Universität Kassel
Fachbereich 10/16
Prof. Dr. A. Bley

Klausur: Diskrete Strukturen

Sommersemester 2021

Name (freiwillig):	Vorname (freiwillig):	Matrikelnummer:

Hinweise:

- Legen Sie Ihren Immatrikulationsausweis und Ihren Personalausweis sichtbar auf Ihren Schreibtisch und tragen Sie in obige Felder Ihre Daten ein![1]
- Schreiben Sie Ihre Lösungen bitte unterhalb der jeweiligen Aufgabe und auf der folgenden Leerseite direkt in diese Klausur.
- Schreiben Sie gut lesbar.
- **Geben Sie die Lösungsansätze und Rechenwege in nachvollziehbarer Weise mit an. Begründen Sie alle Antworten, Lösungsansätze und Rechenschritte.**

Die Bearbeitungszeit beträgt 90 Minuten.

Es können maximal **32** Punkte erreicht werden.

Aufgabe 1	Aufgabe 2	Aufgabe 3	Aufgabe 4	Aufgabe 5

Punkte:	**Note:**

	Note	Min. Punkte
	0.7	32.0
	1.0	30.5
	1.3	29.0
	1.7	27.5
	2.0	26.0
Notenschlüssel:	2.3	24.5
	2.7	23.0
	3.0	21.5
	3.3	20.0
	3.7	18.5
	4.0	16.0
	n.B.	≤ 15.5

[1] Sie müssen Ihren Namen und Vornamen nicht angeben. Ohne Name und Vorname muss die Matrikelnummer sehr gut lesbar sein (und natürlich stimmen).

Aufgabe 1. **(1+3+1+1+3 Punkte)**

Wir betrachten den Restklassenring $\mathbb{Z}/80\mathbb{Z}$.

a) Berechnen Sie die Anzahl der Einheiten im Ring $\mathbb{Z}/80\mathbb{Z}$.

b) $[3]_{80}$ ist eine Einheit in $\mathbb{Z}/80\mathbb{Z}$.

i) Berechnen Sie das multiplikative Inverse $[3]_{80}^{-1}$.

ii) Geben Sie die von $[3]_{80}$ erzeugte Untergruppe $[3]_{80}^{\mathbb{N}}$ von $((\mathbb{Z}/80\mathbb{Z})^*, \cdot)$ explizit durch Auflisten ihrer Elemente an.
Hinweis: Die Ordnung von $[3]_{80}$ *ist 4.*

c) Geben Sie ein anderes Element $[x]_{80} \neq [3]_{80}$ der Ordnung 4 in $((\mathbb{Z}/80\mathbb{Z})^*, \cdot)$ an.

d) Berechnen Sie $([5]_{80} \cdot [30]_{80} + [13]_{80})^{121}$.

e) Bestimmen Sie die kleinste positive ganze Zahl x mit

$$x \equiv 0 \mod 80 \quad \text{und}$$
$$x \equiv 1 \mod 9 \ .$$

Lösungsskizzen und Hinweise:

a) Die Anzahl der Einheiten ist $\varphi(80) = \varphi(2^4 \cdot 5) = \varphi(2^4) \cdot \varphi(5^1) = 2^3 \cdot (2-1) \cdot (5-1) = 32$. (1 Pkt)

(0 Pkt bei schwerwiegenden Fehlern in φ-Rechenregeln.)

b) Invertieren mit „Erweitertem Euklidischem Algorithmus“:

$$\begin{aligned} 80 &= 26 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + \mathbf{1} \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Also $1 = 1 \cdot 3 - 1 \cdot 2 = 1 \cdot 3 - 1 \cdot (80 - 26 \cdot 3) = \mathbf{27} \cdot 3 - 80$.

Also $[3]_{80}^{-1} = [27]_{80}$.

(0.5 Pkt für Vorwärts EA / ggT.)

(0.5 Pkt für Rückwärts EEA)

(0.5 Pkt für Angabe Inverse.)

(„Sehen“ der Inversen erlaubt, dann aber Nachweis $[27] \cdot [3] = [1]$ erforderlich.)

