Technische Universität München
Fakultät für Informatik
Lehrstuhl für Informatik 15
Computergraphik & Visualisierung
Prof. Dr. Rüdiger Westermann
Dr. Werner Meixner

Wintersemester 2007/08
Lösungsblatt 11
30. Januar 2008

Diskrete Strukturen

Hausaufgabe 1 (5 Punkte)

Wir gehen von dem in der Tutoraufgabe 1 von Übungsblatt 10 gegebenen Graphen aus, der die Entfernung zwischen bestimmten Städten beschreibt.

Bestimmen Sie mit dem Algorithmus von Kruskal einen minimalen Spannbaum dieses Graphen.

Lösungsvorschlag

Wir konstruieren einen Spannbaum $T = (V, E_T)$ mit der vorgegebenen Knotenmenge V, bestehend aus den 10 Städten und einer Kantenmenge E_T mit minimaler Summe der Kantengewichte.
Wir beginnen mit $E_T = \emptyset$ und fügen sukzessive zu E_T Kanten mit minimalem Gewicht hinzu, die T kreisfrei belassen.

$$
\begin{array}{lcllcl}
e_1 & = & \{\text{Mannheim}, \text{Karlsruhe}\}, & w(e_1) & = & 68\,, \\
e_2 & = & \{\text{Stuttgart}, \text{Karlsruhe}\}, & w(e_2) & = & 82\,, \\
e_3 & = & \{\text{Köln}, \text{Dortmund}\}, & w(e_3) & = & 83\,, \\
e_4 & = & \{\text{Mannheim}, \text{Frankfurt}\}, & w(e_4) & = & 88\,, \\
e_5 & = & \{\text{Stuttgart}, \text{Ulm}\}, & w(e_5) & = & 92\,, \\
e_6 & = & \{\text{Ulm}, \text{München}\}, & w(e_6) & = & 139\,, \\
e_7 & = & \{\text{Dortmund}, \text{Kassel}\}, & w(e_7) & = & 165\,, \\
e_8 & = & \{\text{München}, \text{Nürnberg}\}, & w(e_8) & = & 167\,, \\
e_9 & = & \{\text{Köln}, \text{Frankfurt}\}, & w(e_9) & = & 189\,.
\end{array}
$$

Hausaufgabe 2 (5 Punkte)

Wir gehen wieder von dem in der Tutoraufgabe 1 von Übungsblatt 10 gegebenen Graphen aus, der die Entfernung zwischen bestimmten Städten beschreibt. Wir nehmen zusätzlich an, dass durch einen Unfall die Verbindung von Nürnberg nach München in beiden Richtungen gesperrt ist.

Bestimmen Sie nun nach dem Algorithmus von Dijkstra die durch den entsprechend modifizierten Verbindungsgraphen gegebene Entfernung zwischen München und Köln.

Lösungsvorschlag

Wir modifizieren die Tabelle der direkten Entfernungen entsprechend der Angabe.

	Dortmund	Frankfurt	Karlsruhe	Kassel	Köln	Nürnberg	Mannheim	München	Stuttgart	Ulm
Dortmund	-	-	-	165	83	-	-	-	-	-
Frankfurt	-	-	-	-	189	228	88	-	-	294
Karlsruhe	-	–	-	-	-	-	68	-	82	-
Kassel	165	-	-	-	-	-	-	-	-	465
Köln	83	189	-	-	-	-	-	-	-	-
Nürnberg	-	228	-	-	-	-	-	~~167~~	-	-
Mannheim	-	88	68	-	-	-	-	-	-	-
München	-	-	-	-	-	~~167~~	-	-	-	139
Stuttgart	-	-	82	-	-	-	-	-	-	92
Ulm	-	294	-	465	-	-	-	139	92	-

Mit dem Algorithmus von Dijkstra berechnet man sukzessive die Entfernungen $u_1, u_2, \ldots$ vom Startknoten s aus zu Knoten $k_1, k_2, \ldots$ beginnend bei dem zum Startknoten nächststehenden Knoten. In jedem Schritt i berechnet man für alle Nachbarn des gerade berechneten Knotens k_i eine neue Entfernung als Länge eines kürzesten Pfades über $s, k_1, k_2, \ldots, k_i$. Wir protokollieren alle Zwischen- und Endergebnisse in der Spalte bzw. Zeile des Startknotens. (Dafür haben wir in der Zeile für München etwas Raum gelassen, der eventuell benötigt wird, wenn Ergebnisse überschrieben werden müssen.)

