Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

Einführung in die Zahlentheorie 2 - Übung

Prof. Dr. Josef F. Bürgler

I.BA_DMATH, Semesterwoche 10

Die Aufgaben sind zusammen mit dem Lösungsweg in möglichst einfacher Form darzustellen. Numerische Resultate sind mit einer Genauigkeit von 4 Stellen anzugeben. Skizzen müssen qualitativ und quantitativ richtig sein.

Sie sollten im Durchschnitt 75% der Aufgaben bearbeiten. Die mit grossen römischen Zahlen gekennzeichneten Aufgaben **müssen** bearbeitet werden und die Lösungen dieser Aufgaben werden kontrolliert und bewertet. Abgabetermin ihrer Übungsaufgaben ist die letzte Vorlesungsstunde in der Woche, nachdem das Thema im Unterricht besprochen wurde.

Referenz: *Kenneth H. Rosen, Discrete Mathematics and its Applications, McGraw-Hill International Edition, 6. Auflage,* ***kurz: KR***

1. Berechnen Sie:

$$
\begin{aligned}
3 \odot_{11} (2 \oplus_{11} 7) &= \\
3 \odot_{11} 2 \oplus_{11} 10 &= \\
(3 \oplus_{12} 9) \odot_{12} (3 \oplus_{12} 9) &= \\
7 \odot_{11} 2 \oplus_{11} 9 \odot_{11} 9 &= \\
((3 \oplus_{11} 6) \odot_{11} 3) \ominus_{11} 9 &= \\
3 \odot_{11} 6 \ominus_{11} 3 \ominus_{11} 9 &=
\end{aligned}
$$

I. Berechnen Sie:

$$
\begin{aligned}
3 \odot_{9} (2 \oplus_{9} 5) &= \\
3 \odot_{10} 2 \oplus_{10} 8 &= \\
(3 \oplus_{12} 9) \odot_{12} (3 \oplus_{12} 9) &= \\
7 \odot_{9} 2 \oplus_{9} 4 \odot_{9} 6 &= \\
((3 \oplus_{9} 6) \odot_{9} 3) \ominus_{9} 8 &= \\
3 \odot_{8} 6 \ominus_{8} 2 \ominus_{8} 3 &=
\end{aligned}
$$

2. Rechnen in $\mathbb{Z}_6$

a) Ergänzen Sie alle fehlenden Einträge:

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1					
2	2					
3	3					
4	4					
5	5					

$\odot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0					
2	0					
3	0					
4	0					
5	0					

b) Bestimmen Sie alle Elemente in $\mathbb{Z}_6^*$, die bezüglich der Multiplikation $\odot_6$ invertierbar sind und geben Sie jeweils die zugehörigen (multiplikativen) Inversen an.

c) Bestimmen Sie alle Nullteiler in $\mathbb{Z}_6$.

d) Ergänzen Sie alle fehlenden Einträge:

$\ominus_6$	0	1	2	3	4	5
0	0	5	4	3	2	1
1	1					
2	2					
3	3					
4	4					
5	5					

II. Rechnen in $\mathbb{Z}_7$

a) Ergänzen Sie alle fehlenden Einträge:

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

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

b) Bestimmen Sie alle Elemente in $\mathbb{Z}_7$, die bezüglich der Multiplikation $\odot_7$ invertierbar sind und geben Sie jeweils die zugehörigen (multiplikativen) Inversen an.

3. Berechnen Sie **Schritt für Schritt** mit Hilfe des SMA (Square and Multiply Algorithm) die modulare Potenz 3^{21} **mod** 11.

III. Berechnen Sie **Schritt für Schritt** mit Hilfe des SMA (Square and Multiply Algorithm) die modulare Potenz 3^{13} **mod** 13. Hätte man die Lösung hier auch einfacher finden können?

4. Sei $n = 10$ und $\mathbb{Z}_{10}^* = \{1,3,7,9\}$. Ergänzen Sie die folgenden Tabellen:

x	1	3	7	9
$x \odot_{10} x$				

a	1	3	7	9
$\sqrt{a}$ **mod** 10				

IV. Sei $n = 15$ und $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$. Ergänzen Sie die folgenden Tabellen:

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

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

5. Finden Sie eine Lösung k der Gleichung $12 = 5^k$ **mod** 13.
6. Bestimmen Sie $\log_9(16)$ **mod** 17.

Lösungen

1. 5, 5, 0, 7, 7, 6

I. -

2.

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\odot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\ominus_6$	0	1	2	3	4	5
0	0	5	4	3	2	1
1	1	0	5	4	3	2
2	2	1	0	5	4	3
3	3	2	1	0	5	4
4	4	3	2	1	0	5
5	5	4	3	2	1	0

Invertierbar bezüglich der Multiplikation sind 1 (mit $1^{-1} = 1$ denn $1 \odot_6 1 = 1$) und 5 (mit $5^{-1} = 5$ denn $5 \odot_6 5 = 1$)

Nullteiler sind die drei Elemente 2, 3 und 4, denn $2 \odot_6 3 = 3 \odot_6 2 = 3 \odot_6 4 = 4 \odot_6 3 = 0$

II. -

3. $21 = (10101)_2 \rightarrow QQMQQM$ und somit

$$3 \xrightarrow{Q} 9 \equiv 9 \xrightarrow{Q} 81 \equiv 4 \xrightarrow{M} 12 \equiv 1 \xrightarrow{Q} 1 \equiv 1 \xrightarrow{Q} 1 \equiv 1 \xrightarrow{M} 3$$

III. -

4.

x	1	3	7	9
$x \odot_{10} x$	1	9	9	1

a	1	3	7	9
$\sqrt{a}$ **mod** 10	1, 9	–	–	3, 7

IV. -

5. $k = 9$ (durch Probieren gelöst)

6. $\log_9(16)$ **mod** 17 $=$ 4, denn 9^4 **mod** 17 $=$ 16