Durch einfaches Ausrechnen des jeweils nächsten Elementes aus dem vorherigen durch Multiplikation mit [3] erhält man

$$< [3] >= \{[3], [9], [27], [81] = [1]\} \ .$$

(1,5 Pkt für alle Elemente, je falschem Element 0.5Abzug.)

(0.5 Abzug bei fehlenden Klammern für Restklassen. (Es werden Restklassen gesucht!))

c) Nach Aufgabe b) ist $ord([3]) = 4$.

Ein anderes Element der Ordnung 4 ist offenbar das Element $[-3] = [77]$, denn $[-3]^4 = [-1]^4[3]^4 = [1][1]$ und $[-3]^i \neq [1]$ für $i = 1, \ldots, 3$.

Man erhält die zyklische Untergruppe

$$< [3] >= \{[-3] = [77], [-3]^2 = [9], [-3]^3 = [-27] = [53], [-3]^4 = [81] = [1]\} \ .$$

(1 Pkt für korrektes Element.)

d)

$$([5] \cdot [30] + [13])^{121} = ([163])^{121} = ([3]^4)^{30} \cdot [3] = [1]^{30}[3] = [3]$$

(1 Pkt für korrekter Rechnung.)

e) Offenbar sind 9 und 80 teilerfremd (nach Teil b) ist [9] Element einer Untergruppe der Einheitengruppe), also ist chinesischer Restsatz anwendbar. (0.5 Pkt)

Danach hat die Lösungsmenge des Systems die Form $L = \bar{x} + M\mathbb{Z}$, wobei $M = 9 \cdot 80 = 720$ und $\bar{x}$ eine beliebige, spezielle Lösung des Systems sind. (0.5 Pkt)

Die Bestimmung einer Lösung $\bar{x}$ ist möglich entweder durch systematisches Probieren z.B. aller Werte $x = k \cdot 80 + 0$ (vgl. erste Kongruenz) mit $k = 0, 1, \ldots$ oder mit dem Standard-Verfahren.

Man erhält mit dem Standard-Verfahren $[80]_9^{-1} = [8]_9^{-1} = [-1]_9^{-1} = [-1]_9 = [8]_9$ und $[9]_{80}^{-1} = [9]_{80}$ (vgl. Teil b) bzw. $9 \cdot 9 = 81$) und damit

$$x = 1 \cdot 8 \cdot 80 + 0 \cdot 9 \cdot 9 = 640 \bmod 720$$

Die Menge aller Lösungen ist folglich

$$\mathbb{L} = 640 + 720\mathbb{Z}.$$

(1.5 Pkt)

Die kleinste positive ganzzahlige Lösung x ist folglich $x = 640$. (0.5 Pkt)

(Die Lösungsmenge $\mathbb{L}$ muss nicht explizit angegeben werden, nach dieser war nicht gefragt. Es muss aber (implizit) begründet werden, wieso 640 die kleinste positive Lösung ist.)

Aufgabe 2. **(1+3+2 Punkte)**

Um sich mit dem RSA-Verfahren verschlüsselte Nachrichten schicken lassen zu können, hat Alice zwei Primzahlen $p \neq q$ gewählt und $N = pq$ berechnet. Zudem hat sie zwei Zahlen $e, d \in \{2, \ldots, \varphi(N)\}$ mit $ed = 1 \bmod \varphi(N)$ gewählt. Sie hat $N = 77$ und $e = 7$ als öffentlichen Schlüssel bekannt gemacht.

a) Die Nachricht $l = [76] \in \mathbb{Z}/N\mathbb{Z}$ soll an Alice übermittelt werden. Was ist die Verschlüsselung von l?

b) Bestimmen Sie den geheimen Entschlüsselungsexponenten d von Alice.

c) Entschlüsseln Sie eine abgefangene (verschlüsselte) Nachricht $a = [7]$ an Alice.

Geben Sie bei a) und c) jeweils die kleinste Zahl $x \geq 0$ als Repräsentanten der Restklasse $[x]$ an!

