Präsenzaufgaben

Verständnisfragen

1. Erklären Sie, wann eine Abbildung zwischen zwei Gruppen ein Homomorphismus ist. Was muss zusätzlich gelten, damit sie ein Isomorphismus ist?
   Eine Abbildung $f : (G, \circ) \to (H, *)$ ist genau dann ein Homomorphismus, wenn für alle $a, b \in G$ gilt: $f(a \circ b) = f(a) * f(b)$. Wenn die Abbildung zusätzlich bijektiv ist, nennt man sie einen Isomorphismus.

2. Warum ist $\phi : \mathbb{Z}_6 \to \mathbb{Z}_3$, $\phi(n) = n \mod 3$ ein Homomorphismus? Ist ϕ auch ein Isomorphismus?*Lösung:* Seien $n, m \in \mathbb{Z}_6$, dann ist

$$\phi(n+m) = (n+m) \mod 3 = n \mod 3 + m \mod 3 = \phi(n) + \phi(m).$$

3. Für welche $n \in \mathbb{Z}$ ist $\mathbb{Z}_n^*$ zyklisch?
   Lösung: Eine mögliche Antwort ist: Wenn es ein Element $a \in \mathbb{Z}_n^*$ gibt mit Ordnung ord(a) = ϕ(n). Die allgemeine Antwort lautet: genau dann, wenn $n = 1, 2, 4$ oder $n = p^k$ oder $n = 2p^k$, wenn p eine beliebige ungerade Primzahl ist $k > 0$. Die ersten zyklischen Gruppen sind also $\mathbb{Z}_2^*$, $\mathbb{Z}_4^*$, $\mathbb{Z}_3^*$, $\mathbb{Z}_5^*$, $\mathbb{Z}_6^*$. Ich habe hier allerdings nicht erwartet, dass Sie auf diese allgemeine Antwort kommen.

4. Sei $p \in \mathbb{P}$. Warum gilt in $\mathbb{Z}_p$ $(p-1)(p-1) = 1$? Wir rechnen $(p-1)(p-1) = p^2 - 2p + 1$. Dies dürfen wir so ausrechnen, da $\mathbb{Z}_p$ ein Körper ist. Dann wenden wir die Rechenregeln an:

   $$(p-1)(p-1) \mod p = p^2 - 2p + 1 \mod p = p^2 \mod p - 2p \mod p + 1 \mod p = 1 \mod p.$$

5. Sei $p \in \mathbb{P}$. Berechnen Sie in $\mathbb{Z}_p$ die Zahl p. Es ist $p \mod p = 0 \mod p$.

6. Finden Sie Beispiele für Elemente a, b, c, $a \neq 0$, so dass $ab = ac$ und $b \neq c$ für
   (a) $\mathbb{Z}_8$: Wenn wir die Gleichung $ab = ac$ umstellen, lautet sie $a(b-c) = 0$. Eine Lösung in $\mathbb{Z}_8$ ist z.B. $a = 2$ und $b - c = 4$, also $b = 4$, $c = 0$ oder $b = 5$,$c = 1$.
   (b) $\mathbb{Z}_2 \times \mathbb{Z}_2$. Die Elemente in $\mathbb{Z}_2 \times \mathbb{Z}_2$ lauten $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$. Wir multiplizieren einfach elementweise: Dann ist beispielsweise $(0,1) \cdot (1,1) = (0,1) \cdot (0,1) = (0,1)$.

