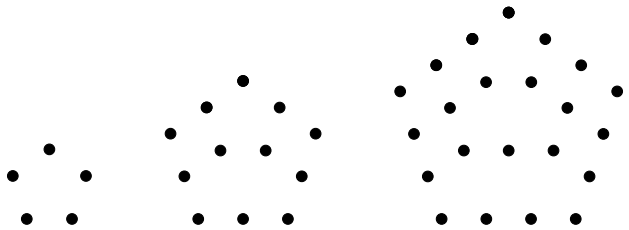
Aufgabe 1. Beweise durch vollständige Induktion die folgende Identität:

$$\sum_{k=1}^{n}(3k-2) = \frac{n(3n-1)}{2}.$$

Zusatzaufgabe. Finde die Folge $\left(\frac{n(3n-1)}{2}\right)_{n\in\mathbb{N}}$ in der *On-line Encyclopedia of Integer Sequences*[1] und erkläre den Zusammenhang mit den folgenden Diagrammen:



Welche Zahlen erhält man, wenn man für n negative Werte einsetzt?

Aufgabe 2. Zeige durch vollständige Induktion: Für jedes $n \in \mathbb{N}$ ist die Zahl

$$10^{2n-1} + 3^{4n-2}$$

durch 19 teilbar.

Aufgabe 3. Der Divisionssatz besagt, dass es für jedes Zahlenpaar $m \in \mathbb{N}$ und $n \in \mathbb{N}$ eindeutig bestimmte Zahlen $q \in \mathbb{N}_0$ und $r \in \{0, 1, \ldots, m-1\}$ gibt, sodass $n = qm + r$.

Verfasse einen Algorithmus mit Input (m, n) und Output (q, r), der lediglich die folgenden Operationen/Abfragen verwendet:

- Addition $(+)$
- Subtraktion $(-)$
- Abfrage, ob eine Gleichung oder Ungleichung erfüllt ist $(=, <, \leq)$.

Führe den Algorithmus an der Tafel mit dem Input $m = 22$ und $n = 153$ durch.

Aufgabe 4. Bestimme alle Zahlen $m, n \in \mathbb{N}$, für die gilt

(a) $\mathrm{ggT}(m, n) = 7$ und $\mathrm{kgV}(m, n) = 2730$.
(b) $\mathrm{ggT}(m, n) = 1$ und $\mathrm{kgV}(m, n) = 36$.

Hinweis: Die Identität $\mathrm{ggT}(m, n) \cdot \mathrm{kgV}(m, n) = m \cdot n$ darf verwendet werden.

[1] `www.oeis.org`

Aufgabe 5. Finde mithilfe des euklidischen Algorithmus für die folgenden Zahlenpaare (m, n) den größten gemeinsamen Teiler d und Zahlen a und b, sodaß $am + bn = d$.

(a) $(231, 142)$ (b) $(228, 141)$

(c) $(89, 55)$ (d) $(2023, 314)$

Aufgabe 6. Sei F_n die Folge der Fibonacci-Zahlen, gegeben durch die Rekursion

$$F_0 = F_1 = 1 \qquad F_{n+1} = F_n + F_{n-1}$$

Zeige, daß $\mathrm{ggT}(F_n, F_{n+1}) = 1$ für jedes n (Induktion).

Aufgabe 7. Zeige, daß $2^n - 1$ keine Primzahl ist, wenn n keine Primzahl ist.

Aufgabe 8. Zeige: Wenn $k \geq 6$ und sowohl $k - 1$ als auch $k + 1$ Primzahlen sind, dann ist k durch 6 teilbar.

Aufgabe 9. Finde (mit dem Computer[2]) die kleinste Zahl $n \in \mathbb{N}$, für die $n^2 + n + 41$ *keine* Primzahl ist.

[2]Der entsprechende Code/die Vorgangsweise ist zu präsentieren!

Untersuche in den folgenden Aufgaben, welche der angegebenen Relationen die Eigenschaften Reflexivität, Symmetrie, Antisymmetrie, Transitivität, Äquivalenzrelation oder Halbordnungsrelation erfüllen und bestimme ggf. die Äquivalenzklassen.

Aufgabe 10.
(a) $X = \mathbb{N}$ Relation $mRn \iff 2 \mid m \cdot n$
(b) $X = \mathbb{Z}$, $xRy \iff x \cdot y > 0$.
(c) X eine beliebige Menge, Relation $xRy \iff x \neq y$.

Aufgabe 11. $X = \{a, b, c, d\}$, R entsprechend der folgenden Tabelle:

	a	b	c	d
a	×			
b	×	×	×	×
c	×		×	×
d				×

Aufgabe 12. Sei $X = \{1, 2, 3, 4, 5, 6\}$. Bilde die kleinste Äquivalenzrelation auf A, die die Elemente $(1, 3)$, $(6, 3)$ und $(4, 5)$ enthält. Bestimme die Äquivalenzklassen und ein Repräsentantensystem.

Aufgabe 13. Sei X eine Menge und R eine Relation auf X. Die *inverse Relation* R^{-1} ist definiert durch

$$xR^{-1}y \quad \iff \quad yRx.$$

Die *Verknüpfung* zweier Relationen $S = R_1 \cdot R_2$ ist definiert durch

$$xSy \quad \iff \exists z : xR_1z \wedge zR_2y$$

Sei X eine Menge von Personen und R die Relation

$$xRy \quad \iff \quad x \text{ ist ein Kind von } y$$

Welche Relationen stellen die Verknüpfungen $R \cdot R$, $R^{-1} \cdot R$ und $R \cdot R^{-1}$ dar?

Aufgabe 14. Zeige die *Elferprobe*: Eine Zahl $n \in \mathbb{Z}$ ist genau dann durch 11 teilbar, wenn die alternierende Quersumme durch 11 teilbar ist, d.h., mit der Ziffernentwicklung

$$n = \sum a_i 10^i$$

ist n durch 11 teilbar genau dann, wenn

$$\sum a_i (-1)^i$$

durch 11 teilbar ist.

Aufgabe 15. Es gibt zwei Standards der *Internationalen Standardbuchnummer*.

