1. Übung zur Vorlesung „Diskrete Strukturen“ (SS 01)

Prof. Dr. H. Pahlings

Lösung zu Aufgabe 2.

Es ist zu zeigen: Für $m, n \in \mathbb{N}_0$ gilt $\displaystyle\sum_{k=0}^{m} \binom{n+k}{k} = \binom{n+m+1}{m}$.

Algebraischer Beweis

Es sei $n \in \mathbb{N}_0$ beliebig. Wir beweisen die Behauptung durch Induktion nach m.

Induktionsanfang: Für $m = 0$ ist

$$\sum_{k=0}^{m} \binom{n+k}{k} = \binom{n}{0} = 1 = \binom{n+1}{0} = \binom{n+m+1}{m}.$$

Induktionsannahme: Es sei $m \geq 0$ und die Behauptung sei bereits bewiesen für m.

Induktionsschritt (Schluss von m auf $m+1$):

$$\begin{aligned}\sum_{k=0}^{m+1} \binom{n+k}{k} &= \sum_{k=0}^{m} \binom{n+k}{k} + \binom{n+m+1}{m+1} \\ &= \binom{n+m+1}{m} + \binom{n+m+1}{m+1} \quad \text{nach Induktionsannahme} \\ &= \binom{n+(m+1)+1}{m+1} \quad \text{nach Vorlesung Kap. I, §1, Satz2.}\end{aligned}$$

Kombinatorischer Beweis

Es sei $M = \{1, \ldots, m+n+1\}$. Für $k = 1, \ldots, m+1$ setzen wir

$$\mathcal{M}_k = \{\, X \in \binom{M}{m} \mid \min(M \setminus X) = k \,\}$$

(das ist die Menge aller m-Teilmengen von M, die die $k-1$ kleinsten Zahlen aus M enthalten, aber nicht die Zahl k selber). Dann ist

$$\binom{M}{m} = \mathcal{M}_1 \,\dot\cup\, \mathcal{M}_2 \,\dot\cup \cdots \dot\cup\, \mathcal{M}_{m+1}$$

und

$$|\mathcal{M}_k| = \binom{(n+m+1)-k}{m-(k-1)} = \binom{n+(m+1-k)}{m+1-k} \quad \text{für } 1 \leq k \leq m+1,$$

also

$$\sum_{k=0}^{m} \binom{n+k}{k} = \sum_{k=0}^{m} |\mathcal{M}_{m+1-k}| = |\binom{M}{m}| = \binom{n+m+1}{m}.$$

2. Übung zur Vorlesung „Diskrete Strukturen“ (SS 01)

Prof. Dr. H. Pahlings

Lösung zu Aufgabe 6.
Es sei $A = \underline{n} = \{1, \ldots, n\}$ und $B = \underline{k} = \{1, \ldots, k\}$. Dann ist $k! \cdot S_{n,k} = |\operatorname{Surj}(A, B)|$ die Anzahl der surjektiven Abbildungen und $k^n = |\operatorname{Abb}(A, B)|$ die Anzahl aller Abbildungen von A nach B. Wir beweisen die gegebene Formel, indem wir die $t := k^n - k! \cdot S_{n,k}$ nicht surjektiven Abbildungen von A nach B abzählen. Dazu betrachten wir für jedes $i \in B$ die Menge

$$X_i = \{f \colon A \to B \mid i \notin \operatorname{Bild} f\}$$

der Abbildungen von A nach B, in deren Bild i nicht enthalten ist. Dann ist

$$t = |X_1 \cup \ldots \cup X_k|.$$

Nach dem Inklusion-Exklusion-Prinzip ergibt sich t zu

$$t = |\bigcup_{i=1}^{k} X_i| = \sum_{j=1}^{k} \sum_{I \in \binom{B}{j}} (-1)^{j+1} |X_I|$$

mit $X_I = \bigcap_{i \in I} X_i$. Da $X_I = \operatorname{Abb}(A, B \setminus I)$ ist, also $|X_I| = (k-j)^n$, ergibt sich

$$t = \sum_{j=1}^{k} (-1)^{j+1} \binom{k}{j} (k-j)^n = \sum_{j=0}^{k-1} (-1)^{k-j+1} \binom{k}{j} j^n$$

(mit Summationsverschiebung $j' = k - j$). Also ist

$$k! \cdot S_{n.k} = k^n + \sum_{j=0}^{k-1} (-1)^{k-j} \binom{k}{j} j^n$$

woraus die Behauptung unmittelbar folgt.

