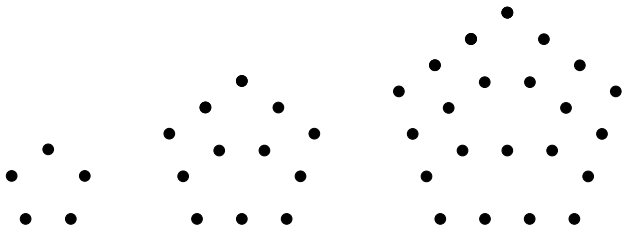
Aufgabe 1. Beweise durch vollständige Induktion die folgende Formel für die Summe:

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

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. Beweise durch Induktion, daß für jedes $n \in \mathbb{N}$ die Zahl $n^5 - n$ durch 5 teilbar ist.

Aufgabe 3. 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) $(429, 2017)$

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

Aufgabe 5. Seien m und n ganze Zahlen. Zeige: wenn ganze Zahlen a und b existieren mit $am + bn = 1$, dann ist $\mathrm{ggT}(m, n) = 1$.

[1] `www.oeis.org`

Aufgabe 6. Löse Aufgabe 3 noch einmal mit dem Rechenschema aus der Vorlesung (Nr. (2.7) im Skriptum).

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

Aufgabe 7. Sei F_n die Folge der Fibonacci-Zahlen, gegeben durch die Rekursion

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

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. Untersuche, welche der folgenden Relationen die Eigenschaften Reflexivität, Symmetrie, Antisymmetrie, Transitivität, Äquivalenzrelation oder Halbordnungsrelation erfüllen.

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

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

(c) $X = \mathbb{R}^2$, $(x_1, x_2)R(y_1, y_2) \iff y_1 \leq y_2$.
(d) $X = \mathbb{N}$, $mRn \iff 3 \,\big|\, (m-n)n$
(e) $X = \mathbb{N}$, $mRn \iff m \,\big|\, n$
(f) $X = \mathbb{N}$, $mRn \iff \mathrm{ggT}(m, n) = 5$
(g) X eine beliebige Menge, Relation $xRy \iff x = y$.
(h) X eine beliebige Menge, Relation $xRy \iff x \neq y$.

Aufgabe 9. Sei $A = \{1, 2, 3, 4\}$. Bilde die kleinste Äquivalenzrelation auf A, die die Elemente $(1, 3)$ und $(4, 3)$ enthält.

Aufgabe 10. Zeige, daß die folgenden Relationen Äquivalenzrelationen sind und bestimme die Äquivalenzklassen.

(a) $X = \mathbb{R}^2$,

$$(x, y) \sim (u, v) : \Longleftrightarrow \; x - y = u - v$$

(b) $X = \mathbb{R}$,

$$x \sim y : \Longleftrightarrow \; x - y \in \mathbb{Z}$$

Aufgabe 11. Erstelle die Multiplikationstabellen von $\mathbb{Z}_7$ und $\mathbb{Z}_8$.

Aufgabe 12. Für die *Internationale Standardbuchnummer* gibt es zwei Standards.

1. Die alte ISBN-10 hat 10 Ziffern,

   $$x_1 x_2 x_3 \cdots x_{10},$$

   wobei $x_1, x_2, \ldots, x_9 \in \{0, 1, \ldots, 9\}$ 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

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

   Beispiel: 3540257829
2. Die neue ISBN-13 hat 13 Ziffern,

   $$z_1 z_2 z_3\text{-}z_4 \cdots z_{13},$$

   wobei $z_i \in \{0, 1, \ldots, 9\}$ und der Präfix $z_1 z_2 z_3$ entweder 978 oder 979 ist und die letzte Ziffer z_{13} eine Prüfziffer ist, die so gewählt wird, daß

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

   (gerade Stellen mit 3 multiplizieren) z.B. entspricht die obige ISBN-10 im neuen Standard der Nummer 978-3540257820.