7. Bestimmen Sie alle Lösungen von $x^2 - 5x + 6 = 0$ in $\mathbb{Z}$ und $\mathbb{Z}_{12}$. Warum gibt es in $\mathbb{Z}_{12}$ mehr als zwei Lösungen? *Lösung:* Die Lösungen von $x^2 - 5x + 6 = 0$ lauten in $\mathbb{Z}$ (mit der abc-Formel oder durch scharfes Hinschauen): $x_1 = 2$ und $x_2 = 3$. Wir können die Gleichung umschreiben als $x^2 - 5x + 6 = (x-2)(x-3) = 0$. In $\mathbb{Z}_{12}$ wollen wir also lösen

   $$(x-2)(x-3) \mod 12 = 0 \mod 12$$

   Da 12 keine Primzahl ist (und deswegen $\mathbb{Z}_{12}$ kein Körper), erhalten wir zusätzliche Lösungen, wenn die Faktoren $(x-2)$ und $(x-3)$ als Produkt 12 (bzw. ein Vielfaches von 12) ergeben. Wir haben also mehr als zwei Lösungen, denn der Satz vom Nullprodukt gilt nicht! Wenn $x = 6$ ist, ist $(x-2)(x-3) = 4 \cdot 3 = 12$ und $x = 6$ ist eine weitere Lösung, ebenso $x = 11$, denn es ist $(x-2)(x-3) = 9 \cdot 8 = 72 = 0 \mod 12$.

8. *Wir bestimmen die Lösungen hier mit Hilfe des Chinesischen Restsatzes, um seine Anwendung noch einmal zu üben. Bei diesen Aufgaben kann man natürlich auch die richtigen Lösungen raten!*

   (a) Welche Zahlen $n \in \mathbb{Z}$ haben Rest 1 bei Division durch 2 und 3? *Lösung:* Wir müssen das Gleichungssystem lösen:

   $$x \mod 2 = 1 \mod 2, \quad x \mod 3 = 1 \mod 3.$$

   Da $2, 3$ teilerfremd sind, gilt mit dem Chinesischen Restsatz, dass es eine eindeutige Lösung in $\mathbb{Z}_{2\cdot 3}$ gibt. Es ist $1 = (-1)2 + 1 \cdot 3$. Also berechnet sich die Lösung als $x = (-1)2 \cdot 1 + 1 \cdot 3 \cdot 1 = 1 \mod 6$. Somit sind die gesuchten Zahlen alle von der Form $1 + 6k$, $k \in \mathbb{Z}$.

   (b) Welche Zahlen $n \in \mathbb{Z}$ haben Rest 1 bei Division durch 2,3 und 5? *Lösung:* Wie oben stellen wir das Gleichungssystem auf:

   $$x \mod 2 = 1 \mod 2, \quad x \mod 3 = 1 \mod 3, \quad x \mod 5 = 1 \mod 5.$$

   Die Zahlen $2, 3, 5$ sind teilerfremd, hier ist $n = 30$.
   Zu $n_1 = 2$: Wir haben $1 = 8 \cdot 2 + (-1) \cdot 15$, also $a_1 = -15$.
   Zu $n_2 = 3$: Wir haben $1 = (-3) \cdot 3 + 1 \cdot 10$, also $a_2 = 10$.
   Zu $n_3 = 5$: Wir haben $1 = (-1) \cdot 5 + 1 \cdot 6$, also $a_3 = 6$.
   Die Lösung berechnet sich als

   $$x = a_1x_1 + a_2x_2 + a_3x_3 = -15 \cdot 1 + 10 \cdot 1 + 6 \cdot 1 = 1.$$

   Die gesuchten Zahlen sind also von der Form $1 + 30k$, $k \in \mathbb{Z}$.

   (c) Welche Zahlen $n \in \mathbb{Z}$ haben Rest 1 bei Division durch 2,3,5 und 7? *Lösung:* Wie oben stellen wir das Gleichungssystem auf:

   $$x \mod 2 = 1 \mod 2,\ x \mod 3 = 1 \mod 3,\ x \mod 5 = 1 \mod 5,\ x \mod 7 = 1 \quad \text{m}$$