Lösung zu Aufgabe 8.

Die Regeln des Wechselns kann man auch als Permutation der Positionen betrachten:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 9 & 8 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = (1\ 10\ 7\ 4)(2\ 9\ 6\ 3\ 8\ 5) \in S_{10}.$$

(a) Es ist $(1\ 10\ 7\ 4)^4 = id$, aber $(1\ 10\ 7\ 4)^n \neq id$ für $n \in \mathbb{N}$, $n < 4$. Also fährt der erste Fahrer nach vier Wechseln zum ersten Mal wieder vorne.

(b) Für $n \in \mathbb{N}_0$ gilt genau dann $\sigma^n = id$, wenn n ein gemeinsames Vielfaches der Längen der beiden Zyklen von σ ist. Das kleinste gemeinsame Vielfache von 4 und 6 ist 12. Also fahren die Fahrer jeweils nach dem 12., 24., 36., ... Wechsel wieder in der ursprünglichen Reihenfolge. Da es 125 Wechsel gibt, geschieht das zum letzten Mal nach dem 120. Wechsel und damit insgesamt 10 mal.

(c) Die Fahrer wechseln 125 mal. Das entspricht der Permutation

$$\sigma^{125} = \sigma^{10 \cdot 12 + 5} = id^{10} \circ \sigma^5 = (1\,10\,7\,4)(2\,5\,8\,3\,6\,9) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 5 & 6 & 1 & 8 & 9 & 4 & 3 & 2 & 7 \end{pmatrix}.$$

Die Fahrer kommen also in der Reihenfolge 4, 9, 8, 7, 2, 3 ,10, 5, 6, 1 im Ziel an.

5. Übung zur Vorlesung „Diskrete Strukturen“ (SS 01)

Prof. Dr. H. Pahlings

Lösung zu Aufgabe 19.

(a) Ist $A = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ und $s_n = \sum_{k=0}^{n} a_k$ für $n \in \mathbb{N}_0$, so gilt offensichtlich

$$\frac{A}{1-x} = \sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k \cdot 1 \right) x^n = \sum_{n=0}^{\infty} s_n x^n.$$

(b) Mit Hilfe von Folgerung 2 aus §4 erhalten wir

$$\begin{aligned}
\frac{x(1+x)}{(1-x)^3} &= (x+x^2) \sum_{n=0}^{\infty} \binom{n+2}{2} \cdot x^n \\
&= \sum_{n=1}^{\infty} \binom{n+1}{2} x^n + \sum_{n=2}^{\infty} \binom{n}{2} x^n \\
&= \sum_{n=0}^{\infty} \left(\binom{n+1}{2} + \binom{n}{2} \right) x^n \quad \text{(wegen } \binom{k}{2} = 0 \text{ für } k < 2\text{)} \\
&= \sum_{n=0}^{\infty} \frac{n(n+1) + n(n-1)}{2} x^n = \sum_{n=0}^{\infty} n^2 x^n.
\end{aligned}$$

(c) Setzen wir $A = \sum_{n=0}^{\infty} a_n x^n$ mit $a_n = n^2$ und $s_n = \sum_{k=0}^{n} k^2 = \sum_{k=0}^{n} a_k$ für $n \in \mathbb{N}_0$, so folgt

$$\begin{aligned}
\sum_{n=0}^{\infty} s_n x^n &= \frac{A}{1-x} \quad \text{(nach (a))} \\
&= \frac{\sum_{n=0}^{\infty} n^2 x^n}{1-x} = \frac{x(1+x)}{(1-x)^4} \quad \text{(nach (b))} \\
&= (x+x^2) \sum_{n=0}^{\infty} \binom{n+3}{3} x^n \quad \text{(nach §4 Folgerung 2)} \\
&= \sum_{n=1}^{\infty} \binom{n+2}{3} x^n + \sum_{n=2}^{\infty} \binom{n+1}{3} x^n \\
&= \sum_{n=0}^{\infty} \left(\binom{n+2}{3} + \binom{n+1}{3} \right) x^n \quad \text{(wegen } \binom{k}{3} = 0 \text{ für } k < 3\text{)}
\end{aligned}$$

und damit $\sum_{k=0}^{n} k^2 = s_n = \binom{n+1}{3} + \binom{n+2}{3} = \frac{1}{6} n(n+1)(2n+1)$.

