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** 17.
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

1. Berechnen Sie:

a) $3 \odot_{11} (2 \oplus_{11} 7) =$
b) $3 \odot_{11} 2 \oplus_{11} 10 =$
c) $(3 \oplus_{12} 9) \odot_{12} (3 \oplus_{12} 9) =$
d) $7 \odot_{11} 2 \oplus_{11} 9 \odot_{11} 9 =$
e) $((3 \oplus_{11} 6) \odot_{11} 3) \ominus_{11} 9 =$
f) $3 \odot_{11} 6 \ominus_{11} 3 \ominus_{11} 9 =$

1. a) $3 \odot_{11} (2 \oplus_{11} 7) = 3 \cdot (2+7) \mod 11$
$= 27 \mod 11$
$= 5$

b) $3 \odot_{11} 2 \oplus_{11} 10 = 3 \cdot 2 + 10 \mod 11$
$= 16 \mod 11$
$= 5$

c) $(3 \oplus_{12} 9) \odot_{12} (3 \oplus_{12} 9) = 0 \odot_{12} 0$
$= 0 \mod 12$
$= 0$

d) $7 \odot_{11} 2 \oplus_{11} 9 \odot_{11} 9 = 7 \cdot 2 + 9 \cdot 9 \mod 11$
$= 14 + 81 \mod 11$
$= 95 \mod 11$
$= 7$

e) $((3 \oplus_{11} 6) \odot_{11} 3) \ominus_{11} 9 = ((3+6) \cdot 3) - 9 \mod 11$
$= (9 \cdot 3) - 9 \mod 11$
$= 27 - 9 \mod 11$
$= 18 \mod 11$
$= 7$

f) $3 \ominus_{11} 6 \ominus_{11} 3 \ominus_{11} 9 = 3 \cdot 6 - 3 - 9 \mod 11$

$= 6 \mod 11$

$= \underline{\underline{6}}$

I. Berechnen Sie:

$3 \odot_9 (2 \oplus_9 5) =$ a)

$3 \odot_{10} 2 \oplus_{10} 8 =$ b)

$(3 \oplus_{12} 9) \odot_{12} (3 \oplus_{12} 9) =$ c)

$7 \odot_9 2 \oplus_9 4 \odot_9 6 =$ d)

$((3 \oplus_9 6) \odot_9 3) \ominus_9 8 =$ e)

$3 \odot_8 6 \ominus_8 2 \ominus_8 3 =$ f)

I. a) $3 \odot_9 (2 \oplus_9 5) = 3 \cdot (2+5) \mod 9$

$= 21 \mod 9$

$= \underline{\underline{3}}$

b) $3 \odot_{10} 2 \oplus_{10} 8 = 3 \cdot 2 + 8 \mod 10$

$= 14 \mod 10$

$= \underline{\underline{4}}$

c) $(3 \oplus_{12} 9) \odot_{12} (3 \oplus_{12} 9) = (3+9)(3+9) \mod 12$

$= 12 \cdot 12 \mod 12$

$= \underline{\underline{0}}$

d) $7 \odot_9 2 \oplus_9 4 \odot_9 6 = 7 \cdot 2 + 4 \cdot 6 \mod 9$

$= 14 + 24 \mod 9$

$= 38 \mod 9$

$= \underline{\underline{2}}$

e) $((3 \oplus_9 6) \odot_9 3) \ominus_9 8 = ((3+6)\cdot 3) - 9 \mod 9$

$= ((9)\cdot 3) - 9 \mod 9$

$= 0$

f) $3 \odot_8 6 \ominus_8 2 \odot_8 3 = 3 \cdot 6 - 2 - 3 \mod 8$

$= 13 \mod 8$

$= 5$

## 2. $\mathbb{Z}_6$

a) Ergänzen Sie alle fehlenden Einträge:

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

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 | 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 |

b) $1^{-1} = 1$ weil $1 \odot_6 1 = 1$

$5^{-1} = 5$ weil $5 \odot_6 5 = 1$

c) Nullteiler: 2, 3, 4

$2 \odot_6 3 = 3 \odot_6 2 = 3 \odot_6 4 = 4 \odot_6 3 = 0$

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 | 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 |

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.

b) $1^{-1} = 1$ weil $1 \odot_7 1 = 1$

$4^{-1} = 2$ weil $4 \odot_7 2 = 1$

$2^{-1} = 4$ weil $2 \odot_7 4 = 1$

$5^{-1} = 3$ weil $5 \odot_7 3 = 1$

$3^{-1} = 5$ weil $3 \odot_7 5 = 1$

$6^{-1} = 6$ weil $6 \odot_7 6 = 1$

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?

3. $3^{21} \bmod 11 \Rightarrow 21 = (10101)_2$

$= 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

$= 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2^0$

$= (2 \cdot 2 + 1) \cdot 2 \cdot 2 + 1$

$3^{21} \bmod 11 = 3^{(2 \cdot 2 + 1) \cdot 2 \cdot 2 + 1} \bmod 11$

$= (((3^2)^2 \cdot 3)^2)^2 \cdot 3 \bmod 11$

$= ((9^2 \cdot 3)^2)^2 \cdot 3 \bmod 11$

$= ((4 \cdot 3)^2)^2 \cdot 3 \bmod 11$

$= (1^2)^2 \cdot 3 \mod 11$

$= 3$

III. $3^{13} \mod 13 \Rightarrow 13 = (1101)_2$

$= 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

$= 2^3 + 2^2 + 1$

$= 2 \cdot 2 \cdot 2 + 2 \cdot 2 + 1$

$3^{13} \mod 13 = 3^{2 \cdot 2 \cdot 2 + 2 \cdot 2 + 1} \mod 13$

$= ((3^2)^2)^2 \cdot (3^2)^2 \cdot 3 \mod 13$

$= (9^2)^2 \cdot 9^2 \cdot 3 \mod 13$

$= 81^2 \cdot 81 \cdot 3 \mod 13$

$= 3^2 \cdot 3 \cdot 3 \mod 13$

$= 9 \cdot 3 \cdot 3 \mod 13$

$= 27 \cdot 3 \mod 13$

$= 3$

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

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

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

$x \cdot x \mod 10$

**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 |
|---|---|---|---|---|---|---|---|---|
| $x \odot_{15} x$ | 1 | 4 | 1 | 4 | 4 | 1 | 4 | 1 |

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

$x \cdot x \mod 15$ → = 1, 4, 11, 14

→ = 2, 7, 8, 13

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

5. $12 = 5^k \mod 17$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | ⇒ | $5^1 \mod 17$ | = 5 | 6 | ⇒ | $5^6 \mod 17$ | = 2 |
| 2 | ⇒ | $5^2 \mod 17$ | = 8 | 7 | ⇒ | $5^7 \mod 17$ | = 10 |
| 3 | ⇒ | $5^3 \mod 17$ | = 6 | 8 | ⇒ | $5^8 \mod 17$ | = 16 |
| 4 | ⇒ | $5^4 \mod 17$ | = 13 | 9 | ⇒ | $5^9 \mod 17$ | = 12 |
| 5 | ⇒ | $5^5 \mod 17$ | = 14 | | | | |

6. $\log_9(16) \mod 17 = 4$

⇒ $9^4 \mod 17 = 16$