

# Mathematik und Simulation



**Grundlagen der IT-Sicherheit /  
Kryptographische Verfahren**

**5**

**Prof. Dr. Thomas Schneider**

**Stand: 01.06.2022**

## 1 Etwas Zahlentheorie

- Division mit Rest und Euklidische Eigenschaft von  $\mathbb{Z}$
- Kongruenz modulo  $n$
- Modulare Arithmetik

## 2 Kryptographie - vom Geheimhalten, Verschlüsseln und Entschlüsseln

- Einführung
- Kategorien kryptographischer Verfahren
- Das RSA-Verfahren
- RSA-Verfahren – Demonstrationsbeispiel
- Erweiterter euklidischer Algorithmus

## 3 Faktorisierung von Restklassenringen

- Chinesischer Restsatz – Lösung simultaner Kongruenzen

## 4 Satz vom korrekten Dechiffrieren

## 5 Anhang – Relationen

# Etwas Zahlentheorie

## Motivation

- Algorithmen der Kryptographie beruhen auf Ergebnissen der Zahlentheorie
- Suche von Datensätzen in großen Dateien (Hashing)
- Prüfziffern (ISBN, Barcodes)

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

## Der Ring $\mathbb{Z}$ der ganzen Zahlen

Die Menge aller ganzen Zahlen mit der bekannten Addition und Multiplikation bildet einen sogenannten **Ring**, der mit  $\mathbb{Z}$  bezeichnet wird.

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Erinnerung: Teilbarkeit und Division mit Rest für ganze Zahlen

## Ein Beispiel:

Die Zahl 21 ist durch 7 teilbar, denn es gilt

$$21 = 3 \cdot 7.$$

Wir schreiben auch

$$21 : 7 = 3.$$

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Erinnerung: Teilbarkeit und Division mit Rest für ganze Zahlen

## Ein zweites Beispiel:

Die Zahl 26 ist *nicht* durch 7 teilbar, vielmehr gilt

$$26 = 3 \cdot 7 + 5.$$

Sprechweise: Bei der ganzzahligen Division von 26 durch 7 ergibt sich der **Rest** 5.

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Euklidische Eigenschaft der ganzen Zahlen

## Satz

Zu jeder Zahl  $a \in \mathbb{Z}$  und jeder Zahl  $n \in \mathbb{N}$  mit  $n > 0$  gibt es eindeutig bestimmte Zahlen  $q, r \in \mathbb{Z}$  mit  $a = q \cdot n + r$ ,  $0 \leq r < n$ .

Wir nennen  $q$  den **Quotienten** und  $r$  den **Rest** der Division von  $a$  durch  $n$ . Die Zahl  $a$  heißt **Dividend**,  $n$  ist der **Divisor**.

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Euklidische Eigenschaft der ganzen Zahlen

## Bezeichnungsweise

- 1 Gilt  $a = q \cdot n + r$  mit  $0 \leq r < n$ , so heißt  $r$  der **Rest** von  $a$  bei ganzzahliger Division durch  $n$ .

Wir schreiben hierfür  $a \bmod n = r$ .

- 2 Im Falle  $r = 0$  sagen wir:  
 $a$  ist durch  $n$  **teilbar** oder  $n$  ist ein Teiler von  $a$ .



# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Euklidische Eigenschaft der ganzen Zahlen

## Bezeichnungsweise

- ① Gilt  $a = q \cdot n + r$  mit  $0 \leq r < n$ , so heißt  $r$  der **Rest** von  $a$  bei ganzzahliger Division durch  $n$ .

Wir schreiben hierfür  $a \bmod n = r$ .

- ② Im Falle  $r = 0$  sagen wir:  
 $a$  ist durch  $n$  **teilbar** oder  $n$  ist ein Teiler von  $a$ .

## Beispiele

$$\begin{aligned} 26 \bmod 13 &= 0, & \text{denn } 26 &= 2 \cdot 13 + 0 \\ 29 \bmod 13 &= 3, & \text{denn } 29 &= 2 \cdot 13 + 3 \\ 1003 \bmod 13 &= 2, & \text{denn } 1003 &= 77 \cdot 13 + 2 \\ -29 \bmod 13 &= 10, & \text{denn } -29 &= -3 \cdot 13 + 10 \end{aligned}$$

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Euklidische Eigenschaft der ganzen Zahlen

**Bemerkung zur Definition von Resten und  $\bmod$  :**

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

## Euklidische Eigenschaft der ganzen Zahlen

### Bemerkung zur Definition von Resten und $\bmod$ :

#### Unsere Definition

Wir haben **für unseren Kontext** festgelegt, dass für jede natürliche Zahl  $n > 0$  und jede ganze Zahl  $a \in \mathbb{Z}$  das Ergebnis der Operation

$$a \bmod n =: r$$

stets eine Zahl  $r$  mit  $0 \leq r < n$  ergibt. Dies gilt insbesondere auch für negative Zahlen. Zum Beispiel:

$$\begin{aligned} 29 \bmod 13 &= 3, & \text{denn } 29 &= 2 \cdot 13 + 3, \\ -29 \bmod 13 &= 10, & \text{denn } -29 &= -3 \cdot 13 + 10. \end{aligned}$$

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

## Euklidische Eigenschaft der ganzen Zahlen

### Bemerkung zur Definition von Resten und $\text{mod}$ :

#### Unsere Definition

Wir haben **für unseren Kontext** festgelegt, dass für jede natürliche Zahl  $n > 0$  und jede ganze Zahl  $a \in \mathbb{Z}$  das Ergebnis der Operation

$$a \text{ mod } n =: r$$

stets eine Zahl  $r$  mit  $0 \leq r < n$  ergibt. Dies gilt insbesondere auch für negative Zahlen. Zum Beispiel:

$$\begin{aligned} 29 \text{ mod } 13 &= 3, & \text{denn } 29 &= 2 \cdot 13 + 3, \\ -29 \text{ mod } 13 &= 10, & \text{denn } -29 &= -3 \cdot 13 + 10. \end{aligned}$$

#### Alternative Definition:

Andernorts (z.B. in der Informatik bzw. in manchen Programmiersprachen) wird eine andere Definition der Operation  $\text{mod}$  verwendet mit sogenannten *symmetrischen Resten*. Wir wollen diese Alternativdefinition an unserem Beispiel illustrieren:

$$\begin{aligned} 29 \text{ mod}_{\text{alternativ}} 13 &= 3, & \text{denn } 29 &= 2 \cdot 13 + 3, \\ -29 \text{ mod}_{\text{alternativ}} &= -3, & \text{denn } -29 &= -2 \cdot 13 + (-3). \end{aligned}$$

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Kongruenz modulo  $n$

Für jede natürliche Zahl  $n$  definieren wir eine Relation  $\equiv_n$  auf der Menge der ganzen Zahlen:

## Definition

Es sei  $n \geq 1$  eine natürliche Zahl  $n$ .

- Für je zwei ganze Zahlen  $a, b$  sei

$$a \equiv_n b$$

genau dann, wenn

$$a \bmod n = b \bmod n$$

gilt.

- Die Relation  $\equiv_n$  heißt **Kongruenzrelation modulo  $n$** .

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Kongruenz modulo  $n$

## Hilfssatz (Lemma)

Für zwei ganze Zahlen  $x, y$  sind die folgenden Aussagen äquivalent:

- 1  $x \equiv_n y$ ,
- 2  $(x - y) \bmod n = 0$ ,
- 3  $(y - x) \bmod n = 0$ ,
- 4  $x - y$  ist durch  $n$  teilbar.
- 5  $y - x$  ist durch  $n$  teilbar.

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Kongruenz modulo  $n$

## Hörsaalübung

- Gilt  $17 \equiv 2 \pmod{5}$  ?
- Gilt  $17 \equiv -3 \pmod{5}$  ?
- Gilt  $18 \equiv 25 \pmod{6}$  ?
- Gilt  $99 \equiv 123 \pmod{24}$  ?
- Welche Beziehung erfüllen die Jahreszahlen  $s$  derjenigen Jahre, in denen Olympische Sommerspiele (der Moderne) stattfanden bzw. stattfinden?
- Welche Beziehung erfüllen die Jahreszahlen  $w$  derjenigen Jahre, in denen Fußball-Weltmeisterschaften stattfanden bzw. stattfinden?
- Fanden im Jahr 1958 (im Jahr 1968) Olympische Sommerspiele statt?

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Kongruenz modulo  $n$

## Satz

Die Relation  $\equiv_n$  ist eine **Äquivalenzrelation**.



# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Kongruenz modulo  $n$

## Satz

Die Relation  $\equiv_n$  ist eine **Äquivalenzrelation**.

## Beweisskizze.

Reflexivität folgt aus  $x - x = 0 = 0 \cdot n$ , Symmetrie aus Lemma 9.

Transitivität: Falls  $x \equiv_n y$  und  $y \equiv_n z$  gilt, so existieren ganze Zahlen  $a$  bzw.  $a'$  mit  $x - y = a \cdot n$  bzw.  $y - z = a' \cdot n$ . Daraus folgt

$$x - z = (x - y) - (y - z) = (a - a') \cdot n.$$

Da  $a - a'$  ganzzahlig ist, gilt  $x \equiv_n z$  (vgl. Lemma 9). □

# Kongruenzrelationen

## Kongruenzklassen bzw. Restklassen

### Definition

- 1 Für jede Zahl  $z \in \mathbb{Z}$  bezeichne

$$[z] := [z]_{\equiv_n} := \left\{ x \in \mathbb{Z} \mid x \equiv_n z \right\}$$

die Äquivalenzklasse von  $z$  bezüglich  $\equiv_n$ .

