Musterlösung Serie 14

Einige (Teil-)Aufgaben sind mit **(∗)** markiert. Versuchen Sie, wenigstens diese Aufgaben zu lösen.

0. **(Haus vom Nikolaus, Eulerscher Kantenzug, Eulertour)** Wir definieren

$$V := \{1, \dots, 5\}, \qquad E := \big\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{3,5\},\{4,5\}\big\},$$
$$\varphi := \text{Inklusion} : E \to \big\{\{v,w\} \,\big|\, v,w \in V\big\}, \qquad G := (V,E,\varphi).$$

Das Tripel G ist ein (ungerichteter) Graph. Siehe Abbildung 1.

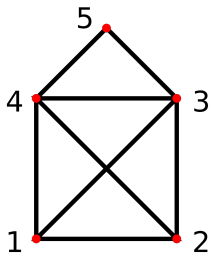

Abbildung 1: Das Haus vom Nikolaus. Quelle: https://de.wikipedia.org/wiki/Haus_vom_Nikolaus

Ziel des Rätsels *Haus vom Nikolaus* ist es, den Graphen G in einem Linienzug zu zeichnen, ohne eine Strecke zweimal zu durchlaufen. Dabei ist es nicht erlaubt, im Kreuzpunkt in der Mitte des Hauses die Richtung zu ändern. Das Ziel ist also, einen Eulerschen Kantenzug in G zu finden.

(a) **(∗)** Beweisen Sie, dass dieses Rätsel lösbar ist.
Hinweis: Verwenden Sie einen Satz aus der Vorlesung (Charakterisierung Eulerscher Graphen, Existenz eines Eulerschen Kantenzuges).

(b) **(∗)** Lösen Sie das Rätsel.

(c) **(∗)** Gibt es in G eine Eulertour?
Hinweis: Verwenden Sie den oben erwähnten Satz aus der Vorlesung.

(d) Sei $G = (V,E,\varphi)$ ein zusammenhängender Graph. Beweisen Sie, dass G genau dann einen offenen Eulerschen Kantenzug besitzt, wenn genau zwei Knoten von G ungeraden Grad besitzen.
Bemerkung: Diese Teilaufgabe ist Teil des oben erwähnten Satzes aus der Vorlesung.

Lösung: In der Vorlesung haben wir den folgenden Satz behandelt:

Satz 1 (Charakterisierung Eulerscher Graphen, Existenz eines Eulerschen Kantenzuges) *Sei $G = (V,E,\varphi)$ ein zusammenhängender Graph.*

(i) Der Graph G ist genau dann Eulersch, wenn jeder Knoten von G geraden Grad besitzt.

(ii) Der Graph G besitzt genau dann einen offenen Eulerschen Kantenzug, wenn genau zwei Knoten von G ungeraden Grad besitzen.

Bemerkung 2 Ein Graph G heisst Eulersch g. d. w. es eine Eulertour in G gibt.

(a) Unser Graph G besitzt genau zwei Knoten mit ungeradem Grad, nämlich die Knoten 1 und 2. Gemäss Satz 1(ii) besitzt G daher einen offenen Eulerschen Kantenzug. Somit ist das Rätsel Haus vom Nikolaus lösbar.

(b) **Lösung:**

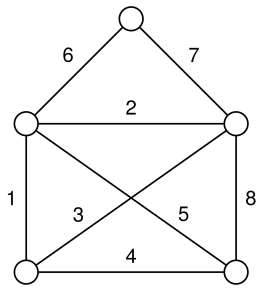

Abbildung 2: Die in dieser Abbildung dargestellte Kantenfolge $1, 2, \ldots, 8$ ist ein Eulerscher Kantenzug im Haus vom Nikolaus. Quelle: L. Halbeisen, *Grundstrukturen*, Skript zur Vorlesung, 2024, ETH Zürich, S. 42.

(c) Nein, wegen Satz 1(i), da nicht jeder Knoten von G geraden Grad besitzt.

