

12. Tutoriumsblatt – Diskrete Strukturen

(Besprechung in den Tutorien in der Woche vom 15.07.2024)

“Es konnte ja keiner wissen, dass das DSsoziativum so ne starke Wirkung hat.”, versucht sich Professor Reztuerk zu verteidigen, nachdem ihr ihn mit dem Zustand des Campus konfrontiert. “Wir wollten nur etwas nachhelfen, damit die Studierenden von sich aus die Übungsaufgaben bearbeiten. Ich hatte nicht erwartet, dass sie selbst bei minimaler Dosierung so fanatisch werden würden.”

Erschöpft fällt der Professor in seinen Stuhl zurück. Die Tür hinter euch fällt ins Schloss und du merkst wie sich die Luft im Raum verdichtet. Du fühlst dich als würdest du der Welt langsam entschweben. Das letzte was noch zu dir durchdringt ist eine intensive flötende Stimme: *“Übungsaufgaben! Die wollt ihr doch am liebsten. Extra viele Übungsaufgaben! Das ist euer größter Wunsch. Frische Übungsaufgaben! Nur für euch bereitet. Lasst euch von ihnen ergreifen und blickt nicht zurück!”*

Aufgabe 1

Sei $a^b := a^b$ die Exponentiation auf den natürlichen Zahlen, sei \mathcal{G}_1 die Menge aller (nicht-leeren) Graphen und sei Σ_{3b}^* die Menge aller Wörter über dem Universum $\Sigma = \{a, b\}$, die maximal 3 Mal den Buchstaben b enthalten.

Bestimme für die Tupel $(\mathbb{N}, ^\wedge), (\Sigma_{3b}^*, \circ), (\mathcal{G}_1, \cup), (\{0\}, +), (\{0, 1\}, \cdot)$ welche der folgenden Eigenschaften sie haben.

- (i) Es ist eine Algebra.
- (ii) Es ist ein Monoid.
- (iii) Es ist eine Gruppe.

Aufgabe 2

Sei $m \geq 2$. Seien weiter $A_m = \{0, 1, \dots, m - 1\}$ und $A_m^+ = A_m \setminus \{0\}$. Wir definieren $a +_m b = a + b \bmod m$ und $a \cdot_m b = a \cdot b \bmod m$ als die modulare Addition und die modulare Multiplikation.

- (i) Beweise, dass $(A_m, +_m)$ eine Gruppe ist.
- (ii) Beweise, dass (A_m, \cdot_m) ein Monoid ist.
- (iii) Bestimme unter welchen Bedingungen (A_m^+, \cdot_m) eine Gruppe ist.

Anmerkung: Die Rechenregeln für modulare Arithmetik aus der Vorlesung müssen nicht erneut bewiesen werden.

Aufgabe 3

Bestimmen Sie alle Gruppenhomomorphismen von $(\mathbb{Z}, +)$ nach $(\mathbb{Q}, +)$. Gibt es darunter Isomorphismen?

Aufgabe 4

Ein planarer Graph besteht aus 9 Knoten mit Grad k und teilt die Ebene in 11 Gebiete auf. Bestimme k .

Aufgabe 1

Sei $a^b := a^b$ die Exponentiation auf den natürlichen Zahlen, sei \mathcal{G}_1 die Menge aller (nicht-leeren) Graphen und sei Σ_{3b}^* die Menge aller Wörter über dem Universum $\Sigma = \{a, b\}$, die maximal 3 Mal den Buchstaben b enthalten.

Bestimme für die Tupel $(\mathbb{N}, \wedge), (\Sigma_{3b}^*, \circ), (\mathcal{G}_1, \cup), (\{0\}, +), (\{0, 1\}, \cdot)$ welche der folgenden Eigenschaften sie haben.

- (i) Es ist eine Algebra.
- (ii) Es ist ein Monoid.
- (iii) Es ist eine Gruppe.

(\mathbb{N}, \wedge) : Algebra, denn \wedge abgeschlossen in \mathbb{N} , d.h. für alle $a, b \in \mathbb{N}$ ist $a \wedge b \in \mathbb{N}$
kein Monoid, kein Gruppe, da \wedge nicht assoziativ, dann es gilt nicht immer $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

(Σ_{3b}^*, \circ) : kein Algebra, da \emptyset nicht in Σ_{3b}^* abgeschlossen ist
Bsp. $bbb \in \Sigma_{3b}^*$, $b \in \Sigma_{3b}^*$ aber $bbbob \notin \Sigma_{3b}^*$

$(M, *)$ heißt Algebra, falls gilt:

- $M \neq \emptyset$
- $* : M^n \rightarrow M$ ist eine „innere Verknüpfung“
 $\hookrightarrow n$ ist die „Stelligkeit“ von $*$

(\mathcal{G}_1, \cup) : Algebra, da f.a. Graphen $g_1, g_2 \in \mathcal{G}_1$, $g_1 \cup g_2 \in \mathcal{G}_1$
kein Monoid, \cup assoziativ
es gibt kein neutrales Element.

