GRUPPEN UND SYMMETRIEN
LÖSUNG VON TRAININGSZETTEL II

JULIA SAUTER

Aufgaben zu Kongruenzen und multiplikativen Restklassengruppen.

(1) Berechnen Sie die Ordnungen aller Elemente in $\mathbb{Z}/12\mathbb{Z}$. Zeigen Sie dann, dass es für jeden Teiler k von 12 genau eine Untergruppe dieser Ordnung gibt.
Hinweis: Alle Untergruppen von $\mathbb{Z}/12\mathbb{Z}$ sind zyklisch.
Lösung: Nach Vorlesung ist bekannt, dass $\mathrm{ord}_{\mathbb{Z}/12\mathbb{Z}}(\overline{\mathrm{k}}) = \frac{12}{\mathrm{ggT(k,12)}}$ für alle $k \in \mathbb{Z}$ gilt. Somit ergibt sich:

k	0	1	2	3	4	5	6	7	8	9	10	11
$\mathrm{ord}_{\mathbb{Z}/12\mathbb{Z}}(\overline{\mathrm{k}})$	1	12	6	4	3	12	2	12	3	4	6	12

Die Teiler von 12 sind $1, 2, 3, 4, 6, 12$, für jeden finden wir ein Element dieser Ordnung in obiger Liste. Sei ℓ einer dieser Teiler. Da alle UG zyklisch sind, müssen sie von einem Element von $\mathbb{Z}/12\mathbb{Z}$ erzeugt sein. Wir müssen sehen, dass alle Elemente der Ordnung ℓ die gleiche UG erzeugen.

- $\ell = 1$ Es gibt nur ein Element der Ordnung 1 (nämlich $\overline{0}$), also klarerweise auch nur eine UG der Ordnung 1 (nämlich $\{\overline{0}\}$).
- $\ell = 2$ Es gibt nur ein Element der Ordnung 2 (nämlich $\overline{6}$), also klarerweise auch nur eine UG der Ordnung 2 (nämlich $\{\overline{0}, \overline{6}\}$).
- $\ell = 3$ Nur die Elemente $\overline{4}$ und $\overline{8}$ haben Ordnung 3. Es gilt aber $\langle\overline{4}\rangle = \{\overline{0}, \overline{4}, \overline{8}\} = \langle\overline{8}\rangle$.
- $\ell = 4$ Nur die Elemente $\overline{3}$ und $\overline{9}$ haben Ordnung 4. Es gilt aber $\langle\overline{3}\rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = \langle\overline{9}\rangle$.
- $\ell = 6$ Nur die Elemente $\overline{2}$ und $\overline{10}$ haben Ordnung 6. Es gilt aber $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} = \langle\overline{10}\rangle$.
- $\ell = 12$ Nur die Elemente $\overline{1}, \overline{5}, \overline{7}$ und $\overline{11}$ haben Ordnung 12. Dies sind aber gerade die teilerfremden Restklassen, von denen wir nach VL wissen, dass sie die ganze Gruppe erzeugen.

(2) Berechnen Sie $\varphi(12)$ und schreiben Sie die Elemente von $(\mathbb{Z}/12\mathbb{Z})^\times$ auf. Berechnen Sie die Ordnungen aller Elemente von $(\mathbb{Z}/12\mathbb{Z})^\times$ und beweisen Sie, dass die Gruppe isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist.

Lösung: $\varphi(12) = \varphi(3)\varphi(4) = (3-1)(4-2) = 4$ und $(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. Die Ordnung eines Elementes muss ein Teiler von 4 sein, also entweder $1, 2$ oder 4. Es gilt aber $5^2 \equiv 25 \equiv 1 \pmod{12}, 7^2 \equiv 49 \equiv 1 \pmod{12}, 11^2 \equiv 121 \equiv 1 \pmod{12}$ und deswegen $\mathrm{ord}_{(\mathbb{Z}/12\mathbb{Z})^\times}(\overline{5}) = \mathrm{ord}_{(\mathbb{Z}/12\mathbb{Z})^\times}(\overline{7}) = \mathrm{ord}_{(\mathbb{Z}/12\mathbb{Z})^\times}(\overline{11}) = 2$ und natürlich $\mathrm{ord}_{(\mathbb{Z}/12\mathbb{Z})^\times}(\overline{1}) = 1$. Nach dem HS ist eine abelsche Gruppe mit vier Elementen isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ oder $\mathbb{Z}/4\mathbb{Z}$. Da es kein Element der Ordnung 4 gibt, ist die Gruppe nicht zyklisch und somit nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$. Dies zeigt, dass sie isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist. □

