Aufgabe 1. (a) Schreibe das gesamte griechische Alphabet eigenhändig (in Groß- und Kleinschreibung).

(b) Benenne die folgenden Symbole und finde jeweils alle, die *nicht* dem griechischen Alphabet entstammen.

$$\alpha\,\beta\,\gamma\,\text{ш}\,\xi\,\pi\,\zeta\,\emptyset\,\chi\,\omega\,đ\,\epsilon\,\vartheta\,\hbar\,\eta\,\hbar\,\lambda\,\varphi\,\kappa\,\text{Þ}\,\wp\,\psi\in\upsilon\,\upsilon\,\text{Ч}\,\partial\,\theta\,\phi\,\delta\,\nu\,\mu$$

$$\text{A}\,\text{B}\,\Gamma\,\Lambda\,\nabla\,\text{M}\,\Upsilon\,\text{N}\,\Phi\,\Pi\,\text{Я}\,\Sigma\,\text{T}\,\dagger\,\text{X}\,\text{Ш}\,\Delta\,\aleph\,\Xi\,\text{E}\,\text{H}\,\text{K}\,\Omega\,\Psi$$

Aufgabe 2. Die sieben Samurai sind zusammen 332 Jahre alt. Zeige, daß drei von ihnen so gewählt werden können, daß sie zusammen mindestens 142 Jahre alt sind.

Aufgabe 3. Ist es möglich, die Ziffern 1–9 nacheinander so anzuordnen, dass zwischen 1 und 2, 2 und 4, 4 und 5, 5 und 7, sowie 7 und 8 jeweils eine ungerade Anzahl von Ziffern steht?

Aufgabe 4. Wir betrachten folgende Bedingungen:

(1) Es stehen fünf Häuser in einer Reihe nebeneinander (von links nach rechts). Jedes Haus hat eine andere Farbe.
(2) In jedem Haus wohnt eine Person einer anderen Nationalität.
(3) Jede Person bevorzugt ein bestimmtes Getränk, spielt ein bestimmtes Musikinstrument und hält ein bestimmtes Haustier.
(4) Alle fünf Getränke, Musikinstrumente und Haustiere sind verschieden.

und die folgenden Angaben:

(1) Der Violinist wohnt neben dem, der eine Katze hält.
(2) Der Däne lebt im roten Haus.
(3) Der Brite trinkt gerne Tee.
(4) Das grüne Haus steht direkt links vom weißen Haus.
(5) Der Norweger wohnt im ersten Haus.
(6) Im gelben Haus steht ein Klavier.
(7) Der Deutsche spielt Trompete.
(8) Der Bewohner des mittleren Hauses trinkt gerne Milch.
(9) Der Violinist hat einen Nachbarn, der gerne Bier trinkt.
(10) Der Gitarrist hält eine Vogel.
(11) Der Schwede hält einen Hund.
(12) Der Norweger wohnt neben dem blauen Haus.
(13) Der Flötenspieler trinkt gerne Wasser.
(14) Der Mann mit dem Pferd wohnt neben dem, der Klavier spielt.
(15) Der Besitzer des grünen Hauses trinkt gerne Kaffee.

Frage: Wem gehört der Fisch?

Aufgabe 5. Konstruiere Wahrheitstafeln für die folgenden Formeln:
(a) $((A \wedge B) \wedge (\neg B \vee C))$
(b) $(A \leftrightarrow (B \leftrightarrow C))$

Aufgabe 6. Zeige anhand von Wahrheitstafeln die Äquivalenz

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

Aufgabe 7. Inspektor Kottan hat drei Tatverdächtige: Schrammel, Schremser und Pilch. Folgende Zusammenhänge sind bekannt:
(a) Ist Schrammel unschuldig, dann ist Pilch Mittäter.
(b) Wenn Schrammel oder Schremser zu den Tätern gehören, dann ist Pilch unschuldig.
(c) Wenn Pilch oder Schrammel unschuldig sein, dann ist Schremser ein Mittäter.
Formalisiere den Sachverhalt und löse den Fall!

Aufgabe 8. Auf einem entfernten Planeten sagen Mathematiker immer die Wahrheit und Physiker immer die Unwahrheit. Untersuche die folgenden Situationen und stelle fest, welche Konstellationen möglich sind:
(a) A sagt: "B ist ein Mathematiker."
B sagt: "A ist kein Mathematiker."
(b) A sagt: "B ist ein Mathematiker."
B sagt: "A ist ein Physiker."