Ist $(M, *)$ eine Algebra und $* : M \times M \rightarrow M$, dann heißt $(M, *)$

→ Monoid, falls gilt: • $*$ ist assoziativ

$$\hookrightarrow \forall a, b, c \in M : (a * b) * c = a * (b * c)$$

• es gibt ein neutrales Element

$$\hookrightarrow \exists e \in M \quad \forall a \in M : e * a = a * e = a$$

→ Gruppe, falls gilt: • $*$ ist assoziativ

• es gibt ein neutrales Element e

• jedes Element $a \in M$ besitzt ein inverses Element

$$\hookrightarrow \forall a \in M \quad \exists x \in M : x * a = a * x = e$$

	(\mathbb{N}, \wedge)	(Σ_{3b}^*, \circ)	(\mathcal{G}_1, \cup)	$(\{0\}, +)$	$(\{0, 1\}, \cdot)$
Algebra	✓	✗	✓	✓	✓
Monoid	✗	✗	✗	✓	✓
Gruppe	✗	✗	✗	✓	✗

Aufgabe 2

Seien $A_m = \{0, 1, \dots, m-1\}$ und $A_m^+ = A_m \setminus \{0\}$. Wir definieren $a+_m b = a+b \bmod m$ und $a \cdot_m b = a \cdot b \bmod m$ als die modulare Addition und die modulare Multiplikation.

(i) Beweise, dass $(A_m, +_m)$ eine Gruppe ist.

(ii) Beweise, dass (A_m^+, \cdot_m) ein Monoid ist.

i) • $A_m \neq \emptyset$, da $m \in \mathbb{N}_{\geq 2}$

• nach Def. gilt $+_m : A_m \times A_m \rightarrow A_m$, da $x \bmod m \in \{0, \dots, m-1\}$ für alle $x \in \mathbb{Z}$

• Assoziativität

↳ Seien $a, b, c \in A_m$. Dann gilt

$$\begin{aligned} (a+_m b) +_m c &= [(a+b) \bmod m + c] \bmod m \\ &\stackrel{(1)}{=} [(a+b) + c] \bmod m \\ &\stackrel{\text{Assoziativität von } +}{\sim} = [a + (b+c)] \bmod m \\ &\stackrel{(2)}{=} [a + (b+c) \bmod m] \bmod m \\ &= a +_m (b +_m c) \end{aligned}$$

(*) Aus $[a \bmod m] \bmod m$

$$\begin{aligned} \text{und } (a+b) \bmod m &= [(a \bmod m) + (b \bmod m)] \bmod m \\ \text{folgt: } (a+b) \bmod m &= [(a \bmod m) + (b \bmod m)] \bmod m \\ &= [(a \bmod m) + (b \bmod m)] \bmod m \\ &= (a+b) \bmod m \end{aligned}$$

• neutrales Element

↳ $0 \in A_m$ ist neutrales Element

inverse Element zu x : $x^{-1} = m-x$

$$\begin{aligned} \exists x \in A_m \text{ mit } x +_m x^{-1} &= 0 \quad \text{d.h. } x +_m (m-x) = x + (m-x) \bmod m \\ &= m \bmod m = 0 \end{aligned}$$

• inverse Elemente

↳ Sei $a \in A_m^+$. Dann ist $0 = m \bmod m = [a + (m-a)] \bmod m = a +_m \underbrace{(m-a)}_{\in A_m}$ $\Rightarrow a^{-1} = m-a$
Ist dagegen $a=0$, so gilt natürlich $a^{-1} := 0 \in A_m$

ii) • $A_m \neq \emptyset$, da $m \geq 2$

• $\cdot_m : A_m \times A_m \rightarrow A_m$ nach Definition wohldefiniert

• Assoziativität zeigt man analog zu oben

• neutrales Element

↳ $1 \in A_m$ und $\forall a \in A_m: a \cdot_m 1 = 1 \cdot_m a = a$

kein Gruppe

(iii) Bestimme unter welchen Bedingungen (A_m^+, \cdot_m) eine Gruppe ist.

Achtung: Hier ist wegen $0 \notin A_m^+$ die Wohldefiniertheit von \cdot_m zu überprüfen.

Ang. es ist $a \cdot_m b = 0 \bmod m = 0$ für $a, b \in A_m^+$.

$\Rightarrow \exists l \in \mathbb{N}: a \cdot b = l \cdot m$.

Wäre m eine Primzahl, dann hätte a oder b m als Primfaktor (nutze Eindeutigkeit der PFZ!).

↳ & zu $a, b \in \{0, \dots, m-1\}$.

Die Kontraposition liefert: m Prim $\Rightarrow a \cdot_m b \in A_m^+$

Ist dagegen m keine Primzahl, dann $\exists x, y \in A_m^+: m = a \cdot b$

↳ aber dann gilt für diese Zahlen: $x \cdot y \bmod m = 0 \notin A_m^+$

Also ist \cdot_m genau dann wohldefiniert, wenn m eine Primzahl ist.

Für die Gruppeneigenschaft ist nun noch auf Inverse Elemente zu überprüfen.

$$\exists z : \forall a \in \{1, \dots, m-1\} \exists x \in \{1, \dots, m-1\} : a \cdot_m x = 1.$$

$$\Rightarrow \text{es muss gelten } a \cdot x \equiv 1 \pmod{m}. \quad (\text{mit } x \in A_m^+)$$

↳ x ist multiplikatives modulares Inverse von a bzgl. $\text{mod } m$

$$\Rightarrow \text{es muss } z \in \mathbb{Z} \text{ mit } a \cdot x - z \cdot m = 1 \text{ geben (und } x \in A_m^+)$$

↳ falls $\text{ggT}(a, m) = 1$, gibt es dieses z nach dem Lemma von Bézout (VL 10, Seite 15)

↳ gibt es ein solches z , so muss aber auch $\text{ggT}(a, m) = 1$ gelten (Übung!)

Also existieren genau dann alle Inversen Elemente, wenn $\forall a \in A_m^+ : \text{ggT}(a, m) = 1$.