- 2 Wir nennen  $[z]_{\equiv_n}$  auch **Restklasse von  $z$  modulo  $n$  in  $\mathbb{Z}$** .

- 3 Die Menge aller Restklassen modulo  $n$  in  $\mathbb{Z}$  bezeichnen wir mit  $\mathbb{Z}/_{\equiv_n}$  (sprich 'Restklassenmenge modulo  $n$ ') oder mit  $\mathbb{Z}/n\mathbb{Z}$  (sprich ' $\mathbb{Z}$  modulo  $n\mathbb{Z}$ '). Das Zeichen  $n\mathbb{Z}$  soll dabei symbolisieren, dass alle die Elemente äquivalent sind, die sich um ein Vielfaches von  $n$  voneinander unterscheiden, also um  $nz$  für ein  $z \in \mathbb{Z}$ .

# Kongruenzrelationen

## Beispiele von Restklassen

### Beispiel: Kongruenz modulo 2

$$[0]_{\equiv_2} = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

(gerade Zahlen)

$$[1]_{\equiv_2} = \{\dots, -3, -1, 1, 3, 5, \dots\}$$

(ungerade Zahlen)

$$[0]_{\equiv_2} = [2]_{\equiv_2} = [4]_{\equiv_2} = [-2]_{\equiv_2} = [-4]_{\equiv_2}, \dots$$

$$[1]_{\equiv_2} = [3]_{\equiv_2} = [5]_{\equiv_2} = [-1]_{\equiv_2} = [-3]_{\equiv_2}, \dots$$

$$\mathbb{Z}/_{\equiv_2} = \left\{ [0]_{\equiv_2}, [1]_{\equiv_2} \right\}$$

# Kongruenzrelationen

## Beispiele von Restklassen

### Beispiel: Kongruenz modulo 4

$$[0]_{\equiv_4} = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

$$[1]_{\equiv_4} = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

...

$$\mathbb{Z}/_{\equiv_4} = \left\{ [0]_{\equiv_4}, [1]_{\equiv_4}, [2]_{\equiv_4}, [3]_{\equiv_4} \right\}$$

# Modulare Arithmetik

Addition und Multiplikation in  $\mathbb{Z}/\equiv_n = \mathbb{Z}/n\mathbb{Z}$

Wir wollen mit Restklassen rechnen und erklären Addition und Multiplikation auf  $\mathbb{Z}/\equiv_n = \mathbb{Z}/n\mathbb{Z}$ .

# Modulare Arithmetik

Addition und Multiplikation in  $\mathbb{Z}/\equiv_n = \mathbb{Z}/n\mathbb{Z}$

Wir wollen mit Restklassen rechnen und erklären Addition und Multiplikation auf  $\mathbb{Z}/\equiv_n = \mathbb{Z}/n\mathbb{Z}$ .

## Definition

Sei  $n \geq 2$  fest gewählt und seien  $[x] := [x]_{\equiv_n}$ ,  $[y] := [y]_{\equiv_n}$  Restklassen in  $\mathbb{Z}/\equiv_n$ . Dann sei

$$[x] + [y] := [x + y],$$

$$[x] \cdot [y] := [x \cdot y].$$

# Modulare Arithmetik

Addition und Multiplikation in  $\mathbb{Z}/\equiv_n$

## Bemerkungen

- Wir halten ohne Beweis fest, dass die so erklärten Verknüpfungen **nicht** davon abhängen, welche Elemente  $x$  bzw.  $y$  der Restklasse gewählt werden (Wohldefiniertheit).
- In der Praxis wird ein festes Vertretersystem gewählt, zum Beispiel das System der kleinsten nichtnegativen Reste

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}.$$

### Bemerkung

Wenn von „modularer Arithmetik“ die Rede ist, kann Unterschiedliches gemeint sein. Da die unterschiedlichen Konzepte jedoch zum einen „äquivalent“ sind und es zum anderen bequem ist, die Unterschiede weder in Notation noch in Denk- und Sprechweise auszudrücken zu müssen, wird nicht immer in aller Schärfe unterschieden:

---

<sup>a</sup>Zur Überprüfung dieser recht überraschenden Aussage gibt es, wie wir noch sehen werden, auch andere Wege als  $1\,000\,000 = 999\,999 + 1 = 142\,857 \cdot 7 + 1$  auszurechnen.



### Bemerkung

Wenn von „modularer Arithmetik“ die Rede ist, kann Unterschiedliches gemeint sein. Da die unterschiedlichen Konzepte jedoch zum einen „äquivalent“ sind und es zum anderen bequem ist, die Unterschiede weder in Notation noch in Denk- und Sprechweise auszudrücken zu müssen, wird nicht immer in aller Schärfe unterschieden:

- Addition und Multiplikation in der Menge  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ , unter Verwendung der Operation  $\text{mod}$ .

Beispiel in  $\mathbb{Z}_8$ :  $\bar{3} \cdot \bar{7} = \overline{21} \text{ mod } 8 = \bar{5}$ .

---

<sup>a</sup>Zur Überprüfung dieser recht überraschenden Aussage gibt es, wie wir noch sehen werden, auch andere Wege als  $1\,000\,000 = 999\,999 + 1 = 142\,857 \cdot 7 + 1$  auszurechnen.

### Bemerkung

Wenn von „modularer Arithmetik“ die Rede ist, kann Unterschiedliches gemeint sein. Da die unterschiedlichen Konzepte jedoch zum einen „äquivalent“ sind und es zum anderen bequem ist, die Unterschiede weder in Notation noch in Denk- und Sprechweise auszudrücken zu müssen, wird nicht immer in aller Schärfe unterschieden:

- Addition und Multiplikation in der Menge  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ , unter Verwendung der Operation  $\text{mod}$ .

Beispiel in  $\mathbb{Z}_8$ :  $\bar{3} \cdot \bar{7} = \overline{21 \text{ mod } 8} = \bar{5}$ .

- Addition und Multiplikation in der Menge der Äquivalenzklassen (Quotientenmenge)  $\mathbb{Z}/\equiv_n$ , wobei, wie immer, wenn Repäsentanten zur Berechnung verwendet werden, die Frage der Wohldefiniertheit zu klären ist.

Beispiel in  $\mathbb{Z}/\equiv_4$ :  $[7]_4 + [10]_4 = [17]_4 = [1]_4$  und auch  $[3]_4 + [2]_4 = [5]_4 = [1]_4$ .

<sup>a</sup>Zur Überprüfung dieser recht überraschenden Aussage gibt es, wie wir noch sehen werden, auch andere Wege als  $1\,000\,000 = 999\,999 + 1 = 142\,857 \cdot 7 + 1$  auszurechnen.

### Bemerkung

Wenn von „modularer Arithmetik“ die Rede ist, kann Unterschiedliches gemeint sein. Da die unterschiedlichen Konzepte jedoch zum einen „äquivalent“ sind und es zum anderen bequem ist, die Unterschiede weder in Notation noch in Denk- und Sprechweise auszudrücken zu müssen, wird nicht immer in aller Schärfe unterschieden:

- Addition und Multiplikation in der Menge  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ , unter Verwendung der Operation  $\text{mod}$ .

Beispiel in  $\mathbb{Z}_8$ :  $\bar{3} \cdot \bar{7} = \overline{21 \text{ mod } 8} = \bar{5}$ .

- Addition und Multiplikation in der Menge der Äquivalenzklassen (Quotientenmenge)  $\mathbb{Z}/\equiv_n$ , wobei, wie immer, wenn Repäsentanten zur Berechnung verwendet werden, die Frage der Wohldefiniertheit zu klären ist.

Beispiel in  $\mathbb{Z}/\equiv_4$ :  $[7]_{\equiv_4} + [10]_{\equiv_4} = [17]_{\equiv_4} = [1]_{\equiv_4}$  und auch  $[3]_{\equiv_4} + [2]_{\equiv_4} = [5]_{\equiv_4} = [1]_{\equiv_4}$ .

- Addition und Multiplikation in der Menge  $\mathbb{Z}$  mit Nachschalten der Operation  $\text{mod}$ :

Beispiel<sup>a</sup>:  $10^6 \text{ mod } 7 = 1$ .

<sup>a</sup>Zur Überprüfung dieser recht überraschenden Aussage gibt es, wie wir noch sehen werden, auch andere Wege als  $1\,000\,000 = 999\,999 + 1 = 142\,857 \cdot 7 + 1$  auszurechnen.