	Dortmund	Frankfurt	Karlsruhe	Kassel	Köln	Nürnberg	Mannheim	München	Stuttgart	Ulm
Dortmund	-	-	-	165	83	-	-	-	-	-
Frankfurt	-	-	-	-	189	228	88	$u_5 = 433$	-	294
Karlsruhe	-	–	-	-	-	-	68	$u_3 = 313$	82	-
Kassel	165	-	-	-	-	-	-	$u_6 = 604$	-	465
Köln	83	189	-	-	-	-	-	$u_7 = 622$	-	-
Nürnberg	-	228	-	-	-	-	-	-	-	-
Mannheim	-	88	68	-	-	-	-	$u_4 = 381$	-	-
München	769	433	313	604	622	661	381	-	231	139
Stuttgart	-	-	82	-	-	-	-	$u_2 = 231$	-	92
Ulm	-	294	-	465	-	-	-	$u_1 = 139$	92	-

Ergebnis: Die Entfernung zwischen München und Köln beträgt nun 622 Kilometer.
Es ist nicht nötig, die Entfernung München – Dortmund oder München – Nürnberg ebenfalls zu berechnen, denn dadurch kann sich die Entfernung München – Köln nicht mehr ändern.

Hausaufgabe 3 (5 Punkte)

Sei $S' = \langle S, \circ \rangle$ eine Halbgruppe. Dann nennen wir ein Element $x \in S$ vertauschbar in S', falls gilt $(\forall a \in S)\,[\,a \circ x = x \circ a]$. Es sei $V(S')$ die Menge aller in S' vertauschbarer Elemente von S.

Zeigen Sie, dass $V(S')$ eine Unterhalbgruppe von S' erzeugt.

Lösungsvorschlag

Seien $x, y \in V(S')$. Zu zeigen ist $(\forall a \in S)\,[a \circ (x \circ y) = (x \circ y) \circ a]$.
Es gilt

$$\begin{aligned} a \circ (x \circ y) &= (a \circ x) \circ y \\ &= (x \circ a) \circ y \\ &= x \circ (a \circ y) \\ &= x \circ (y \circ a) \\ &= (x \circ y) \circ a)\,. \end{aligned}$$

Hausaufgabe 4 (5 Punkte)

Sei $M = \langle S, \circ \rangle$ ein Monoid mit neutralem Element 1. Wir nehmen an, dass für alle $x \in S$ gilt $x \circ x = 1$.

Zeigen Sie, dass M abelsch ist, d. h., es gilt

$$\forall x, y \in S : x \circ y = y \circ x\,.$$

Lösungsvorschlag

$$\begin{aligned} x \circ y &= 1 \circ x \circ y \circ 1 \\ &= (y \circ y) \circ x \circ y \circ (x \circ x) = y \circ ((y \circ x) \circ (y \circ x)) \circ x = y \circ 1 \circ x \\ &= y \circ x\,. \end{aligned}$$

Hinweis: *Die im Folgenden als Vorbereitung bezeichneten Aufgaben werden nicht bewertet und dienen der häuslichen Vorbereitung der Tutoraufgaben, die ebenfalls nicht bewertet werden. Die Abgabe einer Bearbeitung der Vorbereitungsaufgaben zusammen mit der Bearbeitung der Hausaufgaben wird empfohlen. Tutoraufgaben werden in den Übungsgruppen bearbeitet.*