↳ wegen $1 \leq a \leq m-1$ ist dies aber dazu äquivalent, dass m prim ist.

Also ist (A_m^+, \cdot_m) genau dann eine Gruppe, wenn m prim ist.

Aufgabe 3

Bestimmen Sie alle Gruppenhomomorphismen von $(\mathbb{Z}, +)$ nach $(\mathbb{Q}, +)$. Gibt es darunter Isomorphismen?

Gesucht: $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Q}, +)$ mit $f(x+y) = f(x) + f(y)$ für alle $x, y \in \mathbb{Z}$.

$$\text{I: } f(0) = f(0+0) = f(0) + f(0) \Rightarrow 0 = f(0) + (-f(0)) = f(0) = \underbrace{f(0)}_{=0 \in \mathbb{Q}} + \underbrace{f(0) + (-f(0))}_{\mathbb{Q}}$$

$$h(0) = h(0+0) = \underbrace{\frac{h(0)+h(0)}{2}}_{\mathbb{Q}} = h(0) + h(0)$$

$$\text{II: } 0 = f(0) = f(x+(-x)) = f(x) + f(-x)$$

$$\Rightarrow f(-x) = -f(x) \quad \forall x$$

$$\text{III: Es gilt } f(2) = f(1+1) = f(1) + f(1) = 2 \cdot f(1)$$

und mit Induktion über $n \in \mathbb{N}$ zeigt man:

$$f(n) = n \cdot f(1).$$

整数
↓
0 + 正整数
↓

IV: Aus II und III folgt für $z \in \mathbb{Z} \setminus \mathbb{N}$, dass $-z \in \mathbb{N}$ und

$$f(z) = f(-(-z)) \stackrel{\text{II}}{=} -f(-z) \stackrel{\text{III}}{=} -(-z \cdot f(1)) = z \cdot f(1)$$

definiere $\underbrace{z \cdot f(1)}_{\text{z mal}} := \underbrace{f(1) + \dots + f(1)}_{\text{z mal}}$ für $z \geq 0$

und $\underbrace{z \cdot f(1)}_{-z \text{ mal}} := -(\underbrace{f(1) + \dots + f(1)}_{-z \text{ mal}})$ für $z < 0$

\leadsto Also gilt $f(z) = z \cdot f(1)$ für alle $z \in \mathbb{Z}$.

$\Rightarrow \mathcal{F} \{ f_x : z \mapsto z \cdot x \mid x \in \mathbb{Q} \}$ ist gesuchte Menge

Gesucht ist ein bijektiver Homomorphismus $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Q}, +)$.

Sei dafür $f_y \in \mathcal{F}$ für $y \in \mathbb{Q}$.

↳ ist $y=0$, dann gilt $f_0[\mathbb{Z}] = \{0\} \subseteq \mathbb{Q}$

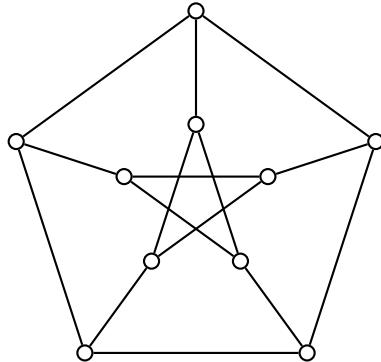
↳ ist $y \neq 0$, dann gilt $f_y[\mathbb{Z}] = \{z \cdot y \mid z \in \mathbb{Z}\} \subseteq \mathbb{Q}$

denn es ist $\frac{y}{3} \in \mathbb{Q}$, aber $\frac{y}{3} \notin \{z \cdot y \mid z \in \mathbb{Z}\}$.

denn gäbe es $z \in \mathbb{Z}$: $\frac{y}{3} = y \cdot z \stackrel{y \neq 0}{\Rightarrow} z = \frac{1}{3} \not\in \mathbb{Z}$

Aufgabe 5

Wir betrachten den folgenden Graphen *Pete*, der als der *Petersen Graph* bekannt ist.



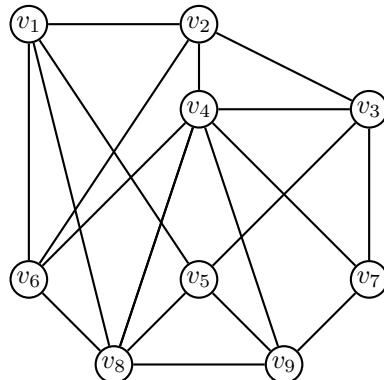
- (i) Zeigen Sie, dass *Pete* nicht planar ist, indem sie eine Unterteilung von $K_{3,3}$ finden.
- (ii) Können Sie eine Unterteilung von K_5 finden?

Aufgabe 6

Beweise: Für jeden dreiecksfreien planaren Graphen $G = (V, E)$ mit $|V| \geq 3$ Knoten gilt $|E| \leq 2|V| - 4$. Folgern Sie daraus, dass der $K_{3,3}$ nicht planar ist. (Ein Graph heißt dreiecksfrei, wenn er keinen K_3 als Teilgraphen enthält.)