9. Übung zur Vorlesung „Diskrete Strukturen“ (SS 01)

Prof. Dr. H. Pahlings

Bemerkung zu Aufgabe 32.

Diese Aufgabe ist völlig analog zu dem Beispiel am Ende von § 5 (Kap. II) der Vorlesung.

Lösung zu Aufgabe 34.

(a) Es soll gezeigt werden, dass $R = \mathbb{Z}[\sqrt{-5}\,] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ein kommutativer Ring ist. Da R in $\mathbb{C}$ liegt und da $\mathbb{C}$ ein Körper und damit erst recht ein kommutativer Ring ist, genügt es zu zeigen, dass R ein Teilring von $\mathbb{C}$ ist, also dass R die Zahlen 0 und 1 enthält und dass mit je zwei Elementen $r_1 = a_1 + b_1\sqrt{-5}$ und $r_2 = a_2 + b_2\sqrt{-5}$ aus R auch die Zahlen $r_1 + r_2$ und $r_1 - r_2$ und $r_1 \cdot r_2$ in R liegen. Dass die ersten vier dieser fünf Bedingungen erfüllt sind, sieht man sofort. Für das Produkt gilt

$$r_1 \cdot r_2 = (a_1 + b_1\sqrt{-5}) \cdot (a_2 + b_2\sqrt{-5}) = (a_1a_2 - 5b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{-5} \in R.$$

Also is R ein kommutativer Ring.

(b) Für $\overline{R} = R/3R$ bildet die Menge $V = \{a + b\sqrt{-5} \mid a, b \in \{0, 1, 2\}\} \subseteq R$ offensichtlich ein vollständiges Vertretersystem. Also hat $\overline{R}$ genau 9 Elemente.

(c) Wir betrachten die Abbildung

$$\varphi\colon (\overline{R}, +) \to (\mathbb{Z}_3 \times \mathbb{Z}_3, +) \quad \text{mit} \quad [a + b\sqrt{-5}\,]_3 \mapsto (\,[a]_3, [b]_3)$$

von der additiven Gruppe $(\overline{R}, +)$ in die additive Gruppe $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$. Diese Abbildung ist einerseits ein (Gruppen-)Homomorphismus, denn für alle $a_1, B_1, a_2, b_2 \in \mathbb{Z}$ gilt

$$\begin{aligned} \varphi((a_1 + b_1\sqrt{-5}) + (a_2 + b_2\sqrt{-5})) &= (\,[a_1 + a_2]_3, [b_1 + b_2]_3)) \\ &= \varphi(a_1 + b_1\sqrt{-5}) + \varphi(a_2 + b_2\sqrt{-5}). \end{aligned}$$

Andererseits ist sie offensichtlich surjektiv und deshalb wegen $|\overline{R}| = |\mathbb{Z}_3 \times \mathbb{Z}_3| = 9 < \infty$ bijektiv. Insgesamt folgt, dass φ ein (Gruppen-)Isomorphismus von $\overline{R}$ auf $\mathbb{Z}_3 \times \mathbb{Z}_3$ ist.

Dieser Isomorphismus erlaubt es uns, die Elemente $[a + b\sqrt{-5}\,]_3$ aus $\overline{R}$ in der Form $(\,[a]_3, [b]_3)$ zu schreiben. Diese Schreibweise vereinfacht sich noch weiter, wenn wir für $[0]_3$, $[1]_3$ und $[2]_3$ einfach 0, 1 und 2 schreiben (und dann natürlich modulo 3 rechnen). Die Multiplikation in $\overline{R}$ sieht in dieser Notation so aus:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1\,a_2 + b_1\,b_2,\ a_1\,b_2 + a_2\,b_1).$$