   Die Zahlen $2, 3, 5, 7$ sind teilerfremd, hier ist $n = 210$.
   Zu $n_1 = 2$: Wir haben $1 = 53 \cdot 2 + (-1) \cdot 105$, also $a_1 = -105$.
   Zu $n_2 = 3$: Wir haben $1 = (-23) \cdot 3 + 1 \cdot 70$, also $a_2 = 70$.
   Zu $n_3 = 5$: Wir haben $1 = 17 \cdot 5 + 2 \cdot 42$, also $a_3 = 84$.
   Zu $n_4 = 7$: Wir haben $1 = 13 \cdot 7 + (-3) \cdot 30$, also $a_4 = -90$. Die Lösung berechnet sich als

   $$x = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 = -105 \cdot 1 + 70 \cdot 1 + 84 \cdot 1 - 90 \cdot 1 = -41 \mod 210 = 169 \mod 210.$$

   Die gesuchten Zahlen sind also von der Form $169 + k210$, $k \in \mathbb{Z}$.

Standardaufgaben

1. Bestimmen Sie die Ordnung der Untergruppe, die von dem jeweils angegebenen Element erzeugt wird:

(a) $(\mathbb{Z}_{25}, +)$, 15. *Lösung:* Wir berechnen die Ordnung von 15: Es ist

$$\begin{aligned} 2 \cdot 15 \mod 25 &= 5 \mod 25 \\ 3 \cdot 15 \mod 25 &= 20 \mod 25 \\ 4 \cdot 15 \mod 25 &= 10 \mod 25 \\ 5 \cdot 15 \mod 25 &= 0 \mod 25 \end{aligned}$$

Damit ist $\text{ord}(15) = 5$ und das ist auch die Ordnung der Untergruppe $\{0, 5, 10, 15, 20\}$, die von 15 erzeugt wird.

(b) $(\mathbb{Z}_4 \times \mathbb{Z}_9, +)$,$(2, 6)$. *Lösung:* Wir berechnen die Ordnung von $(2, 6)$:

$$\begin{aligned} (2 \cdot 2 \mod 4, 2 \cdot 6 \mod 9) &= (0 \mod 4, 3 \mod 9) \\ (3 \cdot 2 \mod 4, 3 \cdot 6 \mod 9) &= (2 \mod 4, 0 \mod 9) \\ (4 \cdot 2 \mod 4, 4 \cdot 6 \mod 9) &= (0 \mod 4, 6 \mod 9) \\ (5 \cdot 2 \mod 4, 5 \cdot 6 \mod 9) &= (2 \mod 4, 3 \mod 9) \\ (6 \cdot 2 \mod 4, 6 \cdot 6 \mod 9) &= (0 \mod 4, 0 \mod 9) \end{aligned}$$

Also ist die Ordnung $\text{ord}((2, 6)) = 6$.

2. Welche der folgenden Gruppen ist/ sind zyklisch?

   ☐ $(\mathbb{Q}, +)$ ist nicht zyklisch. Man kann kein Element $\frac{n}{m} \in \mathbb{Q}$ finden, so dass jedes andere Element $\frac{p}{q} \in \mathbb{Q}$ als $k \cdot \frac{n}{m}$ für $k \in \mathbb{Z}$ dargestellt werden kann. Sobald die Nenner m und q teilerfremd sind, geht das nicht.

   ☐ $(6\mathbb{Z}, +)$ ist zyklisch, denn 1 ist ein Erzeuger dieser Gruppe.

   ☐ $(\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}, +)$. Die Zahlen $2, 9$ und 25 sind teilerfremd. Somit ist diese Gruppe isomorph zu $\mathbb{Z}_{2 \cdot 9 \cdot 25} = \mathbb{Z}_{450}$. Diese Gruppe ist wie alle Gruppen $(\mathbb{Z}_n, +)$ zyklisch mit dem Erzeuger 1, somit ist auch $\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$ zyklisch mit dem Erzeuger $(1, 1, 1)$.

3. Welche der folgenden Abbildungen sind Homomorphismen?

   (a) $\phi : \mathbb{R} \setminus \{0\} \to \mathbb{R}^+$, $\phi(a) = |a|$. *Lösung:* Die Gruppenoperation ist hier jeweils die Multiplikation: $(\mathbb{R} \setminus \{0\}, \cdot)$ und $(\mathbb{R}^+, \cdot)$ sind Gruppen. Seien $a, b \in \mathbb{R} \setminus \{0\}$ beliebig, dann ist (wegen der Rechenregel für den Betrag):

   $$\phi(a \cdot b) = |a \cdot b| = |a|\,|b| = \phi(a) \cdot \phi(b).$$

   Also ist ϕ ein Homomorphismus.

