



Probeklausur

Diskrete Mathematik 2 I168

Tutorium 2020 - Noah Peeters, Julian Burmester, Tim Schröder

Dauer: 90 min

Hilfsmittel: Nordakademie Taschenrechner, Stifte, aber kein roter Stabilo 88/40.

Bemerkungen: Diese Klausur enthält 10 Aufgaben. Es können 100 Punkte erreicht werden. Zum Bestehen der Klausur benötigen Sie 50 Punkte.

Trennen Sie nicht die Heftung. Bitte schreiben Sie Ihre Lösungen auf die jeweiligen Aufgabenblätter. Falls Sie mit dem Platz nicht auskommen, verwenden Sie auch die Rückseiten oder die Zusatzseiten am Ende des Klausurheftes.

Aufgabe 1 (8 Punkte)

In den folgenden Multiple Choice Aufgaben sind je 3 Antworten richtig.

Bewertungshinweis:

- Es gibt maximal vier Punkte pro Frage
- Wenn Sie mehr als drei Kreuze pro Frage ankreuzen, erhalten Sie keine Punkte
- Haben Sie ein Kreuz in einer Frage falsch gesetzt, erhalten Sie die halbe Punktzahl
- Haben Sie mehr als ein Kreuz in einer Frage falsch gesetzt, erhalten Sie keine Punkte

(1.1) (4 Punkte) Kreuzen Sie die drei richtigen Antworten an:

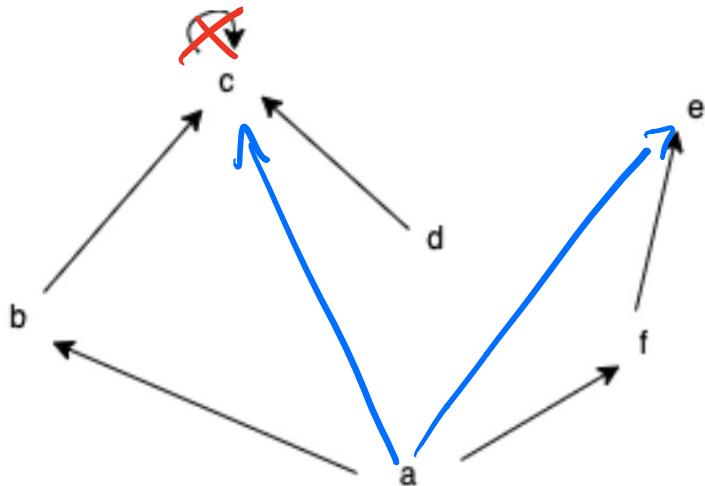
- Sei M eine Menge. Dann ist $M \times M$ im allgemeinen keine Relation.
- Jede Ordnungsrelation hat mindestens ein kleinstes oder mindestens ein größtes Element.
- Seien a, b Elemente einer beliebigen Menge E mit einer beliebig zugehörigen Äquivalenzrelation \equiv . Es gilt: $a \equiv b \Rightarrow a = b$.
- Aus der Gleichheit von Äquivalenzklassen folgt die Äquivalenz der Repräsentanten und umgekehrt. (X)
- Wenn R und S reflexiv sind, dann ist auch $R \cup S$ reflexiv. (X)
- $(R_2 \circ R_1)^{-1} = R_1^{-1} \circ R_2^{-1}$ (X)

(1.2) (4 Punkte) Kreuzen Sie die drei richtigen Antworten an:

- Sei R eine Relation. Aus der Asymmetrie von R folgt auch die Irreflexivität von R . (X)
- Sei R_1 eine Relation. Es gilt: $R_1 \circ R_1^{-1} = R_1$.
- Auf der Menge $M := \{1, 2, 3, 4, 5\}$ gibt es $5! = 120$ Relationen.
- Sei R eine Relation. Wenn R nicht reflexiv ist, dann ist R irreflexiv..
- Die leere Menge ist eine transitive Relation auf M , wobei M eine beliebige Menge sei. (X)
- Aus der Gleichheit zweier Relationen folgt die Gleichheit der respektiven inversen Relationen. (X)

Aufgabe 2 (5 Punkte)

Gegeben sei das vereinfachte Pfeildiagramm der Relation R auf der sechs-elementigen Menge $M := \{a, b, c, d, e, f\}$:



(2.1) (1 Punkt) Warum ist R keine strikte Ordnungsrelation? Begründen Sie Ihre Antwort.

