Aufgabe 28. Die maschinelle Verifikation einer IBAN erfordert Rechnungen mit 30bit INT. Auf eingeschränkter Hardware, die diese Operationen nicht beherrscht, kann die Überprüfung schrittweise wie folgt durchgeführt werden:

1. Zerlege die Zahl $N = b_1b_2b_3b_4b_5k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11}1029p_1p_2$ in drei Teile $b_1b_2b_3b_4b_5k_1k_2k_3k_4$, $k_5k_6k_7k_8k_9k_{10}k_{11}$, $1029p_1p_2$ (9+7+6 Ziffern).
2. Nehme die ersten 9 Stellen $N_1 = b_1b_2b_3b_4b_5k_1k_2k_3k_4$.
3. Berechne den Rest $r_1r_2 \equiv N_1 \mod 97$.
4. Füge diese beiden Ziffern zu den nächsten 7 Stellen hinzu und bilde die Zahl $N_2 = r_1r_2k_5k_6k_7k_8k_9k_{10}k_{11}$
5. Berechne den Rest $r_3r_4 \equiv N_2 \mod 97$.
6. Füge diese beiden Ziffern zu den verbleibenden Stellen hinzu und bilde die Zahl $N_3 = r_3r_41029p_1p_2$.
7. Der Rest $N_3 \mod 97$ muß 1 ergeben.

(a) Überprüfe die IBAN aus Aufgabe 27 mit dieser Methode.
(b) Zeige, daß der Algorithmus wirklich das gleiche Ergebnis liefert wie die Division der kompletten IBAN modulo 97.

Aufgabe 29. Zeige, daß eine IBAN ungültig wird, wenn

(a) eine Ziffer falsch eingegeben wird.
(b) zwei benachbarte Ziffern vertauscht werden.

Aufgabe 30. Finde, wenn möglich, die folgenden multiplikativen Inversen:

(a) $[5]_{173}^{-1}$ (b) $[14]_{93}^{-1}$
(c) $[51]_{85}^{-1}$ (d) $[15]_{93}^{-1}$

Aufgabe 31. Löse, wenn möglich, das Gleichungssystem

$$\begin{aligned} 3\,x + y &= 4 \\ 2\,x + 3\,y &= 3 \end{aligned}$$

(a) in $\mathbb{Z}_5$ (b) in $\mathbb{Z}_7$

Aufgabe 32. Finde alle Lösungen $x \in \mathbb{Z}$, der folgenden Gleichungen.

(a) $6\,x \equiv 3 \mod 9$
(b) $6\,x \equiv 4 \mod 9$
(c) $4\,x \equiv 2 \mod 7$
(d) $4\,x \equiv 6 \mod 9$

Aufgabe 33. Löse das folgende Kongruenzgleichungssystem mithilfe des chinesischen Restsatzes.

$$\begin{aligned} x &\equiv 3 \mod 9 \\ x &\equiv 2 \mod 10 \\ x &\equiv 1 \mod 11 \end{aligned}$$