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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 1.

[Vordiplom-Aufgabe 1999.] Beweisen Sie einmal algebraisch und dann kombinatorisch mit Hilfe von Teilmengen die Formel

$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k} \quad \text{für } k \le r \le n \in \mathbb{N}_0$$

und leiten Sie daraus ab:

$$\sum_{k=0}^{r} \binom{n}{k}\binom{n-k}{r-k} = 2^r \binom{n}{r}.$$

Aufgabe 2.

Zeigen Sie: Für $m, n \in \mathbb{N}_0$ gilt

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

Aufgabe 3.

Wie viele $(x_1, \ldots, x_r) \in \mathbb{N}_0^r$ gibt es zu gegebenem $n \in \mathbb{N}$ mit

$$n = x_1 + \cdots + x_r \ ?$$

Geben Sie eine (kurze) kombinatorische Lösung und zusätzlich einen Induktionsbeweis, z. B. unter Benutzung von Aufgabe 2.

Aufgabe 4.

Es sei wie in der Vorlesung für $n \in \mathbb{N}_0$ und $x \in \mathbb{C}$

$$x^{\underline{n}} = x\,(x-1)\cdots(x-n+1) \quad \text{und} \quad x^{\overline{n}} = x\,(x+1)\cdots(x+n-1).$$

Zeigen Sie: Für $x, y \in \mathbb{C}$ gilt

$$(x+y)^{\underline{n}} = \sum_{k=0}^{n} \binom{n}{k} x^{\underline{k}}\, y^{\underline{n-k}} \quad \text{und} \quad (x+y)^{\overline{n}} = \sum_{k=0}^{n} \binom{n}{k} x^{\overline{k}}\, y^{\overline{n-k}}.$$

Abgabe: Mittwoch, den 25. 4., bis 14.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 5.
Zeigen Sie, dass für die Binomialkoeffizienten $\binom{n}{k}$ gilt:

$$\binom{n}{0} < \binom{n}{1} < \ldots < \binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil} > \ldots > \binom{n}{n},$$

wobei wie üblich für $a \in \mathbb{R}$

$$\lfloor a \rfloor = \max\{k \in \mathbb{Z} \mid k \leq a\}$$

und

$$\lceil a \rceil = \min\{k \in \mathbb{Z} \mid a \leq k\}$$

definiert sei.

Aufgabe 6.
Geben Sie einen kombinatorischen Beweis der folgenden Darstellung der Stirlingzahlen zweiter Art an:

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

Hinweis: Zählen Sie mit Hilfe des Inklusion-Exklusion-Prinzips die Anzahl der surjektiven Abbildungen von $\underline{n}$ nach $\underline{k}$.

Aufgabe 7.
Zeigen Sie (z. B. mittels Induktion): $S_{m+n+1,m} = \sum_{k=0}^{m} k\, S_{n+k,k}$.
Vergleichen Sie dies mit Aufgabe 2.

Aufgabe 8.
[Klausuraufgabe TU München 2001.] Zehn befreundete Radrennfahrer nehmen an einem Radrennen der Länge $125,5$ km teil und fahren immer hintereinander. Jeden Kilometer wechseln sie ihre Reihenfolge wie folgt:

- Der erste Fahrer wird der letzte,
- der zweite Fahrer der vorletzte,
- der dritte Fahrer der drittletzte,
- alle anderen Fahrer wechseln um 3 Positionen nach vorne.

(a) Nach wie vielen Wechseln ist zum ersten Mal wieder derselbe Fahrer wie zu Beginn des Rennens an der Spitze? Begründen Sie Ihre Antwort.

(a) Wie häufig kommt es insgesamt im Laufe des Rennens vor, dass alle zehn Radfahrer in derselben Reihenfolge fahren wie zu Beginn des Rennens (die Startaufstellung ist hierbei nicht mit zu zählen)? Begründen Sie Ihre Antwort.

(a) In welcher Reihenfolge kommen die zehn Fahrer ins Ziel? Geben Sie als Antwort neben der Begründung auch die Reihenfolge der Startnummern der Fahrer an, wenn zu Beginn des Rennens der Radfahrer an Position i die Startnummer i hatte.

Abgabe: Montag, den 30. 4., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 9.

Für $n \in \mathbb{N}_0$ sei $B_n = \sum_{k=0}^{n} S_{n,k}$ (die Anzahl aller Partitionen einer n-Menge = Zeilensumme im Stirling-Dreieck 2. Art).

(a) Zeigen Sie: $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.

Anleitung: Betrachten Sie für $k = 0, \ldots, n$ die Menge

$$X_k = \{\mathcal{P} = \{A_1, \ldots, A_l\} \in \mathrm{Part}_l\{1, \ldots, n+1\} \mid n+1 \in A_l,\ |A_l| = k+1,\ l \in \mathbb{N}_0\}.$$

(b) Zeigen Sie mit Hilfe von (a): $\sum_{k=1}^{n} k\, S_{n,k} = \sum_{k=0}^{n-1} \binom{n}{k} B_k$.

Aufgabe 10.

[Vordiplomklausur-Aufgabe September 2000.]

(a) Bestimmen Sie für $n \geq 4$ die Anzahl $F(n, n-3)$ der Permutationen aus S_n mit mindestens $n-3$ Fixpunkten.

(b) Gibt es mehr oder weniger als $2\binom{n+1}{3}$ solcher Permutationen?

Aufgabe 11.

Für $n \in \mathbb{N}$ sei $F_i = \{\sigma \in S_n \mid \sigma(i) = i\}$, und für $I \subseteq \{1, \ldots, n\}$ sei $F_I = \bigcap_{i \in I} F_i$.

(a) Was ist $|F_I|$?

(b) Berechnen Sie

$$f_n = \left| S_n \setminus \bigcup_{i=1}^{n} F_i \right|,$$

also die Anzahl der „fixpunktfreien” Permutationen.

(c) Was ist $\frac{f_{10000}}{10000!}$ ungefähr?

Abgabe: Montag, den 7. 5., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 12.

Es sei $M = \{a, b, c, \ldots, z\}$, $N = \{0, 1\}$ und C_n der „Code”, der aus allen Folgen der Länge k mit $1 \leq k \leq n$ besteht, die man aus $0 < i < k$ Buchstaben aus M gefolgt von $k - i$ Ziffern aus N bilden kann.

Wie viele Folgen der Länge k gibt es in C_n? Was ist $|C_n|$? Es wird eine summationsfreie Darstellung der Ergebnisse (mittels erzeugender Funktionen) verlangt.

Wie groß muss man n machen, wenn man mit C_n einen Text mit 20000 verschiedenen Worten verschlüsseln (d. h. komprimieren) will?

Aufgabe 13.

Berechnen Sie explizit $(1 + x + x^2)^{-1} \in \mathbb{F}_2[[x]]$. Dabei ist $\mathbb{F}_2$ der Körper mit 2 Elementen.

Aufgabe 14.

Es sei $\displaystyle\sum_{n=0}^{\infty} a_n x^n = \frac{4 + x - x^2}{3 - 5x + x^2 + x^3} \in \mathbb{Q}[[x]]$. Bestimmen Sie die a_n.

Anleitung: Faktorisieren Sie den Nenner und finden Sie so $\alpha_1, \alpha_2 \in \mathbb{Q}$ mit

$$3 - 5x + x^2 + x^3 = (\alpha_1 - x)(\alpha_1 - x)(\alpha_2 + x).$$

Bestimmen Sie dann $a, b, c \in \mathbb{Q}$ mit

$$\frac{4 + x - x^2}{3 - 5x + x^2 + x^3} = \frac{a}{\alpha_1 - x} + \frac{b}{(\alpha_1 - x)^2} + \frac{c}{\alpha_2 + x}.$$

Aufgabe 15.

Mr. John F. Moneymaker, der berühmte New Yorker Millionär, hat neulich verraten wie er seine erste Million „gemacht hat”. Er begann völlig mittellos, und nach einem Jahr harter ehrlicher Arbeit betrug sein Nettovermögen genau einen Dollar. Am Ende des zweiten Jahres waren es fünf Dollar. Da beschloss er, in Zukunft in jedem Jahr für das Sechsfache dessen, was er zu Beginn des vorhergehenden Jahres besessen hatte, Waren zu kaufen und sie für das Vierfache dessen, was er zu Beginn des laufenden Jahres besaß, wieder zu verkaufen.