(1) Die alte ISBN-10 hat 10 Ziffern, $x_1x_2x_3\cdots x_{10}$, mit $x_1, x_2, \ldots, x_9 \in \{0, 1, \ldots, 9\}$ und $x_{10} \in \{0, 1, \ldots, 9\} \cup \{X\}$, wobei das Symbol X für den Wert 10 steht und die letzte Ziffer x_{10} eine Prüfziffer ist, sodaß

$$x_1 + 2x_2 + 3x_3 + \cdots + 9x_9 + 10x_{10} \equiv 0 \mod 11$$

(2) Die neue ISBN-13 hat 13 Ziffern, $z_1z_2z_3$-$z_4\cdots z_{13}$, wobei $z_i \in \{0, 1, \ldots, 9\}$ und der Präfix $z_1z_2z_3$ entweder 978 oder 979 ist und die letzte Ziffer z_{13} eine Prüfziffer ist, sodaß

$$z_1 + 3z_2 + z_3 + 3z_4 + \cdots z_{11} + 3z_{12} + z_{13} \equiv 0 \mod 10.$$

(a) Berechne die Prüfziffern der folgenden unvollständigen ISBN

310403060

978-0-676-97800

(b) Erkläre, warum auch die Regel

$$10x_1 + 9x_2 + 8x_3 + \cdots + 2x_9 + x_{10} \equiv 0 \mod 11$$

für die Überprüfung einer ISBN-10 verwendet werden kann.

(c) Begründe, daß die Prüfziffer einer ISBN-10 nach einem Eingabefehler (d.h., eine Ziffer falsch oder 2 benachbarte Ziffern vertauscht) nicht mehr korrekt ist.

(d) Gilt das auch für ISBN-13?

Aufgabe 16. Berechne, wenn möglich, $[13]_{91}^{-1}$, $[15]_{91}^{-1}$ und $[16]_{91}^{-1}$.

Aufgabe 17. Für welche $n \in \mathbb{N}$ ist $43 \equiv 1 \mod n$?

Aufgabe 18. Bestimme alle Lösungen $x \in \mathbb{Z}$ der Gleichungen

(a) $15x \equiv 10 \mod 25$

(b) $15x \equiv 9 \mod 25$

Aufgabe 19. Bestimme alle Lösungen $(x, y) \in \mathbb{Z}^2$ des linearen Gleichungssystems

$$\begin{aligned} 4x + 2y &\equiv 5 \mod m \\ 3x + 5y &\equiv 5 \mod m \end{aligned} \quad \text{für} \quad (a)\ m = 7 \qquad (b)\ m = 11$$

Aufgabe 20. Bestimme alle Lösungen der diophantischen Gleichung

$$63x - 12y = 15$$

Aufgabe 21. Löse das Kongruenzgleichungssystem

$$\begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 2 \mod 7 \\ x &\equiv 3 \mod 8 \end{aligned}$$

Aufgabe 22. Löse, wenn möglich, die folgenden Kongruenzgleichungssysteme

$$(a)\quad \begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 9 \\ x &\equiv 1 \mod 10 \end{aligned} \qquad (b)\quad \begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 3 \mod 9 \\ x &\equiv 2 \mod 10 \end{aligned}$$

Aufgabe 23. Bestimme, wenn möglich, alle Lösungen der folgenden Kongruenzgleichungssysteme.

(a)
$$\begin{aligned} x &\equiv 1 \mod 6 \\ x &\equiv 5 \mod 14 \\ x &\equiv 13 \mod 15 \\ x &\equiv 33 \mod 35 \end{aligned}$$

(b)
$$\begin{aligned} x &\equiv 1 \mod 6 \\ x &\equiv 9 \mod 14 \\ x &\equiv 13 \mod 15 \\ x &\equiv 33 \mod 35 \end{aligned}$$

Aufgabe 24. Berechne $2^{31} \mod 3465$.
Hinweis:
(1) 3465 in Primfaktoren $p_i^{k_i}$ zerlegen.
(2) $2^{31} \mod p_i^{k_i}$ für alle Primfaktoren berechnen.
(3) Die Lösung mit dem chinesischen Restsatz ermitteln.

Aufgabe 25. Welche der folgenden Strukturen $(X, \circ)$ bilden Halbgruppen, Monoide, Gruppen? In welchen gilt das Kommutativgesetz? Bestimme ggf. das neutrale Element, die invertierbaren Elemente und die jeweiligen Inversen.

a. $(\mathbb{Q}, \circ)$ mit $x \circ y = x + 2y$
b. $(\mathbb{N}, \circ)$ mit $x \circ y = \max(x, y)$.
c. $(\mathbb{N}, \circ)$ mit $x \circ y = \min(x, y)$.
d. $(\mathbb{N}_0, \circ)$ mit $x \circ y = |x - y|$.
e. $(\mathbb{R} \setminus \{-1\}, \circ)$ mit $x \circ y = x + y + xy$.
f. X beliebig, $x \circ y = x$.
g. Sei U eine Menge, und $X = \{A : A \subseteq U\}$ die *Potenzmenge* ausgestattet mit der Verknüpfung
$$A \circ B = A \cap B$$
h. X wie vorher mit der Verknüpfung
$$A \circ B = A \Delta B := (A \setminus B) \cup (B \setminus A)$$

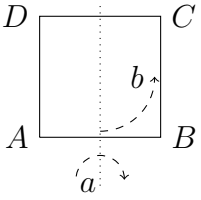
Aufgabe 26. Ergänze die folgende Verknüpfungstabelle so, daß die Gruppenaxiome erfüllt sind. Welches ist das neutrale Element? Ist die Gruppe abelsch?

$\circ$	a	b	c	d
a		d	a	b
b	d	c		
c	a	b		d
d			d	

Es kann die Tatsache verwendet werden, daß genau eine Lösung existiert.

