Aufgabenblatt 2

40 Punkte

Aufgabe 1 (ganzzahlige Lösungen)
Betrachte die Gleichung

$$680 \cdot x + 2431 \cdot y = 1105 \ .$$

a) Weise nach, dass diese Gleichung ganzzahlige Lösungen hat. 2

b) Bestimme eine (sog. *partikuläre*) ganzzahlige Lösung. 2

c) Gib *alle* ganzzahligen Lösungen (Parameter $m \in \mathbb{Z}$). 1

d) Bestimme die „kleinste“ Lösung $(x|y)$, also diejenige mit minimalem $|x| + |y| \in \mathbb{N}$. 1

e) Nur eine der zwei folgenden Gleichungen hat ganzzahlige Lösungen,

$$1105 \cdot x + 2431 \cdot y = 680 \quad , \quad 385 \cdot x + 429 \cdot y = 341 \ .$$

Führe mit dieser die Schritte 1 a) bis 1 d) durch. 6

Bemerkung: Siehe Unterabschnitt 1.1.4 im Skript.
Die Berechnungen grösster gemeinsamer Teiler sind zu dokumentieren (Euklid, ohne Taschenrechner). **12**

Aufgabe 2 (Rechnen im Ring $\mathbb{Z}_m$)
Im Ring $\mathbb{Z}_7$ ist Addition und Multiplikation wie folgt definiert (Notation: n statt $\overline{n}$),

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

,

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

.

a) Gib entsprechende Tabellen für „+“ und „·“ in $\mathbb{Z}_{10}$ und $\mathbb{Z}_{11}$. Was bedeutet die Symmetrie? 4

b) Gib zu jedem Element in $\mathbb{Z}_{10}^{\times}$ — also zu jeder Einheit in $\mathbb{Z}_{10}$ — ihr multiplikatives Inverse. 2

c) Der Ring $\mathbb{Z}_{11} = \mathbb{F}_{11}$ ist ein *Körper*. Was heisst das? 1
Bestimme die zwei Lösungen $x_1, x_2 \in \mathbb{Z}_{11}$ der quadratischen Gleichung

$$3 \cdot x^2 + 5 \cdot x + 10 \equiv 0 \quad (\text{ in } \mathbb{Z}_{11})$$

durch eine gültige Interpretation in $\mathbb{Z}_{11}$ der bekannten Formel (*„Mitternachtsformel“).* 2

9

Aufgabe 3 (Reste)

a) Welches sind *alle* möglichen 15er–Reste $\pi_{15}(3^n)$ von 3^n für $n = 1, 2, 3, \ldots$? 1
Berechne $\pi_{15}(3^{1291})$. 2

b) $\pi_{11}(2^{2017}) = ?$ Weshalb hilft hier der *Kleine Satz von Fermat*? (Skript S.16) 2

5

Aufgabe 4 (ein Vergleich)
Wir vergleichen die *multiplikativen Gruppen* der Einheiten in $\mathbb{Z}_{15}$ und in $\mathbb{Z}_{16}$, also $M_{15} = \mathbb{Z}_{15}^{\times}$ mit $M_{16} = \mathbb{Z}_{16}^{\times}$.

a) Erstelle zwei Listen der Elemente in M_{15} und der Elemente in M_{16}. 2

b) Gib zu jedem Element der zwei obigen Listen seine Ordnung in M_{15} bzw. in M_{16}. 2

c) Die Multiplikation in M_{15} werde mit „$\cdot$“ bezeichnet, die Multiplikation in M_{16} mit „$\otimes$“ .
Gibt es eine Bijektion (sog. *Gruppenisomorphismus*)

$$\varphi\colon M_{15} \longrightarrow M_{16} \ ,$$

so dass für alle $a, b \in M_{15}$ gilt

$$\varphi(a \cdot b) = \varphi(a) \otimes \varphi(b) \ ?$$

Weshalb ist dabei 4 b) zu beachten? 2

6

Aufgabe 5 (diskreter Logarithmus)
Wir betrachten den *diskreten Logarithmus* in $M_{13} = \mathbb{Z}_{13}^{\times} = \mathbb{Z}_{13} \setminus \{0\}$.

a) Bestimme alle Primitivwurzeln in M_{13}. (Skript, S.16) 2

b) Seien a und b gemäss 5 a) die Primitivwurzeln mit $b = a + 1$. Rechne nach, dass gilt

$$\log_a(8) = \frac{\log_b(8)}{\log_b(a)} \quad \text{(vgl. Skript, S.19, Logarithmusgesetz III)} \ .$$

Beachte dabei, dass $\log_a(\cdot)$ und $\log_b(\cdot)$ zwei verschiedene Isomorphismen von M_{13} nach der *additiven* Gruppe $A_{12} = \mathbb{Z}_{12}$ sind. (Skript, S.19/20) 2

4

Aufgabe 6 (Kettenbruch)
In der Vorlesung (Skript, S.24) wird nachgewiesen, dass alle Näherungsbrüche von $[1,1,1,3,1,1,26,3]$, also

$$[1] = 1 = \frac{1}{1} = \frac{p_0}{q_0} \quad \leq \quad \frac{p_7}{q_7} = [1,1,1,3,1,1,26,3] \ ,$$

$$[1,1] = 1 + \frac{1}{1} = \frac{2}{1} = \frac{p_1}{q_1} \quad \geq \quad \frac{p_7}{q_7} \ ,$$

$$[1,1,1] = 1 + \frac{1}{1 + \frac{1}{1}} = \frac{3}{2} = \frac{p_2}{q_2} \quad \leq \quad \frac{p_7}{q_7} \ ,$$

$$[1,1,1,3] = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}} = \frac{11}{7} = \frac{p_3}{q_3} \quad \geq \quad \frac{p_7}{q_7} \ ,$$

$$[1,1,1,3,1] = \quad \text{... etc. etc. ...} \quad = \frac{p_4}{q_4} \quad \leq \quad \frac{p_7}{q_7} \ , \quad \text{... etc. etc. ... ,}$$

immer $|p_k/q_k - p_7/q_7| \leq 1/q_k^2$ erfüllen (alle Brüche gekürzt, $k = 0, 1, \ldots, 7$). Für die meisten gilt sogar

$$\left| \frac{p_k}{q_k} - \frac{p_7}{q_7} \right| < \frac{1}{2q_k^2} \ .$$

Für welche $k \in \{0, 1, \ldots, 7\}$ ist dies nicht der Fall? Dokumentiere alle Rechnungen.
Bemerkung: Diese Frage wird sich im Zusammenhang mit dem *Kriterium von Legendre* (Skript, S.27) stellen. 4