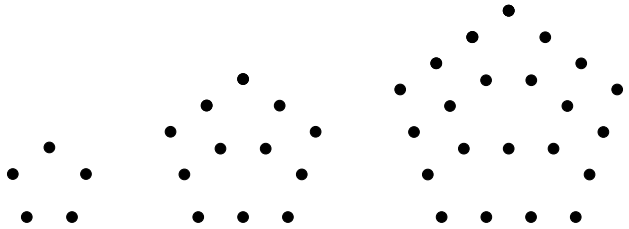
Aufgabe 1. Beweise durch vollständige Induktion die folgende Identität:

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

Zusatzaufgabe. Finde die Folge $\left(\frac{n(3n-1)}{2}\right)_{n\in\mathbb{N}}$ in *Sloane's Database*[1] und zeige den Zusammenhang mit den folgenden Diagrammen:



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

Aufgabe 2. Zeige durch Induktion: Für jedes n ist die Zahl $n(n+1)(n+2)$ durch 6 teilbar.

Aufgabe 3. Zeige durch Induktion (unter Verwendung des vorhergehenden Resultats): Für jedes n ist die Zahl $a^{2n+1} - a$ durch 6 teilbar.

Aufgabe 4. 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) $(429, 2017)$

[1] `www.oeis.org`

Aufgabe 5. Löse Aufgabe 4 noch einmal mit dem Rechenschema aus der Vorlesung (Nr. (A.3.7) im Skriptum), und berechne außerdem

$$\mathrm{ggT}(89, 55) \qquad \mathrm{ggT}(2021, 301)$$

Aufgabe 6. Seien m und n ganze Zahlen, sodass $\mathrm{ggT}(m, n) = 1$. Zeige, dass $\mathrm{ggT}(m + n, m - n) = 1$ oder 2.

Aufgabe 7. 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).

Zusatzaufgabe. Bestimme den Kettenbruch der Zahl

$$\frac{1 + \sqrt{5}}{2}.$$

Aufgabe 8. Zeige, daß $2^n - 1$ keine Primzahl ist, wenn n keine Primzahl ist.

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!

Aufgabe 10. 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 $\mathrm{kgV}(m, n) = 56$.

☯ ☯ ☯

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

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

(b) $X = \mathbb{N}$, $mRn \iff \mathrm{ggT}(m, n) = 5$

Aufgabe 12. (a) $X = \mathbb{R}^2$, $(x_1, x_2)R(y_1, y_2) \iff x_2 \leq y_2$.
(b) $X = \mathbb{R}$, $xRy \iff x - y \in \mathbb{Z}$.

Aufgabe 13. (a) X eine beliebige Menge, Relation $xRy \iff x \neq y$.
(b) A eine beliebige Menge, $X = \mathcal{P}(A) \setminus \{\emptyset\}$ (Potenzmenge ohne die leere Menge),
$xRy \iff x \cap y \neq \emptyset$

Aufgabe 14. Sei $A = \{1, 2, 3, 4\}$. Bilde die kleinste Äquivalenzrelation auf A, die die Elemente $(1, 3)$ und $(2, 3)$ enthält.

Aufgabe 15. 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 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

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

Aufgabe 20. Bestimme alle Lösungen der diophantischen Gleichung

$$63x - 12y = 15$$

Aufgabe 21. Löse das Kongruenzgleichungssystem

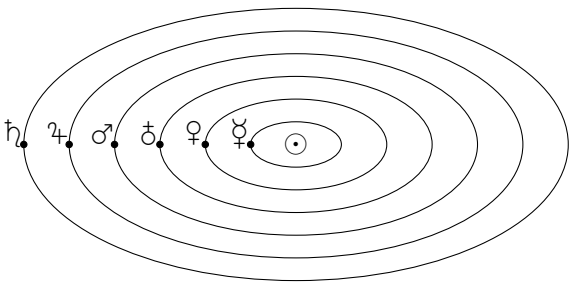
$$\begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 2 \mod 7 \\ x &\equiv 3 \mod 8 \end{aligned}$$

Aufgabe 22. Löse, wenn möglich, die folgenden Kongruenzgleichungssysteme

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

Zusatzaufgabe. Die folgende Tabelle zeigt die Umlaufzeiten (U) der frei sichtbaren Planeten, sowie die Zeit in Tagen (D), die am 13.4.2021 jeweils vergangen sind, seit jeder einzelne das letzte Mal den Punkt der Wintersonnenwende durchlaufen hat.