Da $(c, c) \in R$ und R so nicht asymmetrisch ist.

(2.2) (3 Punkte) S sei die strikte Ordnungsrelation auf M , die entsteht, wenn Sie aus R genau ein Paar entfernen und genau zwei Paare hinzufügen. Geben Sie das Hasse-Diagramm von S an.



(2.3) (1 Punkt) Gilt für die Relation S aus (2.2) die Gleichung $(S^N)^* = S$?

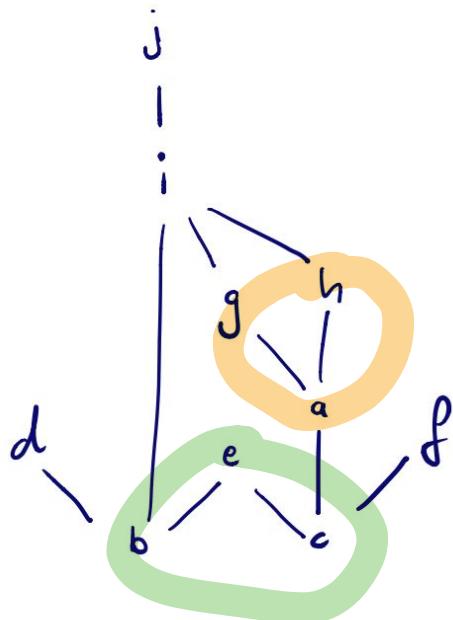
Begründen Sie Ihre Antwort.

Nein, da bspw. $(a, a) \in (S^N)^*$, aber $(a, a) \notin S$.

Hinweis: Es würde aber gelten $(S^N)^* \setminus \text{Id}_M = S$ oder $(S^N)^+ = S$.

Aufgabe 3 (10 Punkte)

Gegeben sei das folgende Hasse-Diagramm der zehn-elementigen Menge $M := \{a, b, c, d, e, f, g, h, i, j\}$:



Geben Sie größte/kleinste und maximale/minimale Elemente sowie obere/untere Schranken, obere/untere Grenzen und Supremum/Infimum von $\{a, g, h\}$ und $\{b, c, e\}$ an, falls existent.

	$\{a, g, h\}$	$\{b, c, e\}$		$\{a, g, h\}$	$\{b, c, e\}$
Größte Elemente	-	e	Kleinste Elemente	a	-
Maximale Elemente	g, h	e	Minimale Elemente	a	b, c
Obere Schranken	i, j	e	Untere Schranken	a, c	-
Obere Grenzen	i	e	Untere Grenzen	a	-
Supremum	i	e	Infimum	a	-

Aufgabe 4 (17 Punkte)

Gegeben sei die Relation \equiv auf der Menge der ganzen Zahlen, die durch $a \equiv b \Leftrightarrow a^2 - b^2 = 2a - 2b$ definiert wird.

(4.1) (10 Punkte) Zeigen Sie, dass \equiv eine Äquivalenzrelation ist.

- [Z.z. \equiv ist reflexiv]
Sei $a \in \mathbb{Z}$. Es gilt $a^2 - a^2 = 0 = 2a - 2a$. Also gilt nach Def. der Relation $(a, a) \in \equiv$.
- [Z.z. \equiv ist symmetrisch]
Seien $a, b \in \mathbb{Z}$ und $(a, b) \in \equiv$. [Z.z. $(b, a) \in \equiv$]
Nach Def. \equiv gilt $a^2 - b^2 = 2a - 2b$. Durch Termumformung erhalten wir $a^2 - b^2 = 2a - 2b \Leftrightarrow 2b - 2a = -a^2 + b^2 \Leftrightarrow b^2 - a^2 = 2b - 2a$. Also gilt $(b, a) \in \equiv$.
- [Z.z. \equiv ist transitiv]
Seien $a, b, c \in \mathbb{Z}$ und $(a, b), (b, c) \in \equiv$. [Z.z. $(a, c) \in \equiv$]
Nach Def. \equiv gilt $a^2 - b^2 = 2a - 2b$ und $b^2 - c^2 = 2b - 2c$. Addieren wir zuerst die zweite Gleichung erhalten wir $a^2 - b^2 + b^2 - c^2 = 2a - 2b + 2b - 2c \Leftrightarrow a^2 - c^2 = 2a - 2c$. Also gilt $(a, c) \in \equiv$.
- Da \equiv nachweislich reflexiv, symmetrisch und transitiv ist, ist \equiv eine Äquivalenzrelation.

