Probeprüfung 2

1.) Gegeben ist die Restklassengleichung

$[\mathbf{7}]_{\mathbf{m}} \cdot [\mathbf{x}]_{\mathbf{m}}$ **=** $[\mathbf{b}]_{\mathbf{m}}$ **, m ∈ {2, 3, 4, . . .}, b ∈ $\mathbb{Z}$.**

(a) Angenommen m = 9 und x = 2. Wofür steht dann $[7]_9 \cdot [2]_9$?
(b) Angenommen m = 9 und b = 2. Lösen Sie die Gleichung für diese Werte.
(c) Angenommen b = 2. Beschreiben Sie die Werte m, für die die Gleichung eine Lösung besitzt? Warum?
(d) Erklären Sie schlüssig: $\mathbb{Z}_{\mathbf{m}}$ ist ein Körper, wenn m eine Primzahl ist. Was bedeutet das? Warum?

---

a)

$[7]_9 \cdot [2]_9$ steht für die Multiplikation der Restklassen $[7]_9$ und $[2]_9$ innerhalb des Restklassenrings modulo 9.

b)

$[7]_9 \cdot [x]_9 = [2]_9 \qquad | * ([7]_9)^{-1}$

$([7]_9)^{-1} \cdot [7]_9 \cdot [x]_9 = ([7]_9)^{-1} \cdot [2]_9$

Das multiplikative Inverse von $[7]_9$ ist $[4]_9$, da $[7]_9 \cdot [4]_9 = [28]_9 = [1]_9$

$[x]_9 = [2]_9 \cdot [4]_9 = [8]_9$

c)

$[7]_m \cdot [x]_m = [2]_m$

m = {2, 3, 4, 5, 6, 8, 9, 10, 11, ...}

Die Gleichung hat eine Lösung, wenn der ggT von 7 und m gleich 1 ist.
Das liegt daran, dass das multiplikative Inverse von $[7]_m$ nur dann existiert, wenn ggT(7, m) = 1. Da 7 eine Primzahl ist, wird die Gleichung eine Lösung haben, solange m nicht ein Vielfaches von 7 ist.

d)

Wenn m eine Primzahl ist, sind alle Elemente in $\mathbb{Z}_{\mathbf{m}}$ teilerfremd zu m, was bedeutet, dass der ggT jedes Elements und m gleich 1 ist. Daher hat jedes Element in $\mathbb{Z}_{\mathbf{m}}$ ein multiplikatives Inverses, und $\mathbb{Z}_{\mathbf{m}}$ erfüllt alle Axiome eines Körpers.

Wenn m keine Primzahl ist, gibt es mindestens ein Element in $\mathbb{Z}_{\mathbf{m}}$ (außer 0), das einen ggT größer als 1 mit m hat. In diesem Fall hat dieses Element kein multiplikatives Inverses in $\mathbb{Z}_{\mathbf{m}}$ und würde damit nicht alle Axiome eines Körpers erfüllen.

Probeprüfung 2

2.)

(a) Berechnen Sie mit schneller Exponentiation (direkt ohne Satz von Euler) $\mathbf{3^{31} \bmod 7}$

(b) Bestätigen Sie Ihr Resultat aus (a), indem Sie nun die Aufgabe mit dem Satz von Euler vereinfachen und anschließend berechnen.

---

a)

$31 = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 1 + 2 + 4 + 8 + 16$

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 3^1 * 3 \bmod 7 = 9 \bmod 7 = 2$
$3^4 \bmod 7 = 3^2 * 3^2 \bmod 7 = 2 * 2 \bmod 7 = 4 \bmod 7 = 4$
$3^8 \bmod 7 = 3^4 * 3^4 \bmod 7 = 4 * 4 \bmod 7 = 16 \bmod 7 = 2$
$3^{16} \bmod 7 = 3^8 * 3^8 \bmod 7 = 2 * 2 \bmod 7 = 4 \bmod 7 = 4$

$3^{31} \bmod 7 = 3^1 * 3^2 * 3^4 * 3^8 * 3^{16} \bmod 7 = 3 * 2 * 4 * 2 * 4 \bmod 7 = 192 \bmod 7 = 3$

b)

φ(7) = 7 - 1 = 6

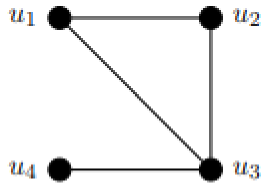
$a^{\varphi(p)} \equiv 1 \pmod{p}$

$3^6 \equiv 1 \pmod{7}$

$3^{31} \bmod 7 = 3^{6*5+1} \bmod 7 = 3^{6^5} * 3^1 \bmod 7 = 1^5 * 3^1 \bmod 7 = 3 \bmod 7 = 3$