(d) Jedes Ideal von $\overline{R}$ ist insbesondere eine additive Untergruppe von $\overline{R}$. Um die Ideale zu bestimmen, genügt es also, die additiven Untergruppen zu betrachten, Die „triviale” Untergruppe $U_0 = \{(0, 0)\}$ der Ordnung 1 und die ganze Gruppe $\overline{R}$ der Ordnung 9 sind bekanntlich Ideale. Alle anderen Untergruppen müssen nach dem Satz von Lagrange die Ordnung 3 haben. Es gibt 4 solche Untergruppen,

$$\begin{aligned} U_1 &= \{\,(1, 0), (2, 0), (0, 0)\,\}, \quad & U_3 &= \{\,(1, 1), (2, 2), (0, 0)\,\}, \\ U_2 &= \{\,(0, 1), (0, 2), (0, 0)\,\}, \quad & U_4 &= \{\,(1, 2), (2, 1), (0, 0)\,\}, \end{aligned}$$

und jede dieser Untergruppen ist genau dann ein Ideal, wenn $\overline{R} \cdot U_i \subseteq U_i$ gilt.

Wegen $(1, 1) \cdot (1, 0) = (1, 1)$ und $(1, 1) \cdot (0, 1) = (1, 1)$ ist $\overline{R} \cdot U_1 \not\subseteq U_1$ und $\overline{R} \cdot U_2 \not\subseteq U_2$. Andererseits gilt $(a, b) \cdot (c, c) = (ac + bc, ac + bc)$ und $(a, b) \cdot (c, -c) = (ac - bc, -(ac - bc))$ für alle $a, b, c \in \mathbb{Z}_3$ und damit $\overline{R} \cdot U_3 \subseteq U_3$ und $\overline{R} \cdot U_4 \subseteq U_4$.

$\overline{R}$ hat also genau die 4 Ideale U_0, U_3, U_4 und $\overline{R}$.

Lösung zu Aufgabe 33 (a).

Gegeben sind die simultanen Kongruenzen

$$x \equiv 1 \bmod 4, \qquad x \equiv 2 \bmod 5, \qquad x \equiv 3 \bmod 7.$$

Da die drei Zahlen 4, 5 und 7 paarweise teilerfremd sind, gibt es nach dem chinesischen Restsatz eine Lösung und wir können sie berechnen, indem wir dem (konstruktiven) Beweis dieses Satzes folgen. Benutzen wir dabei die Bezeichnungen aus der Vorlesung, d. h., schreiben wir die gegebenen Kongruenzen in der Form $x \equiv a_i \bmod q_i$ und setzen wir $m = q_1 q_2 q_3$ sowie $q_i' = \frac{m}{q_i}$, so erhalten wir

$$\begin{aligned} &a_1 = 1, \;\; a_2 = 2, \;\; a_3 = 3, \\ &q_1 = 4, \;\; q_2 = 5, \;\; q_3 = 7, \;\; m = 140, \\ &q_1' = 35, \;\; q_2' = 28, \;\; q_3' = 20. \end{aligned}$$

Man sieht leicht (oder berechnet mit dem euklidischen Algorithmus)

$$1 = 9{\cdot}4 + (-1){\cdot}35 = (-11){\cdot}5 + 2{\cdot}28 = 3{\cdot}7 + (-1){\cdot}20.$$

Schreiben wir dafür wieder wie in der Vorlesung jeweils $1 = y_i\, q_i + z_i\, q_i'$, so erhalten wir

$$z_1 = -1, \;\; z_2 = 2, \;\; z_3 = -1$$

und daraus schließlich

$$[x]_m = \left[\sum_{i=1}^{3} a_i\, q_i'\, z_i\right]_m = [\,1{\cdot}35{\cdot}(-1) + 2{\cdot}28{\cdot}2 + 3{\cdot}20{\cdot}(-1)\,]_{140} = [17]_{140}.$$

Also löst jede Zahl der Form $x = 140\,z + 17$ mit $z \in \mathbb{Z}$ die gegebenen simultanen Kongruenzen.

Lösung zu Aufgabe 33 (b).