# Modulare Arithmetik

Addition und Multiplikation in  $\mathbb{Z}/\equiv_4 = \mathbb{Z}/4\mathbb{Z}$

**Beispiel: Addition und Multiplikation in  $\mathbb{Z}/\equiv_4$**

$$[2] + [3] = [2 + 3] = [5] = [1]$$

$$[2] \cdot [3] = [2 \cdot 3] = [6] = [2]$$

# Modulare Arithmetik

Addition und Multiplikation in  $\mathbb{Z}/\equiv_4 = \mathbb{Z}/4\mathbb{Z}$

**Beispiel: Addition und Multiplikation in  $\mathbb{Z}/\equiv_4$**

$$[2] + [3] = [2 + 3] = [5] = [1]$$

$$[2] \cdot [3] = [2 \cdot 3] = [6] = [2]$$

**Alternative Notationen:**

$$2 + 3 \equiv_4 1 \quad \text{bzw.} \quad 2 + 3 \bmod 4 = 1$$

$$2 \cdot 3 \equiv_4 2 \quad \text{bzw.} \quad 2 \cdot 3 \bmod 4 = 2$$

# Modulare Arithmetik

Verknüpfungstabeln für  $\mathbb{Z}/\equiv_2$  bzw.  $\mathbb{Z}/2\mathbb{Z}$

Die Verknüpfungstabeln für Addition und Multiplikation in  $\mathbb{Z}/\equiv_2$  bzw.  $\mathbb{Z}/2\mathbb{Z}$  sind wie folgt:

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

·	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

# Modulare Arithmetik

Verknüpfungstabeln für  $\mathbb{Z}/\equiv_6$  bzw.  $\mathbb{Z}/6\mathbb{Z}$ .

## Hörsaalübung

Wir stellen die Additions- und die Multiplikationstafel in  $\mathbb{Z}/\equiv_6$  bzw.  $\mathbb{Z}/6\mathbb{Z}$  auf; zur Vereinfachung wählen wir die Reste als Repräsentanten der Restklassen, um die eckigen Klammern nicht mehr zu schreiben.

+	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

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2			2	
3	0	3		3		
4	0	4		0		
5	0	5				1

# Modulare Arithmetik

Multiplikation in  $\mathbb{Z}/\equiv_6 = \mathbb{Z}/6\mathbb{Z}$

## Bemerkungen:

- Wir stellen fest, dass es Elemente in  $\mathbb{Z}/\equiv_6$  bzw.  $\mathbb{Z}/6\mathbb{Z}$  gibt, die **keine** multiplikative Inverse besitzen bzw. **Nullteiler** sind.
- Dagegen besitzen die Elemente 1 und 5 jeweils multiplikative Inverse.
- Wir halten fest, dass 1 und 6 bzw. 5 und 6 jeweils **teilerfremd** sind, d.h. es gilt  $\text{ggT}(1, 6) = 1$  und  $\text{ggT}(5, 6) = 1$ .



# Modulare Arithmetik

Einheiten in  $\mathbb{Z}/\equiv_n$  bzw.  $\mathbb{Z}/n\mathbb{Z}$

## Definition

Ein Element  $x \neq 0$  in  $\mathbb{Z}/n\mathbb{Z}$  heißt **Einheit** in  $\mathbb{Z}/n\mathbb{Z}$ , wenn es eine multiplikative Inverse in  $\mathbb{Z}/n\mathbb{Z}$  besitzt.

# Modulare Arithmetik

Einheiten in  $\mathbb{Z}/\equiv_n$  bzw.  $\mathbb{Z}/n\mathbb{Z}$

## Definition

Ein Element  $x \neq 0$  in  $\mathbb{Z}/n\mathbb{Z}$  heißt **Einheit** in  $\mathbb{Z}/n\mathbb{Z}$ , wenn es eine multiplikative Inverse in  $\mathbb{Z}/n\mathbb{Z}$  besitzt.

## Satz

Ein Element  $x \neq 0$  in  $\mathbb{Z}/n\mathbb{Z}$  ist genau dann eine Einheit in  $\mathbb{Z}/n\mathbb{Z}$ , wenn  $\text{ggT}(x, n) = 1$  gilt.

# Modulare Arithmetik

## Eulersche Phi-Funktion

### Definition

Es sei  $n \geq 1$ . Dann bezeichne  $\varphi(n)$  die **Anzahl** der Einheiten in  $\mathbb{Z}/n\mathbb{Z}$ .

# Modulare Arithmetik

## Eulersche Phi-Funktion

### Definition

Es sei  $n \geq 1$ . Dann bezeichne  $\varphi(n)$  die **Anzahl** der Einheiten in  $\mathbb{Z}/n\mathbb{Z}$ .

### Beispiel

Es gilt  $\varphi(6) = 2$ , denn die Einheiten in  $\mathbb{Z}/6\mathbb{Z}$  sind, wie gesehen, die beiden Elemente 1 und 5.

# Modulare Arithmetik

## Eulersche Phi-Funktion

### Hörsaalübung

Wir bestimmen die Werte von  $\varphi(n)$  für  $1 \leq n \leq 12$ . Hierzu listen wir jeweils die Menge  $E(n)$  der (zu  $n$  **teilerfremden**) Zahlen  $x$  mit  $1 \leq x \leq n$  und  $\text{ggT}(x, n) = 1$  auf und bestimmen  $\varphi(n) = |E(n)|$ :

$n$	$E(n)$	$\varphi(n)$	$n$	$E(n)$	$\varphi(n)$
1	{1}	1	7	{1, 2, 4, 5, 7, 8}	6
2	{1}	1	8		
3	{1, 2}	2	9		
4	{1, 3}	2	10		
5			11		
6	{1, 5}	2	12		

Ende RSA-Sitzung 1 am 01.06.2021

### Primzahlen und eulersche Phi-Funktion

Wir formulieren drei wichtige Resultate über die eulersche Phi-Funktion. Hierzu sei daran erinnert, dass wir unter einer **Primzahl** eine ganze Zahl  $p > 1$  verstehen, deren Teiler genau die Zahlen 1 und  $p$  sind.

### Primzahlen und eulersche Phi-Funktion

Wir formulieren drei wichtige Resultate über die eulersche Phi-Funktion. Hierzu sei daran erinnert, dass wir unter einer **Primzahl** eine ganze Zahl  $p > 1$  verstehen, deren Teiler genau die Zahlen 1 und  $p$  sind.

### Satz

- 1 Es sei  $p$  eine Primzahl. Dann gilt  $\varphi(p) = p - 1$ .
- 2 Es seien  $p$  und  $q$  zwei voneinander verschiedene Primzahlen. Dann gilt
$$\varphi(p \cdot q) = (p - 1) \cdot (q - 1).$$
- 3 Es seien  $p$ ,  $q$  und  $r$  drei (paarweise) voneinander verschiedene Primzahlen. Dann gilt

$$\varphi(p \cdot q \cdot r) = (p - 1) \cdot (q - 1) \cdot (r - 1).$$

# Modulare Arithmetik

## Eulersche Phi-Funktion

Vor dem Beweis des vorstehenden Satzes betrachten wir

### Beispiele

$$\varphi(5) = 5 - 1 = 4 \quad (\text{nach } 1)$$

$$\varphi(6) = \varphi(2 \cdot 3) = (2 - 1) \cdot (3 - 2) = 1 \cdot 2 = 2 \quad (\text{nach } 2)$$

$$\varphi(15) = \varphi(3 \cdot 5) = (3 - 1) \cdot (5 - 1) = 2 \cdot 4 = 8 \quad (\text{nach } 2)$$

$$\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = (2 - 1) \cdot (3 - 1) \cdot (5 - 1) = 8 \quad (\text{nach } 3)$$



# Modulare Arithmetik

## Eulersche Phi-Funktion

Vor dem Beweis des vorstehenden Satzes betrachten wir

### Beispiele

$$\varphi(5) = 5 - 1 = 4 \quad (\text{nach 1})$$

$$\varphi(6) = \varphi(2 \cdot 3) = (2 - 1) \cdot (3 - 1) = 1 \cdot 2 = 2 \quad (\text{nach 2})$$

$$\varphi(15) = \varphi(3 \cdot 5) = (3 - 1) \cdot (5 - 1) = 2 \cdot 4 = 8 \quad (\text{nach 2})$$

$$\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = (2 - 1) \cdot (3 - 1) \cdot (5 - 1) = 8 \quad (\text{nach 3})$$

### Warnung

Die Werte  $\varphi(9)$  und  $\varphi(12)$  etwa lassen sich **nicht** mit dem vorstehenden Satz bestimmen. Denn 9 und 12 sind weder Primzahlen noch besitzen sie Zerlegungen in zwei bzw. drei voneinander verschiedene Primzahlen:

$$9 = 3 \cdot 3, \quad 12 = 2 \cdot 2 \cdot 3, \quad \varphi(9) = 6 \neq (3-1) \cdot (3-1), \quad \varphi(12) = 4 \neq (2-1) \cdot (2-1) \cdot (3-1).$$

# Modulare Arithmetik

## Beweis des Satzes über die Eulersche Phi-Funktion

### Beweis:

- 1 Wenn  $p$  eine Primzahl ist, so sind die Zahlen  $1, 2, \dots, p - 1$  sämtlich teilerfremd zu  $p$ . Damit gilt  $\varphi(p) = p - 1$ .
- 2 Es seien  $p$  und  $q$  zwei voneinander verschiedene Primzahlen. Wir zählen zunächst die natürlichen Zahlen  $x$  mit  $1 \leq x \leq p \cdot q$ , die **nicht** teilerfremd zu  $p \cdot q$  sind: Es sind dies zum einen die Produkte

$$1 \cdot p, 2 \cdot p, \dots, q \cdot p,$$

ferner die Produkte

$$1 \cdot q, 2 \cdot q, \dots, (p - 1) \cdot q,$$

insgesamt also  $q + (p - 1)$  Zahlen.