Aufgabe 7

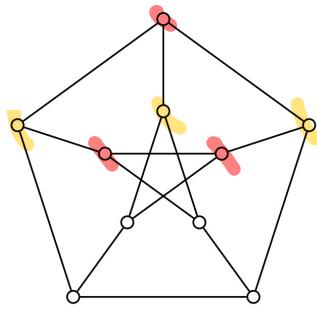
Sei G folgender Graph:



- (i) Bestimmen Sie $\chi(G)$ und geben Sie eine Färbung der Knoten von G mit $\chi(G)$ Farben an. Sie brauchen Ihre Antwort nicht zu begründen.
- (ii) Zeigen oder Widerlegen Sie: G ist planar.
- (iii) Geben Sie eine Menge $S \subseteq E(G)$ minimaler Kardinalität an, sodass $G - S$ 3-färbbar ist. Geben Sie dazu ohne Begründung eine 3-Färbung von $G - S$ an.
- (iv) Geben Sie ohne Begründung eine unabhängige Menge maximaler Kardinalität auf G an.
- (v) Sei G ein planarer Graph mit n Knoten. Geben Sie eine möglichst genaue untere Schranke (in Abhängigkeit von n) für die minimale Größe einer größtmöglichen unabhängigen Menge auf G .

Aufgabe 5

Wir betrachten den folgenden Graphen *Pete*, der als der *Petersen Graph* bekannt ist.

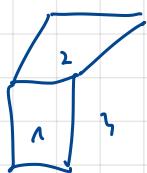


(i) Zeigen Sie, dass *Pete* nicht planar ist, indem sie eine Unterteilung von $K_{3,3}$ finden.

(ii) Können Sie eine Unterteilung von K_5 finden? **nein**

Aufgabe 6

Beweise: Für jeden dreiecksfreien planaren Graphen $G = (V, E)$ mit $|V| \geq 3$ Knoten gilt $|E| \leq 2|V| - 4$. Folgern Sie daraus, dass der $K_{3,3}$ nicht planar ist. (Ein Graph heißt dreiecksfrei, wenn er keinen K_3 als Teilgraphen enthält.)



$$|F| = |E| - |V| + 2$$

$$2|E| \geq 4|F|$$

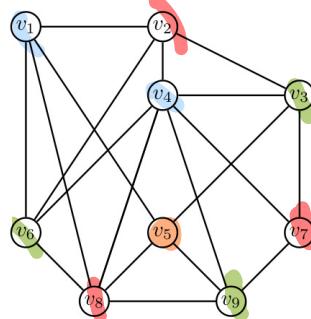
$$|F| \leq \frac{1}{2}|E|$$

$$|E| - |V| + 2 \leq \frac{1}{2}|E|$$

$$|E| \leq 2|V| - 4$$

Aufgabe 7

Sei G folgender Graph:



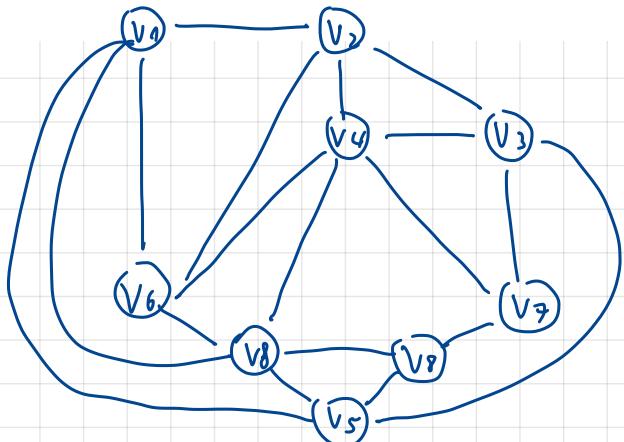
(i) Bestimmen Sie $\chi(G)$ und geben Sie eine Färbung der Knoten von G mit $\chi(G)$ Farben an. Sie brauchen Ihre Antwort nicht zu begründen. **$\chi(G)=4$**

(ii) Zeigen oder Widerlegen Sie: G ist planar.

(iii) Geben Sie eine Menge $S \subseteq E(G)$ minimaler Kardinalität an, sodass $G - S$ 3-färbbar ist. Geben Sie dazu ohne Begründung eine 3-Färbung von $G - S$ an.

(iv) Geben Sie ohne Begründung eine unabhängige Menge maximaler Kardinalität auf G an.

(v) Sei G ein planarer Graph mit n Knoten. Geben Sie eine möglichst genaue untere Schranke (in Abhängigkeit von n) für die minimale Größe einer größtmöglichen unabhängigen Menge auf G .



$$\text{(i)} \quad S = E(G) \setminus \{v_1, v_5\}$$

(ii) 3 看同色点的最大小量

$$(v) \lceil \frac{n}{4} \rceil$$

Aufgabe 8

Sei G ein planarer Graph, eingebettet in die Ebene, so dass keine zwei seiner Kanten sich überschneiden.

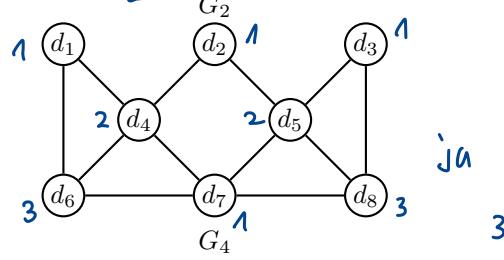
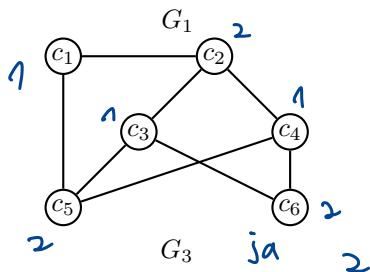
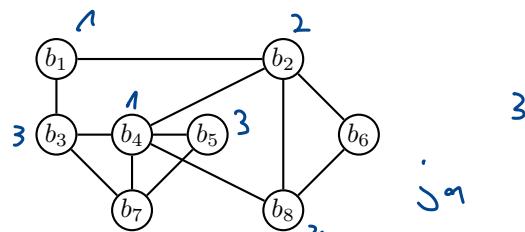
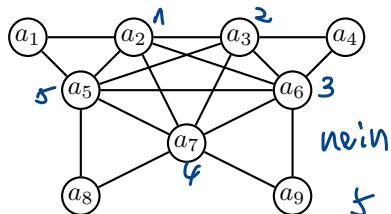
(i) Zeigen Sie, dass eine Kante $e \in E(G)$ genau dann im Rand zweier Gebiete liegt, wenn sie keine Brücke ist.