(a) Berechne die Prüfziffern der folgenden unvollständigen ISBN

978-3-642-37971

364254273

(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.

Aufgabe 13. 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 14. Berechne, wenn möglich, $[13]_{91}^{-1}$, $[15]_{91}^{-1}$ und $[16]_{91}^{-1}$.

Aufgabe 15. Für welche $n \in \mathbb{N}$ ist $43 \equiv 1 \mod n$?

Aufgabe 16. Bestimme alle Lösungen $x \in \mathbb{Z}$ der Gleichungen

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

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

Aufgabe 17. Bestimme alle Lösungen $(x, y) \in \mathbb{Z}^2$ des linearen Gleichungssystems

$$\begin{aligned} 4x + 2y &\equiv 5 \mod m \\ 3x + 5y &\equiv 5 \mod m \end{aligned}$$

für

(a) $m = 7$ (b) $m = 11$

Aufgabe 18. Bestimme alle Lösungen der diophantischen Gleichung

$$45x - 105y = 75$$

Aufgabe 19. Löse das Kongruenzgleichungssystem

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

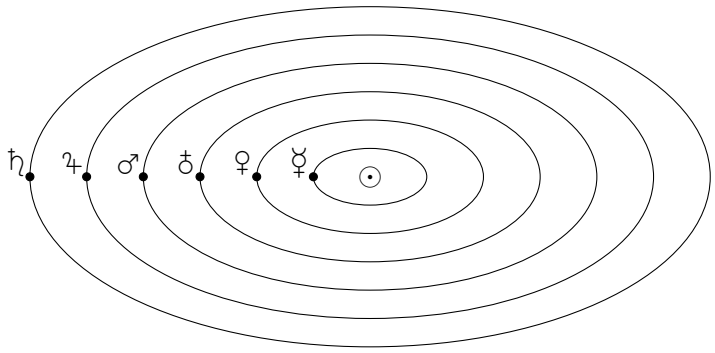
Aufgabe 20. Löse, wenn möglich, die folgenden Kongruenzgleichungssysteme

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

Aufgabe 21. Seien $m, n \in \mathbb{N}$. Zeige: Für zwei Zahlen $a, b \in \mathbb{Z}$ gilt: $a \equiv b \mod m$ und $a \equiv b \mod n$, genau dann, wenn $a \equiv b \mod \text{kgV}(m, n)$.

Zusatzaufgabe (Für den 9.4.)**.** Die folgende Tabelle zeigt die Umlaufzeiten (U) der frei sichtbaren Planeten, sowie die Zeit in Tagen (D), die am 9.4.2019 jeweils vergangen sind, seit jeder einzelne das letzte Mal den Punkt der Wintersonnenwende durchlaufen sind.

	U	D
Merkur	88	33
Venus	225	184
Erde	365	109
Mars	687	679
Jupiter	4333	1861
Saturn	10759	2995



Wir nehmen der Einfachheit halber an, daß das Sonnensystem fix ist und sich der Punkt der Wintersonnenwende nicht ändert. Wieviele Tage sind seit dem letzten *Shangyuan* 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, vorher Aufgabe 21 anwenden.

Aufgabe 22. 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 23. Welche der folgenden Strukturen $(X, \circ)$ bilden Halbgruppen, Monoide, Gruppen? In welchen gilt das Kommutativgesetz?

(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) A eine Menge, $X = A^A = \{f : A \to A\}$ die Menge aller Funktionen von $f : A \to A$ mit der Verknüpfung

$$f \circ g$$

(Hintereinanderausführung von Funktionen).

Aufgabe 24. Berechne $\varphi(3465)$ und $\varphi(10125000)$.

