Übung zu Mathematik I für Informatik

1. (a) Bekanntlich läßt sich für $\overline{a} \in \mathbb{Z}_n$ die inverse Restklasse $\overline{a}^{-1}$ mit Hilfe des erweiterten Euklidischen Algorithmus berechnen. Es besteht aber die zusätzliche Möglichkeit, $\overline{a}^{-1}$ mit Hilfe eines geeigneten positiven Exponenten $t \in \mathbb{N}$ zu berechnen:

$$\overline{a}^{-1} \;=\; \overline{a}^{t} \tag{1}$$

   Wie nämlich? *Hinweis*: Satz von Euler.

   (b) Wie lautet dieser Exponent bei $n = 21$? Berechnen Sie auf beide Arten $\overline{10}^{-1} \in \mathbb{Z}_{21}$.

2. Finden Sie in dem Restklassenkörper $\mathbb{Z}_{163}$ Nullstellen des Polynoms

$$\mathrm{p}(X) \;=\; X^2 + \overline{127} \cdot X + \overline{99} \tag{2}$$

   Hinweis: 163 ist eine Primzahl mit $163 \equiv 3 \mod 4$. An geeigneter Stelle können Sie den Algorithmus zum schnellen Potenzieren einsetzen.

3. Gegeben seien die beiden Vektoren

$$\vec{a} = \begin{pmatrix} 3 \\ -4 \end{pmatrix} \quad \text{und} \quad \vec{b} = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

   a) Finden Sie zwei Vektoren $\vec{a}_1, \vec{a}_2 \in \mathbb{R}^2$ mit

   - $\vec{a} = \vec{a}_1 + \vec{a}_2$
   - $\vec{a}_1$ und $\vec{b}$ sind linear abhängig.
   - $\vec{a}_2$ steht senkrecht auf $\vec{b}$.

   b) Finden Sie einen Vektor $\vec{c} \in \mathbb{R}^2$, der senkrecht auf $\vec{b}$ steht und für den

$$\vec{c} \cdot \vec{a} \;=\; -30$$

   gilt.

4. Zeigen Sie: Die Gerade

$$G \;=\; \{\vec{a}_0 + \lambda\vec{a}_1 \,|\, \lambda \in \mathbb{R}\} \;\subset\; \mathbb{R}^2$$

   mit $\vec{a}_1 \neq 0$ enhält genau dann den Nullvektor, wenn $\vec{a}_0$ und $\vec{a}_1$ *linear abhängig* sind.

5. Gegeben seien

$$\vec{x}_1 = \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \vec{x}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \vec{x}_3 = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 2 \end{pmatrix} \in \mathbb{R}^5 \;.$$

   Zeigen Sie, daß diese Vektoren linear unabhängig sind. Ergänzen Sie weiterhin diese Vektoren zu einer Basis des $\mathbb{R}^5$, d. h. finden Sie zwei weitere Vektoren $\vec{x}_4, \vec{x}_5 \in \mathbb{R}^5$, so daß $(\vec{x}_1, \vec{x}_2, \vec{x}_3, \vec{x}_4, \vec{x}_5)$ eine Basis des $\mathbb{R}^5$ ist.

6. Wählen Sie aus

$$\vec{a}_1 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \quad \vec{a}_2 = \begin{pmatrix} -2 \\ -2 \\ 3 \end{pmatrix} \quad \vec{a}_3 = \begin{pmatrix} 2 \\ 2 \\ -2 \end{pmatrix} \quad \vec{a}_4 = \begin{pmatrix} 0 \\ 9 \\ -1 \end{pmatrix} \quad \vec{a}_5 = \begin{pmatrix} 3 \\ 3 \\ 0 \end{pmatrix}$$

drei zueinander linear unabhängige Vektoren aus und stellen Sie die restlichen beiden als Linearkombinationen der drei ausgewählten Vektoren dar.

7. Gegeben sei in Hessescher Normalform die Gerade $G \subset \mathbb{R}^2$:

$$G \;=\; \left\{ \vec{x} \in \mathbb{R}^2 \;\middle|\; \begin{pmatrix} \frac{2}{\sqrt{13}} \\ \frac{3}{\sqrt{13}} \end{pmatrix} \cdot \vec{x} \;=\; \sqrt{52} \right\}$$

   (a) Geben Sie die Gerade G in Parameterform, d. h. in der Form $\{\vec{a} + t\,\vec{b} \mid t \in \mathbb{R}\}$, an.