(4.2) (4 Punkte) Geben Sie die Äquivalenzklassen [0], [1], [2] und [3] explizit an.

Hinweis: Die Äquivalenz kann auch folgend dargestellt werden: $a \equiv b \Leftrightarrow (a - b) \cdot (a + b - 2) = 0$.

$$[0] = \{0, 2\} = [2]$$

$$[1] = \{1\}$$

$$[3] = \{3, -1\}$$

a, b

(4.3) (3 Punkte) Zeigen Sie, dass $[a] \oplus [b] := [a + b]$ für alle ~~$x, y \in \mathbb{Z}$~~ nicht wohldefiniert bzw. nicht unabhängig vom Repräsentanten ist.

Hinweis: Nutzen Sie dazu die Äquivalenzklassen [0] und [1].

$$[0] \oplus [1] = [1]$$

$$[2] \oplus [1] = [3]$$

Es gilt $[0] = [2]$, aber nicht $[1] = [3]$.

Folglich ist die Abbildung \oplus in diesem Fall nicht wohldefiniert.

Aufgabe 5 (7 Punkte)

Gegeben sei die Äquivalenzrelation \equiv auf \mathbb{Z} , die durch $a \equiv b \Leftrightarrow |a| = |b|$ definiert wird. Zeigen Sie, dass die Relation $f := \{([a]_\equiv, |a|) \mid a \in \mathbb{Z}\}$ auf $(\mathbb{Z}/\equiv) \times \mathbb{Z}$ eine Abbildung ist.

Erinnerung: $\mathbb{Z}/\equiv := \{[a]_\equiv \mid a \in \mathbb{Z}\}$

Linkstotal: $\left[\exists x \in (\mathbb{Z}/\equiv) : \exists y \in \mathbb{Z} : (x, y) \in f \right]$
Sei $[a]_\equiv \in (\mathbb{Z}/\equiv)$. Dann ist $([a]_\equiv, |a|) \in f$.

[Das heißt zu jedem Element der „Linken“ Menge gibt es ein „paarendes“ Element aus der „rechten Menge“.]

rechteindeutig:

Seien $y_1, y_2 \in \mathbb{Z}$ und $x \in \mathbb{Z}/\equiv$ mit
 $(x, |y_1|) \in f \wedge (x, |y_2|) \in f$.

Dann existiert ein $a \in \mathbb{Z}$ mit
 $x = \{a, -a\} = [a]_\equiv$.

Dann gilt $|a| = |y_1| \wedge |a| = |y_2|$ also auch $|y_1| = |y_2|$

Aufgabe 6 (13 Punkte)

Wir betrachten die Algebraische Struktur $(\mathbb{Z}_{25725}, \otimes)$.

(6.1) (11 Punkte) Welche der Gleichungen

1. $[627]_{25725} \otimes x = [8575]_{25725}$
2. $[627]_{25725} \otimes x = [3675]_{25725}$

besitzt eine Lösung x in \mathbb{Z}_{25725} ? Falls Lösungen existieren, berechnen Sie alle Lösungen mit den in der Vorlesung verwendeten Verfahren. Falls keine Lösung existieren, begründen Sie dies. Zeigen Sie dazu mit dem erweiterten Euklidischen Algorithmus, dass $t = -1436$.