	U	D
Merkur	88	51
Venus	225	103
Erde	365	113
Mars	687	361
Jupiter	4333	2230
Saturn	10759	3364



Wir nehmen der Einfachheit halber an, daß das Sonnensystem fix ist und sich der Punkt der Wintersonnenwende nicht ändert. Wieviele Tage sind laut diesem Modell seit dem letzten *Shàngyuán* vergangen, d.h., seit dem Zeitpunkt, als alle Planeten zur Wintersonnenwende am 21.Dezember in einer Reihe standen wie in der Skizze?

Hinweis: Mit dem Computer berechnen! Um den chinesischen Restsatz anwenden zu können, ist vorher das Gleichungssystem unter Beachtung von Bemerkung (A 7.8) aus dem Skriptum umzuformen.

Aufgabe 23. 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 24. Berechne $2^{15} \mod 3465$.

Hinweis:

(1) 3465 in Primfaktoren $p_i^{k_i}$ zerlegen.

(2) $2^{15} \mod p_i^{k_i}$ 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) Sei U eine Menge, und $X = \{A : A \subseteq U\}$ die *Potenzmenge* ausgestattet mit der Verknüpfung

$$A \circ B = A \cup B$$

(g) X wie vorher mit der Verknüpfung

$$A \circ B = A\Delta B := (A \setminus B) \cup (B \setminus A)$$

(h) X beliebig mit der Verknüpfung

$$a \circ b = a$$

für alle $a, b \in X$.

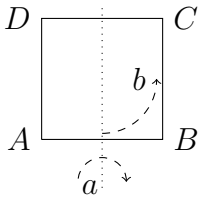
Aufgabe 26. Ergänze die folgende Verknüpfungstabelle so, daß die Gruppenaxiome erfüllt sind. Welches ist das neutrale Element? Ist die Gruppe abelsch?

$\circ$	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

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



(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. Sei G eine Gruppe mit neutralem Element e. Die *Ordnung* eines Elements $x \in G$ ist definiert als $\mathrm{o}(x) = \min\{n \in \mathbb{N} \mid x^n = e\}$.

(a) Bestimme alle Elemente der Gruppe (bezüglich Multiplikation) $\mathbb{G}_{30} = \{[k] \in \mathbb{Z}_{30} \mid \mathrm{ggT}(k, 30) = 1\}$.
(b) Bestimme für jedes Element $x \in \mathbb{G}_{30}$ die Ordnung $\mathrm{o}(x)$.

Aufgabe 29. Berechne $\varphi(3465)$ und $\varphi(10125000)$.

Aufgabe 30. Ermittle ohne Taschenrechner Zahlen a, b, c, sodaß

$$(4^{27})^{2021} \equiv a \mod 25 \qquad 2^{(2^{32})} \equiv b \mod 11 \qquad 14^{(2021^{2021})} \equiv c \mod 60.$$

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

Aufgabe 31. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Zeige, daß durch

$$x \equiv_H y \iff x^{-1}y \in H$$

eine Äquivalenzrelation auf G definiert ist. Die Äquivalenzklassen heißen *Linksnebenklassen*.

Aufgabe 32. Wir betrachten die ganzen Zahlen als Gruppe $(\mathbb{Z}, +)$. Seien $m, n \in \mathbb{Z}$. Zeige, daß die kleinste Untergruppe $H \subseteq \mathbb{Z}$, die sowohl m als auch n enthält, gegeben ist durch $H = k\mathbb{Z}$, wobei $k = \mathrm{ggT}(m, n)$.

Aufgabe 33. Berechne die letzten zwei Ziffern in der Dezimaldarstellung der Zahl

$$a = 27^{202104}.$$

Vorgangsweise: Berechne Zahlen r_1 und r_2 sodaß

$$a \equiv r_1 \mod 4 \quad \text{und} \quad a \equiv r_2 \mod 25$$

und bestimme dann $a \mod 100$ mit dem chinesischen Restsatz.