   (b) $\phi : \mathbb{Z}_5 \to \mathbb{Z}_2$, $\phi(n) = \begin{cases} 0, & n \text{ gerade} \\ 1, & n \text{ ungerade} \end{cases}$. *Lösung:* Die Abbildung lässt sich auch schreiben als $\phi(n \mod 5) = n \mod 2$. Seien $n, m \in \mathbb{Z}_5$ beliebig, dann gilt (wegen der Rechenregeln der Modulorechnung):

   $$\phi(n + m) = (n + m) \mod 2 = n \mod 2 + m \mod 2 = \phi(n) + \phi(m).$$

   Also ist ϕ ein Homomorphismus.

(c) $\phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $\phi(x, y) = x + y$ Seien $(x_1, y_1), (x_2, y_2 \in \mathbb{R} \times \mathbb{R})$ beliebig, dann ist (wegen des Kommutativgesetzes der Addition in $\mathbb{R}$):

$$\phi(x_1 + x_2, y_1 + y_2) = x_1 + x_2 + y_1 + y_2 = \phi(x_1, y_1) + \phi(x_2, y_2).$$

Also ist ϕ ein Homomorphismus.

4. Konstruieren Sie einen Körper mit genau 4 Elementen. *Lösung:* Ein Körper enthält immer 0 und 1. Die verbleibenden Elemente nennen wir a und b und stellen die Additions- und Multiplikationstafel auf. 0 ist das neutrale Element der Addition, 1 das neutrale Element der Multiplikation.

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

In jeder Zeile muss die 1 genau einmal auftauchen. Es kann entweder $a \cdot a = 1$ oder $a \cdot b = 1$ sein. Es müssen aber auch die Distributivgesetze gelten, also: $a \cdot a = a \cdot (b+1) = a \cdot b + a$. Ist $a \cdot b = 1$, dann ist also $a \cdot a = b$. Es muss auch gelten $a \cdot b = a \cdot (a+1) = a \cdot a + a$. Ist $a \cdot b = 1$, folgt daraus $1 = a \cdot a + a = a + a = 1$. Das stimmt also.
Würden wir $a \cdot a = 1$ wählen, hätten wir $a \cdot b = a \cdot (a+1) = a \cdot a + a = 1 + a = b$, somit wäre a auch neutrales Element von b und $b^2 = 0$, somit hätte b kein inverses Element. Die einzige Möglichkeit, die Multiplikationstafel aufzustellen, ist also die folgende:

·	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

5. (a) Bestimmen Sie alle $n \in \mathbb{Z}$, die bei Division durch 2 oder 5 Rest 1 besitzen, aber durch 3 teilbar sind.*Lösung:* Wir stellen das folgende Gleichungssystem auf:

$$x \mod 2 = 1 \mod 2, \quad x \mod 3 = 0 \mod 3, x \mod 5 = 1 \mod 5.$$

Die Zahl muss ungerade und durch 3 teilbar sein, also 3, 9, 15, etc. Gleichzeitig muss sie $= 1 \mod 5$ sein, also 11,21,31 etc. Die kleinste Zahl ist also 21, die dies erfüllt. Alle weiteren Zahlen sind vom Typ $21 + k30$ mit $k \in \mathbb{Z}$. *Sie können die Aufgabe natürlich auch mit dem Chinesischen Restsatz lösen.*