Es sei u_n das Vermögen von Mr. Moneymaker am Ende des n-ten Jahres. Finden Sie eine Rekursionsgleichung für u_n und lösen Sie sie. Wie viele Jahre brauchte Mr. Moneymaker um Millionär zu werden?

Abgabe: Montag, den 14. 5., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 16.
Es sei $\mathrm{D}\colon K[[x]] \to K[[x]]$ wie in der Vorlesung die formale Ableitung. Beweisen Sie die Produktregel

$$\mathrm{D}(A \cdot B) = \mathrm{D}(A) \cdot B + A \cdot \mathrm{D}(B)$$

für $A, B \in K[[x]]$.

Aufgabe 17.

[Vordiplomklausur-Aufgabe März 2001.]

Die Folge $(a_n)_{n\in\mathbb{N}_0}$ sei rekursiv definiert durch $a_0 = 0$, $a_1 = 2$ und $a_n = a_{n-1} + 2\,a_{n-2}$ für alle $n \geq 2$. Bestimmen Sie mit Hilfe der erzeugenden Funktion die explizite Darstellung der Folgenglieder a_n.

Aufgabe 18.
Lösen Sie explizit die folgenden gekoppelten Rekursionsgleichungen mittels erzeugender Funktionen.

$$\begin{aligned} &a_0 = 1, \quad b_0 = 0, \\ &a_n = 3\,a_{n-1} + 2\,b_{n-1}, \\ &b_n = a_{n-1} + b_{n-1}. \end{aligned}$$

Aufgabe 19.

(a) Es sei K ein Körper, $A = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ und $s_n = a_0 + a_1 + \ldots + a_n$ für $n \geq 0$.

Zeigen Sie: $$\sum_{n=0}^{\infty} s_n x^n = \frac{A}{1-x}.$$

(b) Zeigen Sie: $$\sum_{n=0}^{\infty} n^2 x^n = \frac{x(1+x)}{(1-x)^3}.$$

(c) Benutzen Sie (a) und (b) um eine Formel für $\sum_{k=0}^{n} k^2$ herzuleiten.

Abgabe: Montag, den 21. 5., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 20.

Es sei $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in \mathbb{Z}^{2\times 2}$. Zeigen Sie:

(a) $A^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ mit den Fibonaccizahlen F_n.

(b) $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ für $n \geq 1$.

(c) $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ für $n \geq 0$.

Aufgabe 21.

Für $n \in \mathbb{N}_0$ sei $a_n = (1+\sqrt{3})^n + (1-\sqrt{3})^n$.

(a) Zeigen Sie: $a_n \in \mathbb{N}$ für alle n.

(b) Geben Sie eine Rekursionsgleichung für a_n an.

(c) Zeigen Sie: 2^{n+1} teilt a_{2n} und es gilt $a_{2n-1} = 2^n \cdot u_n$ mit ungeradem u_n.

(d) Zeigen Sie: $\lfloor (1+\sqrt{3})^{2n-1} \rfloor$ enthält den Faktor 2^n.

Aufgabe 22.

Lösen Sie die folgende Rekursionsgleichung:

$$a_0 = 1,\ a_1 = 0 \ \text{ und } \ a_n = \sum_{k=2}^{n} a_{k-2}\, a_{n-k} \ \text{ für } \ n \geq 2.$$

Aufgabe 23.

Es sei $\mathcal{P}_{n,k} = \{\, (n_1, \ldots, n_j) \mid k \geq n_1 \geq n_2 \geq \ldots \geq n_j \geq 1,\ n_1 + \cdots + n_j = n,\ j \in \mathbb{N} \,\}$.

Bestimmen Sie die erzeugende Funktion für $|\mathcal{P}_{n,k}|$ für festes $k = 1, 2, 3, \ldots$.

Abgabe: Montag, den 28. 5., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 24.

Wie viele Lösungen hat jeweils die Gleichung $x^3 = x$ bzw. $x^2 + x = 1$
(a) in $\mathbb{Z}_2$, (b) in $\mathbb{Z}_5$, (c) in $\mathbb{Z}_6$?

Aufgabe 25.

In welchen der Ringe (Körper) $\mathbb{Z}_p$ für $p \in \{2, 3, 5, 7\}$ gilt die Implikation

$$a^2 + b^2 = 0 \;\Rightarrow\; a = b = 0\,?$$

Aufgabe 26.

Berechnen Sie mit dem euklidischen Algorithmus einen ggT (größten gemeinsamen Teiler) d von

(a) $f = 13090$ und $g = 6239$ in $R = \mathbb{Z}$,

(b) $f = x^4 + 3x^3 + x^2 + 4$ und $g = x^4 + 2x^3 - x - 2$ in $R = \mathbb{Q}[x]$

und stellen Sie d jeweils in der Form $d = af + bg$ mit $a, b \in R$ dar.

Aufgabe 27.

Berechnen Sie alle irreduziblen Polynome vom Grad ≤ 4 in $\mathbb{Z}_2[x]$.

Abgabe: Montag, den 11. 6., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 28.

Auf $M = \mathbb{N}_0 \times \mathbb{N}_0$ sei die Relation $\sim$ definiert durch $(a,b) \sim (c,d) \Leftrightarrow b - a = d - c$.

(a) Ist $\sim$ eine Äquivalenzrelation? Wenn ja, geben Sie ein vollständiges Vertretersystem der Äquivalenzklassen an (also eine Teilmenge $V \subseteq M$ mit $M = \dot{\bigcup}_{v \in V} [v]_\sim$).

(b) Ist $\sim$ eine Kongruenzrelation des Monoids $(M, +, (0,0))$, wobei

$$(a,b) + (c,d) = (a+c, b+d)$$

für $a,b,c,d \in \mathbb{N}_0$ definiert sei?

Aufgabe 29.

Gibt es Zahlen $a,b,c,d \in \mathbb{N}$ mit $a^2 + b^2 - 3\,c^2 - 3\,d^2 = 0$?

Aufgabe 30.

Es sei R ein Hauptidealring (also ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist).

(a) Zeigen Sie:

$$Ra + Rb = Rd$$

für $d \in \operatorname{ggT}(a,b)$. Insbesondere existieren in einem Hauptidealring stets größte gemeinsame Teiler. Hierbei ist die Summe der Ideale Ra und Rb natürlich so definiert:

$$Ra + Rb = \{ya + zb \mid y \in R, z \in R\}.$$

(b) Definieren Sie analog zum ggT ein kgV und zeigen Sie:

$$Ra \cap Rb = Rd$$

für $d \in \operatorname{kgV}(a,b)$.

Aufgabe 31.

Es sei $R = \mathbb{Z}_2[x]$ und $f = x^3 + 1 \in R$ und

$$\overline{R} = R/fR = \{\, [g]_f \mid g \in R \,\},$$

wobei $[g]_f = g + fR$ ist.

(a) Zeigen Sie: $|\overline{R}\,| = 8$.

(b) Bestimmen Sie alle Einheiten in $\overline{R}$ (also $\overline{R}^{\,*}$).

(c) Bestimmen Sie alle Quadrate in $\overline{R}$.

(d) Wie viele $[g]_f$ in $\overline{R}$ gibt es mit $[g]_f^2 = [g]_f$?

Abgabe: Montag, den 18. 6., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 32.

Es sei $K = \mathbb{Z}_2$ und $f = x^3 + x^2 + 1 \in K[x]$ und $L = K[x]\,/\,fK[x]$ (nach § 5 Satz 2 und Aufgabe 27 ist dies ein Körper mit 8 Elementen). Die Elemente von L werden durch 3 Bits dargestellt:

$$[a_0 + a_1x + a_2x^2]_f \longmapsto a_0\ a_1\ a_2 \quad (a_i \in \mathbb{Z}_2).$$

Berechnen Sie die 3-Bit-Darstellungen der Potenzen $([x]_f)^i$ für $i = 1, 2, \ldots, 7$.

Aufgabe 33.

(a) Bestimmen Sie alle Lösungen in $\mathbb{Z}$ von

$$\begin{aligned} x &\equiv 1 \bmod 4 \\ x &\equiv 2 \bmod 5 \\ x &\equiv 3 \bmod 7. \end{aligned}$$

(b) Drei Sender geben alle 5, 7, beziehungsweise 11 Minuten ein Signal ab. Zuletzt wurden ihre Signale vor 1, 4, beziehungsweise 10 Minuten empfangen. Wann werden das nächste Mal alle drei Signale gleichzeitig empfangen?