### Fortsetzung des Beweises

Da  $q + (p - 1)$  Zahlen gemeinsame Teiler mit  $p \cdot q$  besitzen, verbleiben

$$p \cdot q - (q + p - 1)$$

Zahlen, die **teilerfremd** zu  $p \cdot q$  sind.

Wegen

$$p \cdot q - (q + p - 1) = p \cdot q - p - q + 1 = (p - 1) \cdot (q - 1)$$

folgt insgesamt  $\varphi(p \cdot q) = (p - 1) \cdot (q - 1)$ .

# Modulare Arithmetik

## Beweis von Satz 25

### Fortsetzung des Beweises

Da  $q + (p - 1)$  Zahlen gemeinsame Teiler mit  $p \cdot q$  besitzen, verbleiben

$$p \cdot q - (q + p - 1)$$

Zahlen, die **teilerfremd** zu  $p \cdot q$  sind.

Wegen

$$p \cdot q - (q + p - 1) = p \cdot q - p - q + 1 = (p - 1) \cdot (q - 1)$$

folgt insgesamt  $\varphi(p \cdot q) = (p - 1) \cdot (q - 1)$ .

### Hausübung

Verwenden Sie ähnliche Abzählungen, um Teil 3 des Satzes zu beweisen.

### Primzahlen und eulersche Phi-Funktion – allgemeiner Fall

Um den Wert der eulerschen Phi-Funktion für jede beliebige natürliche Zahl auszurechnen, macht man sich die folgenden Resultate<sup>a</sup> zunutze:

---

<sup>a</sup>Siehe etwa *Elementare und algebraische Zahlentheorie* von S. Müller-Stach und J. Piontkowski, vieweg.

### Primzahlen und eulersche Phi-Funktion – allgemeiner Fall

Um den Wert der eulerschen Phi-Funktion für jede beliebige natürliche Zahl auszurechnen, macht man sich die folgenden Resultate<sup>a</sup> zunutze:

- 1 Wenn  $n = p^r$  eine **Primzahlpotenz** ist, so gilt  $\varphi(n) = p^{r-1} \cdot (p - 1)$

<sup>a</sup>Siehe etwa *Elementare und algebraische Zahlentheorie* von S. Müller-Stach und J. Piontkowski, vieweg.

### Primzahlen und eulersche Phi-Funktion – allgemeiner Fall

Um den Wert der eulerschen Phi-Funktion für jede beliebige natürliche Zahl auszurechnen, macht man sich die folgenden Resultate<sup>a</sup> zunutze:

- 1 Wenn  $n = p^r$  eine **Primzahlpotenz** ist, so gilt  $\varphi(n) = p^{r-1} \cdot (p - 1)$
- 2 Wenn  $n$  die **Primzfaktorzerlegung**  $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_N^{r_N}$  besitzt, so gilt

$$\varphi(n) = p_1^{r_1-1} \cdot (p_1 - 1) \cdot p_2^{r_2-1} \cdot (p_2 - 1) \cdot \dots \cdot p_N^{r_N-1} \cdot (p_N - 1).$$

<sup>a</sup>Siehe etwa *Elementare und algebraische Zahlentheorie* von S. Müller-Stach und J. Piontkowski, vieweg.

### Primzahlen und eulersche Phi-Funktion – allgemeiner Fall

Um den Wert der eulerschen Phi-Funktion für jede beliebige natürliche Zahl auszurechnen, macht man sich die folgenden Resultate<sup>a</sup> zunutze:

- 1 Wenn  $n = p^r$  eine **Primzahlpotenz** ist, so gilt  $\varphi(n) = p^{r-1} \cdot (p - 1)$
- 2 Wenn  $n$  die **Primzfaktorzerlegung**  $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_N^{r_N}$  besitzt, so gilt

$$\varphi(n) = p_1^{r_1-1} \cdot (p_1 - 1) \cdot p_2^{r_2-1} \cdot (p_2 - 1) \cdot \dots \cdot p_N^{r_N-1} \cdot (p_N - 1).$$

<sup>a</sup>Siehe etwa *Elementare und algebraische Zahlentheorie* von S. Müller-Stach und J. Piontkowski, vieweg.

### Beispiele

- 1 Für  $n = 9 = 3^2$  gilt nach der ersten der obigen Formeln  $\varphi(9) = 3^{2-1} \cdot (3 - 1) = 6$



### Primzahlen und eulersche Phi-Funktion – allgemeiner Fall

Um den Wert der eulerschen Phi-Funktion für jede beliebige natürliche Zahl auszurechnen, macht man sich die folgenden Resultate<sup>a</sup> zunutze:

- 1 Wenn  $n = p^r$  eine **Primzahlpotenz** ist, so gilt  $\varphi(n) = p^{r-1} \cdot (p - 1)$
- 2 Wenn  $n$  die **Primfaktorzerlegung**  $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_N^{r_N}$  besitzt, so gilt

$$\varphi(n) = p_1^{r_1-1} \cdot (p_1 - 1) \cdot p_2^{r_2-1} \cdot (p_2 - 1) \cdot \dots \cdot p_N^{r_N-1} \cdot (p_N - 1).$$

<sup>a</sup>Siehe etwa *Elementare und algebraische Zahlentheorie* von S. Müller-Stach und J. Piontkowski, vieweg.

### Beispiele

- 1 Für  $n = 9 = 3^2$  gilt nach der ersten der obigen Formeln  $\varphi(9) = 3^{2-1} \cdot (3 - 1) = 6$
- 2 Die Zahl  $n = 12$  hat die Primfaktorzerlegung  $12 = 2^2 \cdot 3^1$ . Nach der zweiten Formel ist  $\varphi(12) = 2^{2-1} \cdot (2 - 1) \cdot 3^{1-1} \cdot (3 - 1) = 4$ .

### Primzahlen und eulersche Phi-Funktion – allgemeiner Fall

Um den Wert der eulerschen Phi-Funktion für jede beliebige natürliche Zahl auszurechnen, macht man sich die folgenden Resultate<sup>a</sup> zunutze:

- 1 Wenn  $n = p^r$  eine **Primzahlpotenz** ist, so gilt  $\varphi(n) = p^{r-1} \cdot (p - 1)$
- 2 Wenn  $n$  die **Primfaktorzerlegung**  $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_N^{r_N}$  besitzt, so gilt

$$\varphi(n) = p_1^{r_1-1} \cdot (p_1 - 1) \cdot p_2^{r_2-1} \cdot (p_2 - 1) \cdot \dots \cdot p_N^{r_N-1} \cdot (p_N - 1).$$

<sup>a</sup>Siehe etwa *Elementare und algebraische Zahlentheorie* von S. Müller-Stach und J. Piontkowski, vieweg.

### Beispiele

- 1 Für  $n = 9 = 3^2$  gilt nach der ersten der obigen Formeln  $\varphi(9) = 3^{2-1} \cdot (3 - 1) = 6$
- 2 Die Zahl  $n = 12$  hat die Primfaktorzerlegung  $12 = 2^2 \cdot 3^1$ . Nach der zweiten Formel ist  $\varphi(12) = 2^{2-1} \cdot (2 - 1) \cdot 3^{1-1} \cdot (3 - 1) = 4$ .

Tatsächlich sind es genau die sechs Zahlen 1, 2, 4, 5, 7 und 8, die mit 9 nur den Teiler 1 gemein haben; und es sind genau die vier Zahlen 1, 5, 7 und 11 zu 12 teilerfremd.

### Hausübung:

Bestimmen Sie die Werte von  $\varphi(81) = \varphi(3^4)$  und  $\varphi(72) = \varphi(2^3 \cdot 3^2)$

- mit den angegebenen Formeln,
- (zur Kontrolle) durch Abzählung der zur jeweiligen Zahl  $n$  teilerfremden Zahlen.

### Hausübung:

Bestimmen Sie die Werte von  $\varphi(81) = \varphi(3^4)$  und  $\varphi(72) = \varphi(2^3 \cdot 3^2)$

- mit den angegebenen Formeln,
- (zur Kontrolle) durch Abzählung der zur jeweiligen Zahl  $n$  teilerfremden Zahlen.

### Bemerkung

Keine Angst vor dem Abzählen! Zum Beispiel lässt sich die Liste der natürlichen Zahlen kleiner 72, die mit 72 nur den Teiler 1 gemein haben, also weder durch 2 noch durch 3 teilbar sind, sehr schön übersichtlich darstellen:

1, 5, 7, 11, 13, 17,  
19, 23, 25, 29, 31, 35,  
37, 41, 43, 47, 49, 53,  
55, 59, 61, 65, 67, 71.

Seien Sie

KHUCOLFK ZLOONRPPHQ

bei den mathematischen Grundlagen von Systemen zur Daten-, Kommunikations- und Transaktionssicherheit.

Na, alles klar?