Probeprüfung 2

3.) Gegeben ist der Graph



(a) Bestimmen Sie mit der Adjazenzmatrix des Graphen die Anzahl der Wege der Länge 3 von u1 nach u3.
(b) Ergänzen Sie den Graphen um zwei Kanten, sodass der ergänzte Graph einen Eulerkreis enthält.
(c) Finden Sie mit dem Algorithmus von Hierholzer in dem erweiterten Graphen einen Eulerkreis. Erklären Sie Ihre Vorgehensweise mit einigen Sätzen.

---

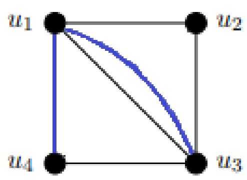
a)

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$A^3 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} * \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} * \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 2 & 4 & 1 \\ 4 & 4 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{pmatrix}$$

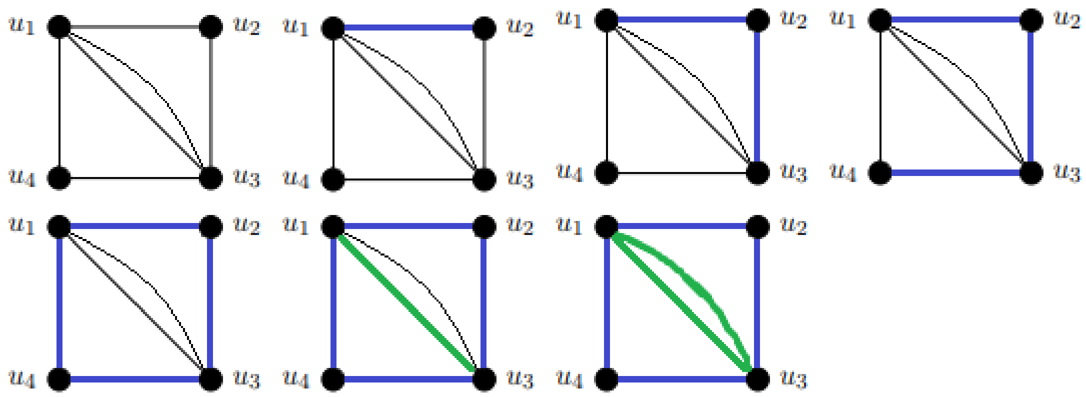
Es gibt vier Wege der Länge 3 von u1 nach u3.

b)



c)

Anleitung: Beliebigen Startknoten wählen, unbesuchten Weg von diesem Knoten zu einem anderen Knoten folgen und besuchte Kante markieren. Wiederholen, bis man zum Startknoten zurückkehrt. Dies bildet einen Kreis. Falls es noch unbesuchte Kanten gibt, Startknoten innerhalb des Kreises wählen, der noch unbesuchte Kanten hat und wiederholen, bis man zum Startknoten zurückkehrt. Daraus ergibt sich ein Eulerkreis.



Probeprüfung 2

4.)
Sei A eine allgemeine n × n Matrix. Beantworten Sie schlüssig:

(a) Welche Bedingungen garantieren, dass A eine Permutationsmatrix ist?
(b) Wenn 3 ein Eigenwert von A ist, dann ist 2 ein Eigenwert der Matrix A−E, wobei E die n×n Einheitsmatrix ist.
(c) Wenn A eine zeilenstochastische Matrix ist, so ist der n–dimensionale Vektor, der nur 1 als Einträge besitzt, ein Eigenvektor von A.

---

a)

A ist eine Permutationsmatrix, wenn folgende Eigenschaften erfüllt sind:

- In jeder Zeile und jeder Spalte der Matrix gibt es genau eine 1, während alle anderen Einträge 0 sind.
- Die Matrix ist orthogonal → P * P^{T} = E, wobei P^{T} die transponierte Matrix von P ist.

b)

Angenommen 3 ist ein Eigenwert von A, dann existiert ein Eigenvektor $\vec{x}$, so dass A $*$ $\vec{x}$ = 3 $*$ $\vec{x}$. Um zu zeigen, dass 2 ein Eigenwert der Matrix A – E ist, lässt sich folgende Gleichung formulieren:

$$(\mathrm{A} - \mathrm{E}) * \vec{x} = \mathrm{A} * \vec{x} - \mathrm{E} * \vec{x} = 3 * \vec{x} - \vec{x} = 2 * \vec{x}$$