(b) Bestimmen Sie alle $n \in \mathbb{Z}$, die bei Division durch 3 oder 7 Rest 2 besitzen, aber durch 8 teilbar sind. *Lösung:*Wir stellen das folgende Gleichungssystem auf:

$$x \mod 2 = 2 \mod 3, \quad x \mod 7 = 2 \mod 7, x \mod 8 = 01 \mod 8.$$

Es ist $n = 3 \cdot 7 \cdot 8 = 168$:
Zu 3: $1 = 19 \cdot 3 + (-1) \cdot 56$. Also $a_1 = -56$.
Zu 7: $1 = 7 \cdot 7 + (-2) \cdot 24$. Also $a_2 = -48$.
Zu 8: $1 = 8 \cdot 8 + (-3) \cdot 21$. Also $a_3 = -63$.
Damit ist $x = -56 \cdot 2 + (-48) \cdot 2 + (-63) \cdot 0 = -208 \mod 168 = 128 \mod 168$.
Wir prüfen nach $128 : 3 = 42R2$, $128 : 7 = 18R2$ und $128 : 8 = 16R0$.

Übungsaufgaben: Abgabe

1. Bestimmen Sie alle Erzeuger der Gruppe $\mathbb{Z}_{11}^*$.
   Lösung: Es ist $\mathbb{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$. Wir bestimmen die Ordnung aller Elemente in $\mathbb{Z}_{11}^*$. Jedes Element der Ordnung $10 = |\mathbb{Z}_{11}^*|$ ist ein Erzeuger der Gruppe. Die Elemente können nur Ordnung $1, 2, 5, 10$ besitzen (Teiler von 10). Deswegen genügt es, sich für ein Element a die Potenzen a^2, a^5 und a^{10} anzuschauen:

$$\begin{aligned}
2^2 = 4,\ 2^5 = 10,\ 2^{10} = 1\\
3^2 = 9,\ 3^5 = 1\\
4^2 = 5,\ 4^5 = 1\\
5^2 = 3,\ 5^5 = 1\\
6^2 = 3,\ 6^5 = 10,\ 6^{10} = 1\\
7^2 = 5,\ 7^5 = 10,\ 7^{10} = 1\\
8^2 = 9,\ 8^5 = 10,\ 8^{10} = 1\\
9^2 = 4,\ 9^5 = 1\\
10^2 = 1
\end{aligned}$$

   Also hat die Gruppe die Erzeuger $2, 6, 7, 8$. **(5 Punkte:2 Punkte Ansatz,2 Punkte Rechnungen, 1 Punkt Ergebnis)**

2. Es ist die folgende Relation auf $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ definiert:

$$(a,b) \sim (c,d) :\Leftrightarrow \quad ad = bc.$$

   (a) Zeigen Sie, dass es sich um eine Äquivalenzrelation handelt.
   Lösung: Reflexiv: Sei $(a,b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, dann ist

$$(a,b) \sim (a,b), \text{ denn } ab = ab.$$

   Symmetrisch: Seien $(a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, so dass $(a,b) \sim (c,d)$, dann gilt:

$$(a,b) \sim (c,d) \ \Leftrightarrow\ ad = bc \ \Leftrightarrow\ bc = ab \ \Rightarrow\ (c,d) \sim (a,b).$$

   Transitiv: Seien $(a,b),(c,d),(e,f) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, so dass $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$, dann gilt

$$\begin{aligned}
(a,b) \sim (c,d) \text{ und } (c,d) \sim (e,f) \ &\Leftrightarrow\ ad = bc \text{ und } cf = de \ \big|\cdot f,\ b,d,f \neq 0\\
&\Rightarrow\ adf = bcf \text{ und } cf = de \ \big|\ 2.\ \text{Gleichung in erste einsetzen}\\
&\Rightarrow\ adf = bde \ \big|\ \text{teilen durch } d, \text{ denn } d \neq 0\\
&\Rightarrow\ af = be \ \Leftrightarrow\ (a,b) \sim (e,f).
\end{aligned}$$