$$\begin{aligned} a &= 627 \\ m &= 25725 \end{aligned}$$

$$g = \text{ggT}(a, m) = 3$$

Euklidischer Algorithmus

a	b	q	s	t
25725	627	41	35	-1436
627	18	34	-1	35
18	15	1	1	-1
15	3	5	0	1
3	0		1	0

Anzahl Lösungen

3 teilt 8575 nicht \Rightarrow keine Lösung

3 teilt 3675 \Rightarrow 3 Lösungen

Lösungen für $b = 3675$

$$n = \frac{b}{g} = \frac{3675}{3} = 1225$$

$$q = \frac{m}{g} = \frac{25725}{3} = 8575$$

$$\begin{aligned} I \quad [n \cdot t]_m &= [1225 \cdot (-1436)]_{25725} \\ &= [15925]_{25725} \end{aligned}$$

$$II \quad [15925 + 8575]_{25725} = [24500]_{25725}$$

$$III \quad [15925 + 2 \cdot 8575]_{25725} = [7350]_{25725}$$

(6.2) (2 Punkte) Gibt es ein $a \in \mathbb{N}$ mit $1 < a < 11$, für das die Gleichung

$$[a]_{25725} \otimes x = [3675]_{25725}$$

genau eine Lösung besitzt? Begründen Sie ihre Antwort.

Für genau eine Lösung muss $\text{ggT}(a, m) = 1$ sein.

Dies ist für $a=2$ gegeben, da 2 eine Primzahl ist und 2 nicht 25725 teilt.

Aufgabe 7 (8 Punkte)

Geben Sie an, ob folgende Aussagen wahr oder falsch sind.

Hinweis: Inkorrekte Antworten führen nicht zu Abzügen. Punkte werden ab drei korrekten Antworten vergeben.

	Aussage	wahr	falsch
1.	Die Vigenere-Chiffre ist ein monoalphabetisches Substitutionsverfahren.		x
2.	Sollen bei einem symmetrischen Kryptosystem 69 Teilnehmer mit jeweils unterschiedlichen Schlüsseln kommunizieren, so benötigt man 4208 Schlüssel.		x
3.	In einem asymmetrischen Kryptosystem ist der Schlüssel zum Entschlüsseln komplett unabhängig vom Schlüssel zum Verschlüsseln.		x
4.	Das Schutzziel "Integrität" besagt, dass die Nachricht tatsächlich von der angegebenen Quelle stammt.		x
5.	Der Klartext "mathemachtspass" kann mit einer Caesar-Chiffre zu "THAOLTHJOAZWHPZ" verschlüsselt werden.		x
6.	Die "A posteriori Wahrscheinlichkeit" ist die Wahrscheinlichkeit, mit der ein bestimmter Klartext übertragen wurde, ohne dass der Geheimtext bekannt ist.		x
7.	Verschlüsselungsverfahren sollten stets geheim gehalten werden, da sie sonst von Experten geknackt werden.		x
8.	Wenn eine Zahl zwei Runden des Miller-Rabin-Tests besteht, ist sie zu maximal 6,25% keine Primzahl.	x	

1. Polyalphabetisches Substitutionsverfahren
2. Symmetrisches Kryptosystem: n Teilnehmer $\rightarrow \frac{n \cdot (n-1)}{2}$ Schlüssel (2.346 Schlüssel bei 69 Teilnehmern)
3. Zwischen den Schlüsseln besteht immer eine Beziehung, jedoch ist der Schlüssel zum Entschlüsseln nicht aus dem Schlüsseln zum Verschlüsseln innerhalb von Polynomialzeit ermittelbar
4. Integrität, stellt sicher, dass Nachricht nicht unbemerkt verändert wurde beim Versand
5. Letzte 2 Ziffern: s einmal mit P & einmal mit Z codiert \rightarrow in monoalphabetischen Substitutionsverfahren nicht möglich
6. Wahrscheinlichkeit, dass ein bestimmter Klartext übertragen wurde, wenn zusätzlich der Geheimtext bekannt ist
7. Kerckhoffsches Prinzip: Öffentliche Begutachtung durch Experten wichtig, Sicherheit hängt allein vom Schlüssel ab, nicht vom Verfahren
8. Jede gewählte Zahl für höchstens ein Viertel der Vasen kleiner n stark pseudoprim \rightarrow Fehlerwahrscheinlichkeit maximal = $(\frac{1}{4})^{\text{Anzahl Iteration}}$