Vorbereitung 1

Ganze Zahlen $a, b \in \mathbb{Z}$ nennt man kongruent modulo m, mit $m \in \mathbb{N}$, i. Z. $a \equiv b \pmod m$, falls sich a und b um ein ganzzahliges Vielfaches von m unterscheiden, d. h., falls es ein $k \in \mathbb{Z}$ gibt, so dass $a = b + k \cdot m$ gilt. Genau dann wenn $a \equiv b \pmod m$ und gleichzeitig $0 \leq b < m$ gilt, dann gilt $b = a \bmod n$. Diesen Zusammenhang kann man der Definition der Operation mod zugrunde legen.
In enger Beziehung zur mod-Operation steht die ganzzahlige Division a div m zweier Zahlen $a \in \mathbb{Z}, m \in \mathbb{N}$. Es gilt

$$a = (a \text{ div } m) \cdot m + (a \bmod m)\,.$$

1. Zeigen Sie: (i) $5 \text{ div } 2 = 2$, (ii) $(-5) \text{ div } 2 = -3$.

2. Zeigen Sie: Für alle $a \in \mathbb{Z}, m \in \mathbb{N}$ gilt

$$a \text{ div } m = \max\{k \in \mathbb{Z} \mid k \cdot m \leq a\}\,.$$

3. Zeigen Sie die folgende, für den Beweis von Gleichungen modulo einer natürlichen Zahl m nützliche Kennzeichnung der Gleichheit von Zahlen x, y.

   Für alle ganzen Zahlen x, y mit $0 \leq x, y < m$ gilt:

$$x = y \quad \Longleftrightarrow \quad x \equiv y \pmod m\,.$$

Lösungsvorschlag

1. Wir verwenden die Formel für div.

   (i) Seien $a = 5$ und $m = 2$. Dann gilt

$$\begin{aligned} (5 \operatorname{div} 2) \cdot 2 &= (5 - (5 \bmod 2)) \\ &= (5 - 1) \\ &= 4\,, \quad \text{und es folgt} \\ 5 \operatorname{div} 2 &= 2\,. \end{aligned}$$

   (ii) Seien $a = -5$ und $m = 2$. Dann gilt

$$\begin{aligned} ((-5) \operatorname{div} 2) \cdot 2 &= (-5 - ((-5) \bmod 2)) \\ &= (-5 - ((-5 + 3 \cdot 2) \bmod 2)) \\ &= (-5 - 1) \\ &= -6\,, \quad \text{und es folgt} \\ (-5) \operatorname{div} 2 &= -3\,. \end{aligned}$$

2. Wir zeigen für $k := (a \operatorname{div} m)$
   i. $k \cdot m \leq a$.
   ii. $(k+1) \cdot m \not\leq a$.

   i.: Wegen $0 \leq a \bmod m$ folgt

$$k \cdot m = (a \operatorname{div} m) \cdot m \leq (a \operatorname{div} m) \cdot m + a \bmod m = a\,.$$

   ii.: Wegen $m > a \bmod m$ folgt

$$(k+1) \cdot m = k \cdot m + m > k \cdot m + a \bmod m = (a \operatorname{div} m) \cdot m + a \bmod m = a\,.$$

3. Die behauptete Äquivalenz ist gleichbedeutend mit der folgenden Kennzeichnung.

   Für alle ganzen Zahlen x, y mit $0 \leq x, y < m$ gilt:

$$x = y \quad \Longleftrightarrow \quad (\exists k \in \mathbb{Z})\,[y = x + k \cdot m]\,.$$

   $\Rightarrow$: Sei $x = y$. Für $k = 0$ folgt dann $y = x + k \cdot m$.

   $\Leftarrow$: Sei $y = x + km$. Aus $0 \leq x, y < m$ folgt einerseits $y - x < m - x \leq m$, und mithin $y - x < m$. Andererseits folgt analog $x - y < m$. D. h. also $|y - x| < m$. Wir erhalten $m > |y - x| = |k \cdot m|$. Aus der letzten Ungleichung folgt $k = 0$, d. h. $x = y$.