(d) Die Lösung zu dieser Aufgabe ist analog zum Beweis des Teils (i) des Satzes 1, welcher in der Vorlesung behandelt wurde. (Falls es einen offenen Eulerschen Kantenzug gibt, dann besitzen die Endknoten des Kantenzuges ungeraden Grad und die anderen Knoten geraden Grad.)

1. **(Graphentheorie, Handschlaglemma)** Auf einem Fest schütteln sich gewisse Gäste die Hände. Zeigen Sie, dass die Anzahl Gäste, die eine ungerade Anzahl Hände schütteln, gerade ist.

Hinweise:

- Formulieren Sie diese Aufgabe als ein Graphenproblem um. (Das ist das *Handschlaglemma*.)
- Zeigen Sie, dass in jedem Graphen die Summe aller Grade gleich zweimal die Anzahl Kanten ist.

Lösung:

Proposition 3 (Handschlaglemma) *Sei $G = (V, E, \varphi)$ ein Graph. Es gilt:*

(i) $\sum_{v \in V} \deg v = 2|E|$

(ii) Die Anzahl Knoten in V mit ungeradem Grad ist gerade.

Im Beweis dieser Proposition verwenden wir folgende Definition. Seien $I, \mathcal{X}$ Mengen und $X : I \to \mathcal{X}$ eine Abbildung. Wir schreiben $X_i := X(i)$.

Definition 4 *Wir definieren die* disjunkte Vereinigung von X *als die Menge*

$$\bigsqcup X := \bigsqcup_{i\in I} X_i := \bigcup_{i\in I} \big\{\langle i,x\rangle \,\big|\, x\in X_i\big\} = \big\{\langle i,x\rangle \,\big|\, x\in X_i,\ i\in I\big\}.$$

Beweis der Proposition 3: (i): **Fall:** G **besitzt keine Schlingen:** Dann gilt

$$|\varphi(e)| = 2, \qquad \forall e\in E. \tag{1}$$

Die Abbildung

$$f : \bigsqcup_{v\in V} \big\{e\in E \,\big|\, v\in\varphi(e)\big\} \to \bigsqcup_{e\in E} \varphi(e), \qquad f(\langle v,e\rangle) := \langle e,v\rangle,$$

ist wohldefiniert und bijektiv. Es gilt

$$\begin{aligned}
\sum_{v\in V} \deg v &= \sum_{v\in V} \big|\big\{e\in E \,\big|\, v\in\varphi(e)\big\}\big| \\
&= \left|\bigsqcup_{v\in V} \big\{e\in E \,\big|\, v\in\varphi(e)\big\}\right| \\
&= \left|\bigsqcup_{e\in E} \varphi(e)\right| \qquad \text{(da } f \text{ eine Bijektion ist)} \\
&= |E|\cdot 2 \qquad \text{(wegen (1)).}
\end{aligned}$$

Im **Fall**, dass G Schlingen besitzt, folgt diese Gleichheit aus einem analogen Argument, wobei wir verwenden, dass der Grad Schlingen doppelt zählt. Das beweist (i).

(ii):

Bemerkung 5 (i) Die Summe einer ungeraden Anzahl ungerader Zahlen ist ungerade.

(ii) Wenn die Summe ungerader Zahlen gerade ist, dann ist ihre Anzahl daher gerade. Das folgt aus (i).