Aufgabe 27. Wir betrachten das Quadrat $ABCD$ und seine Symmetrien. Wir bezeichnen mit a und b die Transformationen

$$\begin{aligned} a : A &\mapsto B \\ B &\mapsto A \\ C &\mapsto D \\ D &\mapsto C \end{aligned} \qquad \begin{aligned} b : A &\mapsto B \\ B &\mapsto C \\ C &\mapsto D \\ D &\mapsto A \end{aligned}$$



(a) Zeige, daß $b \circ a = a \circ b^3$.
(b) Stelle alle Transformationen des Quadrats in der Form $a^m \circ b^n$ dar.
(c) Erstelle die Verknüpfungstabelle.
(d) Bestimme die Linksnebenklassen der Untergruppe $\{e, a\}$.

Aufgabe 28. Berechne $\varphi(2023)$ und $\varphi(10125000)$.

Aufgabe 29. Ermittle ohne Taschenrechner Zahlen a, b, c, sodaß

$$(25^4)^{2023} \equiv a \mod 77 \qquad (25^{(4^{2023})} \equiv b \mod 77 \qquad 14^{(2023^{2023})} \equiv c \mod 60.$$

Hinweis: Sollte der Satz von Euler-Fermat nicht direkt anwendbar sein, den chinesischen Restsatz wie in Aufgabe 24 anwenden!

Aufgabe 30. (a) Berechne die Eulersche Funktion $\varphi(m)$ für die Zahl $m = 6885$.
(b) Zeige, daß $a^{\varphi(81)+1} \not\equiv a \mod 81$ genau dann gilt, wenn $\mathrm{ggT}(a, 81) \in \{3, 9, 27\}$.
(c) Zeige, daß $a^{\varphi(6885)+1} \not\equiv a \mod 6885$ genau dann gilt, wenn $\mathrm{ggT}(a, 81) \in \{3, 9, 27\}$. *Hinweis*: Chinesischer Restsatz!
(d) Überprüfe diese Tatsachen am Computer für $a \in \{1, 2, \ldots, 6885\}$.

Aufgabe 31 (Asmuth-Bloom-Verfahren)**.** Der chinesische Restsatz kann verwendet werden, um ein Geheimnis auf n Personen so aufzuteilen, daß mindestens k Personen nötig sind, um es zu lösen. Hier ist $n = 3$ und $k = 2$.

- Wähle positive teilerfremde Zahlen $m_0 < m_1 < m_2 < m_3$, sodaß $m_0 m_3 < m_1 m_2$.
- Das Geheimnis ist eine Zahl $0 \leq r < m_0$. Wähle eine zufällige natürliche Zahl t, sodass $a = r + t m_0 < m_1 m_2$.
- Berechne $c_i = a \mod m_i$ für $i = 1, 2, 3$.
- Die Zahl m_0 ist öffentlich bekannt, das Geheimnis wird wie folgt aufgeteilt: Alice erhält (c_1, m_1), Bob erhält (c_2, m_2) und Charlie erhält (c_3, m_3).
- Um die geheime Zahl r wiederherzustellen, müssen mindestens zwei, zum Beispiel Alice und Bob, gemeinsam das Gleichungssystem

$$\begin{aligned} x &\equiv c_1 \mod m_1 \\ x &\equiv c_2 \mod m_2 \end{aligned}$$ lösen und können dann $r = x \mod m_0$ berechnen.

(a) Begründe, warum am Ende $x = r \mod m_0$ ist. Worauf ist dabei zu achten?
(b) Seien konkret $m_0 = 5$, $m_1 = 7$, $m_2 = 9$, $m_3 = 11$. Angenommen, Alice erhält das Paar $(0, 7)$ und Bob erhält das Paar $(6, 9)$. Wie lautet das Geheimnis r? Kann t rekonstruiert werden? Welches Paar (c_3, m_3) hat Charlie erhalten?
(c) Angenommen, Charlie erhält das Paar $(8, 11)$ und die Information, daß $0 \leq t \leq 5$ ist (er kennt m_1 und m_2 nicht). Welche möglichen Werte hat r?

Aufgabe 32. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 31$, $g = 7$, $a = 13$, $b = 11$.
(b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$g = 8 \qquad p = 29$$
$$m = 10 \qquad n = 16$$

Bestimme die geheimen Parameter a, b und den Schlüssel r!

Aufgabe 33. Erstelle ein Schema des Diffie-Hellman-Merkle-Schlüsselaustauschs für drei Teilnehmer, sodaß am Ende alle drei Teilnehmer den gleichen Schlüssel haben. Wie kann man die ausgetauschten Botschaften so bündeln, daß möglichst wenige Kontakte getätigt werden müssen?

Führe den Austausch anhand des Beispiels $p = 41$, $g = 11$, $a = 11$, $b = 12$, $c = 13$ durch (Computer erlaubt).

Aufgabe 34. Gegeben sei $m = 1363$.

(a) Welche der folgenden Zahlen sind als öffentliche RSA-Schlüssel geeignet (Begründung!)?

$$r = 21 \qquad r = 23 \qquad r = 25$$

Berechne die zugehörigen inversen Schlüssel.

(b) Wähle einen geeigneten Schlüssel und verschlüssle die Botschaft

"FAKENEWS"

mit der Konvention aus der Vorlesung (Bsp (11.8); ohne Störzeichen).

(c) Die folgende Nachricht wurde mit dem Schlüssel $r = 17$, $m = 1363$ verschlüsselt.

$$[579, 304, 816]$$

Finde den inversen Schlüssel s und entschlüssle die Botschaft.

Hinweis: Für die Zwischenrechnungen ist ein Computer erlaubt.

Aufgabe 35. Die Ver- und Entschlüsselungen beim RSA-Verfahren können effizienter gestaltet werden, wenn man die Potenzfunktionen $e_m(x, k) = x^k \mod m$ zunächst die Funktionen $e_p(x, k) = x^k \mod p$ und $e_q(x, k) = x^k \mod q$ berechnet und dann das Ergebnis mit Hilfe des chinesischen Restsatzes ermittelt. Verwende dieses Prinzip, um die folgende Aufgabe ohne elektronische Hilfsmittel zu lösen:

Für den RSA-Algorithmus wurde der öffentliche Schlüssel $m = 119$ und $r = 13$ bekanntgegeben.

(a) Verschlüssle die Nachricht $(14, 42)$.

(b) Berechne den Geheimschlüssel s und entschlüssle die Botschaft.