Vorbereitung 2

Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$:

$$\begin{aligned} a &\equiv a \bmod m \pmod m\,, \\ (a+b) \bmod m &= [(a \bmod m) + (b \bmod m)] \bmod m\,. \end{aligned}$$

Lösungsvorschlag

1. Die Kongruenz modulo m ist definiert durch

$$x \equiv y \pmod b \quad :\Longleftrightarrow \quad (\exists k \in \mathbb{Z})\,[\,x = y + k \cdot b\,]\,.$$

   Nach Definition von $a \bmod b$ gilt für ein bestimmtes $k \in \mathbb{Z}$ gilt

$$a \bmod b = a + k \cdot b\,, \quad \text{d. h.} \quad a = a \bmod b + k' \cdot b\,,$$

   mithin

$$a \equiv a \bmod b \pmod b\,.$$

2. Wir setzen nun

$$\begin{aligned} x &:= (a+b) \bmod m\,, \\ y &:= [(a \bmod m) + (b \bmod m)] \bmod m\,. \end{aligned}$$

Es gilt $0 \leq x, y < m$ und

$$\begin{aligned} x &= a + b + k_x \cdot m\,, \\ y &= (a \bmod m) + (b \bmod m) + k_y \cdot m\,, \\ (a \bmod m) &= a + k_a \cdot m\,, \\ (b \bmod m) &= b + k_b \cdot m \end{aligned}$$

für gewisse $k_a, k_b, k_x, k_y \in \mathbb{Z}$. Nun folgt

$$\begin{aligned} y &= a + k_a \cdot m + b + k_b \cdot m + k_y \cdot m \\ &= x - k_x \cdot m + k_a \cdot m + k_b \cdot m + k_y \cdot m \\ &= x + (k_a + k_b + k_y - k_x) \cdot m \\ &= x + k \cdot m\,. \end{aligned}$$

Mit der in Vorbereitungsaufgabe 1 gegebenen Kennzeichnung folgt $x = y$.

Vorbereitung 3

Zeigen Sie, dass im Folgenden Algebren $A = \langle S, \circ \rangle$ definiert werden, die bezüglich dem binären Operator $\circ$ eine Gruppe bilden.

1. Sei $S = \mathbb{R} \setminus \{-1\}$ und für alle $x, y \in S$

$$x \circ y = x + y + xy.$$

2. Sei S gleich der Potenzmenge $\mathcal{P}(X)$ $(= 2^X)$ einer beliebigen Menge X und sei $\circ$ gegeben durch

$$A \circ B = (A \cup B) \setminus (A \cap B).$$

3. Sei $1 < n \in \mathbb{N}$ und $S = Z_n^* = \{p \in \mathbb{Z}_n \mid \mathrm{ggT}(p, n) = 1\}$. $\circ$ sei gleich der Multiplikation ganzer Zahlen modulo n.

Lösungsvorschlag

1. (a) Zunächst ist zu prüfen, ob durch die Gleichung $x \circ y = x + y + x \cdot y$ tatsächlich eine Abbildung von $S \times S$ in S definiert ist.
   Seien $x, y \in \mathbb{R} \setminus \{-1\}$. Es gilt offenbar $x \circ y \in \mathbb{R}$, denn wir können zeigen, dass $-1 = x + y + x \cdot y$ einen Widerspruch ergibt und deswegen $x, y \in \mathbb{R} \setminus \{-1\}$ gelten muss.

$$\begin{aligned} -1 = x + y + x \cdot y \quad &\Rightarrow \quad -1 - y = x(1 + y) \\ &\Rightarrow \quad x = \frac{-1 - y}{1 + y} \\ &\Rightarrow \quad x = -1\,. \end{aligned}$$

(b) Wir zeigen die Assoziativität von $\circ$.

$$\begin{aligned} x \circ (y \circ z) &= x + (y \circ z) + x \cdot (y \circ z) \\ &= x + (y + z + y \cdot z) + x \cdot (y + z + y \cdot z) \\ &= x + y + z + y \cdot z + x \cdot y + x \cdot z + x \cdot y \cdot z \\ &= (x + y + x \cdot y) + z + (x + y + x \cdot y) \cdot z \\ &= (x \circ y) + z + (x \circ y) \cdot z \\ &= (x \circ y) \circ z \,. \end{aligned}$$

(c) $x = 0$ ist das Einselement bezüglich $(x \circ y)$.

$$0 \circ y = 0 + y + 0 \cdot y = y \,.$$

Das linke Einselement ist offensichtlich auch rechtes Einselement, d. h. Einselement.