### Sicherheitsaspekte bei Kommunikation

Bei jeder Art von Kommunikation besteht die Möglichkeit der Verletzung

### Sicherheitsaspekte bei Kommunikation

Bei jeder Art von Kommunikation besteht die Möglichkeit der Verletzung

- 1 der Vertraulichkeit / Geheimhaltung,

### Sicherheitsaspekte bei Kommunikation

Bei jeder Art von Kommunikation besteht die Möglichkeit der Verletzung

- 1 der Vertraulichkeit / Geheimhaltung,
- 2 der Nachrichtenintegrität bzw. Nachrichtenechtheit,



### Sicherheitsaspekte bei Kommunikation

Bei jeder Art von Kommunikation besteht die Möglichkeit der Verletzung

- 1 der Vertraulichkeit / Geheimhaltung,
- 2 der Nachrichtenintegrität bzw. Nachrichtenechtheit,
- 3 der Authentizität des Absenders.

# Kryptographie

Einführung ins Verschlüsseln und Entschlüsseln

**$A$  sendet  $B$  eine (Klartext-)Nachricht  $m$ :**

„Rendez-vous morgen um 11.00 Uhr. Gruß, Alice.“

# Kryptographie

Einführung ins Verschlüsseln und Entschlüsseln

**$A$  sendet  $B$  eine (Klartext-)Nachricht  $m$ :**

„Rendez-vous morgen um 11.00 Uhr. Gruß, Alice.“

**Verletzung der Vertraulichkeit**

$E$  hört / liest mit.

# Kryptographie

Einführung ins Verschlüsseln und Entschlüsseln

**A sendet B eine (Klartext-)Nachricht  $m$ :**

„Rendez-vous morgen um 11.00 Uhr. Gruß, Alice.“

**Verletzung der Vertraulichkeit**

$E$  hört / liest mit.

**Verletzung der Nachrichtenintegrität**

$E$  fängt  $m$  ab und schickt  $m'$  an  $B$  weiter:

„Rendez-vous morgen um 13.00 Uhr. Gruß, Alice.“

# Kryptographie

## Einführung ins Verschlüsseln und Entschlüsseln

**A sendet B eine (Klartext-)Nachricht  $m$ :**

„Rendez-vous morgen um 11.00 Uhr. Gruß, Alice.“

**Verletzung der Vertraulichkeit**

$E$  hört / liest mit.

**Verletzung der Nachrichtenintegrität**

$E$  fängt  $m$  ab und schickt  $m'$  an  $B$  weiter:

„Rendez-vous morgen um 13.00 Uhr. Gruß, Alice.“

**Verletzung der Authentizität**

$E$  fängt  $m$  ab und schickt sie mit eigener Unterschrift an  $B$  weiter:

„Rendez-vous morgen um 11.00 Uhr. Gruß, Eve.“

# Kryptographie

Einführung ins Verschlüsseln und Entschlüsseln

## Abhilfe: Verschlüsselung (Chiffrierung)

Es gibt viele verschiedene Methoden zur Verschlüsselung (Chiffrierung) von Nachrichten.

### Abhilfe: Verschlüsselung (Chiffrierung)

Es gibt viele verschiedene Methoden zur Verschlüsselung (Chiffrierung) von Nachrichten.

### Bemerkung

Vom **Chiffrieren** zu unterscheiden ist das **Codieren**, letzteres wird nicht zur Sicherung vor Angriffen, sondern aus anderen Gründen vorgenommen (z.B. Konversion von Text in Zahlen, Nutzung technischer Übertragungskanäle, die Störungen ausgesetzt sind, usw.).

### Verschiebechiffren

Ein sehr einfacher (und daher auch sehr unsicherer) Typ von Chiffren sind die sogenannten **Verschiebechiffren**. Schon Julius Cäsar soll die zyklische Verschiebung um 3 Buchstaben im Alphabet verwendet haben:



### Verschiebechiffren

Ein sehr einfacher (und daher auch sehr unsicherer) Typ von Chiffren sind die sogenannten **Verschiebechiffren**. Schon Julius Cäsar soll die zyklische Verschiebung um 3 Buchstaben im Alphabet verwendet haben:

### Cäsars Chiffre

### Verschiebechiffren

Ein sehr einfacher (und daher auch sehr unsicherer) Typ von Chiffren sind die sogenannten **Verschiebechiffren**. Schon Julius Cäsar soll die zyklische Verschiebung um 3 Buchstaben im Alphabet verwendet haben:

### Cäsars Chiffre

- Beim Verschlüsseln (Chiffrieren) wird jeder Buchstabe des Klartextalphabets durch den entsprechenden Buchstaben des Geheimtextalphabets ersetzt ( $a \rightarrow D, b \rightarrow E, \dots, z \rightarrow C$ ).

### Verschiebechiffren

Ein sehr einfacher (und daher auch sehr unsicherer) Typ von Chiffren sind die sogenannten **Verschiebechiffren**. Schon Julius Cäsar soll die zyklische Verschiebung um 3 Buchstaben im Alphabet verwendet haben:

### Cäsars Chiffre

- Beim Verschlüsseln (Chiffrieren) wird jeder Buchstabe des Klartextalphabets durch den entsprechenden Buchstaben des Geheimtextalphabets ersetzt ( $a \rightarrow D, b \rightarrow E, \dots, z \rightarrow C$ ).
- Beim Entschlüsseln (Dechiffrieren) wird genau umgekehrt verfahren:  $A \rightarrow x, B \rightarrow y, \dots, Z \rightarrow w$ .

# Kryptographie

Einführung ins Verschlüsseln und Entschlüsseln

## Cäsars Chiffre

Klartextalphabet	a	b	c	d	e	...	w	x	y	z
Geheimtextalphabet	D	E	F	G	H	...	Z	A	B	C

# Kryptographie

## Einführung ins Verschlüsseln und Entschlüsseln

### Cäsars Chiffre

Klartextalphabet	a	b	c	d	e	...	w	x	y	z
Geheimtextalphabet	D	E	F	G	H	...	Z	A	B	C

### Hörsaalübung

[Entschlüsselung des eingangs verschlüsselten Grußes] Der Geheimtext KHUCOLFK ZLOONRPPHQ wird (durch Rückverschiebung um drei Buchstaben) dechiffriert zu  
....

# Kategorien kryptographischer Verfahren

## Kategorien kryptographischer Verfahren

Verschlüsselungs- bzw. Entschlüsselungsverfahren (Chiffren, Kryptosysteme) werden unterschieden in

# Kategorien kryptographischer Verfahren

## Kategorien kryptographischer Verfahren

Verschlüsselungs- bzw. Entschlüsselungsverfahren (Chiffren, Kryptosysteme) werden unterschieden in

- **symmetrische** Verfahren (engl. **private-key cryptosystems**) und

# Kategorien kryptographischer Verfahren

## Kategorien kryptographischer Verfahren

Verschlüsselungs- bzw. Entschlüsselungsverfahren (Chiffren, Kryptosysteme) werden unterschieden in

- **symmetrische** Verfahren (engl. **private-key cryptosystems**) und
- **asymmetrische** Verfahren (engl. **public-key cryptosystems**).



# Kategorien kryptographischer Verfahren

## Symmetrische Verfahren

### Symmetrische Verfahren

Sender A und Empfänger B vereinbaren einen Schlüssel  $k$ . Eine Klartextnachricht  $m$  wird mithilfe einer Funktion  $f_k$ , die vom Schlüssel  $k$  abhängt, verschlüsselt, es entsteht die Geheimnachricht  $c$ :

$$c = f_k(m).$$

# Kategorien kryptographischer Verfahren

## Symmetrische Verfahren

### Symmetrische Verfahren

Sender A und Empfänger B vereinbaren einen Schlüssel  $k$ . Eine Klartextnachricht  $m$  wird mithilfe einer Funktion  $f_k$ , die vom Schlüssel  $k$  abhängt, verschlüsselt, es entsteht die Geheimnachricht  $c$ :

$$c = f_k(m).$$

Die Entschlüsselung erfolgt mit der Umkehrfunktion  $f_k^{-1}$  von  $f_k$ . Aus der Geheimnachricht  $c$  entsteht wieder die Klartextnachricht  $m$ :

$$m = f_k^{-1}(f_k(m)) = f_k^{-1}(c).$$

# Kategorien kryptographischer Verfahren

## Symmetrische Verfahren

### Beispiele symmetrischer Verfahren

# Kategorien kryptographischer Verfahren

## Symmetrische Verfahren

### Beispiele symmetrischer Verfahren

- Advanced Encryption Standard (AES):  
aktuelles, sehr sicheres Verfahren

# Kategorien kryptographischer Verfahren

## Symmetrische Verfahren

### Beispiele symmetrischer Verfahren

- Advanced Encryption Standard (AES):  
aktuelles, sehr sicheres Verfahren
- Data Encryption Standard (DES):  
Vorgänger des AES, heute obsolet, weil durch **brute-force attacks** bzw. **exhaustive key searches** mit heutigen Rechnerleistungen angreifbar.

# Kategorien kryptographischer Verfahren

## Symmetrische Verfahren

### Nachteil symmetrischer Verfahren

Vor Beginn der eigentlichen Kommunikations muss ein Schlüssel vereinbart und kommuniziert werden. Dieser Schlüsselaustausch erfolgt notwendigerweise über irgend einen Kommunikationskanal und ist somit prinzipiell gefährdet (durch Mithören, Abhören, Mitschneiden, etc.).

