

# Tutorium: Diskrete Mathematik

Vorbereitung der Bonusklausur am 17.01.2020  
(Teil 2)

15. Januar 2020

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

# Teilbarkeit & modulare Arithmetik

## Definition

Man nennt  $b$  einen *Teiler* von  $a$  und schreibt  $b \mid a$ , falls es ein  $c$  gibt, für das  $a = b \cdot c$  gilt (für  $a, b, c \in \mathbb{Z}$ ).

## Aufgabe 1

Beweise die folgenden Aussagen:

- a) Gilt  $a \mid b$  und  $b \mid c$ , so gilt auch  $a \mid c$ .
- b) Aus  $a_1 \mid b_1$  und  $a_2 \mid b_2$  folgt  $a_1 \cdot a_2 \mid b_1 \cdot b_2$ .
- c) Aus  $a \mid b_1$  und  $a \mid b_2$  folgt für alle  $c_1, c_2 \in \mathbb{Z}$  die Beziehung  $a \mid (c_1 b_1 + c_2 b_2)$ .

## Aufgabe 2

Was ist von der folgenden Aussage zu halten? Begründe deine Antwort!

Aus  $a_1 \mid b_1$  und  $a_2 \mid b_2$  folgt  $a_1 + a_2 \mid b_1 + b_2$ .

## Aufgabe 3

Wahr oder falsch? Gib jeweils eine kurze Begründung.

- a)  $31 \equiv 65 \pmod{17}$
- b)  $42 \equiv 23 \pmod{11}$
- c)  $202 \equiv 101 \pmod{47}$
- d)  $-147 \equiv 312 \pmod{3}$
- e)  $29 \equiv 59 \pmod{23}$

## Aufgabe 4

Beweise die folgende Äquivalenz:

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b).$$

## Euklidischer Algorithmus I

Gegeben seien zwei natürliche Zahlen  $a$  und  $b$  mit  $b \leq a$ , deren *größter gemeinsamer Teiler*  $\text{ggT}(a, b)$  bestimmt werden soll. Hierzu wird zunächst eine *Zerlegung mit Rest* bestimmt, d.h., es werden ganze Zahlen  $q_1, r_1$  mit  $0 \leq r_1 < b$  bestimmt, für die gilt:

$$a = q_1 \cdot b + r_1.$$

Die Grundidee des Euklidischen Algorithmus beruht auf der Tatsache, dass  $\text{ggT}(a, b) = \text{ggT}(b, r_1)$  gilt. Anstelle des größten gemeinsamen Teilers von  $a$  und  $b$  kann also auch der größte gemeinsame Teiler von  $r_0 = b$  und  $r_1$  berechnet werden. Hierzu wird wieder eine Zerlegung mit Rest vorgenommen:

$$r_0 = q_2 \cdot r_1 + r_2.$$

## Euklidischer Algorithmus II

Wie zuvor gilt  $\text{ggT}(r_0, r_1) = \text{ggT}(r_1, r_2)$  und somit auch  $\text{ggT}(a, b) = \text{ggT}(r_1, r_2)$ . Dieses Verfahren wird nun solange wiederholt, bis der Rest 0 auftritt.

$$r_1 = q_3 \cdot r_2 + r_3$$

$$\vdots$$

$$r_{n-1} = q_{n+1} \cdot r_n + 0$$

Die letzte Zeile bedeutet, dass  $r_{n-1}$  ein ganzzahliges Vielfaches von  $r_n$  ist – hieraus folgt direkt  $\text{ggT}(r_{n-1}, r_n) = r_n$  und somit  $\text{ggT}(a, b) = r_n$ .

## Aufgabe 5

- a) Entscheide, ob die Zahlen 224 und 613 teilerfremd sind.  
b) Finde Parameter  $s, t \in \mathbb{Z}$ , so dass gilt:

$$s \cdot 247 + t \cdot 312 = \text{ggT}(247, 312).$$

## Aufgabe 6

Es seien  $a, b \in \mathbb{Z}$  zwei ganze Zahlen, für die die folgenden Zerlegungen mit Rest gegeben sind (für  $m, q_a, q_b, r_a, r_b \in \mathbb{Z}$  mit  $0 \leq r_a < m$  und  $0 \leq r_b < m$ ):

$$\begin{aligned} a &= q_a \cdot m + r_a \\ b &= q_b \cdot m + r_b. \end{aligned}$$

Beweise oder widerlege, dass die folgende Aussage gilt:

$$a \cdot b \equiv r_a \cdot r_b \pmod{m}.$$

## Square-and-Multiply-Verfahren

Das *Square-and-Multiply-Verfahren* ist eine sehr effiziente Methode zum Berechnen von natürlichen Potenzen, also von Ausdrücken der Form  $a^n$  mit natürlichem Exponenten  $n$ .

