

# Tutorium: Diskrete Mathematik

Vorbereitung der Bonusklausur am 17.01.2020  
(Teil 2, Lösungen)

15. Januar 2020

>> 3

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 1

$$\begin{aligned} b &= \lambda a \quad (\lambda \in \mathbb{Z}) \\ c &= \mu b \quad (\mu \in \mathbb{Z}) \\ \Rightarrow c &= (\lambda\mu) a \end{aligned}$$

$$\begin{aligned} b_1 &= \lambda a_1 \quad (\lambda \in \mathbb{Z}) \\ b_2 &= \mu a_2 \quad (\mu \in \mathbb{Z}) \\ \Rightarrow b_1 b_2 &= (\lambda\mu) a_1 a_2 \end{aligned}$$

$$\begin{aligned} b_1 &= \lambda a \quad (\lambda \in \mathbb{Z}) \\ b_2 &= \mu a \quad (\mu \in \mathbb{Z}) \\ \Rightarrow c_1 b_1 + c_2 b_2 &= (c_1 \lambda + c_2 \mu) a \end{aligned}$$

>> 4

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 2

Die Aussage ist im Allgemeinen nicht gültig. Beispielsweise gilt  $2 \mid 4$  und  $3 \mid 9$ , aber  $(5 =) 2 + 3 \nmid 4 + 9 (= 13)$ .

>> 2

© 2020 Steven Köhler

15. Januar 2020

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

>> 2

© 2020 Steven Köhler

15. Januar 2020

### Aufgabe 3

- a) Wahr, da  $65 - 31 = 34$  und  $17 \mid 34$  gilt.
- b) Falsch, da  $42 - 23 = 19$  und  $11 \nmid 19$  gilt.
- c) Falsch, da  $202 - 101 = 101$  und  $47 \nmid 101$  gilt.
- d) Wahr, da  $312 - (-147) = 459$  und  $3 \mid 459$  gilt.
- e) Falsch, da  $59 - 29 = 30$  und  $23 \nmid 30$  gilt.

>> 5

### Aufgabe 4 II

Es sei  $m \mid (a - b)$ . Für  $a$  und  $b$  existieren die folgenden Zerlegungen mit Rest (mit  $q_a, q_b, r_a, r_b \in \mathbb{Z}$  und  $0 \leq r_a < m$  sowie  $0 \leq r_b < m$ ):

$$a = q_a \cdot m + r_a$$

$$b = q_b \cdot m + r_b$$

Für die Differenz  $a - b$  ergibt sich hieraus:

$$\begin{aligned} a - b &= (q_a \cdot m + r_a) - (q_b \cdot m + r_b) \\ &= \underbrace{(q_a - q_b)}_{\equiv 0 \pmod{m}} \cdot m + (r_a - r_b) \\ &\equiv r_a - r_b \pmod{m} \end{aligned}$$

>> 7

### Aufgabe 4 I

Es sei  $a \equiv b \pmod{m}$ . Dann existieren für  $a$  und  $b$  die folgenden Zerlegungen mit Rest (mit  $q_a, q_b, r \in \mathbb{Z}$  und  $0 \leq r < m$ ):

$$a = q_a \cdot m + r$$

$$b = q_b \cdot m + r$$

Für die Differenz  $a - b$  ergibt sich hieraus:

$$\begin{aligned} a - b &= (q_a \cdot m + r) - (q_b \cdot m + r) \\ &= q_a \cdot m - q_b \cdot m + r - r \\ &= (q_a - q_b) \cdot m \end{aligned}$$

Hieraus folgt direkt, dass  $m \mid (a - b)$  gilt.

>> 6

### Aufgabe 4 III

Wegen  $m \mid (a - b)$  muss also  $m \mid (r_a - r_b)$  gelten. Aufgrund der Voraussetzungen  $0 \leq r_a < m$  und  $0 \leq r_b < m$  gilt

$$-m < r_a - r_b < m.$$

Das einzige ganzzahlige Vielfache von  $m$  im Intervall  $(-m, m)$  ist  $0$  – dies entspricht dem Fall  $r_a = r_b$ , woraus direkt  $a \equiv b \pmod{m}$  folgt.

>> 8

## Aufgabe 5a

Mit dem Euklidischen Algorithmus ergibt sich:

$$613 = 2 \cdot 224 + 165$$

$$224 = 1 \cdot 165 + 59$$

$$165 = 2 \cdot 59 + 47$$

$$59 = 1 \cdot 47 + 12$$

$$47 = 3 \cdot 12 + 11$$

$$12 = 1 \cdot 11 + 1$$

$$11 = 11 \cdot 1 + 0$$

Der größte gemeinsame Teiler von 613 und 224 ist folglich 1. Das bedeutet, dass die beiden Zahlen keine gemeinsamen Teiler  $\geq 1$  besitzen und somit teilerfremd sind.