# Kategorien kryptographischer Verfahren

Asymmetrische Verfahren - public-key systems

## Asymmetrische Verfahren

# Kategorien kryptographischer Verfahren

## Asymmetrische Verfahren - public-key systems

### Asymmetrische Verfahren

- Jede/r Teilnehmer/in hat einen öffentlichen Schlüssel  $e$  und einen geheimen („privaten“) Schlüssel  $d$ . Der öffentliche Schlüssel wird in einem Verzeichnis ähnlich wie in einem Telefonbuch veröffentlicht.



# Kategorien kryptographischer Verfahren

Asymmetrische Verfahren - public-key systems

## Asymmetrische Verfahren

- Jede/r Teilnehmer/in hat einen öffentlichen Schlüssel  $e$  und einen geheimen („privaten“) Schlüssel  $d$ . Der öffentliche Schlüssel wird in einem Verzeichnis ähnlich wie in einem Telefonbuch veröffentlicht.
- Möchte A eine Nachricht  $m$  verschlüsselt an B senden, so verwendet A den öffentlichen Schlüssel  $e$  von B und das vereinbarte Verfahren  $f_e$  zum Chiffrieren:

$$c = f_e(m).$$

# Kategorien kryptographischer Verfahren

Asymmetrische Verfahren - public-key systems

## Asymmetrische Verfahren - Fortsetzung

# Kategorien kryptographischer Verfahren

## Asymmetrische Verfahren - public-key systems

### Asymmetrische Verfahren - Fortsetzung

- Der Empfänger B verwendet seinen privaten Schlüssel  $d$  und eine davon abhängige Funktion  $g_d$  zum Dechiffrieren:

$$m = g_d(c).$$

# Kategorien kryptographischer Verfahren

Asymmetrische Verfahren - public-key systems

## Asymmetrische Verfahren - Fortsetzung

- Der Empfänger B verwendet seinen privaten Schlüssel  $d$  und eine davon abhängige Funktion  $g_d$  zum Dechiffrieren:

$$m = g_d(c).$$

- Jeder Teilnehmer errechnet seinen privaten Schlüssel mithilfe einer (nur ihm bekannten) sogenannten **Einwegfunktion** aus dem öffentlichen Schlüssel. Natürlich muss es sehr schwierig bis unmöglich sein, allein aus der Kenntnis des öffentlichen Schlüssels den privaten Schlüssel zu bestimmen.

# Kategorien kryptographischer Verfahren

Asymmetrische Verfahren - public-key systems

## Asymmetrische Verfahren

# Kategorien kryptographischer Verfahren

## Asymmetrische Verfahren - public-key systems

### Asymmetrische Verfahren

- Es gibt *tatsächlich* Einwegfunktionen, mit denen man (mit geeigneter Zusatzinformation) aus einem gegebenen Chiffrierschlüssel  $e$  einen (funktionierenden) Dechiffrierschlüssel  $d$  relativ problemlos errechnen kann, während diese Berechnung ohne Zusatzinformation nur mit extrem hohem Aufwand möglich ist.

# Kategorien kryptographischer Verfahren

## Asymmetrische Verfahren - public-key systems

### Asymmetrische Verfahren

- Es gibt *tatsächlich* Einwegfunktionen, mit denen man (mit geeigneter Zusatzinformation) aus einem gegebenen Chiffrierschlüssel  $e$  einen (funktionierenden) Dechiffrierschlüssel  $d$  relativ problemlos errechnen kann, während diese Berechnung ohne Zusatzinformation nur mit extrem hohem Aufwand möglich ist.
- Das RSA-Verfahren (benannt nach Rivest, Shamir und Adleman, 1977) ist ein Beispiel für ein asymmetrisches Verfahren, das (mit gewissen Modifikationen) auch in der Praxis angewandt wird.

# Das RSA-Verfahren

## Überblick

### Darstellung des RSA-Verfahrens – Überblick:



# Das RSA-Verfahren

## Überblick

### Darstellung des RSA-Verfahrens – Überblick:

- Grundlage der Sicherheit des RSA-Verfahrens

# Das RSA-Verfahren

## Überblick

### Darstellung des RSA-Verfahrens – Überblick:

- Grundlage der Sicherheit des RSA-Verfahrens
- Schlüsselerzeugung: Öffentlicher und privater Schlüssel

# Das RSA-Verfahren

## Überblick

### Darstellung des RSA-Verfahrens – Überblick:

- Grundlage der Sicherheit des RSA-Verfahrens
- Schlüsselerzeugung: Öffentlicher und privater Schlüssel
- Verschlüsselung und Entschlüsselung von Zahlen bzw. Nachrichten

# Das RSA-Verfahren

Grundlage der Sicherheit des RSA-Verfahrens

## Grundlage der Sicherheit des RSA-Verfahrens

# Das RSA-Verfahren

## Grundlage der Sicherheit des RSA-Verfahrens

### Grundlage der Sicherheit des RSA-Verfahrens

- Mit heute bekannten (echten oder stochastischen) Primzahltests lässt sich auch bei großen Stellenzahlen herausfinden, ob eine Zahl (mit sehr hoher Wahrscheinlichkeit) eine Primzahl ist oder nicht.

# Das RSA-Verfahren

## Grundlage der Sicherheit des RSA-Verfahrens

### Grundlage der Sicherheit des RSA-Verfahrens

- Mit heute bekannten (echten oder stochastischen) Primzahltests lässt sich auch bei großen Stellenzahlen herausfinden, ob eine Zahl (mit sehr hoher Wahrscheinlichkeit) eine Primzahl ist oder nicht.
- Dagegen ist die Faktorisierung großer Zahlen, also ihre Zerlegung in ihre Primfaktoren mit den heute bekannten Verfahren im Allgemeinen praktisch nicht durchführbar.

# Das RSA-Verfahren

## Schlüsselerzeugung

### Schlüsselerzeugung beim RSA-Verfahren

Ein öffentlicher Schlüssel ist ein Paar natürlicher Zahlen  $(n, e)$ , der zugehörige private Schlüssel ein Paar  $(n, d)$ . Hierbei heißt  $n$  **RSA-Modul**,  $e$  **Verschlüsselungsexponent** und  $d$  **Entschlüsselungsexponent**.

# Das RSA-Verfahren

## Schlüsselerzeugung

### Schlüsselerzeugung beim RSA-Verfahren

Ein öffentlicher Schlüssel ist ein Paar natürlicher Zahlen  $(n, e)$ , der zugehörige private Schlüssel ein Paar  $(n, d)$ . Hierbei heißt  $n$  **RSA-Modul**,  $e$  **Verschlüsselungsexponent** und  $d$  **Entschlüsselungsexponent**.

- Wähle zwei (große) voneinander verschiedene Primzahlen  $p$  und  $q$ , berechne den **RSA-Modul**  $n := p \cdot q$



# Das RSA-Verfahren

## Schlüsselerzeugung

### Schlüsselerzeugung beim RSA-Verfahren

Ein öffentlicher Schlüssel ist ein Paar natürlicher Zahlen  $(n, e)$ , der zugehörige private Schlüssel ein Paar  $(n, d)$ . Hierbei heißt  $n$  **RSA-Modul**,  $e$  **Verschlüsselungsexponent** und  $d$  **Entschlüsselungsexponent**.

- Wähle zwei (große) voneinander verschiedene Primzahlen  $p$  und  $q$ , berechne den **RSA-Modul**  $n := p \cdot q$
- Berechne  $\varphi(n) = (p - 1) \cdot (q - 1)$ , vgl. Satz 25.

# Das RSA-Verfahren

## Schlüsselerzeugung

### Schlüsselerzeugung beim RSA-Verfahren

Ein öffentlicher Schlüssel ist ein Paar natürlicher Zahlen  $(n, e)$ , der zugehörige private Schlüssel ein Paar  $(n, d)$ . Hierbei heißt  $n$  **RSA-Modul**,  $e$  **Verschlüsselungsexponent** und  $d$  **Entschlüsselungsexponent**.

- Wähle zwei (große) voneinander verschiedene Primzahlen  $p$  und  $q$ , berechne den **RSA-Modul**  $n := p \cdot q$
- Berechne  $\varphi(n) = (p - 1) \cdot (q - 1)$ , vgl. Satz 25.
- Wähle eine Zahl  $e$  mit  $\text{ggT}(e, \varphi(n)) = 1$  und  $1 < e < \varphi(n)$ .

# Das RSA-Verfahren

## Schlüsselerzeugung

### Schlüsselerzeugung beim RSA-Verfahren

Ein öffentlicher Schlüssel ist ein Paar natürlicher Zahlen  $(n, e)$ , der zugehörige private Schlüssel ein Paar  $(n, d)$ . Hierbei heißt  $n$  **RSA-Modul**,  $e$  **Verschlüsselungsexponent** und  $d$  **Entschlüsselungsexponent**.

