

Übungsaufgaben

7

1. Aufgabe

Zeigen Sie:

a. \mathbb{Z}_2 ist Körper

Das folgt aus Satz 7.4 und der Tatsache, dass 2 eine Primzahl ist.

+	0	1	-	-	-	·	1
0	0	1	-	-	-	1	1
1	1	0	-	-	-	-	-

b. Es gibt einen Körper mit 7 Elementen

\mathbb{Z}_7 ist Körper. Das folgt aus Satz 7.4 und der Tatsache, dass 7 eine Primzahl ist.

+	0	1	2	3	4	5	6	-	·	1	2	3	4	5	6
0	0	1	2	3	4	5	6	-	1	1	2	3	4	5	6
1	1	2	3	4	5	6	0	-	2	2	4	6	1	3	5
2	2	3	4	5	6	0	1	-	3	3	6	2	5	1	4
3	3	4	5	6	0	1	2	-	4	4	1	5	2	6	3
4	4	5	6	0	1	2	3	-	5	5	3	1	6	4	2
5	5	6	0	1	2	3	4	-	6	6	5	4	3	2	1
6	6	0	1	2	3	4	5	-	-	-	-	-	-	-	-

c. \mathbf{Z}_6 ist kein Körper

\mathbf{Z}_6 ist kein Körper. Das folgt aus Satz 7.4 und der Tatsache, dass 6 eine zusammengesetzte Zahl ist.

+	0	1	2	3	4	5	-	·	1	2	3	4	5
0	0	1	2	3	4	5	-	1	1	2	3	4	5
1	1	2	3	4	5	0	-	2	2	4	0	2	4
2	2	3	4	5	0	1	-	3	3	0	3	0	3
3	3	4	5	0	1	2	-	4	4	2	0	4	2
4	4	5	0	1	2	3	-	5	5	4	3	2	1
5	5	0	1	2	3	4	-	-	-	-	-	-	-

Stellen Sie außerdem in jedem der drei Fälle die Additions- und die Multiplikationstafel auf.

2. Aufgabe

Sei $m \in \mathbf{N}$, $m > 0$. Zeigen Sie: Jedes Element aus \mathbf{Z}_m besitzt ein additives Inverses.

Sei $[a]_m \in \mathbf{Z}_m$ mit einem Repräsentanten $0 \leq a < m$. Dann gilt für $[m - a]_m$:

$$[a]_m + [m - a]_m = [0]_m$$

3. Aufgabe

Sei $m \in \mathbf{N}$, $m > 0$. Geben Sie mit Hilfe von Repräsentanten aus der Menge $\{1, \dots, m\}$ jeweils die additiven Inversen aus \mathbf{Z}_m an:

a. zu 1 in \mathbf{Z}_{20}

$$- [1]_{20} = [19]_{20}$$

b. zu 4 in \mathbf{Z}_{12}

$$- [4]_{12} = [8]_{12}$$

c. zu 199 in \mathbf{Z}_{200}

$$- [199]_{200} = [1]_{200}$$

4. Aufgabe

Zeigen Sie: Es gilt nicht, dass für alle $m \in \mathbb{N}$, $m > 0$ jedes Element aus \mathbb{Z}_m ein multiplikatives Inverses besitzt.

Die Sätze 7.2 und 7.3 und ihre Beweise zeigen, dass nur für Primzahlen p gilt, dass jedes Element aus \mathbb{Z}_p ein multiplikatives Inverses besitzt. Für alle zusammengesetzten Zahlen m gibt es Elemente in \mathbb{Z}_m ohne multiplikatives Inverses. Es sind die Elemente $[n]_m$, für die gilt: $\text{ggT}(m,n) \neq 1$.

Betrachten Sie beispielsweise die Multiplikationstafel von $\mathbb{Z}_6 \setminus \{0\}$ in Aufgabe 1c). Sie sehen dort, dass die Elemente $[2]_6$, $[3]_6$ und $[4]_6$ alle kein multiplikatives Inverses besitzen.

