Lösungsvorschläge zu Aufgabenblatt 10

(Restklassengruppen mit Multiplikation)

Aufgabe 10.1

Zeigen Sie die folgende Variante das Satzes von Bézout:

Seien $a, b \in \mathbb{N}$. Dann gibt es $s \in \mathbb{N}$ und $t \in \mathbb{Z}$ mit

$$ggT(a, b) = s \cdot a + t \cdot b.$$

Lösung

Nach dem Satz von Bézout finden wir zunächst $s', t' \in \mathbb{Z}$ mit

$$ggT(a, b) = s' \cdot a + t' \cdot b.$$

Ist $s' > 0$, so ist nichts mehr zu tun. Ist $s' \leqslant 0$, so wähle ein $k \in \mathbb{Z}$ mit $s := s' + k \cdot b > 0$ (dies ist möglich, da $b \neq 0$). Setze $t := t' - k \cdot a$. Dann folgt:

$$s \cdot a + t \cdot b \;=\; (s' + kb) \cdot a + (t' - ka) \cdot b = s'a + kba + t'b - kab = s'a + t'b = \mathrm{ggT}(a, b).$$

Aufgabe 10.2

Aufgrund der vielen Studenten soll die Nordakademie in Elmshorn an die U-Bahn angeschlossen werden. Zwei Linien, die U_{15} und die U_{21} fahren im 15- bzw. 21-Minuten Takt. Leider hat der Bahnhof nur einen Bahnsteig, so dass in einer Minute immer nur ein Zug in Elmshorn halten kann.

(a) Ist es möglich, einen Fahrplan zu erstellen so, dass die angegebene Taktung (unfallfrei) eingehalten werden kann?

(b) Wie verhält es sich mit den Linien U_{15} und U_{22}, wenn die Linie U_{22} im 22-Minuten Takt fährt?

Lösung

Zur Modellierung: Wir bezeichnen die Zeitdifferenz, um die Linie U_{15} nach der Linie U_{21} (bzw. U_{21} im Fall (b)) startet, mit $d \in \mathbb{N}$. Wir nehmen also an, dass der erste Zug der Linie U_{2x} ($x \in \{1, 2\}$) zum Zeitpunkt 0 startet und der erste Zug der Linie U_{15} zum Zeitpunkt d Minuten später. Dass sich zwei Züge der Linie U_{15} und U_{2x} ($x \in \{1, 2\}$) treffen ist dann äquivalent dazu, dass es $a, b \in \mathbb{N}_0$ gibt mit

$$2x \cdot a = 15 \cdot b + d.$$

(a) In dieser Situation ist es möglich, einen Fahrplan zu erstellen so, dass die angegebene Taktung (unfallfrei) eingehalten werden kann. Hintergrund ist die Tatsache, dass $\mathrm{ggT}(15, 21) = 3 \neq 1$ ist. Es reicht, d so zu wählen, dass d nicht von 3 geteilt wird, etwa $d = 1$. Es gibt keine Zahlen $a, b \in \mathbb{N}$ mit

$$21 \cdot a = 15 \cdot b + 1,$$

denn dann wäre $3|(21 \cdot a - 15 \cdot b) = 1$, was ein Widerspruch ist.[1]

(b) In dieser Situation ist es *nicht* möglich, einen Fahrplan zu erstellen so, dass die angegebene Taktung (unfallfrei) eingehalten werden kann. In diesem Fall ist nämlich $\mathrm{ggT}(15, 22) = 1$, wir finden nach dem Satz von Bézout in der Fassung von Aufgabe 10.1 Zahlen $s, t \in \mathbb{N}$ mit $22 \cdot s - 15 \cdot t = 1$ (konkret findet man mit dem erweiterten euklidischen Algorithmus und Aufgabe 10.1 z.B. $s = 13$ und $t = 19$). Folglich gilt für jedes $d \in \mathbb{N}_0$

$$22 \cdot (d \cdot s) = 15 \cdot (t \cdot d) + d$$

so dass es eine Kollision des $(d \cdot s)$-ten Zugs der Linie 22 mit dem $(d \cdot t)$-ten Zug der Linie 15 gibt.

Aufgabe 10.3

Welche der folgenden Gleichungen sind lösbar? Geben Sie gegebenenfalls alle Lösungen an.

(a) $[140]_{555} \cdot x = [100]_{555}$,

(b) $[210]_{1100} \cdot x = [147]_{1100}$,

(c) $[21]_{80} \cdot x = [6]_{80}$,

(d) $[207]_{5814} \cdot x = [45]_{5814}$.