(d) Wir zeigen, dass zu einem Element $x \in S$ das Inverse gegeben ist durch $x^{-1} = -\frac{x}{1+x}$. Es gilt

$$\begin{aligned} x \circ y = 0 &\Leftrightarrow x + y + x \cdot y = 0 \\ &\Leftrightarrow y = -\frac{x}{1+x} \,. \end{aligned}$$

Die Existenz eines linken Inversen ist damit bewiesen.

Allein schon aus der offensichtlichen Kommutativität folgt hier, dass jedes linke auch rechtes Inverses ist. Es sei aber bemerkt, dass die Beziehung zwischen linken und rechten Inversen auch ohne Kommutativität ganz allgemein in Gruppen untersucht werden kann. Es genügt, allein die Existenz des linken Inversen nachzuweisen.

Damit ist der Nachweis erbracht, dass G eine Gruppe ist.

2. Die Mengenoperation, die hier betrachtet wird, nennt man die Bildung der symmetrischen Mengendifferenz. Wir führen zunächst die Bildung der einfachen Mengendifferenz auf die Komplementbildung innerhalb X zurück, d. h. $A \setminus B = A \cap \overline{B}$ mit $\overline{Y} = X \setminus Y$. Dies hat den Vorteil, die De Morganschen Gesetze anwenden zu können.

Es gilt

$$\begin{aligned} A \circ B &= (A \cup B) \cap (\overline{A \cap B}) \\ &= (A \cup B) \cap (\overline{A} \cup \overline{B}) \\ &= (A \cap \overline{A}) \cup (A \cap \overline{B}) \cup (B \cap \overline{A}) \cup (B \cap \overline{B}) \\ &= (A \cap \overline{B}) \cup (B \cap \overline{A}) \,, \end{aligned}$$

und folglich

$$\overline{A \circ B} = (A \cap B) \cup (\overline{A} \cap \overline{B}) \,.$$

(a) Offensichtlich ist durch die Gleichung $A \circ B = (A \cup B) \setminus (A \cap B)$ eine Abbildung von $S \times S$ in S definiert, denn die gesamte Potenzmenge von X ist als Bildbereich der Verknüpfung zugelassen.

(b) Die Bildung einer mehrfachen symmetrischen Mengendifferenz läßt sich mit drei Mengen A, B, C gut veranschaulichen. Es werden genau jene Elemente erhalten, die entweder in genau einer der Mengen A, B, C sind oder die im Durchschnitt aller 3 Mengen enthalten sind. Dies wird durch folgende Rechnung bestätigt zum Nachweis der Assoziativität:

$$\begin{aligned}(A \circ B) \circ C &= (A \circ B) \cap \overline{C} \cup (\overline{A \circ B}) \cap C \\ &= [(B \cap \overline{A}) \cup (A \cap \overline{B})] \cap \overline{C} \cup [(A \cap \overline{B}) \cup (B \cap \overline{A})] \cap C \\ &= (A \cap \overline{B} \cap \overline{C}) \cup (B \cap \overline{A} \cap \overline{C}) \cup (C \cap \overline{A} \cap \overline{B}) \cup (A \cap B \cap C).\end{aligned}$$

Substituiert man B für A, C für B und A für C, dann erhält man einerseits den Ausdruck $(B \circ C) \circ A$ und andererseits die gleiche Formel wie oben, denn die Formel ist invariant gegenüber der genannten Permutation von Variablen. Also gilt

$$(A \circ B) \circ C = (B \circ C) \circ A = A \circ (B \circ C)\,.$$

(c) Das Einselement der symmetrischen Mengendifferenz ist offensichtlich die leere Menge.

$$A \circ \emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A\,.$$

(d) Die Inverse von A ist A selbst. Es gilt

$$A \circ A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset\,.$$

Damit ist der Nachweis erbracht, dass G eine Gruppe ist.