(3) Finden Sie alle Erzeuger der zyklischen Gruppe $(\mathbb{Z}/13\mathbb{Z})^\times$.
Hinweis: Sie sollten $\varphi(\varphi(13))$ Erzeuger finden.
Lösung: Es gilt $\varphi(13) = 12$. Nach VL (Satz von Gauß) ist bekannt, dass $(\mathbb{Z}/13\mathbb{Z})^\times$ zyklisch ist, also isomorph zu $\mathbb{Z}/12\mathbb{Z}$, welches wiederum $\varphi(12) = 4$ Erzeuger hat. Somit hat $(\mathbb{Z}/13\mathbb{Z})^\times$ ebensoviele. Somit suchen wir vier Elemente der Ordnung 12 in $(\mathbb{Z}/13\mathbb{Z})^\times$. Die möglichen Ordnungen sind Teiler von 12, also $1, 2, 3, 4, 6, 12$. Jetzt fangen wir an damit Ordnungen zu berechnen, zuerst von $\overline{2}$. Es gilt $\overline{2}^2 = \overline{4} \neq \overline{1}, \overline{2}^3 = \overline{8} \neq \overline{1}, \overline{2}^4 = \overline{16} = \overline{3} \neq \overline{1}, \overline{2}^6 = \overline{64} = \overline{(-1)} \neq \overline{1}$. Somit ist die Ordnung von $\overline{2}$ gerade 12. Um die anderen drei Erzeuger zu finden, betrachten wir die Potenzen $\overline{2}^t$ mit $t \in \{0, 1, \ldots, 11\}$ mit t teilerfremd zu 12, d.h. $t \in \{1, 5, 7, 11\}$. Diese vier Potenzen müssen die Erzeuger der zyklischen Gruppe $(\mathbb{Z}/13\mathbb{Z})^\times$ sein, denn

$$\mathbb{Z}/12\mathbb{Z} \to (\mathbb{Z}/13\mathbb{Z})^\times, t \mapsto \overline{2}^t$$

ist ein Isomorphismus von Gruppen (da $\overline{2}$ ein Erzeuger von $(\mathbb{Z}/13\mathbb{Z})^\times$ ist). Da $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ die vier Erzeuger von $\mathbb{Z}/12\mathbb{Z}$ sind, sind die entsprechenenden Potenzen von $\overline{2}$ die Erzeuger von $(\mathbb{Z}/13\mathbb{Z})^\times$. Es folgt:

$$\overline{2},\ \ \overline{2}^5 = \overline{6},\ \ \overline{2}^7 = \overline{2}^3\overline{2}^4 = \overline{8} \cdot \overline{3} = \overline{(-2)},\ \ \overline{2}^{11} = \overline{2}^5\overline{2}^6 = \overline{6} \cdot \overline{64} = \overline{(-6)}$$

sind die vier Erzeuger der Gruppe.

(4) Lösen Sie die simultane Kongruenz, das heißt finden Sie alle $x \in \mathbb{Z}$ so dass

$$x \equiv 17 \pmod{12}$$
$$x \equiv -2 \pmod{11}$$

Lösung: Da 11 und 12 teilerfremd ist, gibt es nach dem Lemma $a, b \in \mathbb{Z}$ mit $1 = a \cdot 11 + b \cdot 12$. In diesem Fall sehen wir eine Lösung für a, b, denn $1 = (-1) \cdot 11 + 1 \cdot 12$. Die erste Kongruenz vereinfachen wir zu $x \equiv 5 \pmod{12}$. Die Lösung ist eine eindeutige Restklasse module $11 \cdot 12 = 132$. Wir definieren nun

$$x_0 := 5 \cdot (-1) \cdot 11 + (-2) \cdot 1 \cdot 12 = -55 - 24 = -79$$

Somit sind nach VL alle $x \in \mathbb{Z}$ mit $x \equiv (-79) \equiv (132 - 79) \equiv 53 \pmod{132}$ die Lösung der simultanen Kongruenz.