Aufgabe 34 (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 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 Zahl $0 \leq t < \frac{m_1 m_2}{m_0}$ und setze $a = r + t m_0$ (dadurch ist sichergestellt, daß $a < m_1 m_2$).
- 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 Charly erhält (c_3, m_3).
- Um die geheime Zahl s 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 $s = x \mod m_0$ berechnen.

(a) Begründe, warum am Ende $s = r$ 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 $(4, 7)$ und Bob erhält das Paar $(8, 9)$. Wie lautet das Geheimnis r? Kann t rekonstruiert werden? Welches Paar (c_3, m_3) hat Charly erhalten?
(c) Angenommen, Charly 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 35. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 31$, $g = 5$, $a = 13$, $b = 11$. Was fällt auf? Welchen Parameter sollte man ändern?
(b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$g = 8 \qquad p = 29$$
$$m = 22 \qquad n = 2$$

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

Aufgabe 36. 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 37. (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 38. Gegeben sei $m = 1333$.
(a) Welche der folgenden Zahlen sind als öffentliche RSA-Schlüssel geeignet (Begründung!)?

$$r = 41 \qquad r = 42 \qquad r = 43$$

Berechne die zugehörigen inversen Schlüssel.
(b) Wähle einen geeigneten Schlüssel und verschlüssle die Botschaft

"FAKENEWS"

mit der Konvention aus der Vorlesung (Bsp (11.7); ohne Störzeichen).
(c) Die folgende Nachricht wurde mit dem Schlüssel $r = 17$, $m = 1333$ verschlüsselt.

$$[367, 490, 535, 658, 1129, 133, 787, 293, 301]$$

Finde den inversen Schlüssel s und entschlüssle die Botschaft.

Hinweis: Für die Zwischenrechnungen ist ein Computer erlaubt.

Aufgabe 39. 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 $m = 85$ und $r = 13$ bekanntgegeben.
(a) Verschlüssle die Nachricht $(14, 42)$.
(b) Berechne den Geheimschlüssel s und entschlüssle die Botschaft.

Aufgabe 40. Begründe, warum im RSA-Verfahren anstelle von $\phi(m) = (p-1)(q-1)$ auch die Zahl $\lambda(m) = \mathrm{kgV}(p-1, q-1)$ verwendet werden kann.

Hinweis: Chinesischer Restsatz!

Zusatzaufgabe. Zum Abschluß des Kryptographiekapitels und anläßlich des verregneten langen Wochenendes gibt es einen Wettbewerb: Am Freitag 14.5. werden um 14:00 im Teachcenter zwei verschlüsselte Texte angezeigt. Für die jeweils ersten drei abgegebenen Lösungen (inklusive Lösungsweg) gibt es Extrapunkte.

Aufgabe 41. Das folgende Beispiel illustriert, daß die Wahl kleiner Schlüssel die Sicherheit des RSA-Verfahrens verringert.

Tom schickt die gleiche Botschaft an seine Freundinnen Gernot, Wolfi und Sebastian, die ihm vorher die öffentlichen Schlüssel $(m_1 = 1219, r_1 = 3)$, $(m_2 = 799, r_2 = 3)$ und $(m_3 = 1189, r_3 = 3)$ bekanntgegeben haben. Die drei Botschaften sind $y_1 = (248, 1093, 354)$, $y_2 = (274, 648, 178)$ und $y_3 = (682, 40, 1140)$. Entschlüssle die Botschaft, ohne die Primfaktorzerlegung der Schlüssel m_i durchzuführen (Computer oder Taschenrechner für Zwischenrechnungen ist zugelassen).

Aufgabe 42. 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 43. 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 44. 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 45. Beweise mit den Regeln des logischen Schließens[3] den **Modus Tollens**

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

Aufgabe 46. Beweise mit den Regeln des logischen Schließens das Klammer-Änderungsgesetz für "$\to$":

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

[3]siehe `https://www.math.tugraz.at/idm-lv/dmi/2021/Uebungsblaetter/logikregeln.pdf`

Aufgabe 47. Formalisiere die folgenden Aussagen und ermittle, ob der Schluß korrekt ist.