Es gilt

$$\sum_{v\in V:\,\deg v \text{ ungerade}} \deg v = \sum_{v\in V} \deg v - \sum_{v\in V:\,\deg v \text{ gerade}} \deg v.$$

Wegen (i) ist die rechte Seite gerade. Daher gilt dasselbe für die linke Seite. Aus Bemerkung 5(ii) folgt daher, dass die Anzahl der $v\in V$ mit ungeradem Grad gerade ist. Das beweist (ii). □

Wir definieren

$$V := \{\text{Gast}\}, \qquad E := \big\{\{v,w\} \,\big|\, v,w\in V : v \text{ und } w \text{ schütteln sich die Hände}\big\},$$
$$\varphi := \text{Inklusion} : E \to \big\{\{v,w\} \,\big|\, v,w\in V\big\}, \qquad G := (V,E,\varphi).$$

Das ist ein schlichter Graph[1] . Gemäss Proposition 3(ii) ist die Anzahl Knoten ungeraden Grades gerade. Diese Knoten sind genau die Gäste, die eine ungerade Anzahl Hände schütteln.

[1] d. h. schlingenfreier Graph ohne parallele Kanten

2. **(∗) (modulare Arithmetik)** Bestimmen Sie den Rest von 111^{126} beim Teilen durch 127.

Hinweis: Verwenden Sie einen Satz aus der Vorlesung.

Lösung:

Bemerkung 6 Für jede Primzahl p ist

$$\varphi(p) = p - 1.$$

Die Zahlen $1, 2, \ldots, p-1$ sind nämlich teilerfremd zu p, und p ist nicht teilerfremd zu p.

Die Primzahlen kleiner gleich $\sqrt{127}$ sind $2, 3, 5, 7, 11$. Die Zahl 127 ist durch keine dieser Zahlen teilbar. Daher ist 127 eine Primzahl. Gemäss Bemerkung 6 gilt daher $\varphi(127) = 127 - 1 = 126$. Da $n := 127$ prim ist, sind $a := 111$ und n teilerfremd. Gemäss dem Satz von Euler gilt daher

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \qquad \text{d. h.} \qquad 111^{126} \equiv 1 \pmod{127}.$$

Wenn wir 111^{126} durch 127 teilen, erhalten wir daher den Rest 1.

3. **(∗) (multiplikatives Inverses einer primen Restklasse, erweiterter euklidischer Algorithmus, Lemma von Bézout)** Sei $n \in \omega \backslash \{0\}$. Wir schreiben $[a]_n$ für die Restklasse von a modulo n.

(a) Bestimmen Sie die multiplikativen Inversen von

$$[2]_3, \qquad [2]_5, \qquad [7]_{18}.$$

Hinweise für $[7]_{18}$:

- Verwenden Sie den euklidischen Algorithmus, um den grössten gemeinsamen Teiler von 18 und 7 zu bestimmen.
- Der letzte interessante Schritt in diesem Algorithmus liefert $\mathbf{4} = \mathbf{3} \cdot 1 + \mathbf{1}$, also $\mathbf{1} = \mathbf{4} - \mathbf{3} \cdot 1$. Gehen Sie rückwärts durch Ihre Rechnungen, um die fettgedruckten Zahlen auf der rechten Seite umzuschreiben. Dadurch erhalten Sie Zahlen $s, t \in \mathbb{Z}$, sodass $18s + 7t$ gleich dem grössten gemeinsamen Teiler von 18 und 7 ist.

Bemerkung: Diese beiden Punkte entsprechen dem *erweiterten euklidischen Algorithmus*.

(b) Wir schreiben $\mathbb{Z}_n^\times$ für die Menge der primen Restklassen modulo n. In der Vorlesung haben wir im Beweis des Satz von Euler (Zahlentheorie) verwendet, dass $(\mathbb{Z}_n^\times, \cdot_n|_{\mathbb{Z}_n^\times})$ eine Gruppe ist. Die Existenz eines multiplikativen Inversen zu jedem Element von $\mathbb{Z}_n^\times$ basiert auf dem folgenden Satz. Seien $a, b \in \mathbb{Z}$, sodass $a \neq 0$ oder $b \neq 0$.

Satz 7 (Lemma von Bézout) *Es gibt Zahlen $s, t \in \mathbb{Z}$, sodass*

$$as + bt = \mathrm{ggT}(a, b) = \textit{grösster gemeinsamer Teiler von } a \textit{ und } b.$$

Beweisen Sie diesen Satz!