Aufgabe 34.

Es sei $R = \mathbb{Z}[\sqrt{-5}\,] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. (Hierbei ist $\sqrt{-5}$ eine komplexe Zahl, deren Quadrat -5 ist.) Zeigen Sie:

(a) R ist ein kommutativer Ring.

(b) $\overline{R} = R/3R$ hat 9 Elemente.

(c) $(\overline{R}, +) \cong (\mathbb{Z}_3 \times \mathbb{Z}_3, +)$ als abelsche Gruppe.

(d) $\overline{R}$ hat genau 4 Ideale.

Abgabe: Montag, den 25. 6., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 35.

Bestimmen Sie alle $n \in \mathbb{N}$ mit $\varphi(n) = 4$ und untersuchen Sie, für welche dieser n die prime Restklassengruppe $\mathbb{Z}_n^*$ zyklisch ist. Welche der Gruppen $\mathbb{Z}_n^*$ mit $\varphi(n) = 4$ sind isomorph? Geben Sie jeweils explizit einen Isomorphismus an.

Aufgabe 36.

[Vordiplomklausur-Aufgabe September 2000.]

(a) Es sei φ die eulersche φ-Funktion. Bestimmen Sie $\varphi(2000)$.

(b) Bestimmen Sie diejenige ganze Zahl x mit $0 \leq x \leq 1999$, die folgende Kongruenz erfüllt:

$$(123)^{802} \equiv x \bmod 2000.$$

Aufgabe 37.

Es sei $K = \mathbb{Z}_2[x] \,/\, f\mathbb{Z}_2[x]$ mit $f = x^4 + x^3 + x^2 + x + 1$ und G die multiplikative Gruppe von K.

(a) Geben Sie mindestens vier erzeugende Elemente von G an in der Form

$$g = [\, a_0 + a_1 x + a_2 x^2 + a_3 x^3 \,]_f \quad \text{mit} \quad a_i \in \mathbb{Z}_2.$$

(b) Zeigen Sie: Ist $G = \langle g \rangle$, so ist auch $G = \langle g^2 \rangle$.

Aufgabe 38.

Es sei G die Symmetriegruppe eines Quadrats, also die Gruppe aller Drehungen und Spiegelungen, die das Quadrat in sich überführen.

(a) Geben Sie alle Untergruppen von G an and machen Sie eine Skizze, aus der die Inklusionen ersichtlich sind.

(b) Welche Untergruppen sind Normalteiler?

Hinweis: Benutzen Sie, dass das Produkt von zwei Spiegelungen eine Drehung ist.

Hinweis.

Beachten Sie, das für die Teilnahme an der Schein- bzw. Test-Klausur am 13. 7. eine Anmeldung bis zum 2. 7. erforderlich ist.

Abgabe: Montag, den 2. 7., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hausaufgaben

Aufgabe 39.

Es seien $p_1, \ldots, p_k$ Primzahlen mit $p_i \equiv 1 \bmod 4$ und q ein Primteiler von $4(p_1 \cdots p_k)^2 + 1$. Zeigen Sie, dass -1 ein Quadrat in $\mathbb{Z}_q$ ist, und folgern Sie daraus, dass es unendlich viele Primzahlen gibt, die kongruent 1 modulo 4 sind.

Aufgabe 40.

Berechnen Sie die Anzahl $N_n(2)$ der irreduziblen Polynome $f \in \mathbb{Z}_2[x]$ vom Grad n für $1 \leq n \leq 10$. Geben Sie für jedes dieser n näherungsweise $\frac{N_n(2)}{A_n(2)}$ an, wobei $A_n(2)$ die Anzahl aller Polynome $f \in \mathbb{Z}_2[x]$ vom Grad n bezeichne.

Aufgabe 41.

Es sei

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

und $C = \{\, c \in \mathbb{Z}_2^7 \mid H \cdot c^T = 0 \,\}$. Was ist $|C|$ und was ist die Minimaldistanz von C? Wie würden Sie $v = [\,0,0,0,1,1,1,1\,]$ korrigieren, d. h., welches $c \in C$ hat minimalen Hamming-Abstand von v?

Aufgabe 42.

Professor Schlaumeier und seine Frau geben eine Party, an der außer ihnen noch fünf weitere Ehepaare teilnehmen. Bei der Begrüßung geben einige Leute einander die Hand, aber natürlich nicht Ehepartner untereinander. Am Schluss der Party fragt der Professor alle anderen, wie vielen Leuten sie jeweils die Hand gegeben haben, und er erhält elf verschiedene Antworten. Wie viele Gäste hat Frau Schlaumeier mit Handschlag begrüßt?

Hinweis.

Wegen des Hochschulsportfests am 11. 7. können wir die Aufgaben dieses Blattes nicht zur üblichen Zeit am Mittwoch Nachmittag besprechen. Wir bieten deshalb einen Ersatztermin dafür an, nämlich Dienstag, den 10. 7., um 8.15 Uhr in Hörsaal I.

Abgabe: Montag, den 9. 7., bis 12.00 Uhr im Übungskasten des Lehrstuhls.

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

Prof. Dr. H. Pahlings

Hinweis.

Die Aufgaben auf diesem Übungsblatt sind ein Angebot an alle, die sich vor der Vordiplomklausur am 7. September noch etwas mit Graphentheorie beschäftigen wollen. Darüberhinaus bieten wir in der vorlesungsfreien Zeit drei Diskussionsstunden an, und zwar am Freitag, dem **24. August**, am Dienstag, dem **28. August**, und am Montag, dem **3. September**, jeweils um **10.00 Uhr im Hörsaal I**. Dort können insbesondere die unten stehenden Aufgaben besprochen werden.

Wer die Scheinklausur bestanden, aber die Hausaufgabenbedingung um höchstens 4 Punkte verfehlt hat, kann diese Bedingung noch nachträglich durch eine sinnvolle Bearbeitung einer entsprechenden Anzahl der neuen Aufgaben erfüllen und damit den Übungsschein erwerben. Die Abgabe der Lösungen (im Geschäftszimmer des Lehrstuhls) muss dazu allerdings vor der ersten Diskussionsstunde, also bis zum 24. August um 10.00 Uhr erfolgen.

Hausaufgaben

Aufgabe 43.

Ist $G = (V, E)$ ein nummerierter Graph und ist $V = \{v_1, \dots, v_n\}$, so heißt $(\mathrm{d}(v_1), \dots, \mathrm{d}(v_n))$ <u>Gradfolge</u> von G.

(a) Gibt es einen Graphen mit Gradfolge

i) $(4, 3, 2, 2, 1)$,

ii) $(3, 3, 3, 1)$,

iii) $(5, 5, 3, 3, 2, 2, 2)$?

(b) Zeigen Sie: Ist $d_1 \geq \cdots \geq d_n$ (mit $d_i \in \mathbb{N}$), so gibt es einen Graphen mit Gradfolge $(d_1, \dots, d_n)$ genau dann, wenn es einen mit Gradfolge $(d_2 - 1, \dots, d_{d_1+1} - 1, d_{d_1+2}, \dots, d_n)$ gibt.

Aufgabe 44.

Ist $G = (V, E)$ ein Graph, so heißt $\overline{G} = (V, \binom{V}{2} \setminus E)$ <u>Komplementärgraph</u> zu G. Man nennt G <u>selbst-komplementär</u>, wenn $G \cong \overline{G}$ ist. Zeigen Sie, dass für einen selbst-komplementären Graphen $G = (V, E)$ die Kongruenz $|V| \equiv 0$ oder $|V| \equiv 1 \bmod 4$ gilt, und bestimmen Sie alle diese Graphen mit $n \leq 8$ Knoten.

Aufgabe 45.

(a) Skizzieren Sie den Baum, der durch den Prüfercode $(2, 2, 2, 3, 9, 3, 3)$ gegeben ist.

(b) Es sei $d_1, \dots, d_n$ eine Folge natürlicher Zahlen mit $\sum_{i=1}^{n} d_i = 2n - 2$. Zeigen Sie, dass die Anzahl der Bäume auf $V = \{1, \dots, n\}$ mit $\mathrm{d}(i) = d_i$ gerade $\dfrac{(n-2)!}{(d_1 - 1)! \cdots (d_n - 1)!}$ ist.