Aufgabe 25. (a) Sei $(G, \circ)$ eine Gruppe und $x_0 \in G$. Zeige, daß die Abbildung

$$\begin{aligned} f : G &\to G \\ x &\mapsto x_0 \circ x \end{aligned}$$

bijektiv ist.
(b) Folgere daraus, daß die Zahlen a, $2a, \ldots, (p-1)a$ alle verschiedene Reste modulo p haben, wenn p eine Primzahl und $a \not\equiv 0 \mod p$ ist.

Aufgabe 26. Berechne ohne Taschenrechner

(a) $2^{(2^{32})} \mod 11$.

(b) $14^{(2019^{2019})} \mod 60$.

Aufgabe 27. (a) Sei n eine natürliche Zahl mit der Eigenschaft, dass $2^n - 1$ eine Primzahl ist. Zeige, dass auch n eine Primzahl sein muss.

Hinweis:

$$x^s - 1 = (x-1)(1 + x + \cdots + x^{s-1})$$

(b) Die Umkehrung gilt nicht: Finde die kleinste Primzahl p, sodass $2^p - 1$ keine Primzahl ist.

Aufgabe 28. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 29$, $g = 5$, $a = 13$, $b = 11$.

(b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$g = 9 \qquad p = 31$$
$$m = 2 \qquad n = 14$$

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

Zusatzaufgabe. Am Freitag 12.4. um 14:00 werden auf der Internetseite drei verschlüsselte Texte bekanntgegeben (Satzzeichen sind unverschlüsselt, werden aber mitgezählt):

- Text A[2] (Deutsch) ist mit einem einfachen Schlüssel der Form

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
K	*E*	*Y*	*W*	*O*	*R*	*D*	*F*	*G*	*H*	*I*	*J*	*L*	*M*	*N*	*P*	*Q*	*S*	*T*	*U*	*V*	*X*	*Z*	*A*	*B*	*C*

  verschlüsselt.
- Text B[3] (Deutsch) ist mit einem Vigenère-Schlüssel[4] der Länge drei verschlüsselt.
- Text C[5] (Englisch) ist mit einem Vigenère-Schlüssel unbekannter Länge verschlüsselt.

  Hinweis: Die Methode von Babbage/Kasiski[6] verwenden, um zuerst die Länge des Schlüssels zu bestimmen.

Für das Kreuz ist mindestens einer der drei Texte durch statistische Häufigkeitsanalyse zu entschlüsseln (Computer!).

Zusätzlich zu den Kreuzen gibt es für jeden Text jeweils 3 Extrapunkte für die erste Lösung, die im Onlinekreuzesystem hochgeladen wird.

Abzugeben ist (in einer ZIP-Datei): 1. der Klartext, 2. der oder die gefundenen Schlüssel, 3. eine kurze Erläuterung, wie die Lösung gefunden wurde und 4. selbst geschriebene Programme oder Scripts, die verwendet wurden.

[2] https://www.math.tugraz.at/mathc/diskmath/2019/Uebungsblaetter/Zusatz28A.txt

[3] https://www.math.tugraz.at/mathc/diskmath/2019/Uebungsblaetter/Zusatz28B.txt

[4] `https://de.wikipedia.org/wiki/Vigenere-Chiffre`

[5] https://www.math.tugraz.at/mathc/diskmath/2019/Uebungsblaetter/Zusatz28C.txt

[6] `https://de.wikipedia.org/wiki/Kasiski-Test`

Aufgabe 29. Erstelle ein Schema des Diffie-Hellman-Merkle-Schlüsselaustauschs für drei Teilnehmer, sodaß am Ende alle drei Teilnehmer den gleichen Schlüssel haben. Wieviele Botschaften müssen dafür mindestens ausgeschickt werden?

Aufgabe 30. (a) Berechne die Eulersche Funktion $\varphi(m)$ für die Zahl $m = 7371$.
(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 $a^{\varphi(7371)+1} \not\equiv a \mod 7371$ genau dann gilt, wenn $\mathrm{ggT}(a, 81) \in \{3, 9, 27\}$.
Hinweis: Chinesischer Restsatz!