   (b) Geben Sie eine weitere Gerade $H \in \mathbb{R}^2$ an, die denselben Abstand zum Nullpunkt wie die Gerade G besitzt, zur Geraden G parallel verläuft aber nicht gleich der Geraden G ist.

Übung zu Mathematik I für Informatik

1. Lösung:

   (a) Nach dem Satz von Euler ist $\overline{a}^{\varphi(n)} = \overline{1}$ für $\overline{a} \in \mathbb{Z}_n$. Damit erhält man

   $$\begin{aligned} \overline{a}^{-1} &= \underbrace{\overline{a}^{\varphi(n)}}_{=\overline{1}} \cdot \overline{a}^{-1} = \overline{a}^{\varphi(n)-1} \\ &= \overline{a}^{t} \qquad \text{mit} \quad t = \varphi(n) - 1 \geq 0 \end{aligned} \tag{1}$$

   Wegen $\varphi(n) > 1$ für $n > 2$ ist in diesem Fall der Exponent t in (1) sogar positiv. Im Ausnahmefall $n = 2$ ist ohnehin nur $\mathbb{Z}_2^* = \{\overline{1}\}$, und man kann $t = 1$ wählen.

   (b) Für $a = 10$ und $n = 21$ berechnet man $\overline{10}^{-1}$ auf die „traditionelle“ Weise mit dem erweiterten Euklidischen Algorithmus; dieser liefert:

   $$\begin{aligned} 1 &= -2 \cdot 10 + 1 \cdot 21 \\ \Rightarrow \quad \overline{10}^{-1} &= \overline{-2} = \overline{19} \end{aligned}$$

   Für die zweite Möglichkeit berechnet man zunächst

   $$\varphi(21) = \varphi(3 \cdot 7) = (3-1) \cdot (7-1) = 12$$

   Als berechnet man

   $$\begin{aligned} \overline{10}^{-1} &= \overline{10}^{11} = \overline{100}^{5} \cdot \overline{10} = \overline{-5}^{3} \cdot \overline{5}^{2} \cdot \overline{10} \\ &= \overline{-125 + 6 \cdot 21} \cdot \overline{4} \cdot \overline{10} = \overline{40} = \overline{19} \end{aligned}$$

   Man würde hier natürlich besser den Algorithmus zum schnellen Potenzieren einsetzen.

2. Lösung: Man kann bei dem Körper $\mathbb{Z}_{163}$ ebenso wie bei den reellen oder komplexen Zahlen die quadratische Ergänzung („p-q-Formel“) einsetzen. Das liefert hier für die beiden möglichen Nullstellen die Darstellung

   $$x_{1,2} = -\overline{127} \cdot \overline{2}^{-1} \pm \overline{2}^{-1} \cdot \sqrt{\overline{127}^{2} - \overline{4} \cdot \overline{99}} \tag{2}$$

   Man erkennt hier sofort – ohne den erweiterten euklidischen Algorithmus anwenden zu müssen: $\overline{2}^{-1} = \overline{82}$. Wie in der Vorlesung gezeigt, berechnet man die Quadratwurzel durch Potenzieren mit $(163 + 1)/4 = 41$. Das liefert

   $$\begin{aligned} x_{1,2} &= -\overline{127} \cdot \overline{82} \pm \overline{82} \cdot \sqrt{\overline{155} - \overline{70}} \\ &= \overline{18} \pm \overline{82} \cdot \overline{85}^{41} = \overline{18} \pm \overline{82} \cdot \overline{133} \end{aligned} \tag{3}$$

   Achtung: Hier ist nicht sicher, ob die – immer mögliche – Potenzierung mit $(163+1)/4 = 41$ tatsächlich die Quadratwurzel von $\overline{85}$ geliefert hat. Dieses ist nur dann der Fall,

wenn $\overline{85}$ ein Quadrat in $\mathbb{Z}_{163}$ ist[1]. Man muß daher, um sicherzustellen, ob wirklich die Quadratwurzel berechnet wurde, das Ergebnis der Potenzierung noch einmal quadrieren, d. h. hier noch folgende Rechnung durchführen:

$$\left(\overline{85}^{41}\right)^2 \;=\; \overline{133}^{\,2} \;=\; \overline{17689} \;=\; \overline{85} \tag{4}$$

Somit lieferte die Potenz in (3) tatsächlich die Quadratwurzel, und man die Rechnung fortsetzen:

$$x_{1,2} \;=\; \overline{18} \pm \overline{148} \;=\; \begin{cases} \overline{3} \\ \overline{33} \end{cases}$$

Die Potenz in (3) wurde mit dem Algorithmus zum schnellen Potenzieren berechnet.

