Einführung i. d. Kryptopgraphie - Übung 4

12.11.2024

Aufgabe 1

Zeigen Sie das $11^{49} + 4^{49}$ durch 15 teilbar ist (ohne Taschenrechner).

$\varphi(15) = 8$, wir wissen also, dass alle Exponenten die ein Vielfaches von 8 sind in der Modulo Division 1 ergeben. Sie bilden ein Multiplikatives Inverses.

$$\begin{aligned} 11 &\equiv -4 \mod 15 \\ 11^{49} + 4^{49} &\mod 15 = 0 \\ = 11^{48} \cdot 11 + 4^{48} \cdot 4 &\mod 15 = 0 \\ = 11 + 4 &\mod 15 = 0 \\ = -4 + 4 &\mod 15 = 0 \\ = 0 &\mod 15 = 0 \end{aligned}$$

$$11^{49} + 4^{49} \equiv \left(\underbrace{11^{\varphi(15)}}_{\equiv 1}\right)^6 \cdot 11 + \left(\underbrace{4^{\varphi(15)}}_{\equiv 1}\right)^6 \cdot 4 \equiv 11 + 4 \equiv 0 \mod 15$$

Aufgabe 2

Zeigen Sie an einem Beispiel, dass die Kürzungsregel in der Halbgruppe $(Z/mZ, \cdot)$ im allgemeinen nicht gilt

$$\begin{aligned} a \cdot b &= a \cdot c \\ b \cdot a &= c \cdot a \\ a^{-1} \cdot a \cdot b &= a^{-1} \cdot a \cdot c \\ = e \cdot b &= e \cdot c \end{aligned}$$

Dies impliziert jeweils $b = c$.

$$\begin{aligned} ab &= ac \\ &= ab - ac = 0 \\ &= a(b - c) = 0 \end{aligned}$$

Beispiel $(Z/10Z, \cdot)$:

Es Reicht ein Gegenbeispiel um zu zeigen, dass die Kürzungsregel nicht allgemein gilt.

$$0 \equiv 2 \cdot 0 \equiv 2 \cdot 5 \equiv 0 \mod 10$$

Weitere Beispiele:

a	b	c
2	2	7
2	3	8
2	4	9
⋮	⋮	⋮

Aufgabe 3

Bestimmen Sie die Ordnung aller Elemente in:

a. $(\mathbb{Z}/12\mathbb{Z})^*$
b. $(\mathbb{Z}/13\mathbb{Z})^*$
c. $(\mathbb{Z}/14\mathbb{Z})^+$

3.a

$(\mathbb{Z}/12\mathbb{Z})^* = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

	a^1	a^2	a^3	a^4
1	1	1	1	1
5	5	$25 \equiv 1 \mod 12$	5	1
7	7	$49 \equiv 1 \mod 12$	7	1
11	11	$121 \equiv 1 \mod 12$	11	1

Diese Gruppe hat keine Generatoren, jedes Element hat die Ordnung ≤ 2.

3.b

$(\mathbb{Z}/13\mathbb{Z})^* = \{\bar{1}, \bar{2}, \cdots, \bar{12}\}$

	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
2	2	4	8	3	6	12	11	9	5	10	7	1
3	3	9	1	...								
4	4	3	12	9	10	1	⋯					
5	5	12	8	1	⋯							
6	6	10	8	9	2	12	7	3	5	4	11	1
7	7	10	5	9	11	12	6	3	8	4	2	1
8	8	12	5	1	⋯							
9	9	3	1	⋯								
10	10	9	12	3	4	1	⋯					
11	11	4	5	3	7	12	2	9	8	10	6	1
12	12	1	⋯									

Hier sind die Generatoren $\{\bar{2}, \bar{6}, \bar{7}, \bar{11}\}$.

3.c

$(\mathbb{Z}/14\mathbb{Z})^+ = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}\}$

0	a	$2a$	$3a$	$4a$	$5a$	6	$7a$	$8a$	$9a$	$10a$	$11a$	$12a$	$13a$
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	2	4	6	8	10	12	0	$\cdots$					
0	3	6	9	12	1	4	7	10	13	2	5	8	11
0	4	8	12	2	6	10	0	$\cdots$					
0	5	10	1	6	11	2	7	12	3	8	13	4	9
0	6	12	4	10	2	8	0	$\cdots$					
0	7	0	$\cdots$										
0	8	2	10	4	12	6	0	$\cdots$					
0	9	4	13	8	3	12	7	2	11	6	1	10	5
0	10	6		2	12	8	4	0	$\cdots$				
0	11	8	5	2	13	10	7	4	1	12	9	6	3
0	12	10	8	6	4	2	0	$\cdots$					
0	13	12	11	10	9	8	7	6	5	4	3	2	1

Hier sind die Generatoren $\{\bar{1}, \bar{3}, \bar{5}, \bar{9}, \bar{11}, \bar{13}\}$.

Aufgabe 4

Bestimmen Sie die Zahl $a (0 \leq a \leq 22)$ sodass gilt $10^{65} \equiv a \mod 23$.

Wir berechnen $10^{65} \mod 23$ mit der Methode zur schnellen Berechnung von Potenzen in einem Monoid (Folien S. 55).

Es gilt $65_{10} = 1000001_2 = 2^0 + 2^6$.

D.h. $10^{65} = 10^{(2^0+2^6)} = 10^{2^0} \cdot 10^{2^6}$

k	10^{2^k}	$10^{2^{(k-1)}}$	mod 23
0	10^{2^0}	10	10
1	10^{2^1}	$10^2 = 100$	8
2	10^{2^2}	$8^2 = 64$	18
3	10^{2^3}	$18^2 = 324$	2
4	10^{2^4}	$2^2 = 4$	4
5	10^{2^5}	$4^2 = 16$	16
6	10^{2^6}	$16^2 = 256$	3

Daher wissen wir

$$\begin{aligned}(10^{65} \mod 23) &= (10^{2^0} \cdot 10^{2^6}) \mod 23 = \\ &= (10^{2^0} \mod 23) \cdot (10^{2^6} \mod 23) = \\ &= 10 \cdot 3 = \\ &= 30 \equiv 7 \mod 23\end{aligned}$$