5. Aufgabe

457 ist eine Primzahl. Finden Sie multiplikative Inverse zu den folgenden Elementen von \mathbb{Z}_{457} :

a. 12

$$457 = 38 \cdot 12 + 1$$

Also:

$$1 = 457 + (-38) \cdot 12$$

Also:

$$([12]_{457})^{-1} = [-38]_{457} = [419]_{457}$$

b. 200

$$457 = 2 \cdot 200 + 57$$

$$200 = 3 \cdot 57 + 29$$

$$57 = 1 \cdot 29 + 28$$

$$29 = 1 \cdot 28 + 1$$

Also:

$$\begin{aligned} 1 &= 29 + (-1) \cdot 28 = 29 + (-1) \cdot (57 - 1 \cdot 29) = 2 \cdot 29 - 1 \cdot 57 = \\ &= 2 \cdot (200 - 3 \cdot 57) - 1 \cdot 57 = 2 \cdot 200 - 7 \cdot 57 = \\ &= 2 \cdot 200 - 7 \cdot (457 - 2 \cdot 200) = (-7) \cdot 457 + 16 \cdot 200 \end{aligned}$$

Also:

$$([200]_{457})^{-1} = [16]_{457}$$

c. 400

$$457 = 1 \cdot 400 + 57$$

$$400 = 7 \cdot 57 + 1$$

Also:

$$1 = 400 - 7 \cdot 57 = 400 - 7 \cdot (457 - 400) = 8 \cdot 400 - 7 \cdot 457$$

Also:

$$([400]_{457})^{-1} = [8]_{457}$$

(Das hätte ich auch schneller rauskriegen können! Wieso? Beachten Sie Aufgabenteil b)

6. Aufgabe

Beachten Sie bitte meine Bemerkungen zur Lösung von Aufgabe 4.

- a. Gibt es in \mathbf{Z}_{14} Zahlen, die kein multiplikatives Inverses haben? Wenn ja, welche sind das?
Es ist $14 = 2 \cdot 7$, daher gibt es solche Zahlen, es sind $[2]_{14}, [4]_{14}, [6]_{14}, [7]_{14}, [8]_{14}, [10]_{14}, [12]_{14}$
- b. Gibt es in \mathbf{Z}_{91} Zahlen, die kein multiplikatives Inverses haben? Wenn ja, welche sind das?
Es ist $91 = 7 \cdot 13$, daher gibt es solche Zahlen, es sind $[7]_{91}, [13]_{91}, [14]_{91}, [21]_{91}, [26]_{91}, [28]_{91}, [35]_{91}, [39]_{91}, [42]_{91}, [49]_{91}, [52]_{91}, [56]_{91}, [63]_{91}, [65]_{91}, [70]_{91}, [77]_{91}, [78]_{91}, [84]_{91}$
- c. Gibt es in \mathbf{Z}_{11} Zahlen, die kein multiplikatives Inverses haben? Wenn ja, welche sind das?
11 ist eine Primzahl, daher existiert keine derartige Zahl.
- d. Gibt es in \mathbf{Z}_{97} Zahlen, die kein multiplikatives Inverses haben? Wenn ja, welche sind das?
97 ist eine Primzahl, daher existiert keine derartige Zahl.

7. Aufgabe

- a. Eine Mathematikerin argumentiert:

$$3x = 12 \bmod 97 \rightarrow x = 4 \bmod 97$$

Hat sie recht? Falls ja, beweisen Sie ihre Aussage, falls nein, beweisen Sie dies ebenfalls.

Die Mathematikerin hat recht, denn 97 ist eine Primzahl. Genauer:

$$97 = 32 \cdot 3 + 1$$

Also:

$$1 = 97 - 3 \cdot 32$$

Also: $([3]_{97})^{-1} = [-32]_{97} = [65]_{97}$ Und es gilt:

$$\begin{aligned} 3x = 12 \bmod 97 &\rightarrow [3]_{97} \cdot [x]_{97} = [12]_{97} \rightarrow \\ &\rightarrow [65]_{97} \cdot [3]_{97} \cdot [x]_{97} = [65]_{97} \cdot [12]_{97} = [780]_{97} = [4]_{97} \rightarrow \\ &\rightarrow [x]_{97} = [4]_{97} \rightarrow x = 4 \bmod 97 \end{aligned}$$

- b. Eine Kollegin argumentiert:

$$3x = 12 \bmod 87 \rightarrow x = 4 \bmod 87$$

Hat sie ebenfalls recht? Falls ja, beweisen Sie ihre Aussage, falls nein, beweisen Sie dies ebenfalls.

