Aufgabe 7.1 (1 Pkt.)

Seien $a_1, \ldots, a_k$ ganze Zahlen. Beweisen Sie: Es gibt ganze Zahlen $x_1, \ldots, x_k$ mit $a_1x_1 + \ldots a_kx_k = \mathrm{ggT}(a_1, \ldots, a_k)$.

Aufgabe 7.2 (3 Pkt.)

Beweisen Sie: Der folgende iterative Algorithmus berechnet ein Tripel (g, x, y) mit $xa + yb = g = \mathrm{ggT}(a, b)$. (Es handelt sich also um eine Variante des erweiterten Euklidschen Algorithmus, die nur konstant viele Zahlen im Speicher hält.)

Algorithmus 1: ExtEuklidIterativ

Eingaben: ganze Zahlen a und b
Ergebnis: (g, x, y) mit $xa + yb = g = \mathrm{ggT}(a, b)$

$A \leftarrow \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$

// $A[i, j]$ bezeichnet Eintrag in Zeile i, Spalte j von A
while $A[2, 1] \neq 0$ **do**
  $c \leftarrow \lfloor A[1, 1] \,/\, A[2, 1] \rfloor$
  $A \leftarrow \begin{pmatrix} 0 & 1 \\ 1 & -c \end{pmatrix}$ A
return $A[1, :]$ *// Liefere erste Zeile von A als Ergebnis*

Tipp: Bezeichnen Sie den Eintrag in Zeile i, Spalte j von A nach k Durchläufen der While-Schleife mit $A_{i,j}(k)$ und beweisen Sie zunächst folgende Invariante für alle $k \geq 0$:

$$A_{1,1}(k) = A_{1,2}(k)\, a + A_{1,3}(k)\, b\,,$$
$$A_{2,1}(k) = A_{2,2}(k)\, a + A_{2,3}(k)\, b\,.$$

Aufgabe 7.3 (3 Pkt.)

Paul ist ratlos. Mit seiner Theatergruppe will er die Aula für eine Aufführung bestuhlen. Es sollen alle Stühle in gleichlangen Reihen aufgestellt werden. Beim Versuch, Reihen aus je 15 Stühlen aufzubauen, bleibt jedoch ein Stuhl übrig; bei 16er-Reihen sind es zwei Stühle zu wenig, und bei 17er-Reihen drei Stühle zu viel.

Wieviele Stühle stehen der Gruppe zur Verfügung? Geben Sie Ihren Lösungsweg an.

Aufgabe 7.4 (2+3 Pkt.)

Der Chinesische Restsatz liefert die Lösung zu Systemen von Kongruenzen $x \equiv b_i \pmod{m_i}$ mit paarweise teilerfremden m_i. Es lassen sich aber auch allgemeinere Systeme lösen!

a) Zeigen Sie: Die Kongruenz $ax \equiv b \pmod{m}$ mit $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$ besitzt genau dann eine Lösung $x \in \mathbb{Z}$, wenn b ein Vielfaches von $\mathrm{ggT}(a, m)$ ist. Die Kongruenz soll in eine äquivalente Kongruenz $x \equiv b' \pmod{m'}$ umgewandelt werden, die Lösungsmenge darf sich dabei nicht ändern. Wie können die Parameter b' und m' berechnet werden?

b) Gegeben sei das System von Kongruenzen

$$\left.\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \end{aligned}\right\}$$

mit $b_1, b_2 \in \mathbb{Z}$ und $m_1, m_2 \in \mathbb{N}$; m_1 und m_2 müssen nicht teilerfremd sein. Zeigen Sie: Ist das System lösbar, dann ist es äquivalent zu einer Kongruenz

$$x \equiv b \pmod{m} \quad \text{mit} \quad m \coloneqq \frac{m_1 m_2}{\mathrm{ggT}(m_1, m_2)}\,.$$

Wie kann b berechnet werden? Und wann besitzt das System keine Lösung?

Aufgabe 7.5 (4 Pkt.)

Lösen Sie die SPOX-Aufgabe „Verallgemeinerter Chinesischer Restsatz“.