

Einführung i. d. Kryptographie - 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

$$7 \cdot x \equiv 1 \pmod{29}$$

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

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

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

1.2

$$18 \cdot x \equiv 1 \pmod{47}$$

$$47 = 18 \cdot 2 + 11$$

$$18 = 11 \cdot 1 + 7$$

$$11 = 7 \cdot 1 + 4$$

$$7 = 4 \cdot 1 + 3$$

$$4 = 3 \cdot 1 + 1$$

$$3 = 1 \cdot 3 + 0$$

Erweiterter euklidischer Algorithmus:

$$1 \stackrel{(5)}{=} 4 - 3 \cdot 1$$

$$\stackrel{(4)}{=} 4 - (7 - 4) = 4 - 7 + 4 = 2 \cdot 4 - 7$$

$$\stackrel{(3)}{=} 2 \cdot (11 - 7) - 7 = 2 \cdot 11 - 2 \cdot 7 - 7 = 2 \cdot 11 - 3 \cdot 7$$

$$\stackrel{(2)}{=} 2 \cdot 11 - 3 \cdot (18 - 11) = 2 \cdot 11 - 3 \cdot 18 + 3 \cdot 11 = 5 \cdot 11 - 3 \cdot 18$$

$$\stackrel{(1)}{=} 5 \cdot (47 - 2 \cdot 18) - 3 \cdot 18 = 5 \cdot 47 - 10 \cdot 18 - 3 \cdot 18 = 5 \cdot 47 - 13 \cdot 18$$

Daher ergibt sich $18 \cdot -13 \equiv 1 \pmod{47}$.

1.3

$$9 \cdot x \equiv 1 \pmod{63}$$

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:

$$a_i \pmod{3} = 1$$

$$a_i \pmod{4} = 1$$

$$a_i \pmod{6} = 1$$

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 $\{0 + 30\mathbb{Z}, 1 + 30\mathbb{Z}, \dots, 29 + 30\mathbb{Z}\} = \mathbb{Z}/30\mathbb{Z}$ 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)

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

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 $*_8 : (a, b) \mapsto (a \cdot b) \pmod{8}$ eine Halbgruppe, eine Gruppe oder nichts von alledem?

Weil $2 *_8 4 = 0 \notin X$, ist $*_8$ keine innere Verknüpfung und somit weder Halbgruppe noch Gruppe.

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

$$a *_8 (b *_8 c) = (a \cdot b \pmod{8}) \cdot c \pmod{8} = a \cdot (b \cdot c \pmod{8}) \pmod{8} = (a *_8 b) *_8 c$$

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

Wenn wir X so modifizieren, dass G eine Gruppe ist, erhalten wir die prime Restklassengruppe $(\mathbb{Z}/8\mathbb{Z})^*$:
 $X = \{1, 3, 5, 7\}$.

(Eine weitere Möglichkeit wäre auch $X = \{1\}, X = \{1, 3\}, \dots$)

Jetzt haben wir $1 \in X$, d.h. es gibt das neutrale Element.

Für jedes Element $x \in X$ haben wir ein inverses Element:

- $1 * 1 = 1$
- $3 * 3 = 1$
- $5 * 5 = 1$
- $7 * 7 = 1$