Wenn sich der Wissenschaftsminister nicht um die Universitäten kümmert, wird er deshalb vom Parlament nicht abgewählt, oder die Universitäten protestieren. Wenn er vom Parlament nicht abgewählt wird, kümmert er sich um die Universitäten. Wenn die Universitäten zufrieden sind, protestieren sie nicht. Daher sind die Universitäten nicht zufrieden, wenn er sie im Stich läßt.

Aufgabe 48. Bestimme jeweils die 3-KNF und die 3-DNF der Formeln

$$A \to (B \leftrightarrow C) \qquad \text{und} \qquad (A \to B) \leftrightarrow C.$$

Aufgabe 49. Bestimme die Menge der Folgerungen, die aus der Prämissenmenge

$$\begin{aligned} P_1 &: \Longleftrightarrow\ A \to (B \to C) \\ P_2 &: \Longleftrightarrow\ A \vee ((B \wedge C) \vee (\neg B \wedge \neg C)) \\ P_3 &: \Longleftrightarrow\ B \to C \end{aligned}$$

hergeleitet werden können.

Aufgabe 50. 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 51. 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 52. (a) Bestimme je eine KNF der Aussagen "Von A, B, C ist genau eines erfüllt" und "Von A, B, C sind genau zwei erfüllt".

(b) 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.

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

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

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

Aufgabe 53. Gegeben seien folgende Prädikate

$f(x)$: x kann fliegen
$s(x)$: x kann Feuer spucken
$g(x)$: x ist glücklich
$l(x, y)$: x wird von y geliebt
$V(x)$: x ist ein Vogel
$D(x)$: x ist ein Drache
$T(x)$: x ist ein Tier

Drücke folgende Feststellungen in Prädikatenlogik bzw. Umgangssprache aus:

(a) $\forall x \left((T(x) \wedge f(x) \wedge \neg V(x)) \rightarrow D(x)\right)$

(b) $\exists x \, \forall y \left((T(x) \wedge f(x) \wedge s(x) \wedge l(x, y)) \rightarrow D(y)\right)$

(c) Alle Tiere, die fliegen können und keine Drachen sind, werden von einigen Vögeln geliebt.

(d) Jeder Vogel ist glücklich, wenn ein von ihm geliebtes fliegendes Tier kein Feuer spuckt.

Aufgabe 54. 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 55. 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 56. 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) $$(\forall x \exists y \forall z (R(x, y) \wedge R(y, z) \rightarrow R(x, z))) \wedge \forall x \exists y R(x, y) \implies \forall x \forall y R(x, y)$$

Aufgabe 57. Seien $k \leq m \leq n$ natürliche Zahlen. Zeige durch eine kombinatorische Überlegung (d.h., ohne die Binomialkoeffizienten auszurechnen), dass

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}.$$

Aufgabe 58. Wieviele ganzzahlige Lösungen hat die Gleichung

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

unter der Voraussetzung

(a) $x_j > 0$

(b) $x_j \geq 0$

Wie hängen die Lösungen zusammen?

Aufgabe 59. 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 60. Berechne Formeln für die Koeffizienten a_n und b_n der Potenzreihen

(a) $$\sum_{k=0}^{\infty} a_k x^k = \frac{-13\,x^2 + x + 2}{6\,x^3 + x^2 - 4\,x + 1}$$

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

Hinweis zu (b): Skriptum C.2.15.

Aufgabe 61. Bestimme einen geschlossenen Ausdruck für Zähler und Nenner der rationalen Funktion

$$f(x) = \frac{p(x)}{q(x)} = \sum_{k-0}^{\infty} a_k x^k,$$

deren Koeffizienten die Rekursionsgleichung

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

erfüllen.

Aufgabe 62. (a) Berechne eine geschlossene Formel für die erzeugende Funktion

$$\sum_{n=0}^{\infty} n^2 x^n$$

(b) Berechne eine geschlossene Formel für die Summe

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

Aufgabe 63. 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.
NB: Schleifen sind nicht erlaubt.

Aufgabe 64. 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.