- Wähle zwei (große) voneinander verschiedene Primzahlen  $p$  und  $q$ , berechne den **RSA-Modul**  $n := p \cdot q$
- Berechne  $\varphi(n) = (p - 1) \cdot (q - 1)$ , vgl. Satz 25.
- Wähle eine Zahl  $e$  mit  $\text{ggT}(e, \varphi(n)) = 1$  und  $1 < e < \varphi(n)$ .
- Bestimme die multiplikative Inverse  $d$  von  $e$  modulo  $\varphi(n)$ , löse also die Gleichung

$$e \cdot d \bmod \varphi(n) = 1 \quad \text{bzw.} \quad e \cdot d \equiv_{\varphi(n)} 1.$$

# Das RSA-Verfahren

## Schlüsselerzeugung

### Schlüsselerzeugung beim RSA-Verfahren:

# Das RSA-Verfahren

## Schlüsselerzeugung

### Schlüsselerzeugung beim RSA-Verfahren:

- In der Praxis werden zwei hinreichend große natürliche Zahlen ausgewählt und durch Primzahltests geprüft, dies solange, bis zwei Primzahlen  $p$  und  $q$  der gewünschten Länge gefunden sind.

# Das RSA-Verfahren

## Schlüsselerzeugung

### Schlüsselerzeugung beim RSA-Verfahren:

- In der Praxis werden zwei hinreichend große natürliche Zahlen ausgewählt und durch Primzahltests geprüft, dies solange, bis zwei Primzahlen  $p$  und  $q$  der gewünschten Länge gefunden sind.
- Für den Verschlüsselungsexponenten  $e$  wird in der Praxis oft die Fermat-Zahl  $F_4 = 2^{(2^4)} + 1 = 65537$  verwendet.

# Das RSA-Verfahren

## Schlüsselerzeugung

### Schlüsselerzeugung beim RSA-Verfahren:

- In der Praxis werden zwei hinreichend große natürliche Zahlen ausgewählt und durch Primzahltests geprüft, dies solange, bis zwei Primzahlen  $p$  und  $q$  der gewünschten Länge gefunden sind.
- Für den Verschlüsselungsexponenten  $e$  wird in der Praxis oft die Fermat-Zahl  $F_4 = 2^{(2^4)} + 1 = 65537$  verwendet.
- Die Bestimmung des Entschlüsselungsexponenten  $d$  vermöge der Kongruenz

$$e \cdot d \equiv_{\varphi(n)} 1$$

erfolgt mit dem **erweiterten euklidischen Algorithmus**.

# Das RSA-Verfahren

## Verschlüsselung

### Verschlüsselung beim RSA-Verfahren



# Das RSA-Verfahren

## Verschlüsselung

### Verschlüsselung beim RSA-Verfahren

- Wenn eine Zahl  $m$  gegeben ist, so wird das Chiffre  $c$  mithilfe des öffentlichen Schlüssels  $(n, e)$  wie folgt berechnet:

$$c = m^e \mod n.$$

# Das RSA-Verfahren

## Verschlüsselung

### Verschlüsselung beim RSA-Verfahren

- Wenn eine Zahl  $m$  gegeben ist, so wird das Chiffre  $c$  mithilfe des öffentlichen Schlüssels  $(n, e)$  wie folgt berechnet:

$$c = m^e \bmod n.$$

- Die Berechnung von  $c$  erfolgt in der Praxis mit der sogenannten *binären Exponentiation* bzw. *sukzessivem Quadrieren*.

# Das RSA-Verfahren

## Entschlüsselung

### Entschlüsselung beim RSA-Verfahren

# Das RSA-Verfahren

## Entschlüsselung

### Entschlüsselung beim RSA-Verfahren

- Wenn das Chifftrat  $c$  gegeben ist, so erfolgt die Entschlüsselung mithilfe des privaten Schlüssels  $(n, d)$  wie folgt:

$$m' = c^d \mod n.$$

# Das RSA-Verfahren

## Entschlüsselung

### Entschlüsselung beim RSA-Verfahren

- Wenn das Chiffre  $c$  gegeben ist, so erfolgt die Entschlüsselung mithilfe des privaten Schlüssels  $(n, d)$  wie folgt:

$$m' = c^d \mod n.$$

- Auch die Berechnung von  $m'$  erfolgt in der Praxis mit **binärer Exponentiation**.

### Entschlüsselung beim RSA-Verfahren

- Wenn das Chiffre  $c$  gegeben ist, so erfolgt die Entschlüsselung mithilfe des privaten Schlüssels  $(n, d)$  wie folgt:

$$m' = c^d \mod n.$$

- Auch die Berechnung von  $m'$  erfolgt in der Praxis mit **binärer Exponentiation**.
- Natürlich hat dies nur einen Sinn, wenn  $m'$  gleich der ursprünglichen Nachricht  $m$  ist.
- Die Tatsache, dass tatsächlich  $m' = m$  gilt, wird als **Satz vom korrekten Dechiffrieren** in der Literatur bewiesen (z.B. in A. Beutelsbacher: Kryptologie, Vieweg), vgl. auch Folien 74 ff.

# Das RSA-Verfahren

## Verschlüsselung von Textnachrichten

### Textnachrichten: *Codierung* vor Verschlüsselung

Soll eine Textnachricht verschlüsselt werden, so muss diese zunächst mit einem geeigneten Code als Zahl dargestellt werden. Bei englischen Texten kann dies z.B. mit dem *ASCII* (*American Standard Code for Information Interchange*) bewerkstelligt werden.

# Das RSA-Verfahren

## Demonstrationsbeispiel

### Darstellung des RSA-Verfahrens – Demonstrationsbeispiel

Wir werden nun anhand eines Demonstrationsbeispiels (mit sehr kleinen Zahlen) die einzelnen Schritte des RSA-Verfahrens vorführen, zunächst die Schlüsselerzeugung.



# Das RSA-Verfahren

## Demonstrationsbeispiel

### Darstellung des RSA-Verfahrens – Demonstrationsbeispiel

Wir werden nun anhand eines Demonstrationsbeispiels (mit sehr kleinen Zahlen) die einzelnen Schritte des RSA-Verfahrens vorführen, zunächst die Schlüsselerzeugung.

- Wähle  $p = 13$ ,  $q = 17$ . Dann gilt

$$n = p \cdot q = 13 \cdot 17 = 221$$

und

$$\varphi(n) = 12 \cdot 16 = 192.$$

# Das RSA-Verfahren

## Demonstrationsbeispiel

### Darstellung des RSA-Verfahrens – Demonstrationsbeispiel

Wir werden nun anhand eines Demonstrationsbeispiels (mit sehr kleinen Zahlen) die einzelnen Schritte des RSA-Verfahrens vorführen, zunächst die Schlüsselerzeugung.

- Wähle  $p = 13$ ,  $q = 17$ . Dann gilt

$$n = p \cdot q = 13 \cdot 17 = 221$$

und

$$\varphi(n) = 12 \cdot 16 = 192.$$

- Wähle weiterhin  $e = 5$ , dann ist sicherlich  $\text{ggT}(5, 192) = 1$ .

# Das RSA-Verfahren

## Demonstrationsbeispiel

### Darstellung des RSA-Verfahrens – Demonstrationsbeispiel

Wir werden nun anhand eines Demonstrationsbeispiels (mit sehr kleinen Zahlen) die einzelnen Schritte des RSA-Verfahrens vorführen, zunächst die Schlüsselerzeugung.

- Wähle  $p = 13$ ,  $q = 17$ . Dann gilt

$$n = p \cdot q = 13 \cdot 17 = 221$$

und

$$\varphi(n) = 12 \cdot 16 = 192.$$

- Wähle weiterhin  $e = 5$ , dann ist sicherlich  $\text{ggT}(5, 192) = 1$ .

### Hörsaalübung

Bestimme  $d$  so, dass  $5 \cdot d \equiv 1 \pmod{192}$  gilt.

Versuchen Sie dies zunächst durch geschicktes „Raten“; ein systematisches Verfahren (erweiterter euklidischer Algorithmus) wird später vorgestellt.

# Das RSA-Verfahren

## Demonstrationsbeispiel

### Demonstrationsbeispiel – Verschlüsselung

Mit unserem öffentlichen Schlüssel  $(n, e) = (221, 5)$  werden wir nun die „Nachricht“  $m = 10$  verschlüsseln:

$$c = m^e \bmod n = 10^5 \bmod 221.$$

Wir führen an diesem Beispiel das Verfahren der binären Exponentiation vor.

