FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
25.10.2023

Musterlösung zum 4. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Mit $\gcd(a,b) = \gcd(b, a \bmod b)$, $b \neq 0$ erhält man:

$\gcd(282, 252)$

r_0	282
r_1	252
r_2	$282 \bmod 252 = 30$
r_3	$252 \bmod 30 = 12$
r_4	$30 \bmod 12 = 6$
r_5	$12 \bmod 6 = 0$

$\gcd(87, 20)$

r_0	87
r_1	20
r_2	$87 \bmod 20 = 7$
r_3	$20 \bmod 7 = 6$
r_4	$7 \bmod 6 = 1$
r_5	$6 \bmod 1 = 0$

$\gcd(122354, 267371)$

r_0	122354
r_1	267371
r_2	$122354 \bmod 267371 = 122354$
r_3	$267371 \bmod 122354 = 22663$
r_4	$122354 \bmod 22663 = 9039$
r_5	$22663 \bmod 9039 = 4585$
r_6	$9039 \bmod 4585 = 4454$
r_7	$4585 \bmod 4454 = 131$
r_8	$4454 \bmod 131 = 0$

$\Rightarrow \gcd(282, 252) = 6,\ \gcd(87, 20) = 1,\ \gcd(122354, 267371) = 131.$

Übung 2

a) Gesucht ist x mit $25 \cdot x = 1 \bmod 61$

k	r_k	q_k	x_k
0	61		0
1	25		1
2	11	2	-2
3	3	2	5
4	2	3	-17
5	1	1	22

$\Rightarrow \gcd(25, 61) = 1$, und die Lösung, also das modulare Inverse, kann man ablesen als $x = (25)^{-1} = 22$.

b) Es ist $\gcd(14, 45) = 1 \Rightarrow 14 \cdot x = 1 \bmod 45$ hat eine Lösung, d.h., 14 besitzt ein Inverses $\bmod 45$.
Es ist $\gcd(20, 45) = 5 \Rightarrow 20 \cdot x = 1 \bmod 45$ ist nicht lösbar, d.h., 20 besitzt kein Inverses $\bmod 45$.

c)

$$
\begin{aligned}
& a \in \mathbb{Z}_m \text{ besitzt ein Inverses} \\
\Leftrightarrow\ & \text{die Gleichung } a \cdot x = 1 \bmod m \text{ ist lösbar} \\
\Leftrightarrow\ & \gcd(a, m) | 1 \\
\Leftrightarrow\ & \gcd(a, m) \ = \ 1.
\end{aligned}
$$

d) Wenn m eine Primzahl ist, so gilt für alle $a \in \mathbb{Z}_m \setminus \{0\}$: $\gcd(a, m) = 1$, also hat nach c) jedes $a \in \mathbb{Z}_m \setminus \{0\}$ ein Inverses in $\mathbb{Z}_m$.
Mit der Assoziativität und 1 als neutralem Elements folgt, dass $\mathbb{Z}_m \setminus \{0\}$ eine Gruppe ist.

Übung 3

a) Wie bei Übung 2a) schon mit Hilfe des euklidischen Algorithmus bestimmt, existiert $(25)^{-1} = 22 \ (\bmod 61)$. Also ist

$$25 \cdot x = 13 \bmod 61$$

lösbar mit $x \ = \ 22 \cdot 13 \bmod 61 \ = \ 42$.

b) $252 \cdot x = 48 \bmod 282$

k	r_k	q_k	x_k
0	282		0
1	252		1
2	30	1	-1
3	12	8	9
4	6	2	-19

$\Rightarrow \ \gcd(252, 282) = 6.$

Wegen $6|48$ ist die Gleichung lösbar mit $x \ = \ \frac{48}{6} \cdot (-19) \bmod 282 \ = \ 130$.

c) $9 \cdot x = 13 \bmod 25$

k	r_k	q_k	x_k
0	25		0
1	9		1
2	7	2	-2
3	2	1	3
4	1	3	-11

$\Rightarrow \ \gcd(9, 25) = 1$ und $9^{-1} = -11 = 14 \bmod 25.$

Die Gleichung ist also lösbar mit $x \ = \ 14 \cdot 13 \bmod 25 \ = \ 7$.

d) $24 \cdot x = 9 \bmod 42$

k	r_k	q_k	x_k
0	42		0
1	24		1
2	18	1	-1
3	6	1	2

$\Rightarrow$ $\gcd(24, 42) = 6$.

Wegen $6 \nmid 9$ ist die Gleichung unlösbar.

Bei a) und c) wird zunächst das multiplikative Inverse berechnet.

Übung 4

Beh.: b kann beliebig sein und es muss $\gcd(26, a) = 1$ gelten.

Beweis:

1. Ist $\gcd(26, a) = 1$, so existiert ein multiplikatives Inverses a^{-1}. Damit gilt:

$$\begin{aligned} & a \cdot k + b && = a \cdot k' + b && \bmod 26 \\ \Rightarrow\ & a \cdot k && = a \cdot k' && \bmod 26 \\ \Rightarrow\ & a^{-1} \cdot a \cdot k && = a^{-1} \cdot a \cdot k' && \bmod 26 \\ \Rightarrow\ & k && = k' && \bmod 26, \end{aligned}$$

   d.h., für verschiedene k und k' sind auch die Geheimtextbuchstaben verschieden.

2. Ist $\gcd(26, a) = d \neq 1$, so gilt für $k = \frac{26}{d} \neq 0$, dass $a \cdot k = 0 \bmod 26$, also

$$a \cdot k + b \ = \ b \ = \ a \cdot 0 + b \bmod 26$$

   gilt, d.h., k und 0 besitzen den gleichen Geheimtextbuchstaben.