Aufgabe 9. Bestimme alle paarweise nicht-äquivalenten Aussageformen, die aus den Variablen A und B sowie dem Junktor $\to$ (Implikation) aufgebaut werden können.

Aufgabe 10. 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.

Aufgabe 11. (a) Lies den Monolog des Mephistopheles (Verse 1908–1941 aus Goethes *Faust I*).
(b) Formalisiere die Verse 1928–1933 und bringe sie auf möglichst kompakte Form. Letztere lauten:

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.

Aufgabe 12. Zeige mit den Regeln des logischen Schließens[1] die Allgemeingültigkeit des Ausdrucks

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

Aufgabe 13. (a) Zeige anhand eines Beispiel, daß die Aussagen

$$(\forall a \in A : P(a)) \to Q \qquad \text{und} \qquad \forall a \in A : (P(a) \to Q)$$

im Allgemeinen nicht äquivalent sind.

(b) Finde Prädikate $P(x)$ und $Q(x)$ über $x \in \mathbb{R}$, sodaß die Aussage

$$\forall x \in \mathbb{R} : (P(x) \to Q(x))$$

falsch ist und die Aussage

$$(\forall x \in \mathbb{R} : P(x)) \to (\forall x \in \mathbb{R} : Q(x))$$

wahr ist.

Aufgabe 14. Zeige, daß folgende Aussagen äquivalent sind:

(a) $A \subseteq B$

(b) $A \cup B = B$

(c) $A \cap B = A$

(d) $A \setminus B = \emptyset$

Aufgabe 15. Zeige (anhand von Venndiagrammen *und* durch formale Logik):

(a) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$

(b) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$

[1] `https://www.math.tugraz.at/idm-lv/dmnawi/2019/Uebungsblaetter/logikregeln.pdf`

Aufgabe 16. Untersuche, ob die folgenden Relationen $R \subseteq X \times X$ reflexiv, symmetrisch, transitiv, antisymmetrisch, konnex oder asymmetrisch sind. Welche Relationen sind Äquivalenz-, welche Ordnungsrelationen? Bestimme ggf. die Äquivalenzklassen und ein Repräsentantensystem.

(i) $X = \mathbb{N}$, Relation: $mRn \iff 2|(m \cdot n)$.
(ii) $X = \mathbb{R}^2$, Relation: $(x_1, x_2)R(y_1, y_2) \iff x_2 \leq y_2$.
(iii) $X = \mathbb{R}^2$, Relation: $(x_1, x_2)R(y_1, y_2) \iff x_1 \leq y_1 \wedge x_2 \leq y_2$.
(iv) A eine Menge, $X = \mathcal{P}(A) \setminus \{\emptyset\}$, Relation: $xRy \iff x \cap y \neq \emptyset$.
(v) X beliebig, Relation: $xRy \iff x \neq y$.

Aufgabe 17. Vervollständige den Beweis von Satz 2.12 aus der Vorlesung: Sei X eine Menge und $\mathcal{Z} \subseteq \mathcal{P}(X)$ eine Partition von X, dann wird durch

$$x \sim y :\iff \exists A \in \mathcal{Z} : x \in A \wedge y \in A$$

eine Äquivalenzrelation auf X definiert, sodaß $X/_\sim = \mathcal{Z}$.

Aufgabe 18. Sei X eine Menge.

(a) Auf X sei eine Familie $(R_i)_{i \in I}$ von Äquivalenzrelationen $R_i \subseteq X \times X$ gegeben. Zeige, daß $R = \bigcap_{i \in I} R_i$ ebenfalls eine Äquivalenzrelation auf X ist.
(b) Konstruiere ein Beispiel für zwei Äquivalenzrelationen R_1 und R_2 auf einer Menge X, sodaß $R_1 \cup R_2$ keine Äquivalenzrelation ist.
(c) Sei $A \subseteq X \times X$ eine beliebige Teilmenge. Zeige, daß es eine eindeutige minimale Äquivalenzrelation R_0 auf X gibt, sodaß $A \subseteq R_0$, d.h., daß für jede Äquivalenzrelation R mit $A \subseteq R$ auch $R_0 \subseteq R$ gilt.
(d) Sei $X = \{1, 2, 3, 4, 5, 6, 7\}$. Bestimme die kleinste Äquivalenzrelation, die die Menge $A = \{(1, 3), (1, 4), (2, 7)\}$ enthält, und die Äquivalenzklassen.