Lösung

(a) Hier ist $m = 555 = 3 \cdot 5 \cdot 37$ und $a = 140 = 2^2 \cdot 5 \cdot 7$, also $g := \mathrm{ggT}(m, a) = 5$. Es ist $g = 5$ ein Teiler von $b = 100$, also ist die Gleichung lösbar. Wegen $g = 5$ gibt es insgesamt 5 Lösungen.

Bestimmen einer Lösung: Setze $n := \frac{b}{g} = \frac{100}{5} = 20$. Mit dem erweiteren euklidischen Algorithmus erhält man

$$5 = (-1) \cdot 555 + 4 \cdot 140,$$

also $t = 4$ und damit die Lösung $x_0 := [n \cdot t]_{555} = [20 \cdot 4]_{555} = [80]_{555}$.

Bestimmen aller Lösungen: Man erhält die anderen 4 Lösungen durch sukzessives Addieren von $q := \frac{m}{g} = \frac{555}{5} = 111$:

$$x_1 = [191]_{555}, \quad x_2 = [302]_{555}, \quad x_3 = [413]_{555}, \quad x_4 = [524]_{555}.$$

(b) Hier ist $m = 1100 = 2^2 \cdot 5^2 \cdot 11$ und $a = 210 = 2 \cdot 3 \cdot 5 \cdot 7$, also $g := \mathrm{ggT}(m, a) = 10$. Es ist $g = 10$ keine Teiler von $b = 147$, also besitzt diese Gleichung keine Lösung.

(c) Hier ist $m = 80 = 2^4 \cdot 5$ und $a = 21 = 3 \cdot 7$, also $\mathrm{ggT}(m, a) = 1$ und somit die Gleichung eindeutig lösbar. Die Lösung ist

$$x = [21]_{80}^{-1} \otimes [6]_{80} = [-19]_{80} \otimes [6]_{80} = [-114]_{80} = [46]_{80}.$$

[1] Alternativ kann man die gegebene Gleichung umschreiben zu einer Gleichung in $\mathbb{Z}_{15}$, indem man auf beiden Seiten mod 15 rechnet, die Gleichung lautet dann $[6]_{15} \cdot x = [1]_{15}$, und diese Gleichung besitzt nach Vorlesung keine Lösung, da $\mathrm{ggT}(15, 6) = 3$ kein Teiler von 1 ist.

(d) Die Gleichung besitzt die Lösungen $x = [c]_{5814}$ mit

$$c \in \{253, 899, 1545, 2191, 2837, 3483, 4129, 4775, 5421\}.$$

Aufgabe 10.4

Beweisen Sie die fehlende Richtung vom Satz "*Gesamtheit Lösungen Restklassengleichung*" (Folie 191):

Sei $m \in \mathbb{N}$ ein fester Modulus, und seien $a, b \in \mathbb{Z}$ mit $g := \mathrm{ggT}(a, m)|b$. Es sei $x_0 = [c]_m$ eine Lösung der Gleichung

$$[a]_m \otimes x = [b]_m.$$

Dann ist jede Lösung von der Gestalt

$$x_j = [c + j \cdot q]_m$$

für ein $j \in \{0, \ldots, g-1\}$ mit $q := \frac{m}{g}$.

Lösung

Es sei $y = [d]_m$ eine Lösung der Gleichung, also gilt

$$[a \cdot d]_m = [b]_m \quad \text{und} \quad [a \cdot c]_m = [b]_m.$$

Subtrahieren dieser Identitäten liefert $a \cdot (d-c) \equiv_m 0$, also gibt es ein $k \in \mathbb{Z}$ mit $a \cdot (d-c) = k \cdot m$. Setze $p := \frac{a}{g}$, dann folgt

$$p \cdot g \cdot (d-c) = k \cdot q \cdot g, \quad \text{also} \quad p \cdot (d-c) = k \cdot q,$$

das heißt, $q|p \cdot (d-c)$. Nach Konstruktion sind p und q teilerfremd (denn $g = \mathrm{ggT}(p \cdot g, q \cdot g)$), also folgt $q|(d-c)$, es gibt also ein $\ell \in \mathbb{Z}$ mit $d - c = \ell \cdot q$, also $d = c + \ell \cdot q$. Setze schließlich $j := \ell \bmod g$, dann gilt $\ell = j + s \cdot g$, also

$$d = c + \ell \cdot q = c + j \cdot q + s \cdot g \cdot q = (c + j \cdot q) + s \cdot m \equiv_m c + j \cdot q,$$

also

$$y = [d]_m = [c + \ell \cdot q]_m = [c + j \cdot q]_m = x_j.$$

Aufgabe 10.5

Erstellen Sie ein Programm, das zu einer gegebenen modulo-Gleichung alle Lösungen ausgibt.