# Das RSA-Verfahren

## Demonstrationsbeispiel

### Demonstrationsbeispiel – Verschlüsselung

Wir stellen  $e = 5$  als Summe von Zweierpotenzen dar:  $5 = 1 + 4 = 2^0 + 2^2$  Daraus folgt

$$\begin{aligned} m^e \bmod 221 &= 10^5 \bmod 221 = 10^{(1+4)} \bmod 221 \\ &= 10 \cdot 10^4 \bmod 221. \end{aligned}$$

# Das RSA-Verfahren

## Demonstrationsbeispiel

### Demonstrationsbeispiel – Verschlüsselung

Wir stellen  $e = 5$  als Summe von Zweierpotenzen dar:  $5 = 1 + 4 = 2^0 + 2^2$  Daraus folgt

$$\begin{aligned} m^e \bmod 221 &= 10^5 \bmod 221 = 10^{(1+4)} \bmod 221 \\ &= 10 \cdot 10^4 \bmod 221. \end{aligned}$$

Wir berechnen  $m^e = 10^5 \bmod 221$  durch sukzessives Quadrieren und Multiplizieren:

$$10^2 = 100 \equiv_{221} 100$$

$$10^4 = (10^2)^2 = 100 \cdot 100 = 45 \cdot 221 + 55 \equiv_{221} 55$$

$$10^5 = 10 \cdot 10^4 \equiv_{221} 10 \cdot 55 = 550 = 2 \cdot 221 + 108 \equiv_{221} 108$$

# Das RSA-Verfahren

## Demonstrationsbeispiel

### Demonstrationsbeispiel – Chiffprat

Wir haben somit das Chiffprat

$$c = m^e \mod n = 10^5 \mod 221 = 108$$

erhalten. Dieses wird an den Empfänger bzw. die Empfängerin gesandt

Ende Sitzung 2 zu RSA (08.6.2021)

# Das RSA-Verfahren

## Demonstrationsbeispiel

### Demonstrationsbeispiel – Chiffrat

Wir haben somit das Chiffrat

$$c = m^e \mod n = 10^5 \mod 221 = 108$$

erhalten. Dieses wird an den Empfänger bzw. die Empfängerin gesandt

### Hörsaalübung: Demonstrationsbeispiel – Entschlüsselung

Mit dem privaten Schlüssel  $(n, d) = (221, 77)$  **entschlüsseln** wir das Chiffrat  $c = 108$ :

$$m' = c^d \mod n = 108^{77} \mod 221.$$

*Hinweis: Zur Bearbeitung dieser Aufgabe ist ein Taschenrechner von Nutzen.*

Ende Sitzung 2 zu RSA (08.6.2021)



# Das RSA-Verfahren

## Demonstrationsbeispiel

### Demonstrationsbeispiel – Entschlüsselung

Mit  $77 = 64 + 8 + 4 + 1 = 2^6 + 2^3 + 2^2 + 2^0$  folgt  $c^d = c^{77} = c^{64} \cdot c^8 \cdot c^4 \cdot c$ . Sukzessives Quadrieren:

$$c^2 = 108^2 \equiv_{221} 172 \equiv_{221} -49$$

$$c^4 = (c^2)^2 \equiv_{221} (-49)^2 \equiv_{221} 191 \equiv_{221} -30$$

$$c^8 = (c^4)^2 \equiv_{221} (-30)^2 = 900 \equiv_{221} 16$$

$$c^{16} = (c^8)^2 \equiv_{221} (16)^2 = 256 \equiv_{221} 35$$

$$c^{32} = (c^{16})^2 \equiv_{221} (35)^2 = 1225 = 1105 + 120 \equiv_{221} 120$$

$$c^{64} = (c^{32})^2 \equiv_{221} (120)^2 \equiv_{221} 35$$

# Das RSA-Verfahren

## Demonstrationsbeispiel

### Demonstrationsbeispiel – Entschlüsselung

Damit folgt

$$m' = c^d = c^{77} \equiv_{221} 35 \cdot 16 \cdot (-30) \cdot 108.$$

Ausreduktion modulo 221:

$$35 \cdot 16 = 560 = 2 \cdot 221 + 118 \equiv_{221} 118$$

$$(-30) \cdot 108 \equiv_{221} (-30) \cdot (-113) = 3390 = 15 \cdot 221 + 75 \equiv_{221} 75$$

$$118 \cdot 75 = 8850 = 40 \cdot 221 + 10 \equiv_{221} 10.$$

Somit ist  $m' = 10$ , also ist  $m' = m$ , d.h. bei der Dechiffrierung von  $m$  hat sich in der Tat wieder unsere ursprüngliche Nachricht  $m$  ergeben.

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### Erinnerung

Wenn  $\varphi(n)$  berechnet und ein Verschlüsselungsexponent  $e$  mit  $\text{ggT}(e, \varphi(n)) = 1$  gewählt wurde, so muss ein Entschlüsselungsexponent  $d$  bestimmt werden, der die Gleichung

$$e \cdot d \equiv_{\varphi(n)} 1$$

erfüllt.

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### Erinnerung

Wenn  $\varphi(n)$  berechnet und ein Verschlüsselungsexponent  $e$  mit  $\text{ggT}(e, \varphi(n)) = 1$  gewählt wurde, so muss ein Entschlüsselungsexponent  $d$  bestimmt werden, der die Gleichung

$$e \cdot d \equiv_{\varphi(n)} 1$$

erfüllt.

Hierzu dient der erweiterte euklidische Algorithmus, den wir im Folgenden besprechen.

# Das RSA-Verfahren

Berechnung des Entschlüsselungsexponenten

## Erweiterter euklidischer Algorithmus (EEA)

Es seien zwei ganze Zahlen  $x$  und  $y$  gegeben. Mit dem erweiterten euklidischen Algorithmus können wir

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### Erweiterter euklidischer Algorithmus (EEA)

Es seien zwei ganze Zahlen  $x$  und  $y$  gegeben. Mit dem erweiterten euklidischen Algorithmus können wir

- den **größten gemeinsamen Teiler**  $\text{ggT}(x, y)$  von  $x$  und  $y$  bestimmen,

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### Erweiterter euklidischer Algorithmus (EEA)

Es seien zwei ganze Zahlen  $x$  und  $y$  gegeben. Mit dem erweiterten euklidischen Algorithmus können wir

- den **größten gemeinsamen Teiler**  $\text{ggT}(x, y)$  von  $x$  und  $y$  bestimmen,
- die Zahl  $\text{ggT}(x, y)$  als sogenannte **Vielfachsumme** darstellen, d.h. ganze Zahlen  $a$  und  $b$  derart bestimmen, dass

$$\text{ggT}(x, y) = a \cdot x + b \cdot y \quad \text{gilt.}$$

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### Erweiterter euklidischer Algorithmus (EEA)

Es seien zwei ganze Zahlen  $x$  und  $y$  gegeben. Mit dem erweiterten euklidischen Algorithmus können wir

- den **größten gemeinsamen Teiler**  $\text{ggT}(x, y)$  von  $x$  und  $y$  bestimmen,
- die Zahl  $\text{ggT}(x, y)$  als sogenannte **Vielfachsumme** darstellen, d.h. ganze Zahlen  $a$  und  $b$  derart bestimmen, dass

$$\text{ggT}(x, y) = a \cdot x + b \cdot y \quad \text{gilt.}$$

### Anwendung

Zur Bestimmung des Verschlüsselungsexponenten  $d$  bei gegebenen Werten  $\varphi(n)$  und  $e$  ergibt sich speziell



# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### Erweiterter euklidischer Algorithmus (EEA)

Es seien zwei ganze Zahlen  $x$  und  $y$  gegeben. Mit dem erweiterten euklidischen Algorithmus können wir

- den **größten gemeinsamen Teiler**  $\text{ggT}(x, y)$  von  $x$  und  $y$  bestimmen,
- die Zahl  $\text{ggT}(x, y)$  als sogenannte **Vielfachsumme** darstellen, d.h. ganze Zahlen  $a$  und  $b$  derart bestimmen, dass

$$\text{ggT}(x, y) = a \cdot x + b \cdot y \quad \text{gilt.}$$

### Anwendung

Zur Bestimmung des Verschlüsselungsexponenten  $d$  bei gegebenen Werten  $\varphi(n)$  und  $e$  ergibt sich speziell

- eine Vielfachsummendarstellung von  $1 = \text{ggT}(e, \varphi(n))$  in der Form

$$1 = a \cdot e + b \cdot \varphi(n);$$

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### Erweiterter euklidischer Algorithmus (EEA)

Es seien zwei ganze Zahlen  $x$  und  $y$  gegeben. Mit dem erweiterten euklidischen Algorithmus können wir

- den **größten gemeinsamen Teiler**  $\text{ggT}(x, y)$  von  $x$  und  $y$  bestimmen,
- die Zahl  $\text{ggT}(x, y)$  als sogenannte **Vielfachsumme** darstellen, d.h. ganze Zahlen  $a$  und  $b$  derart bestimmen, dass

$$\text{ggT}(x, y) = a \cdot x + b \cdot y \quad \text{gilt.}$$

### Anwendung

Zur Bestimmung des Verschlüsselungsexponenten  $d$  bei gegebenen Werten  $\varphi(n)$  und  $e$  ergibt sich speziell

- eine Vielfachsummendarstellung von  $1 = \text{ggT}(e, \varphi(n))$  in der Form

$$1 = a \cdot e + b \cdot \varphi(n);$$

- Hieraus ergibt sich

$$a \cdot e = -b \cdot \varphi(n) + 1 \equiv_{\varphi(n)} 1,$$

wir setzen dann  $d = a$ .

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben.

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

$$93 = 2 \cdot 39 + 15$$

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

$$93 = 2 \cdot 39 + 15$$

$$39 = 2 \cdot 15 + 9$$

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

$$93 = 2 \cdot 39 + 15$$

$$39 = 2 \cdot 15 + 9$$

$$15 = 1 \cdot 9 + 6$$

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

$$93 = 2 \cdot 39 + 15$$

$$39 = 2 \cdot 15 + 9$$

$$15 = 1 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$



# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

$$93 = 2 \cdot 39 + 15$$

$$39 = 2 \cdot 15 + 9$$

$$15 = 1 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

$$93 = 2 \cdot 39 + 15$$

$$39 = 2 \cdot 15 + 9$$

$$15 = 1 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

Wir erkennen in der letzten Zeile die Abbruchbedingung „Division geht auf“:

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

$$93 = 2 \cdot 39 