Aufgabe 46.

Zeigen Sie: Ein planarer Graph, in dem es keinen Kreis der Länge 3 gibt, besitzt einen Knoten v vom Grad $\mathrm{d}(v) \leq 3$.

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

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

(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

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

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

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

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

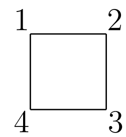
$$[t]_m = \left[\sum_{i=1}^{3} a_i\, q_i'\, z_i\right]_m = [\,(-1)\cdot 77\cdot(-2) + (-4)\cdot 55\cdot(-1) + (-10)\cdot 35\cdot 6\,]_{385} = [-1726]_{385}.$$

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

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

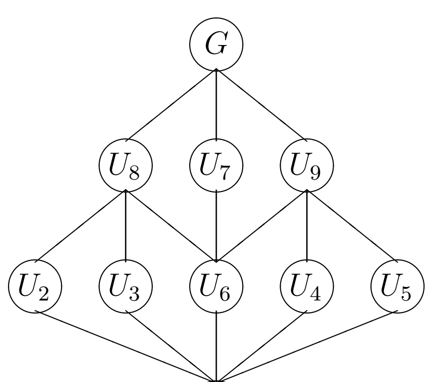
(a) Jedes Element aus G erzeugt eine zyklische Untergruppe von G. Auf diese Weise erhalten wir schon einmal die Untergruppen

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

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 $1 \in \mathrm{ggT}\,(2, 15)$.

Übung zur Vorlesung „Diskrete Strukturen“ (SS 01)

Prof. Dr. H. Pahlings

Präsenzaufgaben für die Übungsstunde am 26. 4. 01

Aufgabe P1.

Zeigen Sie (mit dem Schubfachprinzip): Jede Teilmenge $M \subseteq \{1, \ldots 9\}$ mit $|M| = 6$ enthält zwei Zahlen, deren Summe 10 ist.

Aufgabe P2.

Es sei

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

(a) Schreiben Sie σ als Produkt von ziffernfremden Zyklen.

(b) Zeigen Sie: Sind σ_1, σ_2 ziffernfremde Zyklen, so ist $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

(c) Berechnen Sie σ^{-1}, σ^4, σ^{12}, σ^{123}.

Aufgabe P3.

Schreiben Sie alle Elemente von S_4 als Produkte von ziffernfremden Zyklen und als Produkte von Transpositionen (Zweierzyklen).

Aufgabe P4.

Zeigen Sie:

(a)
$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n},$$

(b)
$$\sum_{k=1}^{n} k \binom{n}{k}^2 = n \binom{2n-1}{n-1}.$$

Präsenzaufgaben am 3. 5. 2001

Aufgabe P5.

Wie viele ungerade Zahlen in $\{1, \ldots, 100\}$ sind weder durch 3 noch durch 5 teilbar? . ☐

Aufgabe P6. An einem Institut sind 10 Professoren und 4 Professorinnen. Wie viele verschiedene paritätisch besetzte Kommissionen mit 4 Mitgliedern kann man bilden? ☐

Aufgabe P7. Welche der folgenden Gleichungen sind richtig?

$\binom{n}{k} = \binom{n}{k-1} + \binom{n}{k-2}$ für $n \geq k \geq 2$ .... ☐ Ja ☐ Nein

$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ .... ☐ Ja ☐ Nein

$\binom{m+n}{k} = \sum_{l=0}^{k} \binom{m}{k-l} \binom{n}{l}$ .... ☐ Ja ☐ Nein

$\sum_{k=0}^{n} S_{n,k} = 2^n$ .... ☐ Ja ☐ Nein

$\sum_{k=0}^{n} s_{n,k} = n!$ .... ☐ Ja ☐ Nein

Aufgabe P8. Es sei $|M| = 4$ und $|N| = 3$. Die Anzahl

der injektiven Abbildungen $f\colon N \to M$ ist .... ☐

der surjektiven Abbildungen $f\colon N \to M$ ist .... ☐

der surjektiven Abbildungen $f\colon M \to N$ ist .... ☐

der surjektiven Abbildungen $f\colon M \to M$ ist .... ☐

der Äquivalenzrelationen auf N ist .... ☐

der surjektiven Abbildungen $f\colon M \to \emptyset$ ist .... ☐

aller Abbildungen $f\colon \emptyset \to M$ ist .... ☐

Aufgabe P9.

Es seien $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix}$ und $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 2 & 4 \end{pmatrix}$ Permutationen aus S_6.

Die Zyklendarstellung von σ ist .... ☐

Die Zyklendarstellung von τ ist .... ☐

Die Zyklendarstellung von $\sigma \circ \tau$ ist .... ☐

Die Zyklendarstellung von σ^2 ist .... ☐

Die Zyklendarstellung von τ^{-1} ist .... ☐

Welches ist das kleinste $n \in \mathbb{N}$ mit $\tau^n = (1)$? .... ☐

Präsenzaufgaben am 10. 5. 2001

Aufgabe P10.

Welche der folgenden formalen Potenzreihen sind invertierbar?

$\sum_{n=0}^{\infty} x^n$ .... ☐ Ja ☐ Nein

$\sum_{n=0}^{\infty} n!x^n$ .... ☐ Ja ☐ Nein

$x + x^2$ .... ☐ Ja ☐ Nein

$\sum_{n=0}^{\infty} n^{n!}x^n$ .... ☐ Ja ☐ Nein

---

Aufgabe P11.

Welche der folgenden Aussagen über formale Potenzreihen sind richtig?

Ist $A = A(x) = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$, so ist

$A(x^2) = \sum_{n=0}^{\infty} a_n x^{2n} \in K[[x]]$ .... ☐ Ja ☐ Nein

$A(x+1) = \sum_{n=0}^{\infty} a_n (x+1)^n \in K[[x]]$ .... ☐ Ja ☐ Nein

$x^3 A(x) = \sum_{n=3}^{\infty} a_{n+3} x^n \in K[[x]]$ .... ☐ Ja ☐ Nein

$(A(x))^2 = \sum_{n=0}^{\infty} a_n^2 x^n \in K[[x]]$ .... ☐ Ja ☐ Nein

$(A(x))^{-1} = \sum_{n=0}^{\infty} a_n x^{-n} \in K[[x]]$ .... ☐ Ja ☐ Nein

$D(A(x)) = \sum_{n=0}^{\infty} a_{n-1} x^n \in K[[x]]$ .... ☐ Ja ☐ Nein

aus $D(A(x)) = 0$ folgt $A = c \in K$ (A ist eine Konstante) .... ☐ Ja ☐ Nein

---

Aufgabe P12.

Wie viele verschiedene Möglichkeiten gibt es, einen Betrag von n (z. B. 50) Euro in 1- und 2-Euromünzen auszuzahlen?

Präsenzaufgaben am 17. 5. 2001

Aufgabe P13.

Gibt es $A \in \mathbb{Q}[[x]]$ mit $A^2 = \sum_{n=0}^{\infty} n!\, x^n$? .... ☐ Ja ☐ Nein

Gibt es für jeden Körper K ein $A \in K[[x]]$ mit $A^2 = 1 + x^2$? .... ☐ Ja ☐ Nein

Gibt es $A \in \mathbb{F}_2[[x]]$ mit $A^2 = 1 + x$? .... ☐ Ja ☐ Nein

Gilt in $\mathbb{F}_2[[x]]$ die Gleichung $\left(\sum_{i=0}^{\infty} a_i x^i\right)^2 = \sum_{i=0}^{\infty} a_i x^{2i}$? .... ☐ Ja ☐ Nein

---

Aufgabe P14.

Ist $f = \sum_{i=0}^{n} a_i x^i \in K[x]$ mit $a_n \neq 0$, so gilt für das reflektierte Polynom f^{R} von f:

$f^{\mathrm{R}} = \sum_{i=0}^{n} a_i x^{n-i}$, ... ☐ Ja ☐ Nein

$f^{\mathrm{R}} = \sum_{i=0}^{n} a_{n-i} x^i$, ... ☐ Ja ☐ Nein

$f^{\mathrm{R}} = \sum_{i=0}^{n} a_{n-i} x^{n-i}$, ... ☐ Ja ☐ Nein

$f^{\mathrm{R}} = x^n \sum_{i=0}^{n} a_i x^i$, ... ☐ Ja ☐ Nein

$f^{\mathrm{R}} = x^n \sum_{i=0}^{n} a_i x^{-i}$, ... ☐ Ja ☐ Nein

$(f^{\mathrm{R}})^{\mathrm{R}} = f$. .... ☐ Ja ☐ Nein

Aufgabe P15.

