Lösungen zu den Präsenzaufgaben in den Übungen

Diskrete Mathematik

WS 04/05

Blatt 6

Aufgabe 6.4

ACHTUNG: Die in der Mittwochs-Übung ausgegebene Aufgabe war so gestellt, dass Aufgabenteil a) und b) nicht zueinander passten. Hier deshalb eine leicht veränderte Variante:

a) Finde die kleinste ganze Zahl x, so dass gilt:

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 8 \pmod{11} \\ x &\equiv 1 \pmod{13} \end{aligned}$$

b) Berechne $237 \cdot 412 \pmod{715}$.

Lösung zu Teilaufgabe a)

Wir berechnen das gesuchte x in fünf Schritten nach dem *Schema zum Erfüllen simultaner Kongruenzen* (Chinesischer Restsatz; siehe dazu auch Material auf der Homepage).

a) *Bestimme* $M_i = \frac{m}{m_i}$ *für* $i = 1, \ldots, k$:

$$M_1 = \frac{715}{5} = 11 \cdot 13 = 143, \qquad M_2 = \frac{715}{11} = 5 \cdot 13 = 65, \qquad M_3 = \frac{715}{13} = 5 \cdot 11 = 55$$

b) *Bestimme* $M_i' = M_i \ (mod\ m_i)$ *für* $i = 1, \ldots, k$:

$$M_1' = 143 \equiv 3 \pmod 5, \qquad M_2' = 65 \equiv 10 \pmod{11}, \qquad M_3' = 55 \equiv 3 \pmod{13}$$

c) *Bestimme* x_i *mit* $x_i \cdot M_i' \equiv 1 \ (mod\ m_i)$ *für* $i = 1, \ldots, k$:

$$\begin{aligned} x_1 &= 7 \pmod 5, && (7 \cdot 3 \equiv 1 \pmod 5) \\ x_2 &= 10 \pmod{11}, && (10 \cdot 10 \equiv 1 \pmod{11}) \\ x_3 &= 9 \pmod{13} && (9 \cdot 3 \equiv 1 \pmod{13}) \end{aligned}$$

d) *Bestimme* $u_i = x_i \cdot M_i \ (mod\ m)$ *für* $i = 1, \ldots, k$:

$$u_1 = 7 \cdot 143 = 1001 \equiv 286 \pmod{715}, \qquad u_2 = 10 \cdot 65 = 650 \equiv 650 \pmod{715},$$
$$u_3 = 9 \cdot 55 = 495 \equiv 495 \pmod{715}$$

e) *Berechne* $x = \sum_{i=1}^{k} u_i b_i \ (mod\ m)$:

$$\begin{aligned} x &= 4 \cdot 286 + 8 \cdot 650 + 1 \cdot 495 \\ &= 1144 + 5200 + 495 \\ &\equiv 429 + 195 + 495 \qquad (\text{mod } 715) \\ &= 1119 \equiv 404 \qquad (\text{mod } 715) \end{aligned}$$

D.h. $x = 404$ löst die simultane Kongruenz:

$$404 \equiv 4 \pmod 5, \qquad 404 \equiv 8 \pmod{11}, \qquad 404 \equiv 1 \pmod{13}$$

Lösung zu Teilaufgabe b)

Wir nutzen zum Lösen der Aufgabe modulare Arithmethik. Da $715 = 5 \cdot 11 \cdot 13$ gilt:

$$\mathbb{Z}_{715} \cong \mathbb{Z}_5 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13} \quad .$$

Der Isomorphismus zwischen diesen beiden Restklassenringen ist gegeben durch:

$$\begin{aligned} h: \quad & \mathbb{Z}_{715} \longrightarrow \mathbb{Z}_5 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13} \\ & a \longmapsto (a \bmod 5, a \bmod 11, a \bmod 13) \end{aligned}$$

Wir können also einfach berechnen:

$$h(237 \cdot 412) = h(237) \cdot h(412) = (2, 6, 3) \cdot (2, 5, 9) = (4, 8, 1) \quad .$$

Um die Rechnung zu vervollständigen, benötigen wir das Bild von $(4, 8, 1)$ unter der Umkehrabbildung, d.h. $x = h^{-1}(4, 8, 1)$. Wir suchen also das Element $x \in \mathbb{Z}_{715}$ für das gilt $h(x) = (4, 8, 1)$, d.h.

$$x \equiv 4 \pmod 5, \qquad x \equiv 8 \pmod{11}, \qquad x \equiv 1 \pmod{13} \quad .$$

Nach Lösen der simultanen Kongruenz aus a) wissen wir $x = 404$. Damit gilt:

$$237 \cdot 412 \equiv 404 \pmod{715}$$