Es gilt

$$a^n = \begin{cases} \left(a^{\frac{n}{2}}\right)^2 & , \text{ für gerade } n \\ a^{n-1} \cdot a & , \text{ für ungerade } n. \end{cases}$$

## Kleiner Satz von Fermat

Es sei  $p$  eine Primzahl und  $a$  sei eine ganze Zahl, für die  $\text{ggT}(a, p) = 1$  gilt;  $a$  und  $p$  sind also teilerfremd. Dann gilt:

$$a^{p-1} \equiv 1 \pmod{p}.$$

## Aufgabe 7

- a) Bestimme den ganzzahligen Rest der Division von  $5^{948}$  durch 23.
- b) Bestimme den ganzzahligen Rest der Division von  $4^{153}$  durch 42.

## Restklassenring I

Wir betrachten die Kongruenzrelation  $\equiv$  modulo  $m$ . Es handelt es sich um eine Äquivalenzrelation, bei deren Äquivalenzklassen es sich um die Restklassen  $[0]_m, [1]_m, \dots, [m-1]_m$  handelt.

Man definiert die Menge  $\mathbb{Z}_m$  (oder  $\mathbb{Z}/m\mathbb{Z}$ ) als die Menge der Äquivalenzklassen der Kongruenzrelation modulo  $m$ :

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}.$$

Wenn klar ist, dass es sich um Elemente aus  $\mathbb{Z}_m$  handelt, kann anstelle von  $[0]_m, [1]_m, \dots, [m-1]_m$  stellvertretend auch einfach  $0, 1, \dots, m-1$  geschrieben werden.

## Restklassenring II

Für alle  $x, y \in \mathbb{Z}$  seien die Operationen  $\oplus$  und  $\odot$  wie folgt definiert:

$$[x]_m \oplus [y]_m = [x + y]_m$$

$$[x]_m \odot [y]_m = [x \cdot y]_m$$

Anstelle von  $\oplus$  und  $\odot$  wird oft auch nur  $+$  und  $\cdot$  geschrieben.

Es handelt sich bei  $(\mathbb{Z}_m, \oplus, \odot)$  bzw.  $(\mathbb{Z}_m, +, \cdot)$  um einen kommutativen Ring.

## Restklassenring III

Für beliebige  $[a]_m, [b]_m, [c]_m \in \mathbb{Z}_m$  gilt:

$$(I) [a]_m \oplus [b]_m = [b]_m \oplus [a]_m$$

$$[a]_m \odot [b]_m = [b]_m \odot [a]_m$$

$$(II) ([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$$

$$([a]_m \odot [b]_m) \odot [c]_m = [a]_m \odot ([b]_m \odot [c]_m)$$

$$(III) [a]_m \oplus [0]_m = [a]_m$$

$$[a]_m \odot [1]_m = [a]_m$$

$$(IV) [a]_m \odot ([b]_m \oplus [c]_m) = ([a]_m \odot [b]_m) \oplus ([a]_m \odot [c]_m)$$

$$(V) [a]_m \oplus [-a]_m = [0]_m$$

## Multiplikatives Inverses

Es sei  $[a]_m \in \mathbb{Z}_m$ . Ein Element  $[x]_m \in \mathbb{Z}_m$  heißt *multiplikatives Inverses* von  $[a]_m$ , falls gilt:

$$[a]_m \odot [x]_m = [1]_m.$$

Besitzt  $[a]_m$  ein multiplikatives Inverses, so nennt man  $[a]_m$  *invertierbar*.

Hinweis: Per Konvention wird für das multiplikative Inverse stets der kleinste, nichtnegative Vertreter der entsprechenden Restklasse angegeben.

## Erweiterter Euklidischer Algorithmus

Zum Bestimmen des *multiplikativen Inversen* von  $x$  in  $\mathbb{Z}_m$  kann der *erweiterte Euklidische Algorithmus* verwendet werden.

- ▶ Bestimmen von  $\text{ggT}(x, m)$ .
- ▶ Gilt  $\text{ggT}(x, m) \neq 1$ , so existiert kein multiplikatives Inverses von  $x$  in  $\mathbb{Z}_m$ .
- ▶ Gilt  $\text{ggT}(x, m) = 1$ , so kann das multiplikative Inverse durch *Rückwärtseinsetzen* bestimmt werden.

## Aufgabe 8

Bestimme, falls möglich, das multiplikative Inverse. Gib im Falle der Nicht-Existenz eine (kurze) Begründung, weshalb das multiplikative Inverse nicht existiert.