Für alle $n \in \mathbb{N}$ und $\alpha \in \mathbb{C}$ gilt

$\binom{\alpha}{n} = \binom{\alpha - 1}{n - 1} + \binom{\alpha - 1}{n}$, ... ☐ Ja ☐ Nein

$\binom{\alpha}{n} = \binom{\alpha}{\alpha - n}$, ... ☐ Ja ☐ Nein

$\alpha^n = \sum_{k=0}^{n} S_{n,k}\, k! \binom{\alpha}{k}$, ... ☐ Ja ☐ Nein

$\binom{\alpha}{n} = 0$ für $n > \alpha$. .... ☐ Ja ☐ Nein

Präsenzaufgaben am 31. 5. 2001

Aufgabe P16.

$(\mathbb{N}_0, +, -, 0, \cdot, 1)$ ist ein Ring .... ☐ Ja ☐ Nein

$(\mathbb{Z}, +, -, 0)$ ist eine Gruppe .... ☐ Ja ☐ Nein

$(\mathbb{R}_{>0}, \cdot, {}^{-1}, 1)$ ist eine Gruppe .... ☐ Ja ☐ Nein

$\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist Unterring von $\mathbb{R}$ .... ☐ Ja ☐ Nein

$\{f \in \mathbb{Q}[x] \mid f = 0 \text{ oder } \operatorname{Grad} f \text{ ist gerade}\}$ ist Unterring von $\mathbb{Q}[x]$ .... ☐ Ja ☐ Nein

Aufgabe P17. Die Relation $\sim$, definiert durch $a \sim b$ genau dann wenn

$a + b \in 2\mathbb{Z}$, ist eine Kongruenzrelation auf $\mathbb{Z}$, ... ☐ Ja ☐ Nein

$a - 4b \in 3\mathbb{Z}$, ist eine Kongruenzrelation auf $\mathbb{Z}$, ... ☐ Ja ☐ Nein

$\operatorname{Grad} a = \operatorname{Grad} b$, ist eine Kongruenzrelation auf $\mathbb{Q}[x]$, ... ☐ Ja ☐ Nein

$a(0) = b(0)$, ist eine Kongruenzrelation auf $\mathbb{Q}[x]$, ... ☐ Ja ☐ Nein

$a - b \in \mathbb{Q}$, ist eine Kongruenzrelation auf $\mathbb{R}$, ... ☐ Ja ☐ Nein

Aufgabe P18. Ist K ein Körper und $f, g \in K[x]$, so gilt:

$f = g \iff f(a) = g(a)$ für alle $a \in K$ .... ☐ Ja ☐ Nein

f ist in $K[x]$ invertierbar $\iff f(a) \neq 0$ für alle $a \in K$ .... ☐ Ja ☐ Nein

$\operatorname{Grad}(f \cdot g) = \operatorname{Grad} f \cdot \operatorname{Grad} g$ .... ☐ Ja ☐ Nein

$\{f \in K[x] \mid f(1) = 0\} \trianglelefteq K[x]$ .... ☐ Ja ☐ Nein

$\{f \in K[x] \mid \operatorname{Grad} f \leq 3\} \trianglelefteq K[x]$ .... ☐ Ja ☐ Nein

Aufgabe P19.

In $\mathbb{Z}$ gilt: $2 \in \operatorname{ggT}(2, 0)$ .... ☐ Ja ☐ Nein

In $\mathbb{Z}$ gilt: aus $1 = ya + zb$ mit $a, b, y, z \in \mathbb{Z}$ folgt $1 \in \operatorname{ggT}(a, b)$ .... ☐ Ja ☐ Nein

In $\mathbb{Z}[x]$ gilt: $2 \in \operatorname{ggT}(2x, 2x^2 + 2x)$ .... ☐ Ja ☐ Nein

Ist R ein Ring und $1 \in I \trianglelefteq R$, so ist $I = R$ .... ☐ Ja ☐ Nein

$\{\sum_{i=3}^{\infty} a_i x^i \mid a_i \in \mathbb{R}\} \trianglelefteq \mathbb{R}[[x]]$ .... ☐ Ja ☐ Nein

Aufgabe P20.

Wie viele Elemente hat $\mathbb{Z}/6\mathbb{Z}$? .... ☐

Wie viele Elemente hat $\mathbb{Z}_2[x] \,/\, (x^2 + 1)\mathbb{Z}_2[x]$? .... ☐

Wie viele Lösungen hat die Gleichung $x^2 + y^2 + 4\,z = 3$ in $\mathbb{Z}$? .... ☐

Präsenzaufgaben am 21. 6. 2001

Aufgabe P21. R sei ein kommutativer Ring.

Sind a, b Einheiten ($a, b \in R^*$), so ist ab Einheit. ☐ Ja ☐ Nein

Ist ab Einheit, so sind a und b Einheiten. . . . . ☐ Ja ☐ Nein

Ist $a + b$ Einheit, so sind a und b Einheiten. . . . . ☐ Ja ☐ Nein

Aufgabe P22.

35 ist ein Teiler von $6^{2n} - 1$ für alle $n \geq 1$ . . . . ☐ Ja ☐ Nein

Aufgabe P23. Es sei $f = x^4 + x \in \mathbb{Z}_2[x]$.

Wie viele Elemente hat $\mathbb{Z}_2[x]/f\mathbb{Z}_2[x]$? . . . . ☐

$\mathbb{Z}_2[x]/f\mathbb{Z}_2[x]$ ist ein Körper. . . . . ☐ Ja ☐ Nein

Es sei $\alpha = [x + 1]_f$. Was ist α^4 ? . . . . ☐

Aufgabe P24. Es sei K ein Körper und $f \in K[x]$.

Ist Grad $f > 1$, so ist f irreduzibel genau dann wenn f keine Nullstelle in K hat. . . . . ☐ Ja ☐ Nein

Ist Grad $f = 1$, so ist f irreduzibel. . . . . ☐ Ja ☐ Nein

Ist Grad $f = 0$, so ist f irreduzibel. . . . . ☐ Ja ☐ Nein

Ist Grad $f = 2$ und $f(a) \neq 0$ für alle $a \in K$, so ist f irreduzibel. . . . . ☐ Ja ☐ Nein

Ist $K = \mathbb{C}$, so ist f irreduzibel genau dann wenn Grad $f = 1$. . . . . . . ☐ Ja ☐ Nein

Aufgabe P25.

Ist $(G, \cdot, ^{-1}, 1)$ eine Gruppe und $a, b \in G$, so ist $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$. . ☐ Ja ☐ Nein

$(\mathbb{Z}_n, +, -, 0)$ ist für alle $n \in \mathbb{N}$ eine zyklische Gruppe. . . . . ☐ Ja ☐ Nein

$(\mathbb{Z}_n^*, \cdot, ^{-1}, 1)$ ist für alle $n \in \mathbb{N}$ eine zyklische Gruppe. . . . . ☐ Ja ☐ Nein

Hat eine Gruppe G nur 2 Untergruppen, so ist G zyklisch. . . . . ☐ Ja ☐ Nein

Präsenzaufgaben am 28. 6. 2001

Aufgabe P26. Es sei G eine Gruppe und $|G| = m \in \mathbb{N}$ und $g \in G$.

Die Abbildung $G \to G$, $h \mapsto g \cdot h$ ist bijektiv. ☐ Ja ☐ Nein

Zu jedem Teiler d von m gibt es ein Element der Ordnung d in G. ☐ Ja ☐ Nein

Hat g die Ordung d, so gilt $d \mid m$. ☐ Ja ☐ Nein

Ist m eine Primzahl, so ist G zyklisch. ☐ Ja ☐ Nein

Ist $m = 15$ und $g^3 \neq 1$ und $g^5 \neq 1$, so ist G zyklisch. ☐ Ja ☐ Nein

Ist $\sim$ eine Äquivalenzrelation auf G, so ist $[1]_\sim$ Untergruppe von G. ☐ Ja ☐ Nein

Ist $\sim$ eine Kongruenzrelation auf G, so ist $[1]_\sim$ Normalteiler von G. ☐ Ja ☐ Nein

Ist $\varphi\colon G \to H$ ein Gruppenhomomorphismus, so ist $\mathrm{Kern}(\varphi) \trianglelefteq G$. ☐ Ja ☐ Nein

---

Aufgabe P27.