Es sei jetzt der Zeitpunkt $t_0 = 0$ min. Nach Voraussetzung geben die Sender jeweils zu den Zeitpunkten

$$t_1 = 5\,n_1 - 1 \text{ min}, \;\; t_2 = 7\,n_2 - 4 \text{ min} \;\; \text{und} \;\; t_3 = 11\,n_3 - 10 \text{ min}$$

Signale ab ($n_1, n_2, n_3 \in \mathbb{Z}$). Gesucht ist der erste Zeitpunkt $t \geq 0$, für den die drei simultanen Kongruenzen

$$t \equiv -1 \bmod 5, \qquad t \equiv -4 \bmod 7, \qquad t \equiv -10 \bmod 11$$

gelten. Wir lösen diese Aufgabe ganz analog zur Aufgabe 28 (a) und erhalten der Reihe nach

$$\begin{aligned} &a_1 = -1, \;\; a_2 = -4, \;\; a_3 = -10, \\ &q_1 = 5, \;\; q_2 = 7, \;\; q_3 = 11, \;\; m = 385, \\ &q_1' = 77, \;\; q_2' = 55, \;\; q_3' = 35. \\ &1 = 31{\cdot}5 + (-2){\cdot}77 = 8{\cdot}7 + (-1){\cdot}55 = (-19){\cdot}11 + 6{\cdot}35. \\ &z_1 = -2, \;\; z_2 = -1, \;\; z_3 = 6 \end{aligned}$$

und daraus schließlich

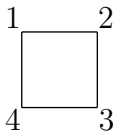
$$[t]_m = \left[\sum_{i=1}^{3} a_i\, q_i'\, z_i\right]_m = [\,(-1){\cdot}77{\cdot}(-2) + (-4){\cdot}55{\cdot}(-1) + (-10){\cdot}35{\cdot}6\,]_{385} = [-1726]_{385}.$$

Gesucht ist die kleinste positive Zahl aus $[-1726]_{385}$, das ist $t = 199$. Also werden die drei Sender in drei Stunden und 19 Minuten zum ersten Mal wieder alle gleichzeitig ein Signal geben.

10. Übung zur Vorlesung „Diskrete Strukturen“ (SS 01)

Prof. Dr. H. Pahlings

Lösung zu Aufgabe 38 (a).



Das abgebildete Quadrat mit den Ecken 1, 2, 3, 4 besitzt offensichtlich acht verschiedene Symmetrieabbildungen, nämlich die Spiegelung an der Mittelhalbierenden der Kanten $\overline{12}$ und $\overline{34}$, die Spiegelung an der Mittelhalbierenden der Kanten $\overline{14}$ und $\overline{23}$, die Spiegelungen an den Diagonalen $\overline{13}$ bzw. $\overline{24}$, die Drehungen im Uhrzeigersinn um den Mittelpunkt des Quadrats um 90°, 180° und 270° und schließlich die identische Abbildung, die alle Ecken fest lässt. Die Symmetriegruppe G hat also acht Elemente. Bezeichnen wir diese in der obigen Reihenfolge mit σ_1, σ_2, τ_1, τ_2, ϱ, ϱ^2, ϱ^3 und ι und schreiben wir sie als jeweils in Form der von ihnen bewirkten Permutation der Ecken, so erhalten wir

$$\begin{array}{llll} \sigma_1 = (1,2)(3,4), & \tau_1 = (2,4), & \varrho = (1,2,3,4), & \varrho^3 = (1,4,3,2), \\ \sigma_2 = (1,4)(2,3), & \tau_2 = (1,3), & \varrho^2 = (1,3)(2,4), & \iota = (1). \end{array}$$

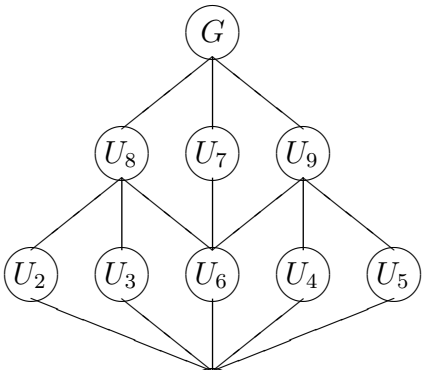
(a) Jedes Element aus G erzeugt eine zyklische Untergruppe von G. Auf diese Weise erhalten wir schon einmal die Untergruppen