(c) Berechne eine digitale Signatur für die Nachricht $(33, 5)$.

Aufgabe 36. Begründe, warum im RSA-Verfahren anstelle von $\phi(m) = (p-1)(q-1)$ auch die Zahl $\lambda(m) = \text{kgV}(p-1, q-1)$ verwendet werden kann.

Hinweis: Chinesischer Restsatz!

Aufgabe 37. Das folgende Beispiel illustriert, daß die Wahl kleiner Schlüssel die Sicherheit des RSA-Verfahrens verringert.

Tom schickt die gleiche Botschaft an seine Freunde Basti, Siggi und Wolfi, die ihm vorher die öffentlichen Schlüssel $(m_1 = 1003, r_1 = 3)$, $(m_2 = 1081, r_2 = 3)$ und $(m_3 = 1189, r_3 = 3)$ bekanntgegeben haben. Die drei verschlüsselten Botschaften sind jeweils $y_1 = (38, 163, 327)$, $y_2 = (426, 955, 989)$ und $y_3 = (891, 728, 144)$. Entschlüssle die Botschaft, ohne die Primfaktorzerlegung der Schlüssel m_i durchzuführen (Computer oder Taschenrechner für Zwischenrechnungen ist zugelassen).

Aufgabe 38. Überprüfe anhand von Wahrheitstafeln, ob die folgenden Aussageformen äquivalent sind:

(a) $(A \to B) \to C$ und $A \to (B \to C)$

(b) $(\neg A \to B) \to (B \vee C)$ und $(A \to B) \vee C$.

Aufgabe 39.
(a) Formalisiere folgende Aussagen mittels Aussagenlogik.
- Von A, B und C gilt genau eines.
- Von A, B und C gelten genau zwei.
- Von A, B und C gilt mindestens eines.

(b) Bestimme jeweils die n-KNF und die n-DNF.

Aufgabe 40. Bestimme die n-KNF und die n-DNF der Formel $(A \vee B) \to C$

Aufgabe 41. Der Speiseplan einer Mensa folgt folgenden Regeln:
(i) Wenn es keine Mehlspeise gibt, dann muß es eine Suppe geben.
(ii) Wenn es Suppe und Mehlspeise gibt, dann gibt es keinen Salat.
(iii) Wenn es Salat gibt oder keine Mehlspeise dabei ist, darf es keine Suppe geben.

Stelle die Bedingungen als logische Aussageformen P_1, P_2, P_3 dar und bestimme eine möglichst einfache Formel, die zu $P_1 \wedge P_2 \wedge P_3$ äquivalent ist.

Aufgabe 42. Graf Orlofsky wurde letzten Donnerstag zwischen 11:00 und 13:00 aus dem Fenster seiner Jacht ins Meer gestürzt und ist ertrunken. Der Koch ist um 12:00 vom Vordeck ins Innere der Jacht gekommen und hat nichts bemerkt. Um am Koch vorbeizukommen, muß der Mörder entweder am Vormittag mit einem Schlüssel über den Steg und durch die Eingangstür in die Jacht gekommen sein oder am Nachmittag aus einem Boot direkt durchs Fenster eingestiegen sein. Inspektor Kottan vermutet einen der drei Erben Alois, Bob oder Clemens als Mörder. Alois hat als einziger einen Schlüssel, kann aber wegen seines Gipsfußes nicht durchs Fenster gestiegen sein. Alois und Bob haben beide ein Alibi für den Vormittag, aber keines nach 12 und Clemens hat kein Alibi für die Zeit vor 12, wohl aber am Nachmittag. Wer von den dreien kommt als Mörder in Frage?

Hinweis: Präzise Aussagen formulieren (wie S: "M hat einen Schlüssel", F: "M kann durchs Fenster steigen", etc.), zu einer logischen Formel verknüpfen und nacheinander die Hypothesen überprüfen, daß A, B, oder C der Mörder ist.

Aufgabe 43. Orpheus steht in der Unterwelt vor drei Türen, von denen genau eine in die Freiheit führt.
- Auf der linken Tür steht: hier geht es hinaus.
- Auf der mittleren Tür steht: rechts geht es nicht hinaus.
- Auf der rechten Tür steht: hier geht es nicht hinaus.

Mindestens eine Aufschrift ist wahr und mindestens eine Aufschrift ist falsch. Wo geht es hinaus?

Aufgabe 44. Beweise mit den Regeln des logischen Schließens[3] den **Modus Tollens**

$$((P \to Q) \wedge \neg Q) \to \neg P.$$

Aufgabe 45. Zeige durch logisches Schließen, dass die folgenden drei Formeln äquivalent sind:

$$A \to (B \to C) \qquad B \to (A \to C) \qquad (A \wedge B) \to C$$

[3]siehe `https://www.math.tugraz.at/idm-lv/dmi/2023/Uebungsblaetter/logikregeln.pdf`

Aufgabe 46. Bestimme die Menge der Folgerungen, die aus der Prämissenmenge

$$P_1 :\iff A \to (B \to C)$$
$$P_2 :\iff A \vee ((B \wedge C) \vee (\neg B \wedge \neg C))$$
$$P_3 :\iff B \to C$$

hergeleitet werden können.

Aufgabe 47. Entscheide mittels Resolutionskalkül/DPLL, ob die folgenden Aussageformen erfüllbar sind und bestimme alle gültigen Belegungen.

(a) $(C \vee \neg D) \wedge (A \vee B) \wedge (\neg B \vee \neg C) \wedge (\neg A \vee B) \wedge (\neg B \vee C \vee D)$

(b) $(C \to (A \vee B)) \wedge (C \vee D) \wedge (A \to D) \wedge (B \to A) \wedge (\neg B \vee \neg D)$

Aufgabe 48. Zeige mithilfe des DPLL-Algorithmus, daß die Ecken eines Fünfecks nicht mit zwei Farben gefärbt werden können, sodaß benachbarte Ecken jeweils verschiedene Farben bekommen.

Aufgabe 49.

(a) Auf einem 3×3-Raster sind Lampen angebracht und sollen so geschaltet werden, daß je nach Zeile oder Spalte die angezeigte Anzahl von Lampen brennt.