(5) Berechnen Sie die Potenzen der Restklassen

$$\overline{11}^{2002} \in \mathbb{Z}/101\mathbb{Z}, \quad \overline{2}^{1234} \in \mathbb{Z}/27\mathbb{Z}, \quad \overline{3}^{1234} \in \mathbb{Z}/27\mathbb{Z}$$

Lösung: Da 101 eine Primzahl ist, sind 11 und 101 teilerfremd und es gilt $\varphi(101) = 101 - 1 = 100$. Nach dem Satz von Fermat gilt damit $\overline{11}^{100} = \overline{1}$. Nun teilen wir 2002 durch 100 mit Rest: $2002 = 20 \cdot 100 + 2$ und erhalten

$$\overline{11}^{2002} = (\overline{11}^{100})^{20}\overline{11}^2 = \overline{11}^2$$

Nun gilt $\overline{11}^2 = \overline{121} = \overline{20} \in \mathbb{Z}/101\mathbb{Z}$.
Es gilt $\varphi(27) = 27 - 9 = 18$. Da 2 und 27 teilerfremd sind, gilt damit nach dem Satz von Fermat $\overline{2}^{18} = \overline{1}$. Nun berechnen wir den Rest bei der Division von 1234 durch 18: Es gilt $1234 \equiv 1 \pmod{9}$ und $1234 \equiv 0 \pmod{2}$ somit muss gelten $1234 \equiv 10 \pmod{18}$ und der Rest bei der Division ist 10, d.h. es gilt $\overline{2}^{1234} = \overline{2}^{10}$. Das Ergebnis können wir jetzt per Hand ausrechnen: $\overline{2}^{10} = \overline{2}^5 \cdot \overline{2}^5 = \overline{32} \cdot \overline{32} = \overline{5} \cdot \overline{5} = \overline{25} \in \mathbb{Z}/27\mathbb{Z}$.

Es gilt 27 teilt 3^n für alle $n \geq 3$, insbesondere auch für $n = 1234$. Dies impliziert $\overline{3}^{1234} = \overline{0} \in \mathbb{Z}/27\mathbb{Z}$.

(6) Eine Lehrerin (mit einer sehr großen Klasse) wendet den RSA mit $N = 34$ und $e = 5$ an beim Geschenkewichteln. Sie nummeriert alle Schüler durch und gibt ihnen dann eine weitere verschlüsselte Nummer. Die ersten drei Schüler erhalten die Nummern $2, 4, 8$. Entschlüsseln Sie die Nummern, um herauszufinden, wem sie ein Geschenk machen sollen.
Lösung: Es gilt $N = 2 \cdot 17$ und damit $\varphi(N) = 16$. Wir berechnen das Inverse von e modulo $16 = \varphi(N)$: Es gilt $1 = (-3)e + \varphi(N)$. Damit ist $d \equiv (-3) \equiv 13 \pmod{16}$ der Exponent zum Entschüsseln. Nun berechnen wir:
$2^{13} \equiv 2^3 \cdot 2^5 \cdot 2^5 \equiv 8 \cdot (-2) \cdot (-2) \equiv 32 \equiv (-2) \pmod{34}$, somit muss der erste Schüler sein Geschenk an den Schüler 32 geben.
$4^{13} \equiv (2^{13})^2 \equiv (-2)^2 \equiv 4 \pmod{34}$. Somit gibt der zweite Schüler sein Geschenk an Schüler 4.
$8^{13} \equiv (2^{13})^3 \equiv (-2)^3 \equiv (-8) \equiv 26 \pmod{34}$. Somit gibt der dritte Schüler sein Geschenk an den Schüler 26.