3. (a) Zunächst ist zu zeigen, dass das Produkt $p \circ q$ zweier Elemente $p, q \in \mathbb{Z}_n^*$ wieder in $\mathbb{Z}_n^*$ liegt. Es ist also zu zeigen

$$\mathrm{ggT}(p, n) = 1 \ \wedge \ \mathrm{ggT}(q, n) = 1 \implies \mathrm{ggT}((p \cdot q) \bmod n, n) = 1\,,$$

wobei $\mathrm{ggT}((p \cdot q) \bmod n, n) = 1$ gleichbedeutend ist mit $\mathrm{ggT}(p \cdot q, n) = 1$. Die folgende Überlegung ist elementar.

Falls $x | (p \cdot q)$ und $x | n$, dann gilt $x = x_1 \cdot x_2$ mit $x_1 | p$ und $x_2 | q$, und natürlich $x_1 | n, x_2 | n$. Mithin gilt $x_1 = 1, x_2 = 1$, falls p und q zu n teilerfremd sind. Damit muss $\mathrm{ggT}(p \cdot q, n) = 1$ gelten.

(b) Die Assoziativität von $\circ$ wird von der Multiplikation modulo n geerbt.

(c) Die 1 ist das Einselement der Multiplikation.

(d) Nun ist die Existenz von Inversen zu zeigen, also, dass für alle $a \in \mathbb{Z}_n^*$ ein $x \in \mathbb{Z}_n^*$ existiert, so dass $a \cdot_n x = 1$ gilt.

Gesetzt den Fall wir hätten ein x und ein y, welche die Gleichung $x \cdot a + y \cdot n = 1$ erfüllen. Dann wäre $x \bmod n$ das Inverse zu a, denn aus $x \cdot a + y \cdot n = 1$ folgt offenbar

$$((x \bmod n) \cdot a) \bmod n = (x \bmod n) \cdot_n a = 1\,,$$

wobei klar ist, dass $\mathrm{ggT}(x, n) = 1$ und damit $\mathrm{ggT}(x \bmod n, n) = 1$, d. h. $x \bmod n \in \mathbb{Z}_n^*$.

Die Existenz des Inversen für ein $a \in \mathbb{Z}_n^*$ folgt also aus

$$(\exists x, y \in \mathbb{Z})\ [\, x \cdot a + y \cdot n = 1 \,],$$

was aber eine Konsequenz aus $\mathrm{ggT}(a, n) = 1$ ist, wie folgendermaßen gezeigt wird.

Sei $U = \{xa + yn \,|\, x, y \in \mathbb{Z}\}$. Offenbar ist U eine Untergruppe von $\mathbb{Z}$, d. h. $U = k \cdot \mathbb{Z}$ für ein bestimmtes $k \in \mathbb{N}_0$ (den Beweis dazu überlassen wir der Hausaufgabe auf Blatt 12). Daraus folgt aber, dass sowohl a als auch n Vielfache von k sind. Also gilt $k \,|\, \mathrm{ggT}(a, n)$. Es folgt $k = 1$. Mithin ist $1 \in U$, d. h. $1 = xa + yn$ für bestimmte $x, y \in \mathbb{Z}$.

Tutoraufgabe 1

Die folgenden Aufgaben stützen sich auf die entsprechenden Vorbereitungsaufgaben.

1. Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$
$$(a \cdot b) \bmod m \;=\; [(a \bmod m) \cdot (b \bmod m)] \bmod m\,.$$
2. Berechnen Sie $(10^{17} + 5^{23} - 30^{100}) \bmod 3$!
3. Bestimmen Sie $2^{7346790100} \bmod 12$!