(ii) Folgern Sie, dass ein Wald immer nur ein Gebiet hat.

(iii) Folgern Sie mit Hilfe der Eulerschen Polyederformel, dass in jedem Baum T gilt: $|E(T)| = |V(T)| - 1$.

Aufgabe 9

Betrachten Sie die folgenden Graphen:



Beantworten Sie die folgenden Fragen zu jedem G_i , für $i \in \{1, 2, 3, 4\}$. Sie brauchen Ihre Antworten nicht zu begründen.

(i) Ist G_i planar?

(ii) Was ist der Wert von $\chi(G_i)$?

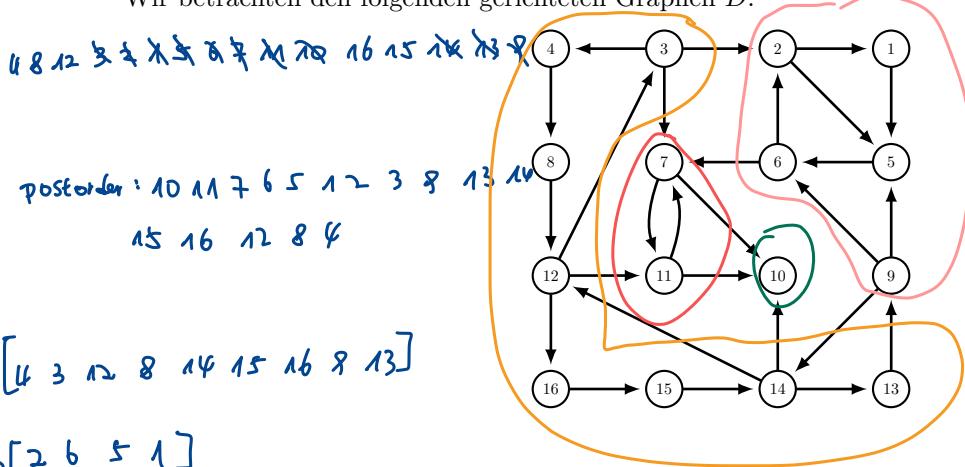
Aufgabe 10

Gebe einen Graphen mit n Knoten an, welcher nicht planar ist und nicht mehr als $3n - 6$ Kanten besitzt.

Aufgabe 11

$$|E| < 3|V| - 6 \quad k_{3,3}$$

Wir betrachten den folgenden gerichteten Graphen D .



$$C_1 = G[4, 3, 12, 8, 14, 15, 16, 9, 13]$$

$$C_2 = G[2, 6, 5, 1]$$

$$C_3 = G[7, 11]$$

$$C_4 = G[10]$$

$$(i) (C_1, C_2, C_3, C_4)$$

- (i) Bestimmen Sie die starken Zusammenhangskomponenten von D .
(ii) Bringen Sie die starken Zusammenhangskomponenten von D in eine Reihenfolge (C_1, \dots, C_ℓ) , sodass für alle Kanten (u, v) mit $u \in V(C_i)$ und $v \in V(C_j)$, $i, j \in \{1, \dots, \ell\}$ gilt: $i \leq j$.

Sie brauchen ihre Antworten nicht zu begründen.

Aufgabe 12

Bestimme den größten gemeinsamen Teiler für die folgenden Paare von Werten

- (i) 4000, 64
- (ii) 99, 15
- (iii) 233, 349

Aufgabe 13

Zeigen Sie, dass für $k, \ell \in \mathbb{N}$ Folgendes gilt:

$$\text{kgV}(k, \ell) = \frac{k \cdot \ell}{\text{ggT}(k, \ell)}$$

Aufgabe 14

Finde eine Zahl k , für die gilt, dass $k \cdot 1843 \bmod 4000 = 1$. k ist das modular multiplikativ Inverse von 1843 bezüglich 4000.

Aufgabe 15

Das sogenannte 'Lemma von Bézout' besagt, dass für jedes Paar von natürlichen Zahlen a und b , ganze Zahlen s und t existieren, sodass $\text{ggt}(a, b) = s \cdot a - t \cdot b$.

- (i) Begründe, dass das Lemma von Bézout gilt.
- (ii) Beweise, dass für jede Kombination von ganzen Zahlen l und k gilt, dass $l \cdot a + k \cdot b$ ein Vielfaches von $\text{ggt}(a, b)$ ist.

Aufgabe 16

Berechne $(8^{98}) \bmod 11$ ohne explizit eine Zahl zu nutzen, die größer als 11^2 ist.

Tipp: Nutze modulare Exponentiation.

Aufgabe 17

Gebe eine Zahl x mit $10000 < x < 100000$ an, für die gilt $x \equiv 3 \pmod{7}$ und $x \equiv 4 \pmod{11}$.

Aufgabe 18

Dir sind die Primzahlen 13 und 17 gegeben. Sei $n = 13 \cdot 17$.