   (b) Bestimmen Sie die Äquivalenzklassen $[(n,1)]$ für $n \in \mathbb{Z}$, $[(3,2)]$ sowie $[-21,15]$.
   Lösung:
   Zu $(n,1)$: wir suchen alle $(a,b) \sim (n,1)$, d.h. alle (a,b), so dass $a = bn$ ist. Das sind gerade alle Pärchen, bei denen a das n-fache von b ist:

$$[(n,1)] = \big\{(bn,b) \ \big|\ b \in \mathbb{Z} \setminus \{0\}\big\} = \{\ldots,(n,1),(2n,2),(3n,3),\ldots\}.$$

Zu $(3,2)$: wir suchen alle $(a,b) \sim (3,2)$, d.h. alle (a,b), so dass $2a = 3b$ ist:

$$[(3,2)] = \left\{(3b, 2b) \;\middle|\; b \in \mathbb{Z} \setminus \{0\}\right\} = \{\dots, (3,2), (6,4), (9,6), \dots\}.$$

Zu $(-21,15)$: wir suchen alle $(a,b) \sim (-21,15)$, d.h. alle (a,b), so dass $15a = -21b$ ist. Wir können diese Gleichung zu $5a = -7b$ vereinfachen und erhalten:

$$[(-21,15)] = \left\{(-7b, 5b) \;\middle|\; b \in \mathbb{Z} \setminus \{0\}\right\} = \{\dots, (-7,5), (-14,10), (-21,15), \dots\}.$$

(c) Sei

$$A = \left\{[(a,b)] \;\middle|\; (a,b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}\right\}$$

die Menge der Äquivalenzklassen. Zeigen Sie, dass A mit der Multiplikation aus $\mathbb{Z}$ eine Gruppe bildet, d.h. wir definieren

$$[(a,b)] \cdot [(c,d)] = [(a \cdot c), (b \cdot d)].$$

Lösung:
Assoziativ:

$$[(a,b)]\cdot([(c,d)] \cdot [(e,f)]) = [(a,b)]\cdot[(ce,df)] = [(ace,bdf)] = [(ac,bd)]\cdot[(e,f)] = ([(a,b)] \cdot [(c,d)]$$

Neutrales Element: $[(1,1)]$ ist ein neutrales Element, denn $[(1,1)]\cdot[(a,b)] = [(a,b)]$ für alle $(a,b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$.
Inverse Elemente: Sei $[(a,b)] \in A$ beliebig, dann ist $[(b,a)] \in A$ das inverse Element, denn $[(a,b)] \cdot [(b,a)] = [(ab,ab)] = [(1,1)]$.

(d) Zeigen Sie, dass $(\mathbb{Q}, \cdot)$ isomorph zu $(A, \cdot)$ ist. Geben Sie dafür eine Abbildung $f : \mathbb{Q} \to A$ an und zeigen Sie, dass diese Abbildung ein Isomorphismus ist.
Lösung: Wir bilden $f : \frac{n}{m} \to [(n,m)]$ ab. Wir zeigen zunächst, dass diese Abbildung ein Homomorphismus ist: Seien $n, n', m, m' \in \mathbb{Z}$, $m, m' \neq 0$ beliebig:

$$f\left(\frac{n}{m} \cdot \frac{n'}{m'}\right) = f\left(\frac{nn'}{mm'}\right) = [(nn', mm')] = [(n,m)] \cdot [(n',m')].$$

Jetzt zeigen wir, dass es sich um einen Isomorphismus handelt:
Injektiv: Seien $n, n', m, m' \in \mathbb{Z}$, $m, m' \neq 0$ beliebig, so dass $f(\frac{n}{m}) = f(\frac{n'}{m'})$ gilt:

$$\Leftrightarrow [(n,m)] = [(n',m')] \Leftrightarrow (n,m) \sim (n',m') \;\Leftrightarrow nm' = mn'.$$

Wenn aber $nm' = mn'$ gilt, dann ist $\frac{n}{m} = \frac{n'}{m'}$. Also ist der Homomorphismus injektiv.
Surjektiv: Sei $[(n,m)] \in A$. Dann gibt es natürlich $\frac{n}{m} \in \mathbb{Q}$, so dass $f(\frac{n}{m}) = [(n,m)]$.
Also ist f ein Isomorphismus.