Aufgabe 31. Sei $m = pq$ und $\mathrm{ggT}(r, \varphi(m)) = 1$. Aus dem euklidischen Algorithmus folgt, daß es ein $s \in \mathbb{Z}$ gibt sodaß $rs \equiv 1 \mod \varphi(m)$. Warum stimmt die Behauptung aus der Vorlesung, daß immer $s \in \mathbb{N}$, d.h. $s > 0$, gewählt werden kann?

Aufgabe 32. Gegeben sei $m = 1247$.
(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

"WOWOAMEILEISTUNG"

mit der Konvention aus der Vorlesung (Bsp (10.7)).
(c) Erstelle eine digitale Signatur für die Nachricht

"FAKENEWS"

(d) Die folgende Nachricht wurde mit dem Schlüssel $r = 17$, $m = 1247$ verschlüsselt.

$$[496, 361, 492, 1217, 226, 821, 486, 164, 516]$$

Finde den inversen Schlüssel s und entschlüssle die Botschaft.

Hinweis: Für die Zwischenrechnungen ist ein Computer erlaubt.

Aufgabe 33. 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 $m = 91$ und $r = 13$ bekanntgegeben.
(a) Verschlüssle die Nachricht $(14, 42)$.
(b) Berechne den Geheimschlüssel s.
(c) Berechne eine digitale Signatur für die Nachricht $(33, 5)$.

Aufgabe 34. Das folgende Beispiel ist mit der Methode aus Aufgabe 33 zu lösen.
Für den RSA-Algorithmus wurde der öffentliche Schlüssel $m = 91$ und $r = 11$ bekanntgegeben.

(a) Verschlüssle die Nachricht $(12, 42)$.
(b) Berechne den Geheimschlüssel s.
(c) Berechne eine digitale Signatur für die Nachricht $(33, 5)$.

Aufgabe 35. Das folgende Beispiel illustriert, daß die Wahl kleiner Schlüssel die Sicherheit des RSA-Verfahrens verringert.
Bob schickt die gleiche Botschaft an seine Freundinnen Alice, Angela und Adina, 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 $y_1 = (108, 1117, 317)$, $y_2 = (210, 220, 88)$ und $y_3 = (657, 1029, 831)$. Entschlüssle die Botschaft, ohne die Primfaktorzerlegung der Schlüssel m_i durchzuführen (Computer oder Taschenrechner für Zwischenrechnungen ist zugelassen).

Aufgabe 36. Überprüfe anhand von Wahrheitstafeln, für welche Belegungen die folgenden Aussageformen erfüllt sind:

(a) $A \vee (C \to (B \wedge (A \wedge (\neg(A \leftrightarrow (B \vee C))))))$

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

Aufgabe 37. Alice, Bob und Charles sind zu einer Geburtstagsfeier eingeladen. Wie das bei den Leuten so ist, haben alle Vorbehalte:

(a) Wenn Alice nicht kommt, dann kommt auch Bob nicht.
(b) Entweder Bob oder Alice kommt, aber nicht beide.
(c) Charles und Alice kommen, wenn sie kommen, nur zusammen.

Formalisiere die Aussagen und stelle fest, wer zur Feier kommt.

Aufgabe 38. Der Kommissar befragt die Verdächtigen Alice, Bob und Charles für eine Tat. Jede Person lügt einmal und sagt einmal die Wahrheit.

Alice sagt: Ich war es nicht. Ich weiß, daß Charles es getan hat.
Bob sagt: Ich war es nicht. Alice hat es getan.
Charles sagt: Ich war es nicht. Alice weiß nicht, wer es war.

Wer hat es getan?

Aufgabe 39. Zeige die Äquivalenz $(A \vee B) \wedge (\neg A \vee B) \iff B$

(a) anhand der Wahrheitstafel
(b) duch logisches Schließen[7]

Aufgabe 40. Beweise mit den Regeln des logischen Schließens[7] daß der Ausdruck $B \to ((A \to (B \to A)) \to B)$ eine Tautologie ist.