Hinweis: Verwenden Sie die Methode, mit der Sie das multiplikative Inverse von $[7]_{18}$ berechnet haben.

Lösung:

(a) Für $A := B := [2]_3$ gilt $A \cdot_3 B = [2]_3 \cdot_3 [2]_3 = [2 \cdot 2]_3 = [1]_3$. Daher ist $B = [2]_3$ das multiplikative Inverse von $A = [2]_3$.
Es gilt $[2]_5 \cdot_5 [3]_5 = [2 \cdot 3]_5 = [1]_5$. Daher ist $[3]_5$ das multiplikative Inverse von $[2]_5$.
Der euklidische Algorithmus liefert

$$\begin{aligned} \mathbf{18} &= \mathbf{7} \cdot 2 + \mathbf{4} \\ \mathbf{7} &= \mathbf{4} \cdot 1 + \mathbf{3} \\ \mathbf{4} &= \mathbf{3} \cdot 1 + \mathbf{1} \\ \mathbf{3} &= \mathbf{1} \cdot 3 + \mathbf{0} \end{aligned}$$

(Es folgt, dass $\mathbf{1}$ der grösste gemeinsame Teiler von $\mathbf{18}$ und $\mathbf{7}$ ist.) Indem wir unsere Rechnungen rückwärts verfolgen, erhalten wir

$$\begin{aligned} \mathbf{1} &= \mathbf{4} - \mathbf{3} \cdot 1 \\ &= \mathbf{4} - \big(\mathbf{7} - \mathbf{4} \cdot 1\big) \cdot 1 \\ &= \mathbf{7}(-1) + \mathbf{4}(1 + 1) \\ &= \mathbf{7}(-1) + \big(\mathbf{18} - \mathbf{7} \cdot 2\big) \cdot 2 \\ &= \mathbf{18} \cdot 2 + \mathbf{7} \cdot (-5). \end{aligned}$$

Daher gilt $18|7 \cdot (-5) - 1$, also $[7]_{18}[-5]_{18} = [7 \cdot (-5)]_{18} = [1]_{18}$. Also ist $[-5]_{18}$ das multiplikativ Inverse zu $[7]_{18}$.

Bemerkung 8 Wir können dieses Inverse auch als $[13]_{18} = [-5]_{18}$ schreiben. Allgemein können wir jede Restklasse A modulo n als $A = [r]_n$ mit $r \in \{0, \ldots, n-1\}$ schreiben.

(b) Ohne Beschränkung der Allgemeinheit gilt $b \neq 0$. Wir schreiben $a_0 := a$, $a_1 := b$. Aus Division mit Rest (siehe Vorlesung) und Induktion folgt, dass es eine Zahl $k \in \omega \backslash \{0\}$ und Zahlen $a_2, \ldots, a_{k+1}, q_1, \ldots, q_k \in \mathbb{Z}$ gibt, sodass

$$a_{i-1} = a_i q_i + a_{i+1}, \qquad \forall i \in \{1, \ldots, k\}, \qquad a_k \neq 0, \qquad a_{k+1} = 0. \tag{2}$$

Bemerkung 9 Der *euklidische Algorithmus* ist die rekursive Konstruktion dieser Zahlen.

Mittels Induktion folgt, dass $a_k | a_i$, für jedes $i = k, \ldots, 0$, also $a_k | a_0 = a, a_1 = b$. Sei d ein gemeinsamer Teiler von $a = a_0$ und $b = a_1$. Mittels Induktion folgt, dass $d | a_i$, für jedes $i = 0, \ldots, k$, also $d | a_k$. Es folgt, dass a_k der grösste gemeinsamer Teiler von a und b ist.
Mit einer *ganzzahligen Linearkombination* zweier Zahlen $m, n \in \mathbb{Z}$ meinen wir eine Zahl der Form $ms + nt$ mit $s, t \in \mathbb{Z}$. Sei $j = k, \ldots, 2$. Gemäss (2) gilt $a_j = a_{j-1}(-q_{j-1}) + a_{j-2} \cdot 1$. Also ist a_j eine ganzzahlige Linearkombination von a_{j-1} und a_{j-2}. Mittels Induktion folgt daraus, dass a_k eine ganzzahlige Linearkombination von $a_1 = b$ und $a_0 = a$ ist. Da a_k der grösste gemeinsamer Teiler von a und b ist, folgt die Aussage des Satzes 7 (Lemma von Bézout).