(20 Punkte: je Teilaufgabe 5 Punkte, anteilige Punkte für Ansatz)

3. Es sind $1234 \in \mathbb{Z}_{2000}$ und $567 \in \mathbb{Z}_{2000}$. Addieren Sie die beiden Zahlen 1234 und 567 in $\mathbb{Z}_{2000}$ bzw. in $\mathbb{Z}_{2^4} \times \mathbb{Z}_{5^3}$. Verwenden Sie dafür den erweiterten euklidischen Algorithmus.
Lösung: Wir verwenden den Isomorphismus $f : \mathbb{Z}_{2000} \to \mathbb{Z}_{2^4} \times \mathbb{Z}_{5^3}$, $f(a) = (a \mod 2^4, a \mod 5^3)$. Damit ist $f(1234) = (2, 109)$ und $f(567) = (7, 67)$. Also ist

$(2, 109) + (7, 67) = (9, 176)$. Wir suchen nun $x \in \mathbb{Z}_{2000}$, so dass $x \mod 2^4 = 9$ und $x \mod 5^3 = 51$. Wir lösen entsprechend den erweiterten euklidischen Algorithmus mit $a = 51$, $b = 9$:

a	b	r	s	k
125	16	1	0	–
16	13	0	1	7
13	3	1	-7	1
3	1	-1	8	4
1	0	5	-39	3

Also ist $1 = 5 \cdot 125 + (-39) \cdot 16$. Damit ist für $x = 9 \cdot 5 \cdot 125 + 51 \cdot (-39) \cdot 16 = -26199 \mod 2000$, also $x = 1801 \mod 2000$. Wie wir nachrechnen können, ist dies das richtige Ergebnis, denn es ist $1234 + 567 = 1801$

(15 Punkte: 5 Punkte Addition in Produktgruppe, 5 Punkte euklid. Algorithmus, 5 Punkte Berechnung von x)

4. Es ist das folgende System an Kongruenzgleichungen gegeben:

$$x \equiv 4 \mod 11,\ x \equiv 3 \mod 17,\ x \equiv 6 \mod 18.$$

(a) Erklären Sie, warum eine Lösung x für dieses Gleichungssystem existiert. *Lösung:* Die Zahlen 11,17 und 18 sind teilerfremd, deswegen existiert nach dem Chinesischen Restsatz eine Lösung.

(b) Wir nennen $n_1 = 11$, $n_2 = 17$ und $n_3 = 18$, es ist $n = 11 \cdot 17 \cdot 18 = 3366$. Zu $n_1 = 11$: Gesucht sind r_1, s_1, so dass $1 = r_1 \cdot 11 + s_1 \cdot \frac{3366}{11}$. Aus dem euklidischen Algorithmus erhalten wir $r_1 = -139$ und $s_1 = -5$. Damit ist $a_1 = 5 \cdot 306 = 1530$. Zu $n_2 = 17$: Gesucht sind r_2, s_2, so dass $1 = r_2 \cdot 17 + s_2 \cdot \frac{3366}{17}$.Aus dem euklidischen Algorithmus erhalten wir $r_2 = 35$ und $s_2 = -3$. Damit ist $a_2 = -3 \cdot 198 = -594$. Zu $n_3 = 18$: Gesucht sind r_3, s_3, so dass $1 = r_3 \cdot 18 + s_3 \cdot \frac{3366}{18}$.Aus dem euklidischen Algorithmus erhalten wir $r_2 = 52$ und $s_2 = -5$. Damit ist $a_3 = -5 \cdot 187 = -935$. Die Lösung lautet also

$$x = a_1x_1 + a_2x_2 + a_3x_3 \mod 3366 = -1272 \mod 3366 = 2094.$$

(10 Punkte: a) 2 Punkte, b) 8 Punkte: jeweils für Ansatz und richtige Koeffizienten)

Abgabe möglich bis zu Beginn der Vorlesung am **18.05.2020** bis zu Beginn der Vorlesung 8:00.