Aufgabe 8 (11 Punkte)

(8.1) (3 Punkte) Ermitteln Sie, ob $[4]_7$ und $[5]_7$ in $(\mathbb{Z}_7 \setminus \{[0]_7\}, \otimes)$ erzeugende Elemente sind. Geben Sie dabei alle Rechenwege an.

$$4 = 4$$

$$4 \cdot 4 = 16 \equiv 2$$

$$2 \cdot 4 = 8 \equiv 1$$

$$1 \cdot 4 = 4$$

$$[4]_7 = \{1, 2, 4\} \neq \mathbb{Z}_7 \setminus \{[0]_7\}$$

$$5$$

$$5 \cdot 5 = 25 \equiv 4$$

$$4 \cdot 5 = 20 \equiv 6$$

$$6 \cdot 5 = 30 \equiv 2$$

$$2 \cdot 5 = 10 \equiv 3$$

$$3 \cdot 5 = 15 \equiv 1$$

$$1 \cdot 5 = 5$$

$$[5]_7 = \{1, 2, 3, 4, 5, 6\} \\ = \mathbb{Z}_7 \setminus \{[0]_7\}$$

(8.2) (3 Punkte) Geben Sie die Anzahl der teilerfremden natürlichen Zahlen von 125 und 126 an. Geben Sie die Zwischenschritte Ihrer Berechnung an.

$$\varphi(125) = \varphi(5^3) = 5^3 - 5^{3-1} = 125 - 25 = 100$$

$$\varphi(126)$$

$$n = 126 = 2 \cdot 3^2 \cdot 7$$

$$\varphi(126) = 126 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right)$$

$$= 36$$

(8.3) (5 Punkte) Prüfen Sie mit Hilfe des Miller-Rabin-Algorithmus, ob $n = 89$ eine Primzahl ist. Nutzen Sie hierfür die Basis $a = 5$. Geben Sie alle Zwischenschritte Ihrer Berechnung an.

Hinweis: Sie dürfen annehmen, dass der $\text{ggt}(5, 89) = 1$ ist.

$$1. a = 5$$

$$2. \text{ggT}(5, 89) = 1$$

$$3. n-1 = 88 = 2^3 \cdot 11; r = 3; s = 11$$

$$x_0 = a^{2^0 \cdot s} \mod n = 5^{1 \cdot 11} \mod 89 = 55$$

$$x_1 = a^{2^1 \cdot s} \mod n = 5^{2 \cdot 11} \mod 89 = 88$$

$$x_2 = a^{2^2 \cdot s} \mod n = 5^{4 \cdot 11} \mod 89 = 1$$

$$x_3 = a^{2^3 \cdot s} \mod n = 5^{8 \cdot 11} \mod 89 = 1$$

$(55, 88, 1, 1)$ ist eine gültige Folge

Aufgabe 9 (9 Punkte)

Bob möchte zur Verschlüsselung das RSA Verfahren verwenden. Bei der Schlüsselgenerierung wählt er $p = 31$ und $q = 43$.

(9.1) (4 Punkte) Als nächstes muss Bob einen Wert für e festlegen. Welche Bedingungen muss e erfüllen? Welches ist das kleinstmögliche e , das Bob verwenden kann?

e muss teilerfremd zu $\varphi(n)$ mit $n = p \cdot q = 1333$ sein
und es muss $1 < e < \varphi(n)$ gelten.

$$\varphi(n) = (p-1)(q-1) = 1260$$

$$1260 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7$$

$$\Rightarrow \text{kleinstes } e = 11$$

(9.2) (2 Punkte) Bob wählt $e = 17$. Ermitteln Sie den öffentlichen und privaten Schlüssel. Geben Sie die Zwischenschritte Ihrer Berechnung an.