Die Kollegin hat nicht recht. Zunächst können wir nicht wie im Aufgabenteil 7 a argumentieren, denn $[3]_{87}$ ist in \mathbf{Z}_{87} mit $87 = 3 \cdot 29$ und $\text{ggT}(3, 87) = 3$ nicht invertierbar. Tatsächlich gilt:

$$3 \cdot 4 = 12 \bmod 87, \quad \text{also} \quad x = 4 \bmod 87$$

$$3 \cdot 33 = 12 \bmod 87, \quad \text{also} \quad x = 33 \bmod 87$$

$$3 \cdot 62 = 12 \bmod 87, \quad \text{also} \quad x = 62 \bmod 87$$

erfüllen alle diese Gleichung. (Beachten Sie: $3 \cdot 33 = 3 \cdot (4 + 29) = 3 \cdot 4 + 87$ und entsprechend für 62)

8. Aufgabe

Zeigen Sie: Sowohl beim 10-stelligen als auch beim 13-stelligen ISBN-Codierungsverfahren werden Einzelfehler – das sind Fehler, bei denen nur eine einzige Ziffer verändert wurde – stets erkannt.

Zur 10-stelligen ISBN-Ziffer vergleiche man Satz 7.7, zur 13-stelligen ISBN-Ziffer vergleiche man Satz 7.9

9. Aufgabe

Von den folgenden 5 zehnstelligen ISBN-Nummern sind einige gültig und einige ungültig. Entscheiden Sie jeweils:

a. 3596159717

$$\begin{aligned} 10 \cdot 3 + 9 \cdot 5 + 8 \cdot 9 + 7 \cdot 6 + 6 \cdot 1 + 5 \cdot 5 + 4 \cdot 9 + 3 \cdot 7 + 2 \cdot 1 + 7 &= 286 = \\ &= 26 \cdot 11 = 0 \bmod 11, \text{ diese Ziffer ist also korrekt.} \end{aligned}$$

b. 342372444X

$$\begin{aligned} 10 \cdot 3 + 9 \cdot 4 + 8 \cdot 2 + 7 \cdot 3 + 6 \cdot 7 + 5 \cdot 2 + 4 \cdot 4 + 3 \cdot 4 + 2 \cdot 4 + 10 &= 201 = \\ &= 18 \cdot 11 + 3 = 3 \bmod 11, \text{ diese Ziffer ist also nicht korrekt.} \end{aligned}$$

c. 3100540204

$$\begin{aligned} 10 \cdot 3 + 9 \cdot 1 + 8 \cdot 0 + 7 \cdot 0 + 6 \cdot 5 + 5 \cdot 4 + 4 \cdot 0 + 3 \cdot 2 + 2 \cdot 0 + 4 &= 99 = \\ &= 9 \cdot 11 = 0 \bmod 11, \text{ diese Ziffer ist also korrekt.} \end{aligned}$$

d. 3518460536

$$\begin{aligned} 10 \cdot 3 + 9 \cdot 5 + 8 \cdot 1 + 7 \cdot 8 + 6 \cdot 4 + 5 \cdot 6 + 4 \cdot 0 + 3 \cdot 5 + 2 \cdot 3 + 6 &= 220 = \\ &= 20 \cdot 11 = 0 \bmod 11, \text{ diese Ziffer ist also korrekt.} \end{aligned}$$

e. 3423342984

$$\begin{aligned} 10 \cdot 3 + 9 \cdot 4 + 8 \cdot 2 + 7 \cdot 3 + 6 \cdot 3 + 5 \cdot 4 + 4 \cdot 2 + 3 \cdot 9 + 2 \cdot 8 + 4 &= 196 = \\ &= 17 \cdot 11 + 9 = 9 \bmod 11, \text{ diese Ziffer ist also nicht korrekt.} \end{aligned}$$

10. Aufgabe

Bei den folgenden 5 zehnstelligen ISBN-Nummern fehlt die Prüfziffer. Ermitteln Sie sie:

a. 363062073..