Lösungsvorschlag

1. Wir setzen
$$\begin{aligned} x &:= (a \cdot b) \bmod m\,, \\ y &:= [(a \bmod m) \cdot (b \bmod m)] \bmod m\,. \end{aligned}$$
Es gilt $0 \le x, y < m$ und
$$\begin{aligned} x &= a \cdot b + k_x \cdot m\,, \\ y &= (a \bmod m) \cdot (b \bmod m) + k_y \cdot m\,, \\ (a \bmod m) &= a + k_a \cdot m\,, \\ (b \bmod m) &= b + k_b \cdot m \end{aligned}$$
für gewisse $k_a, k_b, k_x, k_y \in \mathbb{Z}$. Nun folgt
$$\begin{aligned} y &= (a + k_a \cdot m) \cdot (b + k_b \cdot m) + k_y \cdot m \\ &= x - k_x \cdot m + k_a \cdot m \cdot b + a \cdot k_b \cdot m + k_a \cdot m \cdot k_b \cdot m + k_y \cdot m \\ &= x + (k_a \cdot b + k_b \cdot a + k_a \cdot k_b \cdot m + k_y - k_x) \cdot m \\ &= x + k \cdot m,\,. \end{aligned}$$
Also folgt $x \equiv y (\bmod m)$, und mit der in Vorbereitung 1.3 gegebenen Kennzeichnung folgt $x = y$.
2. Wir benützen die schon bewiesenen Rechenregeln und erhalten
$$\begin{aligned} (10^{17}+5^{23}-30^{100}) \bmod 3 &= [(10 \bmod 3)^{17}+(5 \bmod 3)^{23}-(30 \bmod 3)^{100}] \bmod 3 \\ &= [1^{17} + 2^{23} - 0^{100}] \bmod 3 \\ &= (1 + 4^{11} \cdot 2) \bmod 3 \\ &= (1 + (4 \bmod 3)^{11} \cdot 2) \bmod 3 \\ &= (1 + 2) \bmod 3 = 0\,. \end{aligned}$$
3. Die Potenzen 2^k müssen sich modulo 12 wiederholen. Man rechnet z. B. sofort $2^2 \equiv 2^4 (\bmod 12)$. Also lassen sich die Potenzen $n \ge 4$ von 2 gleichwertig um 2 verringern, d. h. für alle $k \in \mathbb{N}_0$
$$2^{4+k} \equiv 2^{2+k} (\bmod 12)\,.$$
Für gerade, positive Potenzen $n = 2 + 2k$ von 2 ergibt sich per Induktion
$$2^n \equiv 2^2 (\bmod 12)\,.$$
Mithin folgt
$$2^{7346790100} \bmod 12 = 4\,.$$

Tutoraufgabe 2

Zeigen Sie: Die Menge aller Elemente endlicher Ordnung in einer abelschen Gruppe bildet eine Untergruppe.

Lösungsvorschlag

Sei U die Menge aller Elemente endlicher Ordnung einer abelschen Gruppe $\langle G, +, 0\rangle$, d. h. $U = \{x \in G \mid (\exists n \in \mathbb{N})\,[n \cdot x = 0]\}$. Wir zeigen

1. Abgeschlossenheit von U unter $+$: Seien $x, y \in U$, d. h. $mx = 0, ny = 0$ für gewisse $m, n \in \mathbb{N}$. Es folgt $mn(x + y) = 0$, d. h. $x + y \in U$.

2. Neutrales Element in U: Wegen z. B. $1 \cdot 0 = 0$ gilt $0 \in U$.

3. Abgeschlossenheit gegen Inversenbildung: Sei $x \in U$, d. h. $nx = 0$ für ein $n \in \mathbb{N}_0$. Dann gilt auch $nx + n(-x) = 0$, also $n(-x) = 0$, mithin $-x \in U$.

Tutoraufgabe 3

Beweisen Sie die folgenden Aussagen.

1. Jede zyklische Gruppe ist kommutativ.

2. In jeder zyklischen additiven Gruppe mit ungerader Ordnung ist die Summe aller Elemente gleich ihrem neutralen Element 0.

3. Es gibt keine zyklische additive Gruppe mit gerader Ordnung, in der die Summe aller Elemente gleich dem neutralen Element 0 ist.

4. Es gibt keine Gruppe der Ordnung 13, die eine echte Untergruppe enthält, i. e. eine Untergruppe weder von der Ordnung 13, noch von der Ordnung 1.

5. Ist jede Gruppe der Ordnung 13 kommutativ? Begründung!

Hinweis: Eine Gruppe nennt man additiv/multiplikativ, wenn man die Verknüpfung als Summe/Produkt bezeichnen will. Inhaltlich gibt es keinen Unterschied zwischen additiven und multiplikativen Gruppen.

