



Lösungsblatt 5

Aufgabe 1 (Modulo Rechnen)

- (a) $\gcd(7, 11, 21) = \gcd(\gcd(7, 11), 21) = \gcd(1, 21) = 1$.
- (b) Wir verwenden den erweiterten Euklid, um $\gcd(7, 11)$ als Linearkombination von 11 und 7 darzustellen und erhalten: $-3 \cdot 7 + 2 \cdot 11 = 1$ und somit die Lösung $7 \cdot (-3) \cdot 3 + 11 \cdot 2 \cdot 3 \equiv 3 \pmod{21}$.
- (c) Nach dem vorigen Übungsblatt gilt $85 \cdot 18 \equiv 45 \pmod{165}$, woraus folgt, daß $(x, y) = (18, 1)$ eine Lösung der modularen Gleichung ist.
- (d) $11y \equiv 3 - 7x \pmod{21}$ ist für alle $x \in \mathbb{Z}$ lösbar, da $\gcd(11, 21) = 1$. Wir erhalten also $y \equiv 2(3 - 7x) \pmod{21}$ und die Lösungsmenge $L = \{(x, y) \in \mathbb{Z} \mid y = 2(3 - 7x) + k \cdot 21 \text{ mit } k \in \mathbb{Z}\}$.
- (e) $85x \equiv 48 - 3y \pmod{165}$ ist genau dann lösbar, wenn $\gcd(85, 165) \mid (48 - 3y)$, also genau dann, wenn $48 - 3y \equiv 0 \pmod{5}$. Es ergibt sich daher mit dem erweiterten euklidischen Algorithmus, daß $y = 1 + 5k_y$ für ein $k_y \in \mathbb{Z}$ sein muß. Wir setzen dieses in die vorherige Gleichung ein, und erhalten:

$$\begin{aligned} 85x &\equiv 45 - 15k_y \pmod{165} \Leftrightarrow \\ 17x &\equiv 9 - 3k_y, \end{aligned}$$

woraus folgt, daß $x \equiv 2(9 - 3k_y) \pmod{33}$. Wir erhalten die Lösungsmenge

$$L = \{(x, y) \in \mathbb{Z} \mid y = 1 + 5k_y \text{ und } x = 2(9 - 3k_y) + 33k_x \text{ mit } k_y, k_x \in \mathbb{Z}\}.$$

Aufgabe 2 (Matrizenringe)

- (a) $7x_1 \equiv 3 - 12x_2 \pmod{21}$ ist genau dann lösbar, wenn $\gcd(7, 21) \mid (3 - 12x_2)$, also genau dann, wenn $3 - 12x_2 \equiv 0 \pmod{7}$. Es ergibt sich daher mit dem erweiterten euklidischen Algorithmus, daß $x_2 = 2 + 7k_2$ für ein $k_2 \in \mathbb{Z}$ sein muß. Wir setzen dieses in die vorherige Gleichung ein, und erhalten:

$$\begin{aligned} 7x_1 &\equiv 0 \pmod{21} \Leftrightarrow \\ x_2 &\equiv 0 \pmod{3}. \end{aligned}$$

Wir erhalten die Lösungsmenge

$$L = \{(x_1, x_2) = (3x, 2 + 7y) \in \mathbb{Z}_{21}^2 \mid y \in \{0, 1, 2\} \text{ und } x \in \{0, 1, \dots, 6\}\}.$$

- (b) Wir berechnen zunächst:

$$\begin{pmatrix} 4 & 27 \\ 15 & 6 \end{pmatrix}^{-1} \equiv 7 \begin{pmatrix} 6 & -27 \\ -15 & 4 \end{pmatrix} \pmod{29}.$$

Wenn wir die Gleichung nun mit der oben stehenden Matrix von links multiplizieren, erhalten wir

$$\begin{pmatrix} 1 & 0 & -7 \\ 0 & 1 & -6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ -3 \end{pmatrix} \pmod{29}.$$

Daraus ergibt sich die Lösungsmenge

$$L = \left\{ (x_1, x_2, x_3)^\top \in \mathbb{Z}_{29}^3 \mid x_1 \equiv 6 + 7x_3 \pmod{29} \text{ und } x_2 \equiv 6x_3 - 3 \pmod{29} \right\}.$$

Aufgabe 3 (Wahrscheinlichkeiten)

- (a) Die Ergebnismenge kann als $S = \mathbb{Z}_6^2$ dargestellt werden. Die erste Komponente gibt dabei die Augenzahl des grünen Würfels an. Jedes Elementarereignis $s = (x, y) \in S$ hat die Wahrscheinlichkeit $1/36$, da wir die Würfel voneinander unterscheiden können.
- (b) Das Ereignis „Mäxchen“ ist $\{(1, 2), (2, 1)\} \subseteq S$ und hat die Wahrscheinlichkeit $1/18$. Das Ereignis „Pasch“ ist $\{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\} \subseteq S$ und hat die Wahrscheinlichkeit $1/6$.
- (c) Es gibt offensichtlich 21 Elementarereignisse: $11, 21, 22, 31, 32, \dots$. Wir erstellen die folgende Tabelle, wobei der Eintrag in der Tabelle die Wahrscheinlichkeit des Elementarereignisses angibt:

	Zehner	1	2	3	4	5	6
Einer							
1		1/36	1/18	1/18	1/18	1/18	1/18
2			1/36	1/18	1/18	1/18	1/18
3				1/36	1/18	1/18	1/18
4					1/36	1/18	1/18
5						1/36	1/18
6							1/36

Aufgabe 4 (Wahrscheinlichkeiten)

- (a) Es sind nach dem Ziehen der ersten vier Karten noch 48 Karten im Spiel, wovon 4 ein günstiges das gewünschte Ereignis wären. Die gesuchte Wahrscheinlichkeit ist also $4/48$.
- (b) Die Wahrscheinlichkeit, daß (nach den diversen Mischvorgängen) die 21. Karte im Stapel eine 7 oder ein König ist, genau $4/47$.
- (c) Wir verweisen auf das nächste Übungsblatt.

Aufgabe 5 (Geburtstagsparadoxon)

Nach dem Buch J. Buchmann, „Einführung in die Kryptographie“ gilt, daß $p \geq 1 - e^{-(k)(k-1)/(2n)}$. Damit $p \geq 1/2$, muß gelten, daß $(k)(k-1)/(2n) \geq \ln(2) \approx 0.69314$. Für jede Kreditkarte gibt es 10000 mögliche PINs, daher ist es in unserem Fall ausreichend,

$$k = 119 \geq k - 1 \geq 117.741 \approx \sqrt{20000 \cdot 0.69314}$$

zu beantragen, um mit der Wahrscheinlichkeit $1/2$ zwei Kreditkarten mit der gleichen PIN zu erhalten.