Einführung i. d. Kryptographie - Übung 5

Philip Magnus

2024-12-03

Aufgabe 1

Lösen Sie das folgende System simultaner Kongruenzen:

$$\begin{aligned} x &\equiv 3 \mod 7 \\ x &\equiv 8 \mod 9 \\ x &\equiv 2 \mod 13 \end{aligned}$$

Weil $ggT(7,9) = ggT(7,13) = ggT(9,13) = 1$, wissen wir laut chinesischem Restsatz, dass die simultane Kongruenz eine Lösung hat. Für die Lösung x' wissen wir weiters, dass jedes Element aus der Restklasse $x' + (7 \cdot 9 \cdot 19)\mathbb{Z}$ auch die simultane Kongruenz erfüllt.

Wir verwenden den Gauß Algorithmus um die Kongruenz zu lösen:

1. Wir definieren

$$\begin{aligned} M_1 &:= \frac{7 \cdot 9 \cdot 13}{7} = 9 \cdot 13 = \mathbf{117} \\ M_2 &:= \frac{7 \cdot 9 \cdot 13}{9} = 7 \cdot 13 = \mathbf{91} \\ M_3 &:= \frac{7 \cdot 9 \cdot 13}{13} = 7 \cdot 9 = \mathbf{63} \end{aligned}$$

2. Zu jedem M_i berechnen wir $y_i = M_i^{-1} \mod m_i$ mittels Euler-Algorithmus:

$$\begin{aligned} y_1 &= 117^{-1} \mod 7 = 5^{-1} \mod 7 = \mathbf{3} \\ y_2 &= 91^{-1} \mod 9 = 1^{-1} \mod 9 = \mathbf{1} \\ y_3 &= 63^{-1} \mod 13 = 11^{-1} \mod 13 = \mathbf{6} \end{aligned}$$

a) Statt 117^{-1} berechnen wir zuerst, in welche Restklasse bzgl. 7 117 fällt, nämlich 5. Darum wissen wir $117^{-1} = 5^{-1}$.

Euler:

$$\begin{aligned} 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

und $5^{-1} = 3$ weil

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = \\ &= 5 - 2 \cdot (7 - 5) = \\ &= 5 - 2 \cdot 7 + 2 \cdot 5 = \\ &= \mathbf{3} \cdot 5 - 2 \cdot 7. \end{aligned}$$

b) Die Restklasse von $91 = (10 \cdot 9 + 1)$ modulo 9 ist 1, daher $1^{-1} \mod 9 = 1$.

c) Die Restklasse von 63 mod 13 ist 11. Wir rechnen mittels Euklid

$$\begin{aligned} 13 &= 1 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1 \end{aligned}$$

Und $11^{-1} \mod 13 = 6 \mod 13$ weil

$$\begin{aligned} 1 &= 11 - 5 \cdot 2 = \\ &= 11 - 5 \cdot (13 - 11) = \\ &= 11 - 5 \cdot 13 + 5 \cdot 11 = \\ &= \mathbf{6} \cdot 11 - 5 \cdot 13 \end{aligned}$$

3. Jetzt können wir berechnen

$$\begin{aligned} x &= \left(\sum a_i y_i M_i\right) \mod \prod m_i = \\ &= (3 \cdot 3 \cdot 117 + 8 \cdot 1 \cdot 91 + 2 \cdot 6 \cdot 63) \mod 7 \cdot 9 \cdot 13 = \\ &= 2537 \mod 819 = \\ &= 80 \mod 819 \end{aligned}$$

Wir haben $x = 80$, bzw. jedes Element aus $80 + 819\mathbb{Z}$ ist eine Lösung der Kongruenzen.

Aufgabe 2

Berechnen Sie die folgenden Potenzen in $(\mathbb{Z}/37\mathbb{Z})^*$:

(a) 2^{33}

Binärdarstellung: $33 = 2^0 + 2^5$, daher berechnen wir $2^{33} = 2^{2^0+2^5}$

$$\begin{aligned} 2^{2^0} &= 2 = 2 \mod 37 \\ 2^{2^1} &= 2 \cdot 2 = 4 \mod 37 \\ 2^{2^2} &= 4 \cdot 4 = 16 \mod 37 \\ 2^{2^3} &= 16 \cdot 16 = 34 \mod 37 \\ 2^{2^4} &= 34 \cdot 34 = 9 \mod 37 \\ 2^{2^5} &= 9 \cdot 9 = 7 \mod 37 \end{aligned}$$

Darum gilt $2^{33} = 2^{2^0+2^5} = 2^{2^0} \cdot 2^{2^5} = 2 \cdot 7 = 14$.