Aufgabe 41. 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 42. Beweise mit den Regeln des logischen Schließens[7] daß die Ausdrücke $P_1 = A \to B$ und $P_2 = B \to C$ den Ausdruck $A \to (B \leftrightarrow C)$ implizieren.

Aufgabe 43. Formalisiere die folgenden Schlüsse, stelle jeweils fest, ob sie korrekt sind und wenn ja, führe den formalen Beweis.

(a) Wenn die Begleitmusik stimmt, dann lässt Uwe mit sich reden. Uwe lässt nicht mit sich reden, also stimmt die Begleitmusik nicht.
(b) Das Bruttosozialprodukt wird im kommenden Jahr nicht weiter anwachsen, oder der Export wird steigen. Das Bruttosozialprodukt wird aber weiter wachsen. Somit wird auch der Export weiter steigen.
(c) Wenn Josef größer ist als Werner, dann ist Frank kleiner als Arnold. Wenn Josef und Susi gleich groß sind, dann ist Josef größer Werner. Frank ist nicht kleiner als Arnold, daher sind Josef und Susi nicht gleich groß.

Aufgabe 44. Im ersten Teil von Goethes Faust heißt es in der 2. Studierzimmer-Szene

> Der Philosoph, der tritt herein
> Und beweist Euch, es müßt' so sein:
> Das Erst' wär' so, das Zweite so,
> Und drum das Dritt' und Vierte so;
> Und wenn das Erst' und Zweit' nicht wär',
> Das Dritt' und Viert' wär' nimmermehr,

Präzisiere diese Argumentation unter Verwendung von Klammern, erstelle die entsprechende Aussageform und bestimme alle Belegungen, die sie erfüllen.

[7] siehe `https://www.math.tugraz.at/mathc/diskmath/2019/Uebungsblaetter/logikregeln.pdf`

Aufgabe 45. Bestimme die Menge der Folgerungen, die aus der Prämissenmenge

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

hergeleitet werden können.

Aufgabe 46. Bestimme eine möglichst kurze

(a) KNF (b) DNF

der logischen Aussageform

$$((A \to B) \wedge (C \leftrightarrow D)) \to (A \vee E).$$

Aufgabe 47. Sei $\mathcal{L}$ die Sprache der Logik. Eine Teilmenge $\mathcal{L}' \subseteq \mathcal{L}$ heißt *vollständig*, wenn jede Formel aus $\mathcal{L}$ zu einer Formel aus $\mathcal{L}'$ äquivalent ist.
Zu einer Menge $\mathcal{J}$ von Junktoren bezeichne $\mathcal{L}_{\mathcal{J}}$ die Menge aller Formeln, die nur unter Verwendung der Junktoren aus $\mathcal{J}$ aufgebaut werden können.
Zeige:

(a) $\mathcal{L}_{\{|\}}$ ist vollständig, wobei $A \mid B :\Longleftrightarrow \neg(A \wedge B)$ (Schefferscher Strich).
(b) $\mathcal{L}_{\{\neg,\to\}}$ ist vollständig.
(c) $\mathcal{L}_{\{\wedge,\vee,\to,\leftrightarrow\}}$ ist nicht vollständig.
Hinweis: Zeige, dass $\neg A$ nicht darstellbar ist; dies ist äquivalent dazu, dass keine Kontradiktion in der Sprache enthalten ist: wenn $b(A_i) = W$, dann ist $\forall P \in \mathcal{L}\ \bar{b}(P) = W$.