Rechentipp: Es gilt

$$7^6 \equiv -\mathbf{7} \mod 77$$
$$7^3 \equiv \mathbf{35} \mod 77.$$

Lösungsskizzen und Hinweise:

a) Die Verschlüsselung ergibt sich durch

$$[76]^7 = [-1]^7 = [-1] = [76] \mod 77$$

als $[76]_{77}^7 = [76]_{77}$. (1 Pkt)

b) Es ist $\varphi(N) = \varphi(77) = \varphi(7 \cdot 11) = 6 \cdot 10 = 60$. (je 0.5 Pkt für Faktorisierung und für φ)

Das Inverse von $[7]_{60}$ erhält man mit der erweiterten Euklidischen Algorothmus:

$$\begin{aligned} 60 &= 8 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (7 - 4) = 2 \cdot 4 - 7 \\ &= 2 \cdot (60 - 8 \cdot 7) - 7 = 2 \cdot 60 + -\mathbf{17} \cdot 7 \end{aligned}$$

Also ist $[7]_{60}^{-1} = [-17]_{60} = [43]_{60}$.

Somit ist $d = 43$.

(2 Pkt für Invertieren via EEA)

c) Die Entschlüsselung ergibt sich aus

$$[7]^{43} = ([7]^6)^7 \cdot [7] = ([-7])^7 \cdot [7] = [-1] \cdot [7]^6 \cdot [7] \cdot [7] = [-1] \cdot [-7] \cdot [7] \cdot [7] = [7]^3 = [35]$$

als $[7]_{77}^{43} = [35]$.

Die Klartext der abgefangenen Nachricht ist $[35]$. (2 Pkt)

(1 Pkt Abzug bei Rechnung mod 60 statt mod 77.)

(1 Pkt Abzug für Rechenfehler wegen zu großer Repräsentanten.)

(0.5 Pkt Abzug bei Rechenfehlern wegen Vorzeichenfehlern.)

Aufgabe 3. **(1+2+1 Punkte)**

Wir betrachten binäre Blockcodes $\mathcal{C} \subseteq \mathbb{F}_2^6$ der Länge 6.

a) Zeigen Sie, dass der folgende Code $\mathcal{C}'$ nicht 2-fehlerkorrigierend ist:

$$\mathcal{C}' = \{(0,0,0,0,0,0),\ (0,0,0,1,1,1),\ (1,1,1,0,0,0)\}.$$

b) Wie viele Codeworte kann ein 2-fehlerkorrigierender binärer Blockcode $\mathcal{C} \subseteq \mathbb{F}_2^6$ der Länge 6 maximal enthalten? Begründen Sie Ihre Antwort.

c) Geben Sie einen 2-fehlerkorrigierenden binären Blockcode $\mathcal{C} \subseteq \mathbb{F}_2^6$ mit der maximalen Anzahl an Codeworten explizit (durch Auflisten aller Codeworte) an.

Lösungsskizzen und Hinweise:

a) Die minimale Hammingdistanz zwischen den Codeworten in einem Code $\mathcal{C}$ muss $d \geq 5 = 2 \cdot 2 + 1$ betragen, damit $\mathcal{C}$ 2-fehlerkorrigierend ist.

(1/2 Pkt)

Die Hammingdistanz zwischen den ersten beiden Codeworten $(0,0,0,0,0,0)$ und $(0,0,0,1,1,1)$ in $\mathcal{C}'$ beträgt jedoch nur 3 (nur die letzten 3 Einträge unterscheiden sich). Also ist der Code nicht 2-fehlerkorrigierend.

(1/2 Pkt)

Alternative Begründung: Der Code enthält mehr als 2 Codeworte. Wir zeigen in b), dass ein 2-fehlerkorrigierender Code der Länge 6 maximal 2 Codeworte enthalten kann.

b) Mit der Hammingschranke erhalten wir folgende obere Schranke maximale Anzahl an Codeworten: $M(6,2) = 2^6 \cdot \frac{1}{\sum_{i=0}^{2} \binom{6}{i}} = \frac{2^6}{1+6+15} = 64/22 = 32/11$.

Da $2 < 32/11 < 3$, kann ein 2-fehlerkorrigierender Binärcode der Länge 6 maximal 2 Codeworte enthalten.