Aufgabe 19. Zeige, daß durch

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

eine Äquivalenzrelation auf $\mathbb{R}^2$ definiert wird. Bestimme die Faktormenge $\mathbb{R}^2/_\sim$ und interpretiere sie geometrisch.

Aufgabe 20. Seien X und Y Mengen und $f : X \to Y$ eine Funktion. Zeige, daß durch

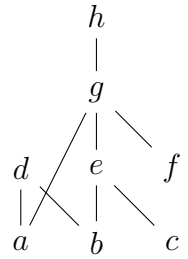
$$x \sim y : \Longleftrightarrow f(x) = f(y)$$

eine Äquivalenzrelation auf X definiert wird und daß die Funktion

$$\begin{aligned} f : X/_\sim &\to Y \\ [x] &\mapsto f(x) \end{aligned}$$

wohldefiniert und injektiv ist.

Aufgabe 21. Wir betrachten die Menge $\{a, b, c, d, e, f, g, h\}$ mit der durch das folgende Hasse-Diagramm gegebenen Ordnungsrelation.



(a) Bestimme, wenn existent, alle minimalen und maximalen Elemente sowie Maximum und Minimum.
(b) Zähle alle *Ketten*[2] auf.
(c) Zähle alle *Antiketten*[3] auf.
(d) Bestimme, wenn möglich, die folgenden *Infima*[4] und *Suprema*[5]:

$$a \vee c, a \wedge c, c \vee f, d \vee g, d \wedge g, d \wedge e, d \wedge f, d \vee f$$

[2]Eine **Kette** ist eine totalgeordnete Teilmenge.
[3]Eine **Antikette** ist eine Teilmenge mit paarweise unvergleichbaren Elementen.
[4]Das **Infimum** $x \wedge y$ von zwei Elementen ist die größte untere Schranke.
[5]Das **Supremum** $x \vee y$ von zwei Elementen ist die kleinste obere Schranke.

Aufgabe 22. Bestimme das Hasse-Diagramm der teilgeordneten Menge Π_4 aller Partitionen der Menge $\{1, 2, 3, 4\}$ mit der Ordnungsrelation

$$\mathcal{Z}_1 \leq \mathcal{Z}_2 : \Longleftrightarrow \forall A \in \mathcal{Z}_1 \exists B \in \mathcal{Z}_2 : A \subseteq B.$$

Aufgabe 23. Zeige, daß aus jeder Menge von 10 verschiedenen natürlichen Zahlen eine Teilmenge ausgewählt werden kann, deren Summe durch 10 teilbar ist.

Aufgabe 24. Nach einer Überschwemmung wurden aus dem Lager eines Schuhgeschäfts 600 Schuhe gerettet, und zwar jeweils 200 in den Größen 41, 42 und 43. Von den 600 Schuhen sind 300 linke und 300 rechte Schuhe. Zeige, daß mindestens 100 passende Paare gebildet werden können.

Aufgabe 25. Seien X eine endliche Menge mit $|X| = m$ Elementen und $Y = \{1, 2, \ldots, n\}$ eine Menge mit n Elementen. Zeige: Wenn Zahlen $r_i \in \mathbb{N}$ gegeben sind mit $r_1 + r_2 + \cdots + r_n < m + n$, dann gibt es für jede Funktion $f : X \to Y$ ein Element $i \in Y$, sodaß $|f^{-1}(i)| \geq r_i$.

Aufgabe 26. (a) Wieviele ungerade Zahlen zwischen 1000 und 9999 haben lauter verschiedene Ziffern?

(b) Wieviele ungerade Zahlen haben lauter verschiedene Ziffern?

Aufgabe 27. Herr S. macht Urlaub auf Ibiza und schickt jeweils eine Postkarte an jeden seiner 3 Freunde. Es stehen 6 Motive mit türkisen Stränden und 5 Motive mit Pferden zur Auswahl, insgesamt also 11 verschiedene Motive. Wieviele Kombinationen von Postkarten sind möglich, wenn

(i) es egal ist, wer welche Postkarte bekommt.
(ii) es auch darauf ankommt, wer welche Postkarte bekommt.

und

(a) alle Motive verschieden sein müssen.
(b) auch gleiche Motive vorkommen dürfen.