Da $\vec{x}$ ein Vektor ist, der die Gleichung (A - E) * $\vec{x}$ = 2 * $\vec{x}$ erfüllt, ist 2 ein Eigenwert der Matrix A - E.

c)

Ein Vektor $\vec{x}$ist ein Eigenvektor von A, wenn das Matrix-Vektor-Produkt A * $\vec{x}$ ein Vielfaches des Vektors $\vec{x}$ ist → A * $\vec{x}$ = λ * $\vec{x}$

$$\vec{x} = (1, 1, 1 \dots 1)^T$$

$$\mathrm{A} * \vec{x} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} * \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

Da A * $\vec{x}$ = $\vec{x}$, ist $\vec{x}$ ein Eigenvektor von A, dessen zugehöriger Eigenwert 1 ist.

Probeprüfung 2

5.)

(a) Erklären Sie allgemein, was die Koordinaten eines Vektors sind. Hat jeder Vektor Koordinaten?

(b) Erklären Sie das Konzept der Lotpunktberechnung allgemein mit einer aussagekräftigen Skizze. Kann man in jedem Vektorraum einen Lotpunkt berechnen?

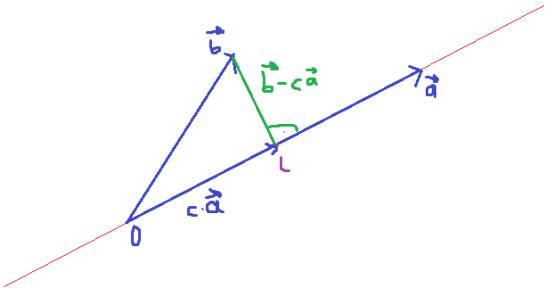
(c) Leiten Sie die allgemeine Formel für die Berechnung der Koordinaten eines Vektors $\vec{u}$ bezüglich einer orthogonalen Basis $\mathbf{b_1}, \ldots, \mathbf{b_n}$ her.

---

a)

Die Koordinaten eines Vektors sind Zahlenwerte, die angeben, wie der Vektor als Linearkombination von Basisvektoren dargestellt werden kann. Jeder Vektor im Vektorraum kann als Linearkombination der Basisvektoren dargestellt werden, die Koordinaten geben die Streckungsfaktor für jeden Basisvektor an. Nicht jeder Vektor hat Koordinaten, es sei denn, es gibt eine bestimmte Basis, auf die er bezogen wird.

b)



Bei der Lotpunktberechnung ist eine Projektion, d.h. der Lotpunkt von $\vec{b}$ auf $\vec{a}$ gesucht. Der Lotpunkt ist der Punkt auf der von $\vec{a}$ erzeugten Gerade, der nächstmöglich zu $\vec{b}$ ist.
In einem Vektorraum kann man einen Lotpunkt berechnen, wenn ein Skalarprodukt definiert ist, da das Skalarprodukt es ermöglicht, die Projektion des gegebenen Punkts auf die Gerade oder Ebene zu berechnen und damit den Lotpunkt zu bestimmen.

c)

Da die Basis orthogonal ist, kann der Vektor $\vec{u}$ als Linearkombination der Basisvektoren geschrieben werden:

$$\vec{u} = c_1 * b_1 + c_2 * b_2 + \cdots + c_n * b_n$$

Um die Koordinate c_1 zu finden, projiziert man den Vektor $\vec{u}$ auf den Basisvektor $\overrightarrow{b_1}$:

$$c_1 = \frac{\langle \vec{u}, \overrightarrow{b_1} \rangle}{\left\| \overrightarrow{b_1}^2 \right\|}$$

Auf die gleiche Weise können die restlichen Koordinaten durch Projektion auf die Basisvektoren berechnet werden:

$$c_n = \frac{\langle \vec{u}, \overrightarrow{b_n} \rangle}{\left\| \overrightarrow{b_n}^2 \right\|}$$

Probeprüfung 2

Daher ist die allgemeine Formel für die Berechnung der Koordinaten eines Vektors $\vec{u}$ in Bezug auf eine orthogonale Basis $\overrightarrow{b_1}$, ..., $\overrightarrow{b_n}$ gegeben durch:

$$c_i = \frac{\langle \vec{u}, \overrightarrow{b_1} \rangle}{\left\| \overrightarrow{b_1}^2 \right\|}, \text{ i = 1,2, …, n}$$