Finde einen öffentlichen Schlüssel (l, n) und den dazugehörigen privaten Schlüssel (k, n) .

Aufgabe 12

Bestimme den größten gemeinsamen Teiler für die folgenden Paare von Werten

- (i) 4000, 64
- (ii) 99, 15
- (iii) 233, 349

$$\begin{aligned} \text{(i)} \quad 4000 - 62 \cdot 64 &= 32 \\ 64 - 2 \cdot 32 &= 0 \\ \text{ggT}(4000, 64) &= 32 = 4000 - 62 \cdot 64 \end{aligned}$$

$$\begin{aligned} \text{(ii)} \quad 99 - 15 \cdot 6 &= 9 & 6 = 15 - (99 - 15 \cdot 6) &= 7 \cdot 15 - 99 \\ 15 - 1 \cdot 9 &= 6 & 3 &= 99 - 6 \cdot 15 - 7 \cdot 15 + 99 \\ 9 - 6 &= 3 & &= 2 \cdot 99 - 13 \cdot 15 \\ 6 - 2 \cdot 3 &= 0 & & \\ \text{(iii)} \quad 349 - 233 &= 116 & \text{ggT} &= 1 = 233 - 2 \cdot (349 - 233) \\ 233 - 2 \cdot 116 &= 1 & &= 3 \cdot 233 - 2 \cdot 349 \end{aligned}$$

Aufgabe 13

Zeigen Sie, dass für $k, \ell \in \mathbb{N}$ Folgendes gilt:

$$\text{最小公倍数} \rightarrow \text{kgV}(k, \ell) = \frac{k \cdot \ell}{\text{ggT}(k, \ell)}$$

$$\begin{aligned} \text{PFZ: } k &= p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \\ \ell &= p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} \quad a_i, b_i, n, m \geq 0 \end{aligned}$$

$$\text{ggT}(k, \ell) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

$$\text{kgV}(k, \ell) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

$$k \cdot \ell = p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n}$$

$$\frac{k \cdot \ell}{\text{ggT}(k, \ell)} = p_1^{a_1+b_1 - \min(a_1, b_1)} \cdots p_n^{a_n+b_n - \min(a_n, b_n)}$$

$$= p_1^{\max(a_1, b_1)} \cdots p_n^{\max(a_n, b_n)}$$

$$= \text{kgV}(k, \ell)$$

Aufgabe 14

Finde eine Zahl k , für die gilt, dass $k \cdot 1843 \bmod 4000 = 1$. k ist das modular multiplikativ Inverse von 1843 bezüglich 4000.

$$\begin{aligned} 4000 - 2 \cdot 1843 &= 314 \\ 1843 - 5 \cdot 314 &= 273 \\ 314 - 273 &= 41 \\ 273 - 6 \cdot 41 &= 27 \\ 41 - 27 &= 14 \\ 27 - 14 &= 13 \\ 14 - 13 &= 1 \end{aligned}$$

$$\begin{aligned} 273 &= 1843 - 5 \cdot (4000 - 2 \cdot 1843) = 11 \cdot 1843 - 5 \cdot 4000 \\ 41 &= 6 \cdot 4000 - 13 \cdot 1843 \\ 27 &= (11 + 13 \cdot 6) \cdot 1843 - (5 + 36) \cdot 4000 \\ &= 89 \cdot 1843 - 41 \cdot 4000 \\ 14 &= 47 \cdot 4000 - 102 \cdot 1843 \\ 13 &= -88 \cdot 4000 + 181 \cdot 1843 \\ 1 &= 135 \cdot 4000 - 283 \cdot 1843 \Rightarrow \text{das modular Inverse von 1843 bezüglich 4000 ist } -283 \end{aligned}$$

Aufgabe 15

Das sogenannte 'Lemma von Bézout' besagt, dass für jedes Paar von natürlichen Zahlen a und b , ganze Zahlen s und t existieren, sodass $\text{ggf}(a, b) = s \cdot a - t \cdot b$.

- (i) Begründe, dass das Lemma von Bézout gilt.
- (ii) Beweise, dass für jede Kombination von ganzen Zahlen l und k gilt, dass $l \cdot a + k \cdot b$ ein Vielfaches von $\text{ggf}(a, b)$ ist.

(i) Der erweiterte euklidische Algorithmus liefert uns genau die Darstellung

$$(ii) \quad \text{ggf}(a, b) = s \cdot a - t \cdot b$$

$$a = \text{ggf}(a, b) \cdot a_1 \quad b = \text{ggf}(a, b) \cdot b_1$$

$$\begin{aligned} l \cdot a + k \cdot b &= l \cdot \text{ggf}(a, b) \cdot a_1 + k \cdot \text{ggf}(a, b) \cdot b_1 \\ &= \text{ggf}(a, b) \cdot (l \cdot a_1 + k \cdot b_1) \\ &= s \cdot \text{ggf}(a, b) \end{aligned}$$

Aufgabe 16

Berechne $(8^{98}) \pmod{11}$ ohne explizit eine Zahl zu nutzen, die größer als 11^2 ist.

