Diskrete Mathematik - Übungen SW10

David Jäggli

5. Mai 2023

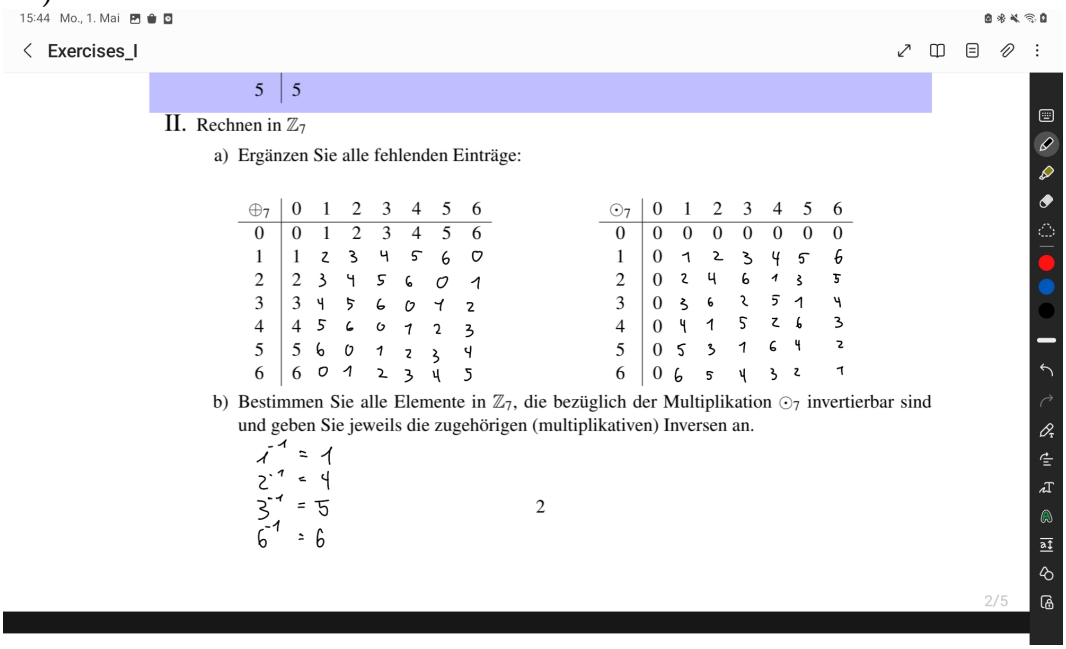
Inhaltsverzeichnis

1 Einführung in die Zahlentheorie II

I.)

$$3 \odot_9 (2 \oplus_9 5) = 3 + (7 \mod 9) \mod 9 = 3$$
$$3 \odot_1 02 \oplus_9 8 = (3 + 2 \mod 10) + 8 \mod 9 = 4$$
$$(3 \odot_{12} 9) \odot_{12} (3 \oplus_{12} 9) = 0$$
$$7 \odot_9 2 \oplus_9 4 \odot_9 6+ = 5 \oplus_9 6 = 2$$
$$((3 \oplus_9 6) \odot_9 3) \ominus_9 8 = 0 \ominus_9 8 = 1$$
$$3 \odot_8 6 \ominus_8 2 \ominus_8 3 = 2 \ominus_8 5 = 5$$

II.)



$\oplus_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\odot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

III.)

$13 = (1101)_2 \rightarrow QMQMQQQM$

$3 \xrightarrow{Q} 9 \xrightarrow{M} 27 \equiv 1 \xrightarrow{Q} 1 \xrightarrow{Q} 1 \xrightarrow{Q} 1 \xrightarrow{M} 3$

Da 13 eine Primzahl ist, gilt der kleine Fermat'sche Satz.
$3^{13} \mod 13 = 3 \mod 13 = 3$

IV.)

x	1	2	4	7	8	11	13	14
$x \odot_{15} x$	1	4	1	4	4	1	4	1

a	1	2	4	7	8	11	13	14
$\sqrt{a} \mod 15$	1,4,11,14	-	2,7,8,13	-	-	-	-	-

V.)

k	1	2	3	4	5	6	7	8	9	10
$k^2 \mod 11$	1	4	9	5	3	3	5	9	4	1

QR: 1,3,4,5,9
NR: 2,6,7,8,10

Nein ist nicht immer so.

VI.)

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$k^2 \mod 21$	1	4	9	16	4	15	7	1	18	16	16	18	1	7	15	4	16	9	4	1

Alle Reste, welche teilerfremd zu 21 sind:
QR: 1,4,16
NR: 2,5,8,10,11,13,17,19,20

Quadratwurzeln von 1 sind 1,8,13,20

VII.)
Schlüssel:
Alice und Bob haben sich auf $n = 13$ und $g = 11$ geeinigt. Alice wählt $a = 5$ und Bob wählt $b = 7$ als Geheimzahl

a) weis nicht

b)

1. Alice: $A = g^a \mod n = 11^5 \mod 13 = 7$
2. Bob: $B = g^b \mod n = 11^7 \mod 13 = 2$
3. Alice: $k_{BA} = B^a \mod n = 2^5 \mod 13 = 6$
4. Bob: $k_{AB} = A^b \mod n = 7^7 \mod 13 = 6$
5. Gemeinsamer Schlüssel: $k = 6$

c) Schlüssel ist 6