$$[p]_{11} = [3 + 2 \cdot 6 + 3 \cdot 3 + 4 \cdot 0 + 5 \cdot 6 + 6 \cdot 2 + 7 \cdot 0 + 8 \cdot 7 + 9 \cdot 3]_{11} = [6]_{11}$$

$$\text{Also } p = 6$$

b. 342333052..

$$[p]_{11} = [3 + 2 \cdot 4 + 3 \cdot 2 + 4 \cdot 3 + 5 \cdot 3 + 6 \cdot 3 + 7 \cdot 0 + 8 \cdot 5 + 9 \cdot 2]_{11} = [10]_{11}$$

$$\text{Also } p = X$$

c. 342311824..

$$[p]_{11} = [3 + 2 \cdot 4 + 3 \cdot 2 + 4 \cdot 3 + 5 \cdot 1 + 6 \cdot 1 + 7 \cdot 8 + 8 \cdot 2 + 9 \cdot 4]_{11} = [5]_{11}$$

$$\text{Also } p = 5$$

d. 360894442..

$$[p]_{11} = [3 + 2 \cdot 6 + 3 \cdot 0 + 4 \cdot 8 + 5 \cdot 9 + 6 \cdot 4 + 7 \cdot 4 + 8 \cdot 4 + 9 \cdot 2]_{11} = [7]_{11}$$

$$\text{Also } p = 7$$

e. 351810068..

$$[p]_{11} = [3 + 2 \cdot 5 + 3 \cdot 1 + 4 \cdot 8 + 5 \cdot 1 + 6 \cdot 0 + 7 \cdot 0 + 8 \cdot 6 + 9 \cdot 8]_{11} = [8]_{11}$$

$$\text{Also } p = 8$$

11. Aufgabe

- a. Bei der Erfassung der zehnstelligen ISBN-Nummer 3608944443 wird bei der Erfassung die 5. und 6. Ziffer versehentlich vertauscht (Statt 94 also 49). Wird das durch die formale Überprüfung des Nummernaufbaus erkannt?

Aus Satz 7.8 folgt sofort, dass diese Vertauschung durch die formale Überprüfung des Nummernaufbaus erkannt wird. Tatsächlich wäre nach der Vertauschung die korrekte Form der zehnstelligen ISBN-Nummer:

3608494448, die Kontrollziffer ist hier also die 8 und nicht die 3.

- b. Bei der Erfassung der entsprechenden dreizehnstelligen ISBN-Nummer 978-3608944440 wird bei der Erfassung die 5. und 6. Ziffer versehentlich vertauscht. (Wieder statt 94 die Reihenfolge 49). Wird das durch die formale Überprüfung des Nummernaufbaus erkannt?

Es lohnt sich hier, Satz 7.10 Punkt (iii) genau anzusehen:

„Sei m ungerade, $1 \leq m \leq 13$ und n gerade, $2 \leq n \leq 12$. Dann können die Ziffer d_m an m -ter Stelle und d_n an n -ter Stelle vertauscht werden, falls gilt: $d_m + 3 \cdot d_n \equiv 3 \cdot d_m + d_n \pmod{10}$. Falls $d_m \neq d_n$ ist, ist das genau dann der Fall, wenn $[d_m - d_n]_{10} = [5]_{10}$ ist. Beachten Sie, dass in einem solchen Falle auch die Vertauschung zweier nebeneinander stehenden Ziffern nicht entdeckt wird.“

Es ist 5 eine ungerade und 6 eine gerade Zahl, $d_5 = 4$, $d_6 = 9$, es ist $d_5 \neq d_6$ und $[d_5 - d_6]_{10} = [-5]_{10} = [5]_{10}$. Also „merkt“ die Prüfziffer diese Vertauschung nicht. Tatsächlich ist sowohl

978-3608944440 als auch 978-3608494440

eine korrekte dreizehnstellige EAN-Nummer.