Für alle $m \in \mathbb{N}$, $a \in \mathbb{Z}$ gilt $a^{\varphi(m)} \equiv a \bmod m$. ☐ Ja ☐ Nein

Für alle $n \in \mathbb{N}$ gilt $70 \mid 101^{6n} - 1$. ☐ Ja ☐ Nein

Für alle $n \in \mathbb{N}$ gilt $70 \mid 1001^{6n} - 1$. ☐ Ja ☐ Nein

Für welche $m \in \mathbb{N}$ ist $\varphi(m)$ ungerade? ☐

Aufgabe P28.

Zu jedem $m \in \mathbb{N}$ gibt es eine Gruppe G mit $|G| = m$. ☐ Ja ☐ Nein

Es gibt eine Gruppe mit genau zwei Elementen der Ordnung 5. ☐ Ja ☐ Nein

Eine Untergruppe einer zyklischen Gruppe ist stets zyklisch. ☐ Ja ☐ Nein

Ein homomorphes Bild einer zyklischen Gruppe ist stets zyklisch. ☐ Ja ☐ Nein

---

Aufgabe P29. Es sei $G = (\mathbb{Z}_{20}, +)$ und $H = \{\, [8n]_{20} \mid n \in \mathbb{Z} \,\}$.

H ist Untergruppe von G. ☐ Ja ☐ Nein

Was ist $|H|$? ☐

Wie viele erzeugende Elemente hat H? ☐

Was ist $[G:H]$? ☐

Es ist $[2]_{20} + H = [6]_{20} + H$. ☐ Ja ☐ Nein

Präsenzaufgaben am 5. 7. 2001

Aufgabe P30. Es sei p eine Primzahl und $n \in \mathbb{N}$. Dann

ist $\mathbb{Z}_{p^n}$ ein Körper, ... ☐ Ja ☐ Nein

ist $\mathbb{Z}_p[x]/(x^n - 1)$ ein Körper, ... ☐ Ja ☐ Nein

gibt es einen Körper mit p^n Elementen, ... ☐ Ja ☐ Nein

gibt es genau ein irreduzibles Polynom $f \in \mathbb{Z}_p[x]$ vom Grad n. ..... ☐ Ja ☐ Nein

---

Aufgabe P31.

Die Anzahl der normierten irreduziblen Polynome vom Grad 3 in $\mathbb{Z}_3[x]$ ist .... ☐

Aufgabe P32. Ist $f \in \mathbb{Z}_p[x]$ irreduzibel mit $\operatorname{Grad} f = d$ und $n \in \mathbb{N}$, so gilt:

wenn $f \mid (x^n - 1)$, so gilt $d \mid n$, ... ☐ Ja ☐ Nein

wenn $f \mid (x^{p^n-1} - 1)$, so gilt $d \mid n$, ... ☐ Ja ☐ Nein

---

Aufgabe P33.

Es sei C der Code über $\mathbb{Z}_2$ mit Generatormatrix $G(C) = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$. Dann gilt:

C ist ein zyklischer Code, ... ☐ Ja ☐ Nein

die Minimaldistanz von C ist 3, ... ☐ Ja ☐ Nein

$\dim C = 3$. .... ☐ Ja ☐ Nein

Aufgabe P34.

Wie viele zyklische Codes C der Länge $n = 3$ gibt es über $\mathbb{Z}_2$ (d. h. $C \subseteq \mathbb{Z}_2^3$)? ...... ☐

Was sind ihre Dimensionen? .... ☐

Was sind ihre Minimaldistanzen? .... ☐

Präsenzaufgaben am 12. 7. 2001

Aufgabe P35.

Wie viele Ideale hat der Ring $\mathbb{Z}_2[x]\,/(x^3+1)$? .... ☐

Aufgabe P36. Ist $G = (V, E)$ ein Graph mit $|V| \geq 2$, so gilt:

Es gibt stets $v_i, v_j \in V$ mit $v_i \neq v_j$ und $d(v_i) = d(v_j)$. .... ☐ Ja ☐ Nein

Ist $\sum_{v \in V} d(v) < |V|$, so ist G nicht zusammenhängend. .... ☐ Ja ☐ Nein

---

Aufgabe P37.

In einer Gruppe von 15 Personen kennt jede Person höchstens 3 andere. Wie viele Paare von Personen, die sich gegenseitig kennen, kann es in dieser Gruppe höchstens geben? ... ☐

Aufgabe P38. Ist $G = (V, E)$ ein nummerierter Graph mit Adjazenzmatrix $A \in \mathbb{Z}^{n\times n}$ und Inzidenzmatrix $B \in \mathbb{Z}^{n\times m}$ und $V = \{\, v_1, \ldots, v_n \,\}$, so ist der Grad $d(v_i)$

die Summe der Einträge der i-ten Spalte von A, ... ☐ Ja ☐ Nein

die Summe der Einträge der i-ten Spalte von B, ... ☐ Ja ☐ Nein

die Summe der Einträge der i-ten Zeile von A, ... ☐ Ja ☐ Nein

die Summe der Einträge der i-ten Zeile von B. .... ☐ Ja ☐ Nein

---

Aufgabe P39.

Ist $G = (V, E)$ ein Graph, so gilt $|V| \leq |E|$. .... ☐ Ja ☐ Nein

Ist $G = (V, E)$ ein Graph, so gilt $|E| \leq |V|^2$. .... ☐ Ja ☐ Nein

Der vollständige Graph K_6 hat 15 Kanten. .... ☐ Ja ☐ Nein

Der vollständige Graph K_6 hat einen 4-regulären induzierten Teilgraphen. ☐ Ja ☐ Nein

Es gibt einen 3-regulären Graphen mit 5 Knoten. .... ☐ Ja ☐ Nein

---

Name: Matrikelnummer:

Klausur zur Vorlesung Diskrete Strukturen (13. 7. 2001)

Professor Dr. H. Pahlings, Lehrstuhl D für Mathematik, RWTH Aachen

---

Ankreuzteil

Aufgabe A1. Es seien $s_{n,k}$ und $S_{n,k}$ die Stirlingzahlen 1. bzw. 2. Art. Dann gilt:

(1) $S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$ für $1 \leq k \leq n$. .... ☐ Ja ☐ Nein

(2) $\sum_{k=0}^{n} s_{n,k} = 2^n$. .... ☐ Ja ☐ Nein

(3) Was ist $S_{4,2}$? .... ☐

Aufgabe A2. Ist $A = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}[[x]]$ eine formale Potenzreihe, so ist:

(1) $A^2 = \sum_{n=0}^{\infty} a_n^2 x^n$ .... ☐ Ja ☐ Nein

(2) $x^2 A = \sum_{n=2}^{\infty} a_{n-2} x^n$ .... ☐ Ja ☐ Nein

(3) A genau dann in $\mathbb{Q}[[x]]$ invertierbar, wenn $a_0 = 1$ ist .... ☐ Ja ☐ Nein

---

Aufgabe A3. Ist K ein Körper und $f \in K[x]$ mit Grad $f \geq 1$, so gilt:

(1) Gibt es kein $c \in K$ mit $(x + c) \mid f$, so ist f irreduzibel. .... ☐ Ja ☐ Nein

(2) Ist $K[x]\,/f\,K[x]$ ein Körper, so ist f irreduzibel. .... ☐ Ja ☐ Nein

(3) $x^3 + x + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel. .... ☐ Ja ☐ Nein

---

Aufgabe A4.

(1) Wie viele Elemente hat $\mathbb{Z}/9\,\mathbb{Z}$? .... ☐

(2) $\mathbb{Z}/9\,\mathbb{Z}$ ist ein Körper. .... ☐ Ja ☐ Nein

(3) Wie viele Elemente hat $\mathbb{Z}_3[x]\,/(x^2 - 1)\,\mathbb{Z}_3[x]$? .... ☐

(4) $\mathbb{Z}_3[x]\,/(x^2 - 1)\,\mathbb{Z}_3[x]$ ist ein Körper. .... ☐ Ja ☐ Nein

---

Aufgabe A5.