(b) 10^{33}

$$
\begin{aligned}
10^{2^0} &= 10 = 10 \mod 37 \\
10^{2^1} &= 10^2 = 26 \mod 37 \\
10^{2^2} &= 26^2 = 10 \mod 37 \\
10^{2^3} &= 10^2 = 26 \mod 37 \\
10^{2^4} &= 26^2 = 10 \mod 37 \\
10^{2^5} &= 10^2 = 26 \mod 37
\end{aligned}
$$

Darum gilt $10^{33} = 10 \cdot 26 = 1$.

(c) 16^{33}

$$
\begin{aligned}
16^{2^0} &= 16 = 16 \mod 37 \\
16^{2^1} &= 16^2 = 34 \mod 37 \\
16^{2^2} &= 34^2 = 9 \mod 37 \\
16^{2^3} &= 9^2 = 7 \mod 37 \\
16^{2^4} &= 7^2 = 12 \mod 37 \\
16^{2^5} &= 12^2 = 33 \mod 37
\end{aligned}
$$

Darum gilt $16^{33} = 16 \cdot 33 \mod 37 = 10$.

Aufgabe 3

Die folgende lineare Outputfolge wurde von einem Schieberegister der Länge 5 erzeugt. Rekonstruieren Sie das Schieberegister.

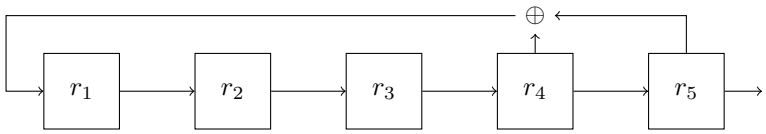
```
> 0000100011   # Outputfolge
```

Weil die ersten 5 bits `00001` sind, ist unsere Anfangsbelegung der Register `10000`. (Die Outputbits sind "gespiegelt" in den Registern, d.h. das 1. Zeichen das ausgegeben wird ist im 5. Register). Die Bits die nachgeschoben werden sind `00011`. Damit wissen wir die Belegung vom Register r_5 zu allen Zeitpunkte t_0 bis t_9, für r_4 wissen wir die Belegung von t_0 bis t_8, etc.

t	r_1	r_2	r_3	r_4	r_5	out
t_0	1	0	0	0	0	-
t_1	0	1	0	0	0	0
t_2	0	0	1	0	0	0
t_3	0	0	0	1	0	0
t_4	1	0	0	0	1	0
t_5	1	1	0	0	0	1
t_6	*	1	1	0	0	0
t_7	*	*	1	1	0	0
t_8	*	*	*	1	1	0
t_9	*	*	*	*	1	1
t_{10}	*	*	*	*	*	1

Weil in Zeitpunkt t_1 das Bit `0` in r_1 nachgeschoben wird, kann r_1 selbt nicht Teil der XOR Verknüpfung sein. Analog gilt dasselbe für Register r_2 und r_3.

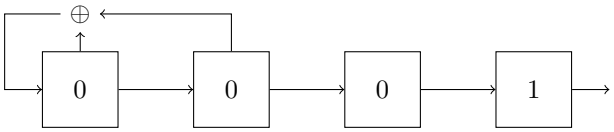
Wir vermuten, dass die lineare Rückkoppelung aus $r_4 \oplus r_5$ entsteht, was mit den Werten zu Zeitpunkten t_4 und t_5 in Einklang steht.



Aufgabe 4

(a) Konstruieren Sie ein lineares Schieberegister der Länge 4, das einen Nicht-Null-Zustand in den Null-Zustand überführt

Hier wird der Zustand `0001` im nächsten Schritt zu `0000`:



(b) Konstruieren Sie ein lineares Schieberegister der Länge 4, das den Null-Zustand in einen Nicht-Null-Zustand überführt

Weil die lineare Rückkoppelung ein XOR verwendet, kann eine 0-Belegung nicht in eine Nicht-0-Belegung überführt werden ($0 \oplus 0 = 0$).