Einführung i. d. Kryptopgraphie - Übung 3

01.11.2024

Aufgabe 1

Finden Sie jeweils die Zahl x mittels des erweiterten euklidischen Algorithmus.

Zu lösen gilt die Gleichungsform $a \cdot x + b \cdot y = n$, hierfür muss $gcd(a, b)$ ein Teiler von n sein.

1.1

$7 \cdot x \equiv 1 \mod 29$

$$29 = 4 \cdot 7 + 1$$
$$7 = 7 \cdot 1 + 0$$

Daraus folgt $1 = 29 - 4 \cdot 7$ wenn wir hierauf mod 29 anwenden, ergibt sich $7 \cdot -4 \equiv 1 \mod 29$.

1.2

$18 \cdot x \equiv 1 \mod 47$

$$47 = 18 \cdot 2 + 11 \quad (1)$$
$$18 = 11 \cdot 1 + 7 \quad (2)$$
$$11 = 7 \cdot 1 + 4 \quad (3)$$
$$7 = 4 \cdot 1 + 3 \quad (4)$$
$$4 = 3 \cdot 1 + 1 \quad (5)$$
$$3 = 1 \cdot 3 + 0 \quad (6)$$

Erweiterter euklidischer Algorithmus:

$$\begin{aligned}
1 &\overset{(5)}{=} 4 - 3 \cdot 1 \\
&\overset{(4)}{=} 4 - (7 - 4) = 4 - 7 + 4 = 2 \cdot 4 - 7 \\
&\overset{(3)}{=} 2 \cdot (11 - 7) - 7 = 2 \cdot 11 - 2 \cdot 7 - 7 = 2 \cdot 11 - 3 \cdot 7 \\
&\overset{(2)}{=} 2 \cdot 11 - 3 \cdot (18 - 11) = 2 \cdot 11 - 3 \cdot 18 + 3 \cdot 11 = 5 \cdot 11 - 3 \cdot 18 \\
&\overset{(1)}{=} 5 \cdot (47 - 2 \cdot 18) - 3 \cdot 18 = 5 \cdot 47 - 10 \cdot 18 - 3 \cdot 18 = 5 \cdot 47 - 13 \cdot 18
\end{aligned}$$

Daher ergibt sich $18 \cdot -13 \equiv 1 \mod 47$.

1.3

$9 \cdot x \equiv 1 \mod 63$

Da $gcd(9, 63) = 9$ und $9 \nmid 1$, gibt es keine Lösung.
siehe Folien S. 29

Aufgabe 2

Finden Sie 3 verschiedene ganze Zahlen $a_i, i = 1, 2, 3$, die folgendes erfüllen:

$$\begin{aligned} a_i &\mod 3 = 1 \\ a_i &\mod 4 = 1 \\ a_i &\mod 6 = 1 \end{aligned}$$

Weil $12 = \text{kgV}(3, 4, 6)$, gilt, dass alle Elemente aus $\{k \cdot 12 + 1 : k \in \mathbb{Z}\}$ die drei Gleichungen erfüllen. Beispiellösung: $a_1 = 1, a_2 = 13, a_3 = 25$.

Aufgabe 3

Bestimmen Sie die Anzahl aller Elemente in $(\mathbb{Z}/30\mathbb{Z})*$.

Primfaktorzerlegung: $30 = 2 \cdot 3 \cdot 5$, dann $\varphi(30) = 30(1 - 1/2)(1 - 1/3)(1 - 1/5) = 8$.

Es wird $(\mathbb{Z}/30\mathbb{Z})*$ eine *prime Restklassengruppe* genannt.
Zuerst überlegen wir uns, dass $\{0 + 30\mathbb{Z}, 1 + 30\mathbb{Z}, \ldots, 29 + 30\mathbb{Z}\} = \mathbb{Z}/30\mathbb{Z}$ der Restklassenring mod 30 ist. (Folien S. 40)

Die Menge aller invertierbaren Restklassen aus $\mathbb{Z}/30\mathbb{Z}$ ergibt die prime Restklassengruppe. (Folien S. 46 + externe Quellen, es steht nicht in den Folien).

Sei $n = \prod_i p_i^{e_i}$ die Primfaktorzerlegung der Zahl n. Mit der eulerschen φ-Funktion (Folien S. 49)

$$\varphi(n) = n \prod_i (1 - \frac{1}{p_i})$$

können wir die Anzahl der Elemente in $(\mathbb{Z}/30\mathbb{Z})*$ bestimmen.

Wir wissen $30 = 2 \cdot 3 \cdot 5$. Daher gilt $\varphi(30) = 30(1 - 1/2)(1 - 1/3)(1 - 1/5) = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$.

Aufgabe 4

a) Ist $G = (X, \circ) = (\{1, 2, 3, 4, 5, 6, 7\}, *_8)$ mit $*_8 : (a, b) \mapsto (a \cdot b) \mod 8$ eine Halbgruppe, eine Gruppe oder nichts von alledem?

In der folgenden Tabelle bzgl. $*_8$ sehen wir alle Ergebnisse der Verknüpfung:

$*_8$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	2	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Obwohl $2, 4 \in X$ haben wir für das Ergebnis $2 *_8 4 = 0 \notin X$, d.h. wir haben keine innere Verknüpfung / die Verknüpfung ist nicht abgeschlossen bzgl. X. Deswegen haben wir weder eine Halbgruppe noch oder eine Gruppe. Es gibt mehrere Ansätze, damit $*_8$ abgeschlossen wird bezüglich X:

Ansatz 1: Wäre $X = \{0, 1, 2, 3, 4, 5, 6, 7\}$, wäre G eine Halbgruppe, weil die Assoziativität gegeben ist:

$$a *_8 (b *_8 c) = (a \cdot b \mod 8) \cdot c \mod 8 = a \cdot (b \cdot c \mod 8) \mod 8 = (a *_8 b) \cdot_8 c$$

$*_8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	2	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Ansatz 2: Wir entfernen die Restklasse 4 (weil 0 nicht in X ist) und in weiterer Folge auch 2 und 6 (weil diese die Restklassen 4 erzeugen). Dann haben wir $X = \{1, 3, 5, 7\}$:

$*_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Auch hier haben wir **Assoziativität** aber auch **das neutrale Element** (1) und **inverse Elemente** (hier sogar: für alle a gilt $a *_8 a = 1$). Mit dieser Teilmenge und $*_8$ haben wir eine Gruppe.

b) Falls es sich um keine Gruppe handelt, modifizieren Sie X entsprechend, um eine Gruppe zu erhalten.

Wir können die Restklassen 2, 4, 6 nicht behalten, weil diese nicht invertierbar sind.

Es gibt folgende Optionen für X

1. $X = \{1, 3, 5, 7\}$
2. $X = \{1\}$
3. $X = \{1, 3\}$
4. $X = \{1, 5\}$
5. $X = \{1, 7\}$

wobei Option 1 die prime Restklassengruppe $(\mathbb{Z}/8\mathbb{Z})^*$ ergibt.