Was ändert sich, wenn

(a′) sein bester Freund unbedingt ein Pferd haben will?
(b′) mindestens ein Strand dabei sein soll?

Aufgabe 28. (a) Wieviele verschiedene 7-stellige Telephonnummern können aus den Ziffern 1, 1, 1, 2, 2, 3, 4 gebildet werden?
(b) Wieviele dieser Nummern beginnen mit 1? mit 2? mit 3? mit 4?
(c) Wir schreiben die gefundenen Telephonnummern der Größe nach in eine Liste. An welcher Stelle steht die kleinste Zahl, die mit 3 beginnt?
(d) wie (c), welche Telephonnummer steht an der 240. Position?
(e) Wieviele verschiedene 7-stellige Telephonnummern können aus den Ziffern 1, 1, 2, 2, 3, 3, 4 gebildet werden, sodaß benachbarte Ziffern verschieden sind?

Aufgabe 29. Wieviele natürliche Zahlen $n \leq 10^6$ können weder als Quadrat $n = k^2$, noch als Kubikzahl $n = k^3$, noch als Potenz $n = k^5$ für ein $k \in \mathbb{N}$ dargestellt werden?

Aufgabe 30. Beweise durch kombinatorische Argumente:

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$$

Aufgabe 31. Ein **Fixpunkt** einer Abbildung $f : X \to X$ ist ein Element $x \in X$, sodaß $f(x) = x$. Bestimme die Anzahl der bijektiven Abbildungen $f : X \to X$, die keinen einzigen Fixpunkt besitzen, wenn $|X| = n$.
Hinweis: Inklusion-Exklusion.

Aufgabe 32. (a) Zeige, daß

$$\left\{ n \atop 2 \right\} = 2^{n-1} - 1$$

(b) Sei $n = pk$. Bestimme die Anzahl der Mengenpartitionen von $\{1, 2, \ldots, n\}$, sodaß alle Klassen k Elemente enthalten.

Aufgabe 33. Zeige, daß die Folge B_n der Anzahl der Mengenpartitionen einer n-elementigen Menge die Rekursion

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

erfüllt.

Aufgabe 34. Seien X und Y Mengen mit $|X| = n$ und $|Y| = n-3$. Zeige, daß die Anzahl aller surjektiven Funktionen von X nach Y gegeben ist durch

$$\frac{n!(n-2)(n-3)^2}{48}$$

Aufgabe 35. Zeige mit kombinatorischen Argumenten, daß

$$m^n = \sum_{k=0}^{n} \left\{ n \atop k \right\} m^{\underline{k}}$$

Aufgabe 36. Sei $\mathcal{M}_n$ die Menge aller Gitterpfade $(y_0, y_1, \ldots, y_n)$ der Länge n, die die Bedingungen

$$y_0 = y_n = 0, \qquad y_k \geq 0, k = 0, 1, \ldots, n \qquad |y_k - y_{k-1}| \leq 1, k = 1, 2, \ldots, n;$$

d.h., die Höhendifferenz zwischen benachbarten Punkten ist -1, 0, oder 1. Zeige, daß die Anzahl $M_n = |\mathcal{M}_n|$ dieser Pfade die Rekursionen

(a) $M_n = M_{n-1} + \sum_{k=0}^{n-2} M_k M_{n-2-k}$

(b) $M_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} C_k$

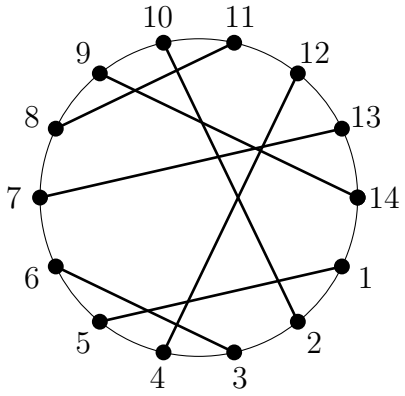
erfüllt, wobei C_n die aus der Vorlesung bekannte Folge der Catalanzahlen bezeichnet.