Aufgabe 48. Gegeben seien folgende Prädikate

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

Drücke folgende Feststellungen in Prädikatenlogik bzw. Umgangssprache aus:

(a) $\forall x\,((T(x) \wedge f(x) \wedge \neg V(x)) \to D(x))$
(b) $\exists x\,\forall y\,((T(x) \wedge f(x) \wedge s(x) \wedge l(x, y)) \to D(y))$
(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 49. In der Fuzzy-Logik werden nicht nur die Wahrheitswerte 0 und 1, sondern beliebige Werte im Intervall $[0, 1]$ zugelassen. Eine Belegung ist daher eine Funktion $\beta : \mathcal{V} \to [0, 1]$; die logischen Operationen sind wie folgt definiert:

$$\beta(\neg A) = 1 - \beta(A) \qquad \beta(A \wedge B) = \min(a, b) \qquad \beta(A \vee B) = \max(a, b)$$

Zeige, daß die Regeln von de Morgan

$$\neg(A \wedge B) \iff (\neg A) \vee (\neg B) \qquad \neg(A \vee B) \iff (\neg A) \wedge (\neg B)$$

auch für die Fuzzy-Logik gelten, d.h., dass links und rechts jeweils das gleiche Ergebnis herauskommt.

Aufgabe 50. Drücke folgende Aussagen über natürliche Zahlen mit Quantoren und den folgenden Symbolen aus: Konstante 0, Funktionssymbole S (einstellig), $+$ (zweistellig), $\cdot$ (zweistellig), mit der üblichen Interpretation in $\mathbb{N}_0$. (S ist die "Nachfolgerfunktion" $S(n) = n + 1$).

(a) x ist gerade.
(b) x ist ein Teiler von y.
(c) x ist kongruent zu $y \mod z$
(d) x ist eine Potenz von 2. (Hinweis: welche Teiler hat x?).
(e) Eine Zahl x ist durch 6 teilbar genau dann, wenn sie durch 2 und durch 3 teilbar ist.

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. Löse die Rekursionsgleichung

$$a_n - 2\,a_{n-1} - 8\,a_{n-2} = 3^n, \quad n \geq 2,$$

mit den Anfangswerten $a_0 = 1$ und $a_1 = 5$.

Aufgabe 55. (a) Berechne geschlossene Formeln für die erzeugenden Funktionen

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

(b) Berechne die Reihenentwicklung der Funktion

$$\frac{1}{(1-x)^4}$$

Hinweis: Ableitungen der geometrischen Reihe betrachten!

Aufgabe 56. Berechne eine geschlossene Formel für die rekursiv gegebene Folge

$$a_n = a_{n-1} + n^2, \quad a_0 = 0.$$

Hinweis: Zunächst die erzeugende Funktion berechnen und dann mit Hilfe der vorhergehenden Aufgabe in eine Potenzreihe entwickeln.

Aufgabe 57. 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?