Tipp: Nutze modulare Exponentiation.

$$\text{kleiner Satz von Fermat} \rightarrow 8^{10} \equiv 1 \pmod{11} \quad \text{da 11 Primzahl ist}$$

$$\Rightarrow (8^{10})^9 \equiv 1^9 \pmod{11}$$

$$\Rightarrow 8^{90} \equiv 1 \pmod{11}$$

$$\Rightarrow 8^{98} \equiv 8^8 \pmod{11}$$

$$8^2 = 64 \equiv 9 \pmod{11}$$

$$81 - 77 = 4$$

$$8^4 \equiv 81 \equiv 4 \pmod{11}$$

$$8^8 = 16 \equiv 5 \pmod{11}$$

$$\Rightarrow 8^{98} \equiv 5 \pmod{11}$$

Aufgabe 17

Gebe eine Zahl x mit $10000 < x < 100000$ an, für die gilt $x \equiv 3 \pmod{7}$ und $x \equiv 4 \pmod{11}$.

Chinesische Restsatz

$$x = 7k + 3 \equiv 4 \pmod{11}$$

$$7k \equiv 0 \pmod{11}$$

$$7k \equiv 1 \pmod{11}$$

$$\text{Modulare Inverse: } 11 - 7 = 4$$

$$7 - 4 = 3 \Rightarrow 1 = 11 - 7 - 2 \cdot 3 = 2 \cdot 11 - 3 \cdot 7$$

$$4 - 3 = 1$$

$$\Rightarrow 7 \cdot (-3) \equiv 1 \pmod{11}$$

$$7 \cdot (-3) + 7 \cdot 11 \equiv 1 \pmod{11}$$

$$\Rightarrow 7 \cdot 8 \equiv 1 \pmod{11}$$

$$7k \equiv 7 \cdot 8 + 7 \cdot 11 \cdot m \equiv 1$$

$$\Rightarrow k = 8 + 11 \cdot m \quad m \in \mathbb{N}$$

$$x = 7k + 3 = 56 + 77 \cdot m + 3 \quad m \in \mathbb{N}$$

$$= 59 + 77m > 10000$$

$$m > 128.1$$

$$\text{wir wählen } m = 130$$

$$x = 10069$$

Aufgabe 18

Dir sind die Primzahlen 13 und 17 gegeben. Sei $n = 13 \cdot 17 = 221$

Finde einen öffentlichen Schlüssel (l, n) und den dazugehörigen privaten Schlüssel (k, n) .

$$\varphi(n) = 12 \cdot 16 = 192$$

$$\text{ggT}(l, \varphi(n)) = 1 \quad lk \equiv 1 \pmod{192}$$

$$\text{ggT}(l, 192) = 1$$

$$\text{Sei } l = 5$$

$$2 \cdot 2 \cdot 5 \equiv 1 \pmod{192}$$

Modulare Inverse

$$192 - 38 \cdot 5 = 2$$

$$5 - 2 \cdot 2 = 1$$

$$1 = 5 - 2 \cdot (192 - 38 \cdot 5)$$

$$= \underline{\underline{77 \cdot 5 - 2 \cdot 192}}$$

$$\Rightarrow k = 77$$

public key $(5, 221)$

private key $(77, 221)$

Aufgabe 19

Wir betrachten die Menge $S = \{1, 2, 3, 4\}$.

- (i) Wie viele symmetrische Relationen können auf S definiert werden?
- (ii) Geben Sie ohne Begründung eine Formel an, mit der Sie die Anzahl der symmetrischen Relationen über einer Menge mit $n \in \mathbb{N}^+$ Elementen berechnen können.

Aufgabe 20

Es seien A und B zwei Mengen und $f: A \rightarrow B$ eine Abbildung. Wir definieren die Relation \sim_f auf A wie folgt: Für alle $a, a' \in A$ gilt

$$a \sim_f a' \text{ genau dann, wenn } f(a) = f(a').$$

Zeigen Sie, dass \sim_f eine Äquivalenzrelation auf A definiert.

Aufgabe 21

Sei (S, \leq) ein Verband in dem für alle $x, y, z \in S$ gilt: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. Folgern Sie daraus, dass auch $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ für alle $x, y, z \in S$.

Anmerkung: Benutze, dass $a \leq a \vee b$ und $a \geq a \wedge b$ ist, sowie die Assoziativität des Supremums $(a \vee (b \vee c)) = ((a \vee b) \vee c)$.

Aufgabe 22

Sei h ein Homomorphismus von $(A_m, +_m)$ nach $(A_k, +_k)$.

- (i) Begründe, dass jeder Homomorphismus von $(A_m, +_m)$ nach $(A_k, +_k)$ die Zahl 0 auf die Zahl 0 abbilden muss.
- (ii) Finde für $m = 6$ und $k = 3$ zwei Homomorphismen h_1, h_2 für die $x, y \in \mathbb{N}$ existieren mit $x \neq y$, sodass $h_1(x) = h_2(y) = 1$.
- (iii) Was muss für k und m gelten, damit ein Homomorphismus $(A_m, +_m)$ nach $(A_k, +_k)$ existieren kann?

Aufgabe 23

Sei $(M, +)$ eine Unteralgebra von $(\mathbb{N}, +)$. Es gelte $k \in M$. Bestimme die Zahlen x für die folgt, dass $x \in M$.

Aufgabe 24

Sei M eine Menge. Sei $O(M)$ die Menge der partiellen Ordnungen von M . Wir definieren den Operator Δ wie folgt: Für $\preceq_1, \preceq_2 \in O(M)$, sei $\preceq_1 \Delta \preceq_2 := (\preceq_1 \cup \preceq_2) \setminus (\preceq_1 \cap \preceq_2)$.

Bestimme, ob $(O(M), \Delta)$ eine Algebra ist.

Aufgabe 19

11	22	33	44
12	13	14	
	23	24	
		34	

$$\frac{n(n+1)}{2}$$

Wir betrachten die Menge $S = \{1, 2, 3, 4\}$.