?	?	?	2
?	?	?	1
?	?	?	1
1	2	1	

Formuliere diese Bedingungen in KNF mit logischen Variablen $A_{i,j}$, $i, j = 1, 2, 3$.

(b) Finde mittels Resolution/DPLL alle gültigen Belegungen, für die die Lampe im mittleren Feld brennt, d.h., $\beta(A_{22}) = 1$.

Aufgabe 50. Drücke die folgenden Aussagen über natürliche Zahlen in Prädikatenlogik mit folgender Signatur aus (Grundmenge $X = \mathbb{N}$):

Konstante: 1
Funktionssymbole: $+$, $-$, $\cdot$
Relationssymbole: $=$

(a) a teilt b.
(b) p ist eine Primzahl.
(c) a ist kongruent zu b mod n
(d) $\mathrm{kgV}(a, b) = ab$.

Aufgabe 51. Bestimme die freien und gebundenen Variablen der Formel

$$(\forall z(Q(z) \wedge \forall x P(x, y))) \vee (\exists y P(x, y))$$

Aufgabe 52. Bringe folgende Formel auf Pränex-Normalform:

$$\forall x((\forall y \exists z R(x, y, z)) \wedge \exists z \forall y \neg R(x, y, z))$$

Aufgabe 53. Welche der folgenden Schlüsse sind korrekt?

(a) $\forall x \exists y R(x, y) \implies \exists x R(x, x)$

(b) $\exists y \forall x R(x, y) \implies \exists x R(x, x)$

(c) $(\forall x \exists y \forall z(R(x, y) \wedge R(y, z) \to R(x, z))) \wedge \forall x \exists y R(x, y) \implies \forall x \forall y R(x, y)$

Aufgabe 54. Wieviele Fahnen mit drei Streifen kann man mit den Farben rot, grün, weiß, schwarz und blau bilden, sodaß benachbarte Streifen verschiedene Farben haben? (d.h. rot-weiss-rot ist erlaubt, aber nicht rot-rot-weiss).

(a) Wenn oben und unten unterscheidbar ist? (d.h., RWG ist verschieden von GWR).
(b) Wenn oben und unten nicht unterscheidbar ist? (d.h., RWG und GWR ist die gleiche Fahne).
(c) Wieviele Fahnen mit k Streifen aus n Farben kann man jeweils bilden?

Aufgabe 55. Wieviele ganzzahlige Lösungen hat die Gleichung

$$x_1 + x_2 + \cdots + x_k = n$$

unter der Voraussetzung

(a) $x_j > 0$ für alle j;
(b) $x_j \geq 0$ für alle j.

Wie hängen die Lösungen zusammen?

Aufgabe 56. Bestimme die Anzahl der ganzzahligen Lösungen der Gleichung

$$x_1 + x_2 + x_3 + x_4 + x_5 = 19$$

unter den Bedingungen

(a) $x_i \geq 0$ für $i = 1, 2, 3, 4, 5$;
(b) $x_i \geq 0$ für $i = 1, 2, 3, 4$ und $x_5 \geq 5$;
(c) $x_i \geq 0$ für $i = 1, 2, 3$, $0 \leq x_4 \leq 4$ und $0 \leq x_5 \leq 4$.

Aufgabe 57. Wieviele Lösungen $(x_1, x_2, \ldots, x_{2n}) \in \{+1, -1\}^{2n}$ hat die Gleichung

$$x_1 + x_2 + \cdots + x_{2n} = 0?$$

Aufgabe 58. Zeige mit kombinatorischen Argumenten, daß

$$\binom{n}{k}\binom{n-k}{j} = \binom{n}{k+j}\binom{k+j}{k} = \binom{n}{j}\binom{n-j}{k}$$

Aufgabe 59.

(a) Wieviele 5-stellige Telephonnummern enthalten mindestens eine Ziffer, die mehrmals vorkommt?
(b) Wieviele 5-stellige Telephonnummern enthalten genau eine Ziffer, die mehrmals vorkommt?

Unterscheide jeweils die Fälle, ob die Nummern mit 0 beginnen dürfen oder nicht.

Aufgabe 60.

(a) Auf wieviele Arten kann man die Buchstaben des Wortes *MISSISSIPPI* zu einem Anagramm anordnen?
(b) Auf wieviele Arten kann man die Buchstaben des Wortes *MISSISSIPPI* so anordnen, daß weder alle I's, S noch P's jeweils hintereinander stehen?

Aufgabe 61. Wieviele Zahlen aus $\{1, 2, \ldots, 1500\}$ sind durch 2, 3 oder 5 teilbar?

Aufgabe 62. Seien $A, B, C \subseteq X$ endliche Mengen und bezeichne $\bar{B} = X \setminus B$. Leite die Formel

$$|A \cup B \cup C| = |A| + |B \cap C| + \left|\bar{B} \cap C\right| + \left|B \cap \bar{C}\right| - |A \cap B \cap C| - \left|A \cap \bar{B} \cap C\right| - \left|A \cap B \cap \bar{C}\right|$$

her.

Aufgabe 63. Gegeben sei die Zahlenfolge $a_n = n \cdot 2^n + 3^n$. Finde geschlossene Ausdrücke für die erzeugenden Potenzreihen

$$(a) \qquad F(x) = \sum_{n=0}^{\infty} a_n x^n \qquad\qquad (b) \qquad E(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n;$$

Letztere bezeichnet man als *exponentielle erzeugende Potenzreihe*.

Aufgabe 64. Bestimme mittels erzeugender Funktionen die Anzahl der Auswahlmöglichkeiten von 7 Kugeln aus einer Urne mit 6 weißen, 6 roten und 6 schwarzen Kugeln, wobei nur eine gerade Zahl weißer, eine ungerade Zahl schwarzer, und eine durch 3 teilbare Zahl roter Kugeln entnommen werden darf.

Hinweis: Die Reihenfolge der Kugeln soll keine Rolle spielen.

Aufgabe 65. Zeige mit Hilfe der Binomialreihe (C.2.6), dass für $n \in \mathbb{N}$ die Reihenentwicklung

$$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{n-1} x^k$$

gilt.

