Diskrete Mathematik für Informatikstudien
Sommersemester 2022

4. Übungsblatt (29.3.2022)

Beispiel 4.1. Welche der folgenden Elemente von $\mathbb{Z}_{80}$ sind invertierbar? (Das Inverse eines Elementes $[a]_{80}$ ist ein Element $[b]_{80}$ mit $[a]_{80} \cdot [b]_{80} = [1]_{80}$.) Bestimmen Sie jeweils das Inverse oder begründen Sie, warum es nicht existiert.

$$[15]_{80}, \quad [33]_{80}, \quad [42]_{80} \quad \text{und} \quad [63]_{80}.$$

Stellen Sie das Inverse, falls es existiert, jeweils in der Form $[b]_{80}$ mit $b \in \{0, 1, \ldots, 79\}$ dar.

Beispiel 4.2. Eine österreichische IBAN (*international bank account number*) hat immer zwanzig Stellen und sieht folgendermaßen aus:

$$ATp_1p_2b_1b_2b_3b_4b_5k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11},$$

wobei $b_1b_2b_3b_4b_5$ die fünfstellige Bankleitzahl, $k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11}$ die (vorne um Nullen ergänzte) herkömmliche Kontonummer und p_1p_2 ein Prüfcode zwischen 02 und 98 ist, der so bestimmt wird, dass

$$b_1b_2b_3b_4b_5k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11}1029p_1p_2 \equiv 1 \bmod 97.$$

(Die Ziffern 1029 werden verwendet, um den Ländercode AT zu codieren: Dabei addiert man 9 zur Stelle der Buchstaben im Alphabet, also $A \to 1 + 9 = 10$ und $T \to 20 + 9 = 29$.)

Zeigen Sie, dass die Zahl

$$\begin{aligned} Z = 79 &- 46b_1 - 24b_2 + 17b_3 - 8b_4 + 38b_5 - 35k_1 + 45k_2 - 44k_3 + 15k_4 \\ &- 47k_5 + 5k_6 - 48k_7 + 34k_8 - 16k_9 - 21k_{10} + 27k_{11} + 10p_1 + p_2 \end{aligned}$$

durch 97 teilbar ist und berechnen Sie mit Hilfe dieser Tatsache die IBAN[1] für die Bankleitzahl 29322 und die Kontonummer 31415926

Beispiel 4.3. Ermitteln Sie für die folgenden Gleichungen jeweils alle ganzzahligen Lösungen oder begründen Sie, warum es keine ganzzahligen Lösungen gibt.

(a) $168x + 228y = 2022$;

(b) $42x + 161y = 504$.

Beispiel 4.4. Bestimmen Sie für die folgenden simultanen Kongruenzen jeweils alle Lösungen oder begründen Sie, warum es keine Lösungen gibt.

(a)
$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 4 \bmod 5 \\ x &\equiv 1 \bmod 7 \\ x &\equiv 3 \bmod 8 \end{aligned}$$

(b)
$$\begin{aligned} x &\equiv 1 \bmod 3 \\ x &\equiv 3 \bmod 4 \\ x &\equiv 7 \bmod 8 \\ x &\equiv 7 \bmod 9 \end{aligned}$$

---

[1] Bitte kein Geld überweisen! Es ist nicht das Konto einer uns bekannten Person und verbessert nicht die Note.

Beispiel 4.5. Ermitteln Sie für die folgenden simultanen Kongruenzen jeweils alle Lösungen oder begründen Sie, warum es keine Lösungen gibt.

(a)
$$x \equiv 13 \bmod 28$$
$$x \equiv 3 \bmod 36$$
$$x \equiv 48 \bmod 63$$

(b)
$$x \equiv 6 \bmod 28$$
$$x \equiv 22 \bmod 36$$
$$x \equiv 13 \bmod 63$$

Hinweis. Finden Sie zuerst Zahlen m_1, m_2, m_3, die relativ prim sind (also $\mathrm{ggT}(m_i, m_j) = 1$ wann immer $i \neq j$) und $28 = m_1 m_2$, $36 = m_1 m_3$ und $63 = m_2 m_3$ erfüllen. Übersetzen Sie dann, falls möglich, die Kongruenzen aus der Aufgabe in die Form

$$x \equiv c_1 \bmod m_1$$
$$x \equiv c_2 \bmod m_2$$
$$x \equiv c_3 \bmod m_3$$

und lösen Sie diese mit Hilfe des chinesischen Restsatzes.