(i) Wie viele symmetrische Relationen können auf S definiert werden?

(ii) Geben Sie ohne Begründung eine Formel an, mit der Sie die Anzahl der symmetrischen Relationen über einer Menge mit $n \in \mathbb{N}^+$ Elementen berechnen können.

$$\text{(i) } 2^{10}$$

$$\approx 2^{\frac{n(n+1)}{2}}$$

Aufgabe 20

Es seien A und B zwei Mengen und $f: A \rightarrow B$ eine Abbildung. Wir definieren die Relation \sim_f auf A wie folgt: Für alle $a, a' \in A$ gilt

$$a \sim_f a' \text{ genau dann, wenn } f(a) = f(a').$$

Zeigen Sie, dass \sim_f eine Äquivalenzrelation auf A definiert.

Äquivalenzrelation: reflexiv, symmetrisch, transitiv

reflexiv: f.a. $a \in A$, gilt $f(a) = f(a) \Rightarrow a \sim_f a$

symmetrisch: f.a. $a, b \in A$, gilt $f(a) = f(b)$, also $a \sim b$
gilt auch $f(b) = f(a) \Rightarrow b \sim a$

transitiv: f.a. $a, b, c \in A$ mit $f(a) = f(b)$ $f(b) = f(c)$
 $\Rightarrow a \sim b$ $b \sim c$
 $\Rightarrow f(a) = f(c)$
 $\Rightarrow a \sim c$

Aufgabe 21

Sei (S, \leq) ein Verband in dem für alle $x, y, z \in S$ gilt: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. Folgern Sie daraus, dass auch $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ für alle $x, y, z \in S$.

Anmerkung: Benutze, dass $a \leq a \vee b$ und $a \geq a \wedge b$ ist, sowie die Assoziativität des Supremums $(a \vee (b \vee c)) = (a \vee b) \vee c$.

$$x \vee (y \wedge z) \leq x \vee y$$

$$x \vee (y \wedge z) \leq x \vee z$$

$$\Rightarrow x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$$

$$x \vee (y \wedge z) \geq x \geq x \wedge y$$

$$x \vee (y \wedge z) \geq x \geq x \wedge z$$

$$\Rightarrow x \vee (y \wedge z) \geq (x \wedge y) \vee (x \wedge z) = x \wedge (y \vee z) \geq$$

$$x \vee (y \wedge z) \geq y \wedge z \geq x \wedge y \wedge z$$

$$(x \vee y) \wedge (x \vee z) \leq x \vee y \leq (x \vee y) \vee z$$

$$\leq x \vee z \leq (x \vee z) \vee y$$

$$\leq$$

Aufgabe 22

$$A_m = \{0, 1, 2, \dots, m-1\}$$

Sei h ein Homomorphismus von $(A_m, +_m)$ nach $(A_k, +_k)$.

- (i) Begründe, dass jeder Homomorphismus von $(A_m, +_m)$ nach $(A_k, +_k)$ die Zahl 0 auf die Zahl 0 abbilden muss.
- (ii) Finde für $m = 6$ und $k = 3$ zwei Homomorphismen h_1, h_2 für die $x, y \in \mathbb{N}$ existieren mit $x \neq y$, sodass $h_1(x) = h_2(y) = 1$.
- (iii) Was muss für k und m gelten, damit ein Homomorphismus $(A_m, +_m)$ nach $(A_k, +_k)$ existieren kann?

vii

$$h(0) = h(0 +_m 0) = h(0) +_k h(0)$$

$$\Rightarrow h(0) = 0$$

viii

$$h_1(x) = x \bmod 3$$

$$h_2(x) = 2x \bmod 3$$

$$\begin{aligned} h(a+b) &= (a+b) \bmod 3 = ((a+b) \bmod 6) \bmod 3 = ((a \bmod 6 + b \bmod 6) \bmod 6) \bmod 3 \\ h(a) +_3 h(b) &= a \bmod 3 +_3 b \bmod 3 = ((a \bmod 3) + (b \bmod 3)) \bmod 3 \\ &= (a+b) \bmod 3 \end{aligned}$$

$$h_1(1) = 1$$

$$h_2(2) = 1$$

vix) $m \bmod k = 0$

Aufgabe 23

Sei $(M, +)$ eine Unterlagebra von $(\mathbb{N}, +)$. Es gelte $k \in M$. Bestimme die Zahlen x für die folgt, dass $x \in M$.

$$M = \{nk \mid n \in \mathbb{N}\}$$

$$x \in M \Rightarrow x = nk \quad \text{für } n \in \mathbb{N}$$

Aufgabe 24

Sei M eine Menge. Sei $O(M)$ die Menge der partiellen Ordnungen von M . Wir definieren den Operator Δ wie folgt: Für $\preceq_1, \preceq_2 \in O(M)$, sei $\preceq_1 \Delta \preceq_2 := (\preceq_1 \cup \preceq_2) \setminus (\preceq_1 \cap \preceq_2)$.

Bestimme, ob $(O(M), \Delta)$ eine Algebra ist.

$$M \neq \emptyset \Rightarrow O(M) \neq \emptyset$$

$$\preceq_1 \Delta \preceq_2 := (\preceq_1 \cup \preceq_2) \setminus (\preceq_1 \cap \preceq_2) \text{ nicht unbedingt in } O(M) \text{ liegt}$$

Wir können nicht garantieren, dass $\preceq_1 \Delta \preceq_2 \in O(M)$