12. Aufgabe

Von den folgenden 5 dreizehnstelligen ISBN-Nummern sind einige gültig und einige ungültig. Entscheiden Sie jeweils:

- a. 978-3462531607
 $9 + 3 \cdot 7 + 8 + 3 \cdot 3 + 4 + 3 \cdot 6 + 2 + 3 \cdot 5 + 3 + 3 \cdot 1 + 6 + 3 \cdot 0 + 7 = 105 =$
 $= 5 \bmod 10$, diese Ziffer ist also nicht korrekt.
- b. 978-3835101630
 $9 + 3 \cdot 7 + 8 + 3 \cdot 3 + 8 + 3 \cdot 3 + 5 + 3 \cdot 1 + 0 + 3 \cdot 1 + 6 + 3 \cdot 3 + 0 = 90 =$
 $= 0 \bmod 10$, diese Ziffer ist also korrekt.
- c. 978-3518456880
 $9 + 3 \cdot 7 + 8 + 3 \cdot 3 + 5 + 3 \cdot 1 + 8 + 3 \cdot 4 + 5 + 3 \cdot 6 + 8 + 3 \cdot 8 + 0 = 130 =$
 $= 0 \bmod 10$, diese Ziffer ist also korrekt.
- d. 978-3602944440
 $9 + 3 \cdot 7 + 8 + 3 \cdot 3 + 6 + 3 \cdot 0 + 2 + 3 \cdot 9 + 4 + 3 \cdot 4 + 4 + 3 \cdot 4 + 0 = 114 =$
 $= 4 \bmod 10$, diese Ziffer ist also nicht korrekt.
- e. 978-3518100684
 $9 + 3 \cdot 7 + 8 + 3 \cdot 3 + 5 + 3 \cdot 1 + 8 + 3 \cdot 1 + 0 + 3 \cdot 0 + 6 + 3 \cdot 8 + 4 = 100 =$
 $= 0 \bmod 10$, diese Ziffer ist also korrekt.

13. Aufgabe

Bei den folgenden 5 dreizehnstelligen ISBN-Nummern fehlt die Prüfziffer. Ermitteln Sie sie:

- a. 978-360894442..
 $[p]_{10} =$
 $= [9 \cdot 9 + 7 \cdot 7 + 9 \cdot 8 + 7 \cdot 3 + 9 \cdot 6 + 7 \cdot 0 + 9 \cdot 8 + 7 \cdot 9 + 9 \cdot 4 + 7 \cdot 4 + 9 \cdot 4 + 7 \cdot 2]_{10}$
 $= [6]_{10}$
Also $p = 6$

b. 978-342311824..

$$\begin{aligned}[p]_{10} &= \\&= [9 \cdot 9 + 7 \cdot 7 + 9 \cdot 8 + 7 \cdot 3 + 9 \cdot 4 + 7 \cdot 2 + 9 \cdot 3 + 7 \cdot 1 + 9 \cdot 1 + 7 \cdot 8 + 9 \cdot 2 + 7 \cdot 4]_{10} \\&= [8]_{10} \\ \text{Also } p &= 8\end{aligned}$$

c. 978-342333052..

$$\begin{aligned}[p]_{10} &= \\&= [9 \cdot 9 + 7 \cdot 7 + 9 \cdot 8 + 7 \cdot 3 + 9 \cdot 4 + 7 \cdot 2 + 9 \cdot 3 + 7 \cdot 3 + 9 \cdot 3 + 7 \cdot 0 + 9 \cdot 5 + 7 \cdot 2]_{10} \\&= [7]_{10} \\ \text{Also } p &= 7\end{aligned}$$

d. 978-363062073..

$$\begin{aligned}[p]_{10} &= \\&= [9 \cdot 9 + 7 \cdot 7 + 9 \cdot 8 + 7 \cdot 3 + 9 \cdot 6 + 7 \cdot 3 + 9 \cdot 0 + 7 \cdot 6 + 9 \cdot 2 + 7 \cdot 0 + 9 \cdot 7 + 7 \cdot 3]_{10} \\&= [2]_{10} \\ \text{Also } p &= 2\end{aligned}$$

e. 978-342334299..

$$\begin{aligned}[p]_{10} &= \\&= [9 \cdot 9 + 7 \cdot 7 + 9 \cdot 8 + 7 \cdot 3 + 9 \cdot 4 + 7 \cdot 2 + 9 \cdot 3 + 7 \cdot 3 + 9 \cdot 4 + 7 \cdot 2 + 9 \cdot 9 + 7 \cdot 9]_{10} \\&= [5]_{10} \\ \text{Also } p &= 5\end{aligned}$$