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.

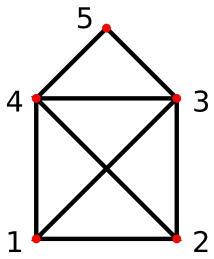

Abbildung 1: Das Haus vom Nikolaus. Quelle: https://de.wikipedia.org/wiki/Haus_vom_Nikolaus

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.

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.

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

Hinweis: Verwenden Sie einen Satz aus der Vorlesung.

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 1 (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.

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 $b = e'$.