Aufgabe 66. Auf wieviele Arten kann man 25 Cent mit 7 Münzen bezahlen?

Hinweis: Beispiel (C.2.23) mit der Bewertung $\textcircled{\text{k}} \to x^k \cdot y$.

Aufgabe 67. Berechne für alle n

$$s_n = \sum_{k=1}^{n} k^2.$$

Hinweis:

(1) Betrachte

$$x \frac{d}{dx} \left(x \frac{d}{dx} \frac{1}{1-x} \right)$$

(2) verwende Bemerkung (C.2.24) um die erzeugende Funktion $\sum s_n x^n$ zu bestimmen.
(3) Verwende Aufgabe 65, um eine Formel für deren Koeffizienten herzuleiten.

Aufgabe 68. Berechne Formeln für die Koeffizienten a_n und b_n der Potenzreihen

$$\text{(a)} \qquad \sum_{k=0}^{\infty} a_k x^k = \frac{-13\,x^2 + x + 2}{6\,x^3 + x^2 - 4\,x + 1} \qquad\qquad \text{(b)} \qquad \sum_{k=0}^{\infty} b_k x^k = \frac{-8\,x^2 + 14\,x - 7}{4\,x^3 - 8\,x^2 + 5\,x - 1}$$

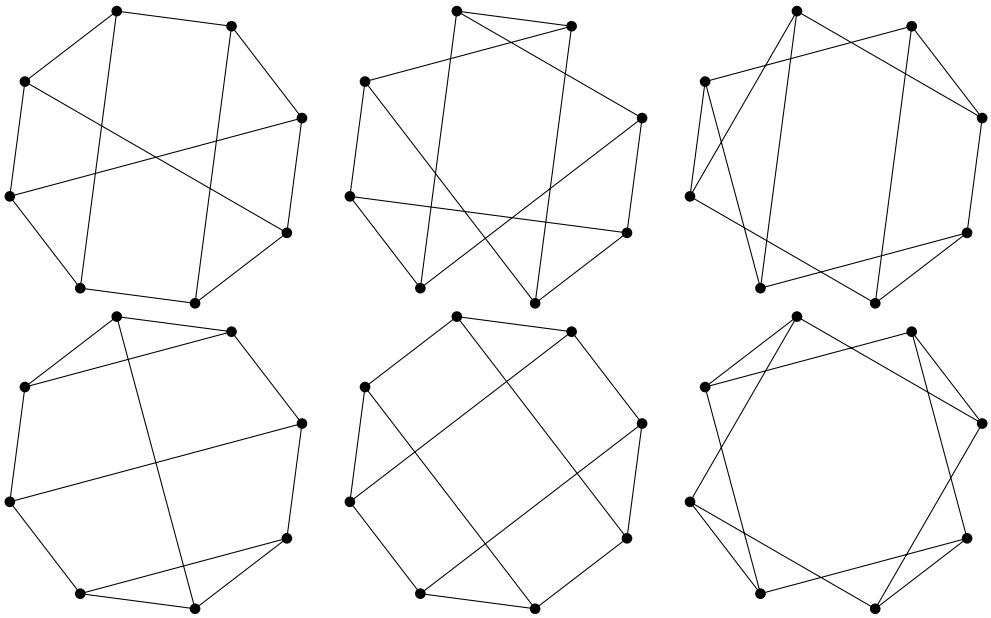
Hinweis zu (b): Skriptum C.2.15.

Aufgabe 69. Löse die Rekursionsgleichungen

$$(a) \qquad a_{n+2} - a_{n+1} - 3a_n = 2^n, \quad n \geq 0 \qquad a_0 = 1 \qquad a_1 = 2$$

$$(b) \qquad a_{n+2} - 2a_{n+1} - 8a_n = (n+1)\,2^n, \quad n \geq 0 \qquad a_0 = 1 \qquad a_1 = 1.$$

Aufgabe 70. Zwei Graphen G_1 und G_2 heißen *isomorph*, wenn es eine bijektive Abbildung $f : V(G_1) \to V(G_2)$ zwischen beiden Knotenmengen gibt, sodass $[x, y] \in E(G_1) \iff [f(x), f(y)] \in E(G_2)$. Isomorphe Graphen werden üblicherweise identifiziert. Die folgenden Bilder zeigen sechs Graphen, von denen jeweils zwei zueinander isomorph sind. Finde die drei isomorphen Paare und begründe jeweils, warum Graphen aus verschiedenen Paaren nicht isomorph sind.



Aufgabe 71. Bestimme alle nicht-isomorphen Graphen mit $n = 2$, 3, oder 4 Knoten (nicht-zusammenhängende Graphen miteingeschlossen).

Aufgabe 72.

(a) Zeige, dass in einem ungerichteten Graphen G die Relation

$$x \, R \, y \iff \exists \text{ Weg von } x \text{ nach } y$$

eine Äquivalenzrelation ist.

(b) Welche Relation erhält man, wenn man "Weg" durch "Pfad" ersetzt?

(c) Weise nach, dass die entsprechende Aussage für gerichtete Wege in gerichteten Graphen falsch ist. Welche Eigenschaften einer Äquivalenzrelation sind nicht erfüllt?

Aufgabe 73. Sei $G = (V, E)$ ein Graph. Der *Abstand* $d(x, y)$ zwischen zwei Knoten x und y ist die Länge des kürzesten Weges von x nach y. Der *Durchmesser* von G ist definiert als

$$\operatorname{diam}(G) = \max_{x,y \in V} d(x, y).$$

Zeige:

(a) $d(x, x) = 0$ für alle $x \in V$.

(b) $d(x, y) = d(y, x)$ für alle $x, y \in V$.

(c) $d(x, y) \leq d(x, z) + d(z, y)$ für alle $x, y, z \in V$.

(d) Für alle $x \in V$ gibt es ein $y \in V$ sodass $d(x, y) \geq \frac{1}{2} \operatorname{diam}(G)$.

☛☛☛

Aufgabe 74. Die Gradfolge eines Graphen ist die Folge der Grade der einzelnen Knoten in absteigender Ordnung.