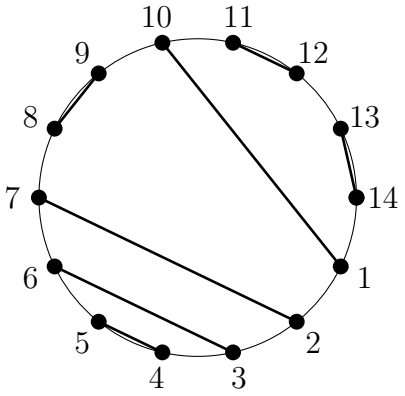
Aufgabe 37. (a) Wir betrachten $2n$ Punkte auf einem Kreis und verbinden sie zu Paaren wie in der untenstehenden linken Abbildung. Wieviele solche Paarungen gibt es?

(b) Zeige, daß die Anzahl der Paarungen, die sich nicht gegenseitig überkreuzen (rechte Abbildung), durch die Catalanzahlen C_n gegeben ist.

(c) Zeige, daß die Anzahl der unvollständigen Paarungen (d.h., Partitionen in Klassen mit höchstens 2 Elementen) von n Punkten, die sich nicht gegenseitig kreuzen, durch die Zahl M_n aus der vorhergehenden Übung gegeben ist.

Hinweis: es kann hilfreich sein, den Kreis an einer Stelle aufzuschneiden und auszurollen.





Aufgabe 38. Zeige, daß es unter 8 natürlichen Zahlen $n_1, n_2, \ldots, n_8 \in \{1, 2, \ldots, 15\}$ stets drei Paare mit der gleichen Differenz gibt.

Aufgabe 39. Zeige: Es gibt eine ganze Zahl der Form $11111\ldots1$, die durch 2019 teilbar ist. Gib eine obere Schranke für diese Zahl an.

Aufgabe 40. Zeige (z.B. durch Induktion), daß für jedes $n \in \mathbb{N}$ und jedes $a \in \mathbb{N}$ die Zahl $a^{2n+1} - a$ durch 6 teilbar ist.

Aufgabe 41. Berechne mit dem euklidischen Algorithmus $\mathrm{ggT}(m,n)$ sowie Zahlen a und b, sodaß $\mathrm{ggT}(m,n) = am + bn$ für die folgenden Zahlenpaare:

$$(144, 89) \qquad (7^{15}+1, 7^{12}-1) \qquad (4711, 2019) \qquad (332211, 112233)$$

Aufgabe 42. Zeige (ohne Verwendung der Primfaktorzerlegung), daß für beliebige Zahlen $m, n \in \mathbb{N}$ gilt

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

Aufgabe 43. Bestimme

$$\min\{126a + 266b + 315c \mid a, b, c \in \mathbb{Z}\} \cap \mathbb{N}$$

sowie Koeffizienten a, b, c, für die das Minimum angenommen wird.

Aufgabe 44. Seien $a, b, c \in \mathbb{Z}$ Zeige (ohne Verwendung der Primfaktorzerlegung): Wenn $a|bc$ und $\mathrm{ggT}(a,b) = 1$, dann gilt $a|c$.

Aufgabe 45. Seien $a, b, c \in \mathbb{Z}$ mit $(a,b) \neq (0,0)$ und $d = \mathrm{ggT}(a,b)$. Wir betrachten die Gleichung

$$ax + by = c$$

Zeige:

(a) Die Gleichung besitzt eine ganzzahlige Lösung genau dann, wenn $d|c$.

(b) Sei (x_0, y_0) eine Lösung, dann haben alle anderen Lösungen die Form $(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d})$ für ein $k \in \mathbb{Z}$.

Hinweis: Aufgabe 44.

Aufgabe 46. Bestimme alle Lösungen $x \in \mathbb{Z}$ der Gleichungen

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

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

Aufgabe 47. Zeige: Es gibt unendlich viele Primzahlen p mit $p \equiv 3 \mod 4$.

Aufgabe 48. 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 Dezimalentwicklung $n = \sum a_i 10^i$ gilt

$$11 \,\big|\, n \qquad \Longleftrightarrow \qquad 11 \,\Big|\, \sum a_i (-1)^i.$$

Aufgabe 49. (a) Zeige:

$$a \equiv b \mod m_1 \quad \wedge \quad a \equiv b \mod m_2 \qquad \Longleftrightarrow \qquad a \equiv b \mod m$$

wobei $m = \mathrm{kgV}(m_1, m_2)$.

