sim 1\} = R^*,$$

d.h. b und n sind teilerfremd.

" $\Rightarrow$ " Sei $x \in R$ mit $ax = rm$ für ein $r \in R$. Aus $bdx = rnd$ und $d \neq 0$ folgt $bx = rn$ mit der Kürzungsregel (1/2 Punkt), insbesondere wird also bx von n geteilt. Da b und n teilerfremd sind, gilt nach III §B Lemma 13 (1/2 Punkt)

$$n \mid bx \quad \Rightarrow \quad n \mid x.$$

Also ist $x = n\ell = \frac{m}{d} \ell$ für ein $\ell \in R$.

" $\Leftarrow$ " Sei $x = \frac{m}{d} \ell = n\ell$ mit $\ell \in R$. Mit $a = bd$ erhalten wir (1 Punkt)

$$ax = bdx = bdn\ell = b\ell m \equiv 0(m).$$

Aufgabe 7 (3 Punkte). Bestimmen Sie alle Lösungen der linearen Kongruenz $6X \equiv -3(9)$. Wieviele modulo 9 inkongruente Lösungen gibt es?

Lösung 7. Offenbar ist $x = 1$ eine Lösung (1 Punkt). Die Lösungen der homogenen Kongruenz $6X \equiv 0(9)$ sind nach Aufgabe 6 gegeben durch

$$\left\{ x_\ell = \frac{9}{\text{ggT}(6, 9)} \ell = 3\ell \mid \ell \in \mathbb{Z} \right\}.$$

Somit erhalten wir die gesuchte Lösungsgesamtheit (1 Punkt)

$$\left\{ x + x_\ell = 1 + 3\ell \mid \ell \in \mathbb{Z} \right\}.$$

Es gibt drei modulo 9 inkongruente Lösungen, z.B. 1, 4 und 7 (1 Punkt).

Aufgabe 8. (4 Punkte) Bestimmen Sie alle Lösungen des Systems simultaner Kongruenzen

$$X \equiv 1(2), \quad X \equiv 0(3), \quad X \equiv 3(6), \quad X \equiv 3(12), \quad X \equiv 8(13).$$

Lösung 8. Aufgrund des gegebenen Systems simultaner Kongruenzen (SSK) und da 2, 3 und 6 Teiler von 12 sind, löst jede Lösung der vierten Kongruenz automatisch auch die ersten drei Kongruenzen (**1 Punkt**). Es genügt also die Lösungen des SSK

$$X \equiv 3 \pmod{12}, \quad X \equiv 8 \pmod{13} \quad (1)$$

zu bestimmen. Nach III §6 bestimmen wir zunächst eine Lösung x_1 von

$$13X \equiv 3 \pmod{12},$$

sowie eine Lösung x_2 von

$$12X \equiv 8 \pmod{13}.$$

Wegen

$$3 \cdot 13 = 39 = 2 \cdot 12 + 3 \equiv 3 \pmod{12}$$

und

$$5 \cdot 12 = 60 = 4 \cdot 13 + 8 \equiv 8 \pmod{13}$$

wählen wir $x_1 = 3$ und $x_2 = 5$ (**1 Punkt**). Nach III §6 löst (**1 Punkt**)

$$x' := 13 \cdot 3 + 12 \cdot 5 = 99$$

das System (1). Also sind alle modulo $m := 12 \cdot 13 = 156$ zu 99 kongruenten ganzen Zahlen die gesuchten Lösungen (**1 Punkt**).

Aufgabe 9. (6 Punkte) Wieviele verschiedene quadratische Reste a modulo 11 gibt es (mit Begründung)? Bestimmen Sie diese (mit Nachweis/Begründung für jedes a).

Lösung 9. Nach dem Theorem von Gauß ist $\mathbb{Z}_{11}^*$ zyklisch. Also gibt es nach IV §3 Satz 4 genau $s := \frac{1}{2}\varphi(11) = 5$ verschiedene quadratische Reste modulo 11 (**1 Punkt**).

(5 Punkte für die Bestimmung der fünf verschiedenen quadratischen Reste).

Version I: Nach demselben Satz genügt es (**1 Punkt**) eine Primitivwurzel c zu 11 zu bestimmen (es gibt $\varphi(10) = 4$ verschiedene), denn dann sind genau die $s = 5$ Restklassen (**1 Punkt**)

$$\overline{1}, \overline{c^2}, \overline{c^4}, \overline{c^6}, \overline{c^8}$$

quadratisch und es verbleibt die Wahl je eines Repräsentanten.

Bestimmung einer Primitivwurzel zu 11: Die zehn Kongruenzen (**1 Punkt**)

$$2 \equiv 2 \pmod{11}, \quad 4 \equiv 4 \pmod{11}, \quad 8 \equiv 8 \pmod{11}, \quad 16 \equiv 5 \pmod{11}, \quad 32 \equiv 10 \pmod{11},$$

und

$$64 \equiv 9 \pmod{11}, \quad 128 \equiv 7 \pmod{11}, \quad 256 \equiv 3 \pmod{11}, \quad 512 \equiv 6 \pmod{11}, \quad 1024 \equiv 1 \pmod{11},$$

zeigen, daß $c := 2$ die maximale Ordnung 10 hat (**1 Punkt**) und somit eine Primitivwurzel zu 11 ist. Weiter zeigen sie, daß

$$\overline{1}, \quad \overline{2^2} = \overline{4}, \quad \overline{2^4} = \overline{16} = \overline{5}, \quad \overline{2^6} = \overline{64} = \overline{9}, \quad \overline{2^8} = \overline{256} = \overline{3}.$$

Also sind 1, 4, 5, 9 und 3 fünf verschiedene quadratische Reste modulo 11 (**1 Punkt**).

Version II: Eine andere Möglichkeit besteht darin mittels des quadratischen Reziprozitätsgesetzes, der beiden Ergänzungssätze, sowie der Produkt- und der Kongruenzregel die Legendre-Symbole

$$\left(\frac{a}{11}\right) \in \{-1, +1\}$$

für $a = 1, 2, \dots, 10$ zu bestimmen (**1/2 Punkt pro richtig bestimmtem Symbol ausgenommen $a = 1$**). Jedes a welches zu einem Wert $+1$ führt ist ein quadratischer Rest modulo 11. Da alle solchen a 's offenbar inkongruent modulo 11 sind, handelt es sich um verschiedene quadratische Reste (**1/2 Punkt**).