(a) Bestimme alle möglichen Gradfolgen eines Graphen mit vier Knoten (nicht-zusammenhängende Graphen miteingeschlossen).

(b) Ist es möglich, Graphen (ohne Schleifen und Mehrfachkanten) mit den folgenden Gradfolgen zu konstruieren?

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

(iii) $(3, 3, 3, 2, 1)$ (iv) $(1, 1, 1, 1, 1)$

(c) Finde zwei zueinander nicht isomorphe Graphen mit der Gradfolge $(3, 3, 3, 3, 2, 2)$.

(d) Zeige, daß die Gradfolge eines Graphen nicht aus lauter verschiedenen Zahlen bestehen kann, d.h., in jedem Graphen haben mindestens zwei Knoten den gleichen Grad.

Aufgabe 75. Gegeben sei der Graph $G = (V, E)$ mit Knotenmenge $V = \{1, 2, 3, 4, 5, 6\}$ und Kanten

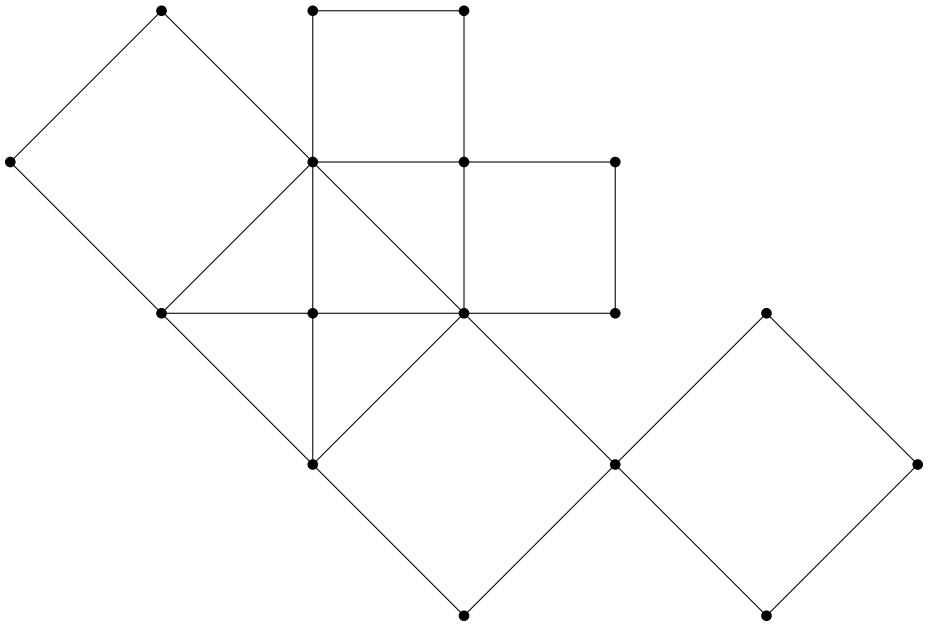
$$E = \{[1, 2], [1, 4], [2, 3], [2, 4], [2, 5], [3, 4], [3, 5], [3, 6], [4, 5], [5, 6]\}.$$

(a) Bestimme die Adjazenzmatrix und die Anzahl der Wege der Länge 6 von Knoten 2 nach Knoten 5.

(b*) Berechne eine Formel für die Anzahl der Wege von Knoten 2 nach Knoten 5.

Hinweis: Die Hilfe des Computers ist erlaubt.

Aufgabe 76. Gegeben sei der Graph

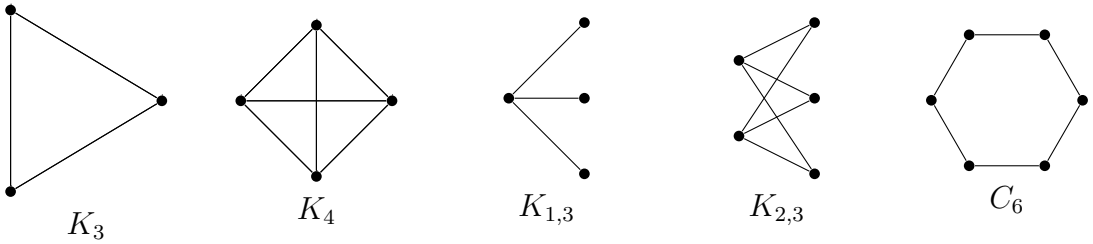


Finde, wenn möglich, einen Eulerschen Kreis bzw. Weg mithilfe des Algorithmus von Fleury.

Aufgabe 77. Sei G ein ungerichteter Graph mit Kanten $e_1, e_2, \ldots, e_m$. Der *Kantengraph* $L(G)$ ist der folgendermaßen definierte ungerichtete Graph:

Die Knoten von $L(G)$ sind $e_1, e_2, \ldots, e_m$.
$[v_i, v_j]$ ist eine Kante von $L(G)$ genau dann, wenn e_i und e_j einen gemeinsamen Knoten in G haben.

(a) Zeichne die Kantengraphen von K_3, K_4, $K_{1,3}$, $K_{2,3}$ und C_6:



(b) Ein *Eulerscher Graph* ist ein Graph, der einen Eulerschen Kreis besitzt. Zeige, dass der Kantengraph eines Eulerschen Graphen wieder Eulerscher Graph ist.
Gilt auch die Umkehrung?

Aufgabe 78. Zeichne alle nicht isomorphen Bäume mit

(a) 6 Knoten (b) 7 Knoten

Aufgabe 79. Zeichne den Baum mit Knoten $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ und Kanten

$$E = \{[1, 5], [1, 8], [1, 9], [2, 3], [2, 7], [2, 8], [4, 7], [6, 8]\},$$

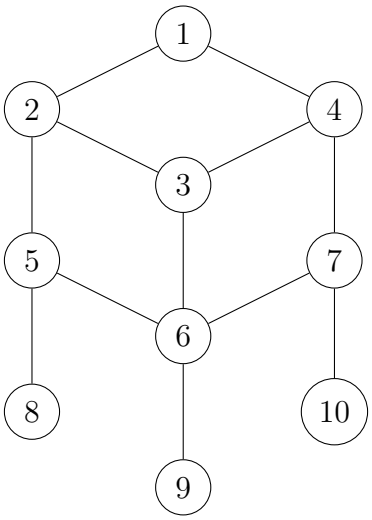
und ermittle seinen Prüfer-Code[4]. Rekonstruiere den Baum anschließend aus dem erhaltenen Prüfer-Code.