$$\begin{aligned} U_1 &= \langle\iota\rangle = \{\iota\}, \\ U_2 &= \langle\sigma_1\rangle = \{\sigma_1, \iota\}, \\ U_3 &= \langle\sigma_2\rangle = \{\sigma_2, \iota\}, \\ U_4 &= \langle\tau_1\rangle = \{\tau_1, \iota\}, \\ U_5 &= \langle\tau_2\rangle = \{\tau_2, \iota\}, \\ U_6 &= \langle\varrho^2\rangle = \{\varrho^2, \iota\}, \\ U_7 &= \langle\varrho\rangle = \langle\varrho^3\rangle = \{\varrho, \varrho^2, \varrho^3, \iota\} \end{aligned}$$

der Ordnungen 1, 2, 2, 2, 2, 2 und 4. Da jede Gruppe der Ordnung 2 zyklisch ist, haben wir damit insbesondere schon alle Untergruppen der Ordnung 2 gefunden. Nach dem Satz von Lagrange können jetzt also nur noch Untergruppen der Ordnung 4 fehlen. Eine solche Untergruppe der Ordnung 4 darf weder ϱ noch ϱ^3 enthalten, da sie sonst schon gleich U_7 wäre. Sie muss daher mindestens zwei Spiegelungen enthalten. Deren Produkt ist dann eine Drehung (da die Ecken nach zwei Spiegelungen wieder im Uhrzeigersinn nummeriert sind), und zwar eine von ι verschiedene Drehung, da die Spiegelungen verschieden sind. Also ist jede der noch fehlenden Untergruppen das Erzeugnis einer Spiegelung und der Drehung ϱ^2. Das ergibt zwei neue Untergruppen

$$\begin{aligned} U_8 &= \langle\sigma_1, \varrho^2\rangle = \langle\sigma_2, \varrho^2\rangle = \{\sigma_1, \sigma_2, \varrho^2, \iota\}, \\ U_9 &= \langle\tau_1, \varrho^2\rangle = \langle\tau_2, \varrho^2\rangle = \{\tau_1, \tau_2, \varrho^2, \iota\} \end{aligned}$$

der Ordnung 4, und weitere kann es dann nicht mehr geben. Die folgende Skizze zeigt die gegenseitigen Inklusionen der Untergruppen.



Lösung zu Aufgabe 38 (b).

(b) Die triviale Untergruppe U_1 und G selbst sind natürlich Normalteiler von G. Aber auch die Untergruppen der Ordnung 4 sind normal in G, denn für sie gilt jeweils $[G:U_i] = 2$ und deshalb $U_i g = U_i = gU_i$ für alle $g \in U_i$ und $U_i g = G \setminus U_i = gU_i$, für alle $g \in G \setminus U_i$. Die Untergruppe U_6 ist ebenfalls ein Normalteiler, denn es ist $g^{-1}\varrho^2 g = \varrho^2 \in U_6$ und $g^{-1}\iota g = \iota \in U_6$ und für alle $g \in G$.

Andererseits sind die Untergruppen U_2 bis U_5 keine Normalteiler, denn wie man leicht anschaulich sieht (oder nachrechnet) ist $\varrho^{-1}\sigma_i\varrho \notin \langle \sigma_i \rangle$ und $\varrho^{-1}\tau_i\varrho \notin \langle \tau_i \rangle$ für $i \in \{1, 2\}$.

Bemerkung: Die Gruppe G aller Spiegelungen und Drehungen eines Quadrats wird im Allgemeinen als „Diedergruppe“ D_8 bezeichnet.

Lösung zu Aufgabe 35.

Ist $n \in \mathbb{N}$ mit $\varphi(n) = 4$ und ist $n = \prod_{i=1}^{s} p_i^{r_i}$ die Zerlegung von n in ein Produkt von paarweise teilerfremden Primzahlpotenzen, so ist $\varphi(n) = \prod_{i=1}^{s}(p_i - 1)p_i^{r_i - 1}$. Also kann n keinen Primteiler größer als 5 und kein Quadrat einer ungeraden Primzahl enthalten, d. h., n hat die Form $n = 2^a\, 3^b\, 5^c$ mit $a \in \mathbb{N}_0$ und $b, c \in \{0, 1\}$. Mit einer kleinen Fallunterscheidung ergibt sich: Ist $b = c = 0$, so ist $n = 8$. Ist $b = 1$, so ist $n = 12$. Ist $c = 1$, so ist $n = 5$ oder $n = 10$.