Es sei C der Code über $\mathbb{Z}_2$ mit der Generatormatrix $G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$.

(1) Was ist die Dimension von C? .... ☐

(2) C ist zyklisch. .... ☐ Ja ☐ Nein

(3) Die Minimaldistanz von C ist 3. .... ☐ Ja ☐ Nein

Aufgabe A6. Gibt es einen Graphen $G = (V, E)$ mit $|V| \leq 5$ und

(1) $\sum_{v \in V} \mathrm{d}(v) = 9$? .... ☐ Ja ☐ Nein

(2) $\sum_{v \in V} \mathrm{d}(v) = 22$? .... ☐ Ja ☐ Nein

(3) Adjazenzmatrix A mit $A^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$? .... ☐ Ja ☐ Nein

---

Rechenaufgaben ohne Begründung

Aufgabe R1. (7 Punkte)

(1) Wie viele injektive Abbildungen $f\colon \{1,2\} \to \{1,2,3,4\}$ gibt es? ....

(2) Wie viele surjektive Abbildungen $f\colon \{1,2,3,4\} \to \{1,2,3\}$ gibt es? ....

(3) Wie viele injektive Abbildungen $f\colon \{1,2,3,4\} \to \{1,2,3,4\}$ gibt es? ....

Aufgabe R2. (4 Punkte)

Es seien die Permutationen $a = (1\ 2\ 5)\,(3\ 6\ 7\ 8\ 4)$ und $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 3 & 8 & 1 & 4 & 2 & 6 \end{pmatrix}$ aus S_8 gegeben.

(1) Die Zyklendarstellung von c ist ....

(2) Die Ordnung von a ist ....

(3) Die Zyklendarstellung von a^3 ist ....

(4) Die Zyklendarstellung von a^{3001} ist ....

Aufgabe R3. (4 Punkte)

Berechnen Sie einen größten gemeinsamen Teiler d der Zahlen 532 und 434 und stellen Sie ihn in der Form $d = a \cdot 532 + b \cdot 434$ mit $a, b \in \mathbb{Z}$ dar. ....

Aufgabe R4. (8 Punkte)

(1) Es sei φ die eulersche φ-Funktion. Berechnen Sie $\varphi(60)$. ....

(2) Wie viele Einheiten (invertierbare Elemente) hat der Ring $\mathbb{Z}/60\,\mathbb{Z}$? ....

(3) Bestimmen Sie die kleinste Zahl $n \in \mathbb{N}_0$ mit $n \equiv 7^{162} \bmod 60$. ....

Aufgabe R5. (6 Punkte)

(1) Die Anzahl der irreduziblen Teiler von $x^{2^5} - x \in \mathbb{Z}_2[x]$ ist ....

(2) Die Anzahl der irreduziblen Polynome vom Grad 5 über $\mathbb{Z}_2$ ist ....

Aufgabe R6. (5 Punkte)

Wie viele Ideale hat der Ring $\mathbb{Z}_2[x]\,/(x^5+1)\,\mathbb{Z}_2[x]$? ....

Aufgaben mit Lösungsweg

Aufgabe L1. (8 Punkte)

Die Folge $(a_n)_{n\in\mathbb{N}_0}$ sei rekursiv definiert durch $a_0 = 0$, $a_1 = 2$ und $a_n = -a_{n-1} + 2\,a_{n-2}$ für alle $n \geq 2$. Bestimmen Sie mit Hilfe der erzeugenden Funktion die explizite Darstellung der Folgenglieder a_n.

Aufgabe L2. (6 Punkte)

Geben Sie explizit einen Isomorphismus $\psi\colon \mathbb{Z}_{220} \to \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{11}$ an und berechnen Sie

$$\psi([135]_{220}), \quad \psi([187]_{220}) \quad \text{und} \quad \psi([135\cdot 187]_{220}).$$

Benutzen Sie dies, um $[135]_{220} \cdot [187]_{220}$ in $\mathbb{Z}_{220}$ auszurechnen.

Ankreuzteil

Aufgabe A1. Es seien $s_{n,k}$ die Stirlingzahlen 1. Art. Dann gilt:

$s_{n,k} = s_{n-1,k-1} + k \cdot s_{n-1,k}$ für $1 \le k \le n$. ☐ Ja ☐ Nein

$\sum_{k=0}^{n} s_{n,k} = n!$. ☐ Ja ☐ Nein

$s_{n,n-1} = \binom{n}{2}$ für $n \ge 1$. ☐ Ja ☐ Nein

$s_{4,2}$ hat den Wert ☐

Aufgabe A2. Es sei $\mathbb{Q}[[x]]$ der Ring der formalen Potenzreihen über $\mathbb{Q}$. Dann gilt:

$\frac{x}{1+x} \in \mathbb{Q}[[x]]$. ☐ Ja ☐ Nein

$\frac{1+x}{x} \in \mathbb{Q}[[x]]$. ☐ Ja ☐ Nein

Ist $A = \sum_{i=0}^{\infty} a_i x^i$, so ist $x^3 A = \sum_{i=3}^{\infty} a_{i-3} x^i$. ☐ Ja ☐ Nein

Ist $A = \sum_{i=0}^{\infty} a_i x^i$, so ist $A^2 = \sum_{i=0}^{\infty} a_i^2 x^i$. ☐ Ja ☐ Nein

Aufgabe A3. Es sei K ein Körper und $f \in K[x]$. Dann gilt:

Ist $\operatorname{Grad} f = 0$, so ist f irreduzibel in $K[x]$. ☐ Ja ☐ Nein

Ist $\operatorname{Grad} f = 1$, so ist f irreduzibel in $K[x]$. ☐ Ja ☐ Nein

Hat f in K keine Nullstelle, so ist f irreduzibel in $K[x]$. ☐ Ja ☐ Nein

$x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel. ☐ Ja ☐ Nein

Aufgabe A4. Es sei $f = x^4 + 1 \in \mathbb{Z}_2[x]$ und $R = \mathbb{Z}_2[x] \,/\, f\,\mathbb{Z}_2[x]$. Dann gilt:

Die Anzahl der Elemente von R ist ☐

R ist ein Körper. ☐ Ja ☐ Nein

Das Inverse von $[x^2 + x + 1]_f$ in R ist $[x^3 + x^2 + 1]_f$. ☐ Ja ☐ Nein

Die Anzahl der Teiler von f in $\mathbb{Z}_2[x]$ ist ☐

Aufgabe A5.

Ist $G = (V, E)$ ein zusammenhängender Graph, so ist $|V| \le |E| + 1$. ☐ Ja ☐ Nein

Es gibt einen 3-regulären Graphen mit 7 Knoten. ☐ Ja ☐ Nein

Die Anzahl der Kanten des vollständigen Graphen K_6 ist ☐

Rechenaufgaben ohne Begründung

Aufgabe R1. (4 Punkte)

Die Anzahl der injektiven Abbildungen $f\colon \{1,2,3\} \to \{1,2,3,4,5\}$ ist ☐

Die Anzahl der surjektiven Abbildungen $f\colon \{1,2,3,4\} \to \{1,2\}$ ist ☐

Aufgabe R2. (4 Punkte)

Es seien die Permutationen $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 3 & 8 & 9 & 4 & 2 & 5 & 6 \end{pmatrix}$ aus S_9 und $b = (1\ 4\ 6)\,(2\ 3\ 7\ 5)$ aus S_7 gegeben.

Die Zyklendarstellung von a ist .... ☐

Die Ordnung von b ist .... ☐

Die Zyklendarstellung von b^{-1} ist .... ☐

Die Zyklendarstellung von b^{27} ist .... ☐

Aufgabe R3. (4 Punkte)

Berechnen Sie einen größten gemeinsamen Teiler d von $f = x^4 + 1$ und $g = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$ und stellen Sie ihn in der Form $d = a \cdot f + b \cdot g$ mit $a, b \in \mathbb{Z}_2[x]$ dar. Geben Sie d, a und b an.