[4]fehlt noch im Skriptum, siehe Vorlesung am 15.6. oder Wikipedia `https://en.wikipedia.org/wiki/Pruefer_sequence`

Aufgabe 80. Bestimme einen

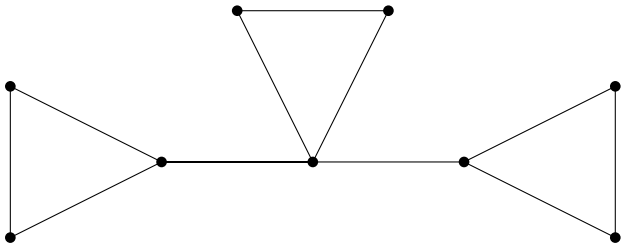
(a) BFS-Spannbaum (b) DFS-Spannbaum

ausgehend vom Knoten Nr. 1 des Graphen

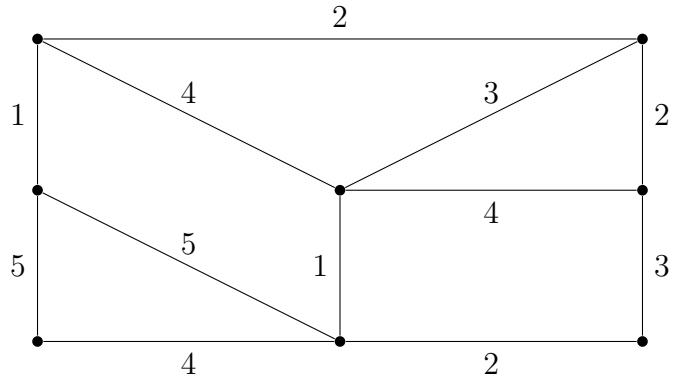


NB: Die einzelnen Schritte und den Stand der Knotenliste ausführlich dokumentieren!

Aufgabe 81. Bestimme alle Spannbäume des Graphen



Aufgabe 82. Bestimme mit dem Algorithmus von Kruskal alle minimalen Spannbäume des folgenden gewichteten Graphen:



Aufgabe 83. Sei G der bipartite Graph mit den Seiten $A = \{a_1, a_2, \ldots, a_5\}$ und $B = \{b_1, b_2, \ldots, b_5\}$, sowie der Kantenmenge

$$E = \{[a_1, b_2], [a_1, b_4], [a_2, b_2], [a_2, b_4], [a_3, b_3], [a_3, b_4], [a_3, b_5], \\ [a_4, b_1], [a_4, b_2], [a_4, b_3], [a_4, b_4], [a_4, b_5], [a_5, b_2], [a_5, b_4]\}$$

Erweitere das Matching $M = \{[a_2, b_2], [a_3, b_3], [a_4, b_4]\}$ durch einen augmentierenden Pfad P (unter Verwendung von BFS, jeweils Knoten mit kleinstem Index wählen). Ist das erhaltene Matching $M' = M \triangle E(P)$ ein maximales Matching in G?

Aufgabe 84. Auf $\mathbb{Z}$ sei die Relation

$$mRn \iff m \text{ und } n \text{ enthalten die gleichen Primteiler}$$

gegeben. Stelle fest (mit ausführlicher Begründung), ob die Eigenschaften

Reflexivität
Symmetrie
Antisymmetrie
Transitivität

erfüllt sind und ob es sich um eine Äquivalenzrelation oder Ordnungsrelation handelt.

Aufgabe 85. Löse das Kongruenzgleichungssystem

$$\begin{aligned} x &\equiv 7 \mod 9 \\ x &\equiv 10 \mod 11 \\ x &\equiv 11 \mod 16 \end{aligned}$$

mithilfe des chinesischen Restsatzes – unter Verwendung des euklidischen Algorithmus und NICHT durch erraten.

Zusatzfrage: Welches ist die kleinste positive Lösung?

Aufgabe 86. Bestimme die multiplikative Inverse von 5 modulo 144, d.h.

$$[5]^{-1} \text{ in } \mathbb{Z}_{144}.$$

Wieviele Zahlen $k \in \{1, 2, \ldots, 143\}$ besitzen eine multiplikative Inverse modulo 144?

Aufgabe 87. Gegeben sei die Zahl $m = 65$. Welche der folgenden Werte für r sind als Verschlüsselungsschlüssel zulässig (Begründung!)?

Finde (für die zulässigen r) den jeweiligen inversen Schlüssel s.

(a) $r = 3$
(b) $r = 25$
(c) $r = 29$

Aufgabe 88. Bestimme n-KNF und n-DNF der logischen Aussageform

$$C \to (A \vee B)$$

Aufgabe 89. Zeige mit den Regeln des logischen Schließens (Skriptum (D.5.7); **ohne** Verwendung von Wahrheitstafeln) die logische Äquivalenz der Aussageformen

$$P :\iff (A \wedge B) \to (C \vee D) \qquad Q :\iff B \to (A \to (C \vee D))$$

Aufgabe 90. Bestimme einen geschlossenen Ausdruck für die erzeugende Potenzreihe $A(x)$ der Folge a_n, gegeben durch die Rekursionsgleichung

$$a_n - a_{n-1} - 3a_{n-2} + (n+1)3^n = 0 \qquad n \geq 2$$

mit den Anfangswerten $a_0 = 1$ und $a_1 = 1$. (Partialbruchzerlegung und Reihenentwicklung ist **nicht** erforderlich).

Aufgabe 91. Gegeben sei der (ungerichtete) Graph G mit Knoten $V(G) = \{1, 2, 3, 4\}$ und Kanten $\{[1, 2], [1, 3], [1, 4], [2, 3], [3, 4]\}$. Bestimme die Adjazenzmatrix und die Anzahl der Wege der Länge 8 vom Knoten 1 zum Knoten 2.