3. **a)**

$$\vec{a}_1 \;=\; \frac{\vec{a}\cdot\vec{b}}{\vec{b}\cdot\vec{b}}\cdot\vec{b} \;=\; \begin{pmatrix} 4 \\ -2 \end{pmatrix}, \qquad \vec{a}_2 \;=\; \vec{a} - \vec{a}_1 \;=\; \begin{pmatrix} -1 \\ -2 \end{pmatrix}$$

b) Der Vektor $\vec{c}$ ist Lösung des linearen Gleichungssystems

$$\begin{aligned} -2\cdot x_1 + 1\cdot x_2 &= 0 \\ +3\cdot x_1 - 4\cdot x_2 &= -30 \end{aligned}$$

Wendet man das Gaußsche Verfahren an, so erhält man die reduzierte Form:

$$\begin{aligned} x_1 - \frac{1}{2}\cdot x_2 &= 0 \\ -\frac{5}{2}\cdot x_2 &= -30 \end{aligned}$$

Es folgt sofort $\vec{c} = (6, 12)^t$.

4. Es ist zu zeigen:

$$0 \in G \;\Leftrightarrow\; \vec{a}_0 \text{ und } \vec{a}_1 \text{ lin. abhg.}$$

1. Richtung: Sei $0 \in G$, dann hat der Nullvektor[2] mit einem $\lambda_0 \in \mathbb{R}$ die Darstellung:

$$0 \;=\; 1\cdot\vec{a}_0 + \lambda_0\cdot\vec{a}_1$$

Dieses ist bereits eine die Null darstellende Linearkombination von $\vec{a}_0$ und $\vec{a}_1$, bei der zumindest der Koeffizient von $\vec{a}_0$ von Null verschieden ist; also sind $\vec{a}_0$ und $\vec{a}_1$ linear abhängig.
2. Richtung: Seien nun $\vec{a}_0$ und $\vec{a}_1$ linear abhängig, d. h. es gebe $\alpha, \beta \in \mathbb{R}$, die nicht beide gleich Null sind, mit

$$0 \;=\; \alpha\vec{a}_0 + \beta\vec{a}_1$$

Ist $\alpha \neq 0$, so erhält man nach Teilung durch α eine Darstellung von 0 als Geradenelement:

$$0 \;=\; \vec{a}_0 + \frac{\beta}{\alpha}\vec{a}_1 \;\in\; G$$

Ist $\beta \neq 0$, so folgt wegen $\vec{a}_1 \neq 0$:

$$-\alpha\vec{a}_0 \;=\; \beta\vec{a}_1 \;\neq\; 0$$

und damit auch $\alpha \neq 0$. Wie oben kann man jetzt wieder $0 \in G$ schließen.

[1] Siehe die Begründung der Formel zu Ziehen der Quadratwurzel in der Vorlesung bzw. im Skript.
[2] Zur Abkürzung wird hier für den Nullvektor statt $\vec{0}$ einfach 0 geschreiben.

5. Um die lineare Unabhängigkeit der $\vec{x}_1, \vec{x}_2, \vec{x}_3$ nachzuweisen, ist zu zeigen, daß die Gleichung

$$\lambda_1\vec{x}_1 + \lambda_2\vec{x}_2 + \lambda_3\vec{x}_3 = 0 \tag{5}$$

nur für $\lambda_1 = \lambda_2 = \lambda_3 = 0$ erfüllt ist. Setzt man in (5) die Komponenten der Vektoren $\vec{x}_1, \vec{x}_2, \vec{x}_3$ ein, so erkennt man, daß es sich dabei um ein lineares homogenes Gleichungssystem mit den Unbestimmten $\lambda_1, \lambda_2, \lambda_3$ handelt. Die Koeffizientenmatrix dieses Gleichungssystems lautet:

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}$$

Die Reduzierung dieser Matrix gemäß des Gaußschen Verfahrens liefert

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Man erkennt, daß das Gleichungssystem den Rang drei besitzt. Insbesondere ist der Rang gleich der Anzahl der Unbestimmten $(\lambda_1, \lambda_2, \lambda_3)$ und damit der Corang Null. Es gibt daher keine von Null verschiedene Lösung dieses homogenen Systems und damit keine Werte für $\lambda_1, \lambda_2, \lambda_3$, die nicht alle gleich Null sind und (5) erfüllen.