## Aufgabe 6

Es gilt

$$\begin{aligned} a \cdot b &= (q_a \cdot m + r_a) \cdot (q_b \cdot m + r_b) \\ &= q_a \cdot m \cdot q_b \cdot m + q_a \cdot m \cdot r_b + r_a \cdot q_b \cdot m + r_a \cdot r_b \\ &= \underbrace{(q_a \cdot q_b \cdot m + q_a \cdot r_b + q_b \cdot r_a) \cdot m + r_a \cdot r_b}_{\equiv 0 \pmod{m}} \\ &\equiv r_a \cdot r_b \pmod{m} \end{aligned}$$

## Aufgabe 5b

Mit dem Euklidischen Algorithmus ergibt sich:

$$312 = 1 \cdot 247 + 65$$

$$247 = 3 \cdot 65 + 52$$

$$65 = 1 \cdot 52 + 13$$

$$52 = 4 \cdot 13 + 0$$

Der größte gemeinsame Teiler von 312 und 247 ist folglich 13. Rückwärtseinsetzen ergibt:

$$\begin{aligned} 13 &= 1 \cdot 65 - 1 \cdot 52 \\ &= 1 \cdot 65 - 1 \cdot (1 \cdot 247 - 3 \cdot 65) \\ &= -1 \cdot 247 + 4 \cdot 65 \\ &= -1 \cdot 247 + 4 \cdot (1 \cdot 312 - 1 \cdot 247) \\ &= 4 \cdot 312 - 5 \cdot 247 \end{aligned}$$

## Aufgabe 7

a) Nach dem Satz von Fermat gilt  $5^{22} \equiv 1 \pmod{23}$ . Es folgt

$$5^{948} \equiv (5^{22})^{43} \cdot 5^2 \equiv 1^{43} \cdot 5^2 \equiv 2 \pmod{23}.$$

b) Berechnen der notwendigen Potenzen mittels Square-and-Multiply-Verfahren:

$$4^{153} \equiv 4 \cdot 4^{152} \equiv 22 \pmod{42} \quad 4^{18} \equiv (4^9)^2 \equiv 22 \pmod{42}$$

$$4^{152} \equiv (4^{76})^2 \equiv 16 \pmod{42} \quad 4^9 \equiv 4 \cdot 4^8 \equiv 22 \pmod{42}$$

$$4^{76} \equiv (4^{38})^2 \equiv 4 \pmod{42} \quad 4^8 \equiv (4^4)^2 \equiv 16 \pmod{42}$$

$$4^{38} \equiv (4^{19})^2 \equiv 16 \pmod{42} \quad 4^4 \equiv (4^2)^2 \equiv 4 \pmod{42}$$

$$4^{19} \equiv 4 \cdot 4^{18} \equiv 4 \pmod{42} \quad 4^2 \equiv 16 \pmod{42}$$

## Aufgabe 8 I

- a) Bestimmen von  $\text{ggT}(149, 23)$  mit dem Euklidischen Algorithmus:

$$\begin{aligned}149 &= 6 \cdot 23 + 11 \\23 &= 2 \cdot 11 + 1 \\11 &= 11 \cdot 1 + 0.\end{aligned}$$

Es folgt  $\text{ggT}(149, 23) = 1$ ; demnach existiert das Inverse.  
Rückwärtseinsetzen ergibt:

$$\begin{aligned}1 &= 23 - 2 \cdot 11 \\ &= 23 - 2 \cdot (149 - 6 \cdot 23) \\ &= -2 \cdot 149 + 13 \cdot 23.\end{aligned}$$

» 13

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 9

Zunächst wird die Primfaktorzerlegung von 24 bestimmt:

$$24 = 2^3 \cdot 3.$$

Es folgt

$$\varphi(24) = \varphi(2^3) \cdot \varphi(3) = (2^3 - 2^2) \cdot (3 - 1) = 8.$$

Bei den acht zur 24 teilerfremden Zahlen handelt es sich um die Zahlen

$$1, 5, 7, 11, 13, 17, 19, 23.$$

» 15

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 8 II

- a) Es folgt:

$$1 \equiv -2 \cdot 149 + 13 \cdot 23 \equiv 13 \cdot 23 \pmod{149}.$$

Demnach ist  $x = 13$  das gesuchte Inverse von 23 in  $\mathbb{Z}_{149}$ .

- b) Es gilt:

$$\begin{aligned}54 &= 2 \cdot 27 \\966 &= 2 \cdot 483.\end{aligned}$$

54 und 966 sind nicht teilerfremd. Folglich existiert kein multiplikatives Inverses für 54 in  $\mathbb{Z}_{966}$ .

- c) Es gilt, dass  $m - 1$  in  $\mathbb{Z}_m$  stets zu sich selbst invers ist. Folglich ist 1336 in  $\mathbb{Z}_{1337}$  zu sich selbst invers.