(7) Beweisen Sie ohne den Hauptsatz zu verwenden, dass $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/9\mathbb{Z}$ nicht isomorph sind.
Beweis: Sind zwei Gruppen isomorph, dann haben sie die gleiche maximale Ordnung eines Elementes. Die maximale Ordnung eines Elementes in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ist laut VL 3, da in jedem der Faktoren die maximale Ordnung 3 ist und somit die maximale Ordnung im Produkt sich als kgV dieser maximalen Ordnungen beschreiben läßt. Die maximale Ordnung eines Elementes in $\mathbb{Z}/9\mathbb{Z}$ ist 9, da sie Gruppe zyklisch ist. Somit sind die beiden Gruppen nicht isomorph. □

(8) Finden Sie die Inversen der folgenden Elemente in den angegebenen multiplikativen Restklassengruppen:

$$10 + 121\mathbb{Z} \in (\mathbb{Z}/121\mathbb{Z})^\times, \quad 17 + 100\mathbb{Z} \in (\mathbb{Z}/100\mathbb{Z})^\times$$

Lösung: Wir teilen 121 durch 10 mit Rest: $121 = 12 \cdot 10 + 1$. Somit ist $1 = 121 + (-12) \cdot 10$. Damit gilt $\overline{(-12)} \cdot \overline{10} = \overline{1} \in \mathbb{Z}/121\mathbb{Z}$. Das impliziert $\overline{10}^{-1} = \overline{(-12)} = \overline{109} \in (\mathbb{Z}/121\mathbb{Z})^\times$. Wir wenden den erweiterten Eukl. Alg. an

$$\begin{aligned} 100 &= 5 \cdot 17 + 15 \\ 17 &= 15 + 2 \\ 15 &= 7 \cdot 2 + 1 \end{aligned}$$

$1 = 15 - 7 \cdot 2 = 15 - 7(17 - 15) = 8 \cdot 15 - 7 \cdot 17 = 8(100 - 5 \cdot 17) - 7 \cdot 17 = 8 \cdot 100 - 47 \cdot 17$. Dies impliziert $\overline{(-47)} \cdot \overline{17} = \overline{1} \in (\mathbb{Z}/100\mathbb{Z})^\times$. Somit ist $\overline{17}^{-1} = \overline{(-47)} = \overline{53} \in (\mathbb{Z}/100\mathbb{Z})^\times$.

(9) Es sei G eine abelsche Gruppe mit Ordnung 81 und die maximale Ordnung eines Elementes in G ist 9. Welche Möglichkeiten gibt es bis auf Isomorphie für G?
Hinweis: Benutzen Sie den Hauptsatz für endliche abelsche Gruppen.
Lösung: Nach dem Hauptsatz gibt es bis auf Isomorphie fünf Gruppen der Ordnung $81 = 3^4$, nämlich
(1.) $\mathbb{Z}/81\mathbb{Z}$,
(2.) $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$,
(3.) $\mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$,
(4.) $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$,

(5.) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
Die maximale Ordnung eines Elementes in $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_3\mathbb{Z} \times \mathbb{Z}/n_4\mathbb{Z}$ (mit $n_i \geq 1$) ist laut Vorlesung $m := \mathrm{kgV}(\mathrm{n}_1, \mathrm{n}_2, \mathrm{n}_3, \mathrm{n}_4)$. Somit berechnen wir (1.) $m = 81$, (2.) $m = 9$, (3.) $m = 27$, (4.) $m = 9$ und (5.) $m = 3$. Für $m = 9$ gibt es also nur die Möglichkeiten (2.) und (4.).

(10) Es sei $G = (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$. Berechnen Sie die Ordnung des Elementes $(\overline{5}, \overline{2})$ in G.
Hinweis: Beachten Sie, dass die Gruppe bezüglich komponentenweiser Multiplikation definiert ist.
Lösung: Die Gruppe G hat $\varphi(8) \cdot \varphi(3) = (8-4)(3-1) = 8$ Elemente. Also ist die Ordnung ein Teiler von 8, diese lauten: $1, 2, 4, 8$. Wir berechnen nun:
$(\overline{5}, \overline{2})^2 = (\overline{25}, \overline{4}) = (\overline{1}, \overline{1}) \in (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$, dies impliziert die Ordnung ist 2.