Für den zweiten Teil der Aufgabe betrachten wir zunächst die beiden Restklassengruppen $\mathbb{Z}_5^*$ und $\mathbb{Z}_{10}^*$. Wegen $[2]_5^2 \neq [1]_5$ und $[3]_{10}^2 \neq [1]_{10}$ sind die Ordnungen von $[2]_5$ und $[3]_{10}$ größer als 2 und damit (als Teiler von 4) gleich 4. Daraus folgt: $\mathbb{Z}_5^*$ und $\mathbb{Z}_{10}^*$ sind beide zyklisch und die Abbildung $\mathbb{Z}_5^* \to \mathbb{Z}_{10}^*$ mit $[2]_5^i \mapsto [3]_{10}^i$ für $i \in \{0, 1, 2, 3\}$ ist ein Isomorphismus.

In $\mathbb{Z}_8^*$ und $\mathbb{Z}_{12}^*$ sind alle Quadrate gleich $[1]_8$ bzw. $[1]_{12}$, diese beiden Gruppen sind also nicht zyklisch. Man sieht (etwa durch Nachrechnen), dass jede bijektive Abbildung von $\mathbb{Z}_8^*$ nach $\mathbb{Z}_{12}^*$, die $[1]_8$ auf $[1]_{12}$ abbildet, ein Isomorphismus ist.

Lösung zu Aufgabe 36.

(a) Es ist $2000 = 2^4 \cdot 5^3$, also $\varphi(2000) = (2-1)\cdot 2^3 \cdot (5-1)\cdot 5^2 = 800$.

(b) Es ist $123 = 3 \cdot 41$, also $1 \in \mathrm{ggT}(123, 2000)$. Nach dem Satz von Euler gilt daher $123^{800} = 123^{\varphi(2000)} \equiv 1 \bmod 2000$. Die gesuchte Zahl x ist demnach die kleinste positive ganze Zahl mit $x \equiv 123^2 = 15129 \bmod 2000$. Das ist offensichtlich $x = 1129$.

Lösung zu Aufgabe 37.

Gegeben sind der Ring $K = \mathbb{Z}_2[x]\,/f\mathbb{Z}_2[x]$ mit $f = x^4 + x^3 + x^2 + x + 1$ und die multiplikative Gruppe G von K. Wegen Grad $f = 4$ hat K 16 Elemente. Nach Aufgabe 27 ist f irreduzibel. Also ist K ein Körper und alle von 0 verschiedenen Elemente aus K sind invertierbar. Somit ist $|G| = 15$, und jedes Element von G hat eine Ordnung, die ein Teiler von 15 ist.

(a) Setzen wir etwa $g = [\,x^3 + x\,]_f$, so ist $g^3 = [\,x\,]_f \neq [1]_f$ und $g^5 = [\,x^3 + x^2\,]_f \neq [1]_f$ und damit $\mathrm{ord}\,(g) \notin \{1, 3, 5\}$. Also ist $\mathrm{ord}\,(g) = 15$ und $\langle g \rangle = G$. Die sämtlichen Erzeugenden von G sind dann gerade alle Potenzen von g mit zu 15 teilerfremden Exponenten, also

$$\begin{aligned} g &= [\,x^3 + x\,]_f, & g^8 &= [\,x^2 + x + 1\,]_f, \\ g^2 &= [\,x^2 + x\,]_f, & g^{11} &= [\,x^3 + x^2 + x\,]_f, \\ g^4 &= [\,x^3 + x + 1\,]_f, & g^{13} &= [\,x^2 + 1\,]_f, \\ g^7 &= [\,x^3 + 1\,]_f, & g^{14} &= [\,x + 1\,]_f. \end{aligned}$$

(b) Es ist zu zeigen: Ist $G = \langle g \rangle$, so ist auch $G = \langle g^2 \rangle$. Die Behauptung folgt mit Satz 2 aus §8 der Vorlesung sofort aus $\mathrm{ord}\,(g) = |G| = 15$ und $1 \in \mathrm{ggT}\,(2, 15)$.