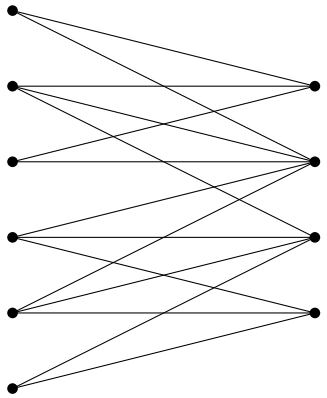
(i) $(3, 3, 3, 3)$ (ii) $(4, 3, 2, 1)$

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

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

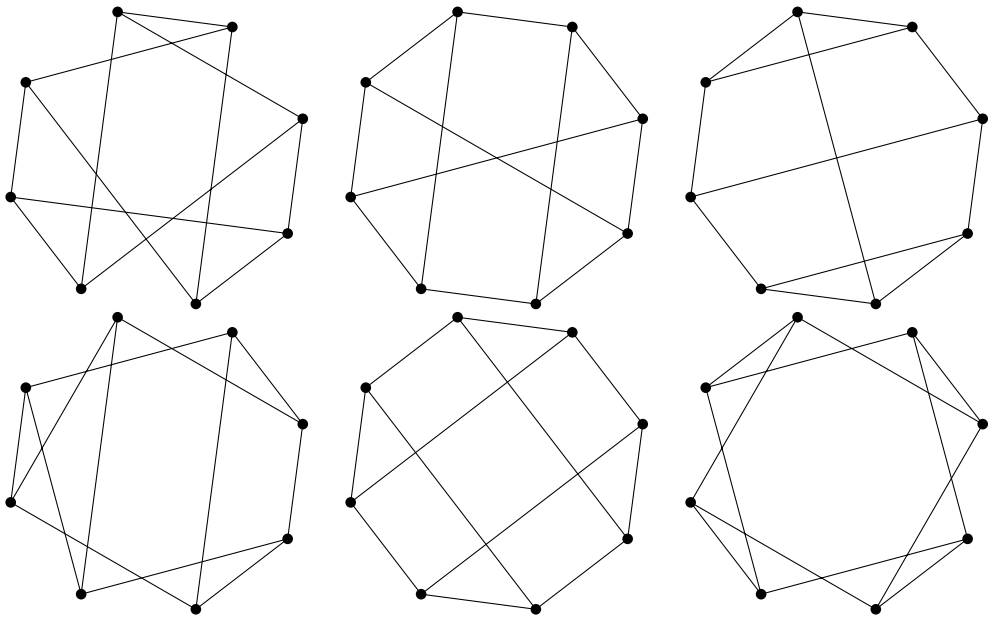
(d) Zeige, daß die Gradfolge eines Graphen nicht aus lauter verschiedenen Zahlen bestehen kann, d.h., in jedem Graphen haben mindestens zwei Knoten den gleichen Grad.
NB: Schleifen sind nicht erlaubt.

Aufgabe 58. Zeige, daß der Graph



keinen Hamiltonschen Kreis besitzt.

Aufgabe 59. 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.



Aufgabe 60. Ein Baum ist ein Graph ohne Kreise. Zeichne alle nicht isomorphen Bäume mit

(a) 6 Knoten
(b) 7 Knoten

Aufgabe 61. Gegeben sei der Graph $G = (V, E)$ mit Knotenmenge

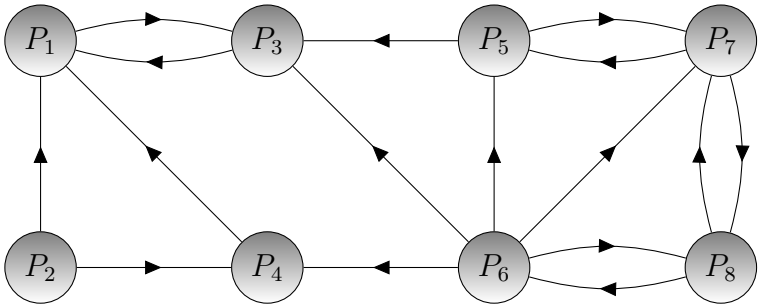
$$V = \{1, 2, 3, 4, 5, 6\}$$

und Kanten

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

(a) Ist dieser Graph planar? Zusammenhängend?
(b) Wieviele Farben sind zur Färbung mindestens notwendig, wenn Nachbarknoten verschiedene Farben erhalten sollen?
(c) Gibt es einen Eulerschen Kreis? Hamiltonschen Kreis?
(d) Bestimme die Adjazenzmatrix und die Anzahl der Wege der Länge 6 von Knoten 1 nach Knoten 6.
(e) Berechne eine Formel für die Anzahl der geschlossenen Wege von Knoten 1 nach Knoten 6 (Computer!).

Aufgabe 62. Gegeben sei das Miniatur-Internet



Erstelle die Google-Matrix und bestimme näherungsweise den Pagerank aller Seiten durch Iteration (50-100 müssten reichen) mit Hilfe eines Computeralgebrasystems, z.B. mit SAGE (`http://www.sagemath.org`), und zwar zunächst mit $\alpha = 1$, dann mit $\alpha = 0.85$. Was fällt auf? Wie kann man das Phänomen erklären?