Hinweis: Das multiplikative Inverse von $1[17]_{1260}$ in \mathbb{Z}_{1260} ist $[593]_{1260}$.

$$\text{öffentlicher Schlüssel: } (n, e) = (1333, 17)$$

$$\text{privater Schlüssel: } (n, d) = (1333, 593)$$

(9.3) (3 Punkte) Verschlüsseln Sie die Nachricht $m = 4$. Erläutern Sie Ihren Rechenweg.

$$c = m^e \bmod n$$

$$= 4^{17} \bmod 1333$$

$$= 4^{16} \cdot 4^1 \bmod 1333$$

$$= 1225$$

Square-and-Multiply

$$e = 17 = 2^4 + 2^0$$

$$4^1 \bmod n = 4$$

$$4^2 \bmod n = 16$$

$$4^4 \bmod n = 256$$

$$4^8 \bmod n = 219$$

$$4^{16} \bmod n = 1306$$

Gegenprobe Entschlüsselung (nicht Teil der Lösung):

$$c^d \bmod n = 1225^{593} \bmod 1333 = 4$$

Aufgabe 10 (12 Punkte)

Alice und Bob möchten einen symmetrischen Schlüssel im Geheimen austauschen. Dazu verwenden sie das Diffie-Hellmann-Key-Exchange-Verfahren. Beide einigen sich auf $p = 43$ und $g = 3$.

(9.1) (1 Punkt) Welche Eigenschaft muss g erfüllen, damit dieses Verfahren funktioniert?

g muss erzeugendes Element der multiplikativen Gruppe \mathbb{Z}_{43}^{\times} sein, also: $\langle g \rangle = \mathbb{Z}_{43}^{\times}$

(9.2) (3 Punkte) Alice wählt im Geheimen $a = 11$ und verschickt $x = 30$ an Bob. Bob wiederum verschickt $y = 32$ an Alice. Wie lautet ihr gemeinsamer Schlüssel?

Alice berechnet gemeinsamen privaten Schlüssel mit $y^a \bmod p = z$

$$\begin{aligned} -> 32^{11} \bmod 43 &= ((32^5 \bmod 43) \cdot (32^5 \bmod 43) \cdot 32) \bmod 43 \\ &= (27 \cdot 27 \cdot 32) \bmod 43 = 22 \bmod 43 \end{aligned}$$

(9.3) (8 Punkte) Berechnen Sie die geheime Zahl b von Bob mithilfe des Babystep-Giantstep-Algorithmus. Geben Sie alle Zwischenschritte ihrer Berechnung an.

Hinweis: Ein Repräsentant des multiplikativen Inversen von $[g]_p$ ist 29.

$x = q \cdot s + r$

$$\hookrightarrow s = \lceil \sqrt{43-1} \rceil = \lceil 6,48 \rceil = 7$$
$$\Rightarrow q, r \in \{0, 1, 2, 3, 4, 5, 6\}$$

Giantsteps: $g^{q \cdot s} \bmod n \equiv 3^{q \cdot 7} \bmod 43$

q	0	1	2	3	4	5	6
$3^{q \cdot 7} \bmod 43$	1	37	36	42	6	7	1

\rightarrow Stop bei $q = s-1$, also $q = 6$!

Balagatras:

Bob berechnet $q = 37$ mit

$$32 = 3^6 \pmod{43}$$

\rightarrow gesucht $b = \text{dlog}_3(32)$ in \mathbb{Z}_{43}

r	0	1	(3)
$32 \cdot 29^r \pmod{43}$	32	15	(37)

\rightarrow Stern, da 37 in Gründaten vorkommt!
(Bei $q=1$)

$$\Rightarrow x = q \cdot s + r = 1 \cdot 7 + 2 = \underline{\underline{9}}$$

mit $9 = x = \text{dlog}_3(32)$ in \mathbb{Z}_{43}

Probe: Gemeinsamer private key $= g^{a \cdot b} \pmod{p} = z$

Wir haben 9 als von Bob gewähltes b ermittelt:

$$\rightarrow 3^{11 \cdot 9} \pmod{43} = (30^3 \cdot 30^3 \cdot 30^3) \pmod{43} = 8 = 39^3 \pmod{43} = 22$$

-> Probe bestanden!