(b) Folgere daraus, daß die Lösung des Kongruenzgleichungssystems

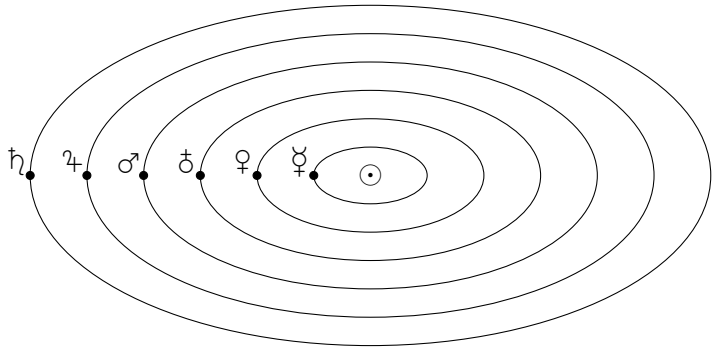
$$\begin{aligned} x &\equiv c_1 \mod m_1 \\ x &\equiv c_2 \mod m_2 \\ &\vdots \\ x &\equiv c_n \mod m_n \end{aligned}$$

eindeutig ist modulo $m = m_1 m_2 \cdots m_n$, wenn $\mathrm{ggT}(m_i, m_j) = 1$ für $i \neq j$.

Aufgabe 50. Berechne $2^{31} \mod 900$.
Hinweis: Rechne modulo der Primfaktoren ($900 = 4 \cdot 9 \cdot 25$) und ermittle das Endresultat mit dem chinesischen Restsatz.

Zusatzaufgabe. Die folgende Tabelle zeigt die Umlaufzeiten (U) der frei sichtbaren Planeten, sowie die Zeit in Tagen (D), die am 7.1.2020 jeweils vergangen sind, seit jeder einzelne das letzte Mal den Punkt der Wintersonnenwende durchlaufen ist.

	U	D
Merkur	88	49
Venus	225	14
Erde	365	24
Mars	687	272
Jupiter	4333	2141
Saturn	10759	3275



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 49 anwenden.

Aufgabe 51. Bestimme, wenn möglich, alle Lösungen der folgenden Kongruenzgleichungssysteme.

$$(a)\quad \begin{aligned} x &\equiv 1 \mod 6 \\ x &\equiv 3 \mod 10 \\ x &\equiv 5 \mod 15 \end{aligned} \qquad (b)\quad \begin{aligned} x &\equiv 4 \mod 6 \\ x &\equiv 2 \mod 10 \\ x &\equiv 7 \mod 15 \end{aligned}$$

Aufgabe 52. Seien $a, b \in \mathbb{Z}$ und $m, n \in \mathbb{N}$ mit $d = \mathrm{ggT}(m, n)$. Zeige, daß das Kongruenzgleichungssystem

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

genau dann lösbar ist, wenn $a \equiv b \mod d$.

Aufgabe 53. Sei $m \in \mathbb{N}$ eine ungerade Zahl mit Primfaktorzerlegung $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Bestimme die Anzahl der Lösungen der Gleichung

$$x^2 \equiv 1 \mod m$$

in $\mathbb{Z}_m$.
Hinweis: Verwende Aufgabe 49 und die Tatsache, daß eine ungerade Primzahl p nicht gleichzeitig $x + 1$ und $x - 1$ teilen kann.

Aufgabe 54. (a) Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$, dann gilt

$$a - b \,\big|\, a^m - b^m$$

(b) Sei $n \in \mathbb{N}$ eine Zahl mit der Eigenschaft, daß $2^n + 1 \in \mathbb{P}$. Zeige, daß $n = 2^k$ für ein $k \in \mathbb{N}$.
(c) Sei $n \in \mathbb{N}$ eine Zahl mit der Eigenschaft, daß $2^n - 1 \in \mathbb{P}$. Zeige, daß $n \in \mathbb{P}$.

Aufgabe 55. Wir betrachten die Funktionen

$$\delta : \mathbb{N} \to \mathbb{N} \qquad \sigma : \mathbb{N} \to \mathbb{N}$$
$$n \mapsto \sum_{\substack{1 \le d < n \\ d \mid n}} d \qquad n \mapsto \sum_{\substack{1 \le d \le n \\ d \mid n}} d$$

Eine Zahl heißt **perfekt** wenn $\delta(n) = n$. Zeige:

(a) Wenn $\mathrm{ggT}(a, b) = 1$, dann ist $\sigma(a \cdot b) = \sigma(a)\sigma(b)$.
(b) Wenn $p = 2^k - 1 \in \mathbb{P}$, dann ist $n = 2^{k-1}(2^k - 1)$ perfekt.