$d =$	$a =$	$b =$

Aufgabe R4. (5 Punkte)

Es sei φ die eulersche φ-Funktion. Berechnen Sie $\varphi(100)$. .... ☐

Bestimmen Sie die kleinste Zahl $n \in \mathbb{N}_0$ mit $n \equiv 13^{162} \bmod 100$. .... ☐

Aufgabe R5. (5 Punkte) Es sei C der binäre zyklische Code der Länge 7 mit Generatorpolynom $g = x^3 + x + 1$, also

$$C = \{\, (c_i)_{i=0}^{6} \mid \left[\sum_{i=0}^{6} c_i x^i\right]_{x^7-1} = [g \cdot h]_{x^7-1} \text{ für ein } h \in \mathbb{Z}_2[x] \,\}.$$

Die Dimension von C ist .... ☐

Die Anzahl der Codeworte in C ist .... ☐

Die Minimaldistanz von C ist .... ☐

$(1,1,0,0,0,0,0)$ wird decodiert als .... ☐

Aufgabe R6. (5 Punkte)

Es sei (V, E) der Baum mit der Knotenmenge $V = \{1, \ldots, 6\}$ und dem Prüfercode $(2, 3, 3, 2)$. Geben Sie die Nachbarn von 3 an, also die Menge $\{a \in V \mid \{a, 3\} \in E\}$. .... ☐

Aufgaben mit Lösungsweg

Aufgabe L1. (8 Punkte)

Die Folge $(a_n)_{n \in \mathbb{N}_0}$ sei rekursiv definiert durch $a_0 = 1$, $a_1 = 1$ und $a_n = a_{n-1} + 2\,a_{n-2} \in \mathbb{Q}$ für $n \geq 2$. Bestimmen Sie mit Hilfe der erzeugenden Funktion die explizite Darstellung der Folgenglieder a_n.

Aufgabe L2. (8 Punkte)

Es sei φ die eulersche φ-Funktion. Bestimmen Sie alle ungeraden natürlichen Zahlen n mit $\varphi(n) = 6$. Für welche dieser n ist die prime Restklassengruppe $\mathbb{Z}_n^*$ zyklisch? Geben Sie jeweils alle erzeugenden Elemente $[a]_n$ dieser Gruppe an.

Ankreuzteil

Aufgabe A1. Es seien $s_{n,k}$ die Stirlingzahlen 1. Art. Dann gilt:

$s_{n,k} = s_{n-1,k-1} + k \cdot s_{n-1,k}$ für $1 \le k \le n$. ☐ Ja ☐ Nein

$\sum_{k=0}^{n} s_{n,k} = n!$. ☐ Ja ☐ Nein

$s_{n,n-1} = \binom{n}{2}$ für $n \ge 1$. ☐ Ja ☐ Nein

$s_{4,2}$ hat den Wert ☐

Aufgabe A2. Es sei $\mathbb{Q}[[x]]$ der Ring der formalen Potenzreihen über $\mathbb{Q}$. Dann gilt:

$\frac{1+x}{x} \in \mathbb{Q}[[x]]$. ☐ Ja ☐ Nein

$\frac{x}{1+x} \in \mathbb{Q}[[x]]$. ☐ Ja ☐ Nein

Ist $A = \sum_{i=0}^{\infty} a_i x^i$, so ist $A^2 = \sum_{i=0}^{\infty} a_i^2 x^i$. ☐ Ja ☐ Nein

Ist $A = \sum_{i=0}^{\infty} a_i x^i$, so ist $x^3 A = \sum_{i=3}^{\infty} a_{i-3} x^i$. ☐ Ja ☐ Nein

Aufgabe A3. Es sei K ein Körper und $f \in K[x]$. Dann gilt:

Hat f in K keine Nullstelle, so ist f irreduzibel in $K[x]$. ☐ Ja ☐ Nein

Ist Grad $f = 0$, so ist f irreduzibel in $K[x]$. ☐ Ja ☐ Nein

Ist Grad $f = 1$, so ist f irreduzibel in $K[x]$. ☐ Ja ☐ Nein

$x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel. ☐ Ja ☐ Nein

Aufgabe A4. Es sei $f = x^4 + 1 \in \mathbb{Z}_2[x]$ und $R = \mathbb{Z}_2[x] \,/\, f\,\mathbb{Z}_2[x]$. Dann gilt:

Die Anzahl der Teiler von f in $\mathbb{Z}_2[x]$ ist ☐

Das Inverse von $[x^2 + x + 1]_f$ in R ist $[x^3 + x^2 + 1]_f$. ☐ Ja ☐ Nein

Die Anzahl der Elemente von R ist ☐

R ist ein Körper. ☐ Ja ☐ Nein

Aufgabe A5.

Es gibt einen 3-regulären Graphen mit 7 Knoten. ☐ Ja ☐ Nein

Ist $G = (V, E)$ ein zusammenhängender Graph, so ist $|V| \le |E| + 1$. ☐ Ja ☐ Nein

Die Anzahl der Kanten des vollständigen Graphen K_6 ist ☐

Rechenaufgaben ohne Begründung

Aufgabe R1. (4 Punkte)

Die Anzahl der injektiven Abbildungen $f\colon \{1,2,3\} \to \{1,2,3,4,5\}$ ist ☐

Die Anzahl der surjektiven Abbildungen $f\colon \{1,2,3,4\} \to \{1,2\}$ ist ☐

Aufgabe R2. (4 Punkte)

Es seien die Permutationen $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 4 & 8 & 9 & 3 & 1 & 5 & 6 \end{pmatrix}$ aus S_9 und $b = (1\ 4\ 6\ 2)\,(3\ 7\ 5)$ aus S_7 gegeben.

Die Zyklendarstellung von a ist .... $\boxed{}$

Die Ordnung von b ist .... $\boxed{}$

Die Zyklendarstellung von b^{-1} ist .... $\boxed{}$

Die Zyklendarstellung von b^{27} ist .... $\boxed{}$

Aufgabe R3. (4 Punkte)

Berechnen Sie einen größten gemeinsamen Teiler d von $f = x^4 + 1$ und $g = x^2 + x + 1$ in $\mathbb{Z}_2[x]$ und stellen Sie ihn in der Form $d = a \cdot f + b \cdot g$ mit $a, b \in \mathbb{Z}_2[x]$ dar. Geben Sie d, a und b an.

$d =$	$a =$	$b =$

Aufgabe R4. (5 Punkte)

Es sei φ die eulersche φ-Funktion. Berechnen Sie $\varphi(100)$. .... $\boxed{}$

Bestimmen Sie die kleinste Zahl $n \in \mathbb{N}_0$ mit $n \equiv 11^{162} \bmod 100$. .... $\boxed{}$

Aufgabe R5. (5 Punkte) Es sei C der binäre zyklische Code der Länge 7 mit Generatorpolynom $g = x^3 + x + 1$, also

$$C = \{\, (c_i)_{i=0}^{6} \mid \left[\sum_{i=0}^{6} c_i x^i\right]_{x^7-1} = [g \cdot h]_{x^7-1} \text{ für ein } h \in \mathbb{Z}_2[x] \,\}.$$

Die Dimension von C ist .... $\boxed{}$

Die Anzahl der Codeworte in C ist .... $\boxed{}$

Die Minimaldistanz von C ist .... $\boxed{}$

$(1, 1, 0, 1, 0, 0, 0)$ wird decodiert als .... $\boxed{}$

Aufgabe R6. (5 Punkte)

Es sei (V, E) der Baum mit der Knotenmenge $V = \{1, \dots, 6\}$ und dem Prüfercode $(2, 3, 3, 2)$. Geben Sie die Nachbarn von 2 an, also die Menge $\{a \in V \mid \{a, 2\} \in E\}$. .... $\boxed{}$

Aufgaben mit Lösungsweg

Aufgabe L1. (8 Punkte)

Die Folge $(a_n)_{n \in \mathbb{N}_0}$ sei rekursiv definiert durch $a_0 = 1$, $a_1 = 0$ und $a_n = a_{n-1} + 2\,a_{n-2} \in \mathbb{Q}$ für $n \geq 2$. Bestimmen Sie mit Hilfe der erzeugenden Funktion die explizite Darstellung der Folgenglieder a_n.

Aufgabe L2. (8 Punkte)

Es sei φ die eulersche φ-Funktion. Bestimmen Sie alle ungeraden natürlichen Zahlen n mit $\varphi(n) = 6$. Für welche dieser n ist die prime Restklassengruppe $\mathbb{Z}_n^*$ zyklisch? Geben Sie jeweils alle erzeugenden Elemente $[a]_n$ dieser Gruppe an.