» 14

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 10a I

Zunächst wird der RSA-Modul  $N$  bestimmt. Es gilt

$$N = p \cdot q = 13 \cdot 17 = 221.$$

Anschließend wird die eulersche  $\varphi$ -Funktion für  $N$  berechnet:

$$\varphi(N) = \varphi(p) \cdot \varphi(q) = 12 \cdot 16 = 192.$$

Im nächsten Schritt wird mithilfe des erweiterten Euklidischen Algorithmus der Wert  $d$  bestimmt, so dass gilt:

$$d \cdot 23 \equiv 1 \pmod{\varphi(N)}.$$

» 16

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 10a II

Bestimmen von  $\text{ggT}(192, 23)$  mit dem Euklidischen Algorithmus:

$$\begin{aligned}192 &= 8 \cdot 23 + 8 \\23 &= 2 \cdot 8 + 7 \\8 &= 1 \cdot 7 + 1 \\7 &= 7 \cdot 1 + 0.\end{aligned}$$

Rückwärtseinsetzen ergibt:

$$\begin{aligned}1 &= 8 - 1 \cdot 7 \\&= 8 - 1 \cdot (23 - 2 \cdot 8) \\&= -1 \cdot 23 + 3 \cdot 8 \\&= -1 \cdot 23 + 3 \cdot (192 - 8 \cdot 23) \\&= 3 \cdot 192 - 25 \cdot 23.\end{aligned}$$

>> 17

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 10b-c

Verschlüsseln der Nachricht mithilfe des öffentlichen Schlüssels liefert

$$42^{23} \equiv 100 \pmod{221}.$$

Entschlüsseln mithilfe des privaten Schlüssels liefert wie erwartet

$$100^{167} \equiv 42 \pmod{221}.$$

>> 19

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 10a III

Es folgt:

$$1 \equiv 3 \cdot 192 - 25 \cdot 23 \equiv -25 \cdot 23 \pmod{192}.$$

Es ist  $-25 \equiv 167$  das gesuchte Inverse von 23 in  $\mathbb{Z}_{192}$ .

Somit ergeben sich die beiden Schlüssel:

- ▶ öffentlicher Schlüssel:  $(23, 221)$
- ▶ privater Schlüssel:  $(167, 221)$

>> 18

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 11

Wegen  $e \cdot d \equiv 1 \pmod{\varphi(N)}$  existiert ein  $k \in \mathbb{Z}$  mit:

$$e \cdot d = k \cdot \varphi(N) + 1.$$

Es gilt:

$$c^d \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m^{k \cdot \varphi(N) + 1} \equiv \left(m^{\varphi(N)}\right)^k \cdot m \stackrel{(*)}{\equiv} 1^k \cdot m \equiv m \pmod{N}.$$

An der Stelle  $(*)$  wurde der Satz von Euler verwendet.

>> 20

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 12 I

Durch die Primfaktorzerlegung von  $N = 253$  müssen zunächst die ursprünglichen Primzahlen  $p$  und  $q$  bestimmt werden. Es gilt

$$253 = 11 \cdot 23.$$

Mit  $p = 11$  und  $q = 23$  kann nun  $\varphi(N)$  berechnet werden. Es gilt

$$\varphi(253) = \varphi(11) \cdot \varphi(23) = 10 \cdot 22 = 220.$$

Zur Berechnung des privaten Schlüssels  $(d, 253)$  muss nun mithilfe des erweiterten Euklidischen Algorithmus das multiplikative Inverse von  $e = 47$  bezüglich  $\varphi(N)$  berechnet werden.

» 21

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 12 III

Es ist 103 das gesuchte Inverse von 47 in  $\mathbb{Z}_{220}$ .

Somit ergibt sich der folgende Schlüssel:

► privater Schlüssel:  $(103, 253)$

Entschlüsseln mithilfe des privaten Schlüssels liefert

$$42^{103} \equiv 135 \pmod{253}.$$

» 23

© 2020 Steven Köhler

15. Januar 2020

## Aufgabe 12 II

Bestimmen von  $\text{ggT}(220, 47)$  mit dem Euklidischen Algorithmus:

$$220 = 4 \cdot 47 + 32$$

$$47 = 1 \cdot 32 + 15$$

$$32 = 2 \cdot 15 + 2$$

$$15 = 7 \cdot 2 + 1$$

Rückwärtseinsetzen ergibt:

$$1 = 15 - 7 \cdot 2$$

$$= 15 - 7 \cdot (32 - 2 \cdot 15)$$

$$= -7 \cdot 32 + 15 \cdot 15$$

$$= -7 \cdot 32 + 15 \cdot (47 - 1 \cdot 32)$$

$$= 15 \cdot 47 - 22 \cdot 32$$

$$= 15 \cdot 47 - 22 \cdot (220 - 4 \cdot 47)$$

$$= -22 \cdot 220 + 103 \cdot 47$$

» 22

© 2020 Steven Köhler

15. Januar 2020