Lösungsvorschlag

1. Sei b ein Generator der zyklischen Gruppe $G = \langle S, \circ\rangle$, d. h. $S = \{b^i \mid i \in \mathbb{Z}\}$. Für alle $x, y \in S$ gibt es dann $n, m \in \mathbb{N}_0$, so dass $x = b^n$ und $y = b^m$. Damit gilt

$$x \circ y = b^n \circ b^m = b^{n+m} = b^{m+n} = b^m \circ b^n = y \circ x\,.$$

2. Vorbemerkung: Der einfachste Beweis der Teilaufgaben 2 und 3 benutzt die Tatsache, dass jede zyklische Gruppe endlicher Ordnung isomorph ist zu $\langle \mathbb{Z}_n, +_n\rangle$. In $\langle \mathbb{Z}_n, +_n\rangle$ aber gilt

$$(\sum_{i=0}^{n-1} i) \bmod n = \left(\frac{n(n-1)}{2}\right) \bmod n = \begin{cases} 0 & : \ n \text{ ungerade,} \\ \frac{n}{2} & : \ n \text{ gerade.} \end{cases}$$

Wir beweisen die Aufgaben nun direkt ohne Benutzung des Isomorphiesatzes.

Für jedes Element a einer Gruppe G gilt, dass $U = \{0, a, a^2, \ldots, a^{\mathrm{ord}(a)-1}\}$ eine Untergruppe von G der Ordnung $\mathrm{ord}(U) = \mathrm{ord}(a)$ ist. Falls G eine zyklische Gruppe der Ordnung n ist mit erzeugendem Element a, dann gilt also $\mathrm{ord}(a) = n$.

Wir schreiben die Gruppe additiv, entsprechend schreiben wir $n \cdot a$ anstelle von a^n. Dann gilt $G = \{0, a, 2a, 3a, \ldots, (n-1)a\}$ mit $|G| = n$.

Zur Summation der Gruppenelemente benutzen wir eine Überlegung von Gauß, indem wir für alle i mit $1 \leq i < n$ die Summation $ia + (n-i)a = na$ durchführen. Wegen $n = \mathrm{ord}(a)$ gilt stets $ia + (n-i)a = na = 0$.

Für ungerades n gilt damit

$$\sum_{i=0}^{n-1} ia = \sum_{i=1}^{\frac{n-1}{2}} (ia + (n-i)a) = 0\,.$$

3. Wir setzen die Überlegung von Teilaufgabe 2 fort und nehmen nun an, dass n gerade ist. Wir zerlegen nun die Summation wie folgt.

$$\sum_{i=0}^{n-1} ia = \left(\sum_{i=1}^{\frac{n}{2}-1} (ia + (n-i)a) \right) + \frac{n}{2}a = \frac{n}{2}a\,.$$

   Da $\frac{n}{2} < \mathrm{ord}(a)$ gilt, folgt $\frac{n}{2}a \neq 0$ mithin $\sum_{i=0}^{n-1} ia \neq 0$.

4. Eine Untergruppe U einer Gruppe G ist echt, wenn sie nicht nur aus dem neutralen Element (Einselement) besteht (einelementige Untergruppe) und nicht gleich G ist. Also ist die Ordnung einer echten Untergruppe nicht 1 und nicht gleich der Ordnung von G. Nach dem Satz von Lagrange ist $\mathrm{ord}(U) \cdot \mathrm{ind}(U) = \mathrm{ord}(G)$. Da $\mathrm{ord}(G) = 13$ eine Primzahl ist, folgt $\mathrm{ord}(U) = 1$ oder $\mathrm{ord}(U) = \mathrm{ord}(G)$, d. h. U ist nicht echte Untergruppe.

5. Jede Gruppe G mit Primzahlordnung ist zyklisch, weil für alle $a \in G$ die Menge $\{a^i \mid i \in \mathbb{Z}\}$ eine Untergruppe von G bildet, die aber bei Primzahlordnung von G nicht echt ist. Für $a \neq 1$ folgt $\{a^i \mid i \in G\} = G$, d. h. G ist zyklisch und damit nach Teilaufgabe 1 kommutativ.