Aufgabe 56. Berechne ohne Hilfsmittel in $\mathbb{Z}_{50}$

$$(a) \quad [3]^{2^{31}} \qquad (b) \quad [2]^{3^{31}}$$

Aufgabe 57. Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$g = 3 \qquad p = 113$$
$$m = 54 \qquad n = 42$$

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

Aufgabe 58. Gegeben sei der RSA-Schlüssel $m = 2701$, $r = 1085$.

(a) Verschlüssle die Botschaft $(3, 4, 5)$.
(b) Bestimme den inversen Schlüssel s und entschlüssle die Botschaft $(2374, 601, 356)$.

Hinweis: Für einen Teil der Berechnungen ist wahrscheinlich ein Computer erforderlich.

Aufgabe 59. Sei $D = \{3k + 1 \mid k \in \mathbb{N}_0\}$.

(a) Zeige, daß D mit der üblichen Multiplikation ein Monoid (=Halbgruppe mit 1) ist.
(b) Eine Zahl $a \in D$ mit $d > 1$ heißt **irreduzibel**, wenn sie nicht in der Form $a = b \cdot c$, $b, c \in D \setminus \{1\}$ geschrieben werden kann. Bestimme alle irreduziblen Elemente ≤ 100.
(c) Zeige, daß jedes Element $a \in D$ als Produkt von irreduziblen Elementen geschrieben werden kann.
(d) Zeige, daß die Zerlegung in irreduzible Elemente nicht eindeutig sein muß.
(e) Ein Element $p \in D$ heißt **prim** wenn gilt:

$$p \mid ab \implies p \mid a \vee p \mid b.$$

Zeige, daß 4 nicht prim ist.

Aufgabe 60. Zeige, daß in einem ungerichteten Graphen G die Relation

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

eine Äquivalenzrelation ist. Welche Relation erhält man, wenn man "Weg" durch "Pfad" ersetzt?

Aufgabe 61. Die Gradfolge eines Graphen ist die Folge der Grade der einzelnen Knoten in absteigender Ordnung. Ist es möglich, Graphen (ohne Schleifen und Mehrfachkanten) mit den folgenden Gradfolgen zu konstruieren?

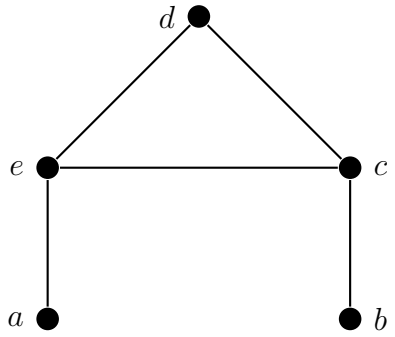
(a)	$(3,3,3,3)$	(b)	$(4,3,2,1)$
(c)	$(3,3,3,2,1)$	(d)	$(1,1,1,1,1)$

Aufgabe 62. Ein Baum ist definiert als zusammenhängender, kreisfreier Graph. Zeige, daß für einen endlichen Graphen $G = (V, E)$ die Aussage "G ist ein Baum" zu jeder der drei folgenden Eigenschaften äquivalent ist.

(a) G ist zusammenhängend und $|E| = |V| - 1$
(b) Für je zwei Knoten u und v gibt es genau einen Pfad von u nach v.
(c) G ist kreisfrei und das Hinzufügen einer beliebigen neuen Kante erzeugt einen Kreis.

Aufgabe 63. Sei $G = (V, E)$ ein Graph. Der *Kantengraph* von G ist der Graph $L(G) = (E, W)$ wobei $[e_1, e_2] \in W \iff e_1 \cap e_2 \neq \emptyset$. (In Worten: Die Knoten von $L(G)$ sind die Kanten von G und zwei Kanten werden verbunden, wenn sie einen Knoten gemeinsam haben). Zeige: Wenn der Graph G eine Eulersche Tour besitzt, dann auch der Kantengraph. Gilt auch die Umkehrung?

Aufgabe 64. Gegeben sei der folgende Graph.



Bestimme die Adjazenzmatrix und die Anzahl der Wege der Länge 7 vom Knoten a zum Knoten b.