(1.5 Pkt korrekte berechnete Hammingschranke)

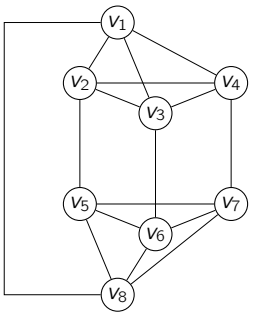
(0.5 Pkt korrekte Schlussfolgerung auf 2 Codeworte (kein krumme Zahl!))

c) $\mathcal{C} = \{(0,0,0,0,0,0),\ (1,1,1,1,1,1)\}$ ist offenbar ein solcher Code: Er enthält die maximale Anzahl von genau zwei Codeworten und die Hamingdistanz zwischen diesen ist mit 6 sogar größer als die erforderliche Minimaldistanz von 5.

(1 Pkt)

Aufgabe 4. **(2+2+3 Punkte)**

Sei $G = (V, E)$ der in der folgenden Abbildung dargestellte Graph.



a) Ist G eulersch? Wenn ja, geben Sie eine Euler-Tour an, wenn nicht, geben Sie eine stichhaltige Begründung dafür an, dass keine Euler-Tour in G existieren kann.

b) Ist G planar? Wenn ja, zeichnen Sie eine ebene Darstellung von G, wenn nicht, geben Sie eine stichhaltige Begründung dafür an, dass keine ebene Darstellung von G existiert.

c) Bestimmen Sie die chromatische Zahl $\chi = \chi(G)$. Zeigen Sie, dass die von Ihnen bestimmte Zahl korrekt ist, indem Sie eine Knotenfärbung mit χ Farben explizit angeben und indem Sie stichhaltig begründen, dass es keine Knotenfärbung mit weniger als χ Farben für G gibt.

Auf der nächsten Seite finden sich einige Kopien dieser Darstellung des Graphen G als Arbeitshilfe.

Lösungsskizzen und Hinweise:

a) G ist eulersch (da G zusammenhängend ist und alle Knoten einen geraden Grad haben). (1 Pkt)

Eine mögliche Eulertour ist (als Knotenfolge geschrieben)

$$(v_1, v_2, v_3, v_4, v_2, v_5, v_6, v_7, v_5, v_8, v_6, v_3, v_1, v_4, v_7, v_8, v_1)$$

(1 Pkt)

b) G ist nicht planar. (1 Pkt)

Er enthält einen K_5 als Minor.

Kontrahiert man beispielsweise die Knotenmenge $\{v_5, v_6, v_7, v_8\}$ zu einem Knoten v_5', so erhält man den K_5. (Es ist egal, in welcher Reihenfolge man die Kanten zwischen diesen Knoten kontrahiert, da die Knoten eine Clique bilden.)

(1 Pkt)

c) $\chi = \chi(G) = 4$ (1 Pkt)

G enthält u.A. die Clique $C = \{v_1, v_2, v_3, v_4\}$ mit $|C| = 4$, also gilt $\chi \geq 4$. (1 Pkt)

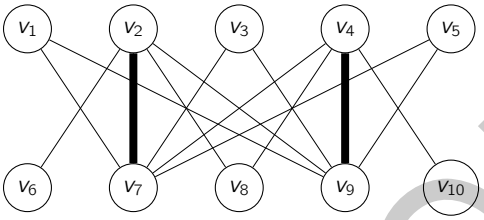
Eine mögliche Knotenfärbung $f : V \to \{1, \ldots, 4\}$ mit 4 Farben ist

$$f(v_i) = \begin{cases} 1 & \text{für } i \in \{1, 5\}, \\ 2 & \text{für } i \in \{2, 6\}, \\ 3 & \text{für } i \in \{3, 7\}, \\ 4 & \text{für } i \in \{4, 8\} \end{cases}$$

Also gilt $\chi \leq 4$. (1 Pkt)

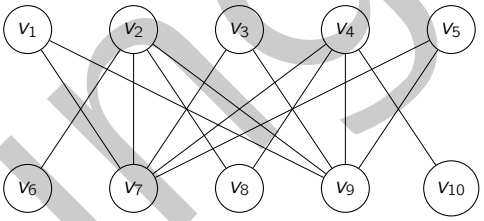
Aufgabe 5. **(1+2+3 Punkte)**

Wir betrachten den in der folgenden Abbildung dargestellten bipartiten Graphen $G = (V, E)$ und das durch die fett gezeichneten Kanten dargestellte Matching $M = \{v_2v_7, v_4v_9\}$:

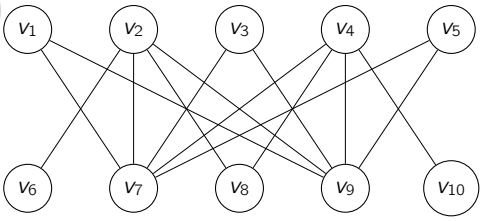


a) Bestimmen Sie einen M-augmentierenden Weg P in G.
Geben Sie P explizit als Kantenfolge an und markieren Sie die Kanten in P in der obigen Grafik.

b) Bestimmen Sie in G ein Matching M^* mit maximaler Kardinalität $|M^*|$.
Geben Sie M^* durch Auflisten der Elemente an und markieren Sie die Kanten in M^* in der folgenden Grafik.



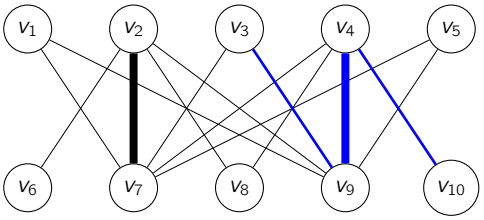
c) Bestimmen Sie für G eine Knotenüberdeckung W^* minimaler Kardinalität $|W^*|$.
Geben Sie W^* explizit durch Auflisten aller Elemente an und markieren Sie W^* in der folgenden Grafik.
Begründen Sie, wieso die von Ihnen angegebene Knotenüberdeckung W^* tatsächlich minimale Kardinalität hat.



Auf der nächsten Seite finden sich einige Kopien dieser Darstellung des Graphen G als Arbeitshilfe.

Lösungsskizzen und Hinweise:

a) Ein möglicher M-augmentierender Weg ist $P = (v_3v_9, v_9v_4, v_4v_{10})$. (1 Pkt)



b) Durch Bilden der symmetrischen Differenz von M und P erhält man das Matching $M' = \{v_2v_7, v_3v_9, v_4v_{10}\}$.
Ein M'-augmentierender Weg ist $P' = (v_1v_7, v_7v_2, v_2v_8)$.
Durch Bilden der symmetrischen Differenz von M' und P' erhält man ein (maximales) Matching

$$M^* = \{v_1v_7, v_2v_8, v_3v_9, v_4v_{10}\} \quad \text{mit} \quad |M^*| = 4$$

Da für alle Knoten $v \in V$ offensichtlich $|M^* \cap \delta(v)| \leq 1$ gilt, ist M^* nach Definition ein Matching.
Teil c) beweist, dass kein Matching M mit $|M| > |W^*| = 4$ existiert, also ist M^* mit $|M^*| = 4$ tatsächlich maximal.
(1.5 Pkt für zweimaliges korrektes Augmentieren.)
(0.5 Pkt für Begründung der Maximalität, als Verweis auf Teil c) mit entsprechendem Satz oder Begründung, dass kein weiterer augmentierender Weg existiert)
(nur 1 Pkt wenn Augmentierung nachvollziehbar, aber Matching M^* nicht maximal)

c) Eine minimale Knotenüberdeckung ist $W^* = \{v_2, v_4, v_7, v_9\}$. (2 Pkt für minimale Überdeckung)
(nur 1 Pkt, wenn Überdeckung, aber nicht minimal)

Da für alle Kanten $uv \in E$ offensichtlich $|W^* \cap \{u, v\}| \geq 1$ gilt, ist W^* nach Definition eine Knotenüberdeckung.

Nach dem schwachen Dualitätssatz gilt für alle Knotenüberdeckungen W und alle Matchings M in G die Ungleichung $|M| \leq |W|$.

Für das unter b) angegeben (maximale) Matching M^* folgt daraus, dass für alle Knotenüberdeckungen W von G auch $|W| \geq |M^*| = 4 = |W^*|$ gilt.

Die Knotenüberdeckung $|W^*|$ ist also tatsächlich Kardinalitätsminimal. (Korrekte Begründung: 1 Pkt)