Um $(\vec{x}_1, \vec{x}_2, \vec{x}_3)$ zu einer Basis des $\mathbb{R}^5$ zu ergänzen, setze man

$$\vec{x}_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \vec{x}_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Zu zeigen bleibt, daß $\vec{x}_1, \ldots, \vec{x}_5$ linear unabhängig sind; aus Dimensionsgründen folgt dann, daß sie eine Basis des $\mathbb{R}^5$ bilden. Sei also

$$0 = \lambda_1\vec{x}_1 + \lambda_2\vec{x}_2 + \lambda_3\vec{x}_3 + \lambda_4\vec{x}_4 + \lambda_5\vec{x}_5.$$

Zu zeigen ist $\lambda_1 = \cdots = \lambda_5 = 0$. Man schließt dazu wie oben: Man stellt ein homogenes lineares Gleichungssystem auf, dessen Unbekannten $\lambda_1, \ldots, \lambda_5$ lauten, und rechnet nach, daß der Corang dieses Gleichungssystems Null beträgt. Das Gleichungssystem ist daher nur erfüllt, wenn alle λ_i gleich Null sind; die Vektoren $\vec{x}_1, \ldots, \vec{x}_5$ sind daher in der Tat linear unabhängig und bilden somit eine Basis des $\mathbb{R}^5$.

6. Zunächst bringe man die Matrix

$$A = (\vec{a}_1\vec{a}_2\vec{a}_3\vec{a}_4\vec{a}_5)$$

mit Hilfe des Gaußschen Verfahrens in eine reduzierte Form. Man erkennt dann, daß die Matrix den Rang 3 hat, und wählt drei Spalten aus, so daß die Matrix aus diesen drei

Spalten auch noch den Rang 3 hat. Sind i, j, k die Indizes dieser drei Spalten, so sind die Vektoren $\vec{a}_i, \vec{a}_j, \vec{a}_k$ zueinander linear unabhängig.

Zum Finden der Darstellung der anderen beiden Vektoren als Linearkombinationen aus $\vec{a}_i, \vec{a}_j, \vec{a}_k$ verwende man wieder das Gaußsche Verfahren. Die reduzierten Formen der beiden zu berechnenden Gleichungssysteme gewinnt man sofort aus der reduzierten Form der Matrix A aus dem ersten Schritt.

7. (a) Zu lösen ist das lineare Gleichungssystem mit nur einer Gleichung und zwei Unbekannten

$$\frac{2}{\sqrt{13}}\, x_1 + \frac{3}{\sqrt{13}}\, x_2 = \sqrt{52}$$

Die Teilung durch $2/\sqrt{13}$ (Normierung) liefert

$$x_1 + \frac{3}{2}\, x_2 = 13$$

Man erkennt Rang 1 und Corang 1. Ein spezielle Lösung $\vec{a}$ erhält man wie üblich mit $x_2 = 0$ und eine Grundlösung $\vec{b}$ des zugehörigen homogenen Systems mit $x_2 = 1$:

$$\vec{a} = \begin{pmatrix} 13 \\ 0 \end{pmatrix} \qquad \vec{b} = \begin{pmatrix} -\frac{3}{2} \\ 1 \end{pmatrix}$$

Das liefert die Parameterform

$$G = \left\{ \begin{pmatrix} 13 \\ 0 \end{pmatrix} + t \begin{pmatrix} -\frac{3}{2} \\ 1 \end{pmatrix} \middle| \, t \in \mathbb{R} \right\}$$

(b) Die gesuchte Gerade H erhält man, indem man in der Hesseschen Normalform das Negative des ursprünglichen Normalenvektors wählt:

$$H = \left\{ \vec{x} \in \mathbb{R}^2 \middle| \begin{pmatrix} \frac{-2}{\sqrt{13}} \\ \frac{-3}{\sqrt{13}} \end{pmatrix} \cdot \vec{x} = \sqrt{52} \right\}$$

Bei der Parameterform kann derselbe Richtungsvektor $\vec{b}$ gewählt werden; beim Stützvektor nimmt man das Negative des ursprünglichen Stützvektors:

$$H = \left\{ \begin{pmatrix} -13 \\ 0 \end{pmatrix} + t \begin{pmatrix} -\frac{3}{2} \\ 1 \end{pmatrix} \middle| \, t \in \mathbb{R} \right\}$$