- a) 23 in  $\mathbb{Z}_{149}$
- b) 54 in  $\mathbb{Z}_{966}$
- c) 1336 in  $\mathbb{Z}_{1337}$

RSA

## Eulersche $\varphi$ -Funktion

Die *eulersche  $\varphi$ -Funktion* ist eine Funktion, die zu einer natürlichen Zahl  $n$  angibt, wie viele zu  $n$  teilerfremde natürliche Zahlen es gibt, die kleiner gleich  $n$  sind.

$$\varphi(n) = \left| \left\{ a \in \mathbb{N} : 1 \leq a \leq n \wedge \text{ggT}(a, n) = 1 \right\} \right|$$

## Berechnung der eulerschen $\varphi$ -Funktion I

Da eine Primzahl  $p$  nur durch 1 und sich selbst teilbar ist, ist sie zu den Zahlen 1 bis  $p - 1$  teilerfremd. Da  $p \geq 2$  gilt und somit  $p$  niemals zu sich selbst teilerfremd ist, gilt stets

$$\varphi(p) = p - 1.$$

## Berechnung der eulerschen $\varphi$ -Funktion II

Sind  $m$  und  $n$  zwei teilerfremde ganze Zahlen, so gilt:

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

## Berechnung der eulerschen $\varphi$ -Funktion III

Eine Potenz  $p^k$  einer Primzahl  $p$  besitzt als einzigen Primfaktor die Zahl  $p$ . Daher hat  $p^k$  nur mit Vielfachen von  $p$  einen von 1 verschiedenen gemeinsamen Teiler. Im Bereich  $1, \dots, p^k$  sind dies die Zahlen

$$1 \cdot p, 2 \cdot p, \dots, p^{k-1} \cdot p.$$

Es gibt also insgesamt  $p^{k-1}$  Zahlen, die nicht teilerfremd zu  $p^k$  sind. Für die eulersche  $\varphi$ -Funktion gilt folglich:

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p - 1) = p^k \cdot \left(1 - \frac{1}{p}\right).$$

## Berechnung der eulerschen $\varphi$ -Funktion IV

Der Wert der eulerschen  $\varphi$ -Funktion lässt sich für jede natürliche Zahl  $n$  aus deren Primfaktorzerlegung berechnen. Hierbei sei

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}.$$

Dann gilt

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \dots \cdot \varphi(p_k^{\alpha_k}).$$

## Aufgabe 9

Berechne  $\varphi(24)$ !

Überprüfe dein Ergebnis, indem du alle zu 24 teilerfremden Zahlen  $a$  mit  $1 \leq a \leq 24$  auflistest.

## Satz von Euler

Es seien  $a$  und  $n$  zwei natürliche Zahlen mit  $\text{ggT}(a, n) = 1$ . Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dieser Satz ist auch als *Satz von Euler-Fermat* bekannt.

## Beschreibung des RSA-Verfahrens I

Zum Erzeugen des öffentlichen und des privaten Schlüssels werden die folgenden Schritte ausgeführt:

1. Auswahl von zwei verschiedenen Primzahlen  $p$  und  $q$ .
2. Bestimmen des RSA-Moduls  $N = p \cdot q$ .
3. Berechnen des Werts  $\varphi(N) = (p - 1) \cdot (q - 1)$ .
4. Auswahl einer zu  $\varphi(N)$  teilerfremden Zahl  $e$  mit  $1 < e < \varphi(N)$ .
5. Berechnen des Werts  $d$  mit  $1 < d < \varphi(N)$ , so dass gilt:

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

Man erhält den *öffentlichen Schlüssel*  $(e, N)$  sowie den *privaten Schlüssel*  $(d, N)$ .

## Beschreibung des RSA-Verfahrens II

Beim *Verschlüsseln* einer Nachricht  $m$  (mit  $1 \leq m < N$ ) kann die verschlüsselte Nachricht  $c$  (mit  $1 \leq c < N$ ) wie folgt berechnet werden:

$$m^e \equiv c \pmod{N}.$$

Beim *Entschlüsseln* einer verschlüsselten Nachricht  $c$  kann die ursprüngliche Nachricht  $m$  wie folgt berechnet werden:

$$c^d \equiv m \pmod{N}.$$

## Aufgabe 10

Gegeben seien die beiden Primzahlen  $p = 13$  und  $q = 17$ .

- Bestimme den öffentlichen Schlüssel  $(e, N)$  sowie den privaten Schlüssel  $(d, N)$ . Es gelte  $e = 23$ .
- Verschlüsse die Nachricht  $m = 42$ .
- Entschlüsse die in b) erhaltene verschlüsselte Nachricht und überprüfe, ob es sich tatsächlich wieder um die ursprüngliche Nachricht  $m$  handelt.

## Aufgabe 11

Es seien die Bezeichnungen wie in der Beschreibung des RSA-Verfahrens. Zeige, dass es sich bei  $c^d$  tatsächlich um die ursprüngliche Nachricht  $m$  handelt.

## Aufgabe 12

Es seien der öffentliche RSA-Schlüssel  $(47, 253)$  sowie die verschlüsselte Nachricht  $c = 42$  gegeben. Wie lautet die unverschlüsselte Nachricht  $m$ ?

Viel Erfolg bei der Bonusklausur :)