Bemerkung 10 Der *erweiterte euklidische Algorithmus* ist der euklidische Algorithmus zusammen mit der rekursiven Konstruktion der Koeffizienten der Darstellung von

a_k als Linearkombination von a_{j-1} und a_{j-2}, die sich aus obigem Induktionsargument ergibt. Ein Beispiel für den erweiterten euklidischen Algorithmus ist unsere Berechnung des multiplikativen Inversen von $[7]_{18}$ in Teilaufgabe (a).

4. **(RSA-Verschlüsselung)** Alice und Carol möchten Bob mittels RSA-Verschlüsselung geheime Nachrichten schicken. Dazu wählt Bob zwei verschiedene grosse Primzahlen p und q, berechnet den RSA-Modul $n := pq$ und wählt zwei verschiedene zu $\varphi(n) = (p-1)(q-1)$ teilerfremde Zahlen e, e', sodass $1 < e, e' < \varphi(n)$. Zufällig sind e und e' teilerfremd. Bob schickt (e, n) an Alice und (e', n) an Carol. Die Nachrichten von Alice und Carol sind zufällig gleich. Sie sind durch m gegeben, wobei $0 < m < n$ und m, n teilerfremd sind. Mittels des RSA-Algorithmus erhalten Alice und Carol aus dem Klartext m die Geheimtexte c und c', die sie an Bob schicken. Eve fängt die Geheimtexte ab.

Wie kann Eve den Klartext m effizient rekonstruieren?

Hinweis: Verwenden sie das Lemma von Bézout mit $a = e$ und $b = e'$.

Lösung: Eve fängt die Geheimtexte

$$c := m^e \mod n, \tag{3}$$

$$c' := m^{e'} \mod n \tag{4}$$

ab. Da e und e' teilerfremd sind, gibt es gemäss dem Lemma von Bézout Zahlen $s, s' \in \mathbb{Z}$, sodass

$$es + e's' = 1. \tag{5}$$

Fall: $s > 0$**,** $s' < 0$**:** Eve berechnet mittels des erweiterten euklidischen Algorithmus ein $i' \in \mathbb{Z}$, sodass $c'i' \equiv 1 \pmod n$. Sie berechnet

$$\widetilde{m} := c^s i'^{-s'} \mod n. \tag{6}$$

Gemäss (3) gilt

$$[c^s]_n = [m^{es}]_n = [m]_n^{es}, \tag{7}$$

$[c']_n[i']_n = [c'i']_n = [1]_n$, also $[i']_n = [c']_n^{-1}$ (Inverses) und daher

$$[i'^{-s'}]_n = [c']_n^{-(-s')} = [c']_n^{s'} = \left[m^{e'}\right]_n^{s'} = [m]_n^{e's'}, \tag{8}$$

wobei wir (4) verwendet haben. Es gilt

$$\begin{aligned}
[\widetilde{m}]_n &= [c^s]_n \left[i'^{-s'}\right]_n && \text{(wegen (6))} \\
&= [m]_n^{es}[m]_n^{e's'} && \text{(wegen (7,8))} \\
&= [m]_n^{es+e's'} \\
&= [m]_n && \text{(wegen (5)).}
\end{aligned}$$

Es folgt, dass $\widetilde{m} = m$. Somit hat Eve den Klartext gefunden. Den **Fall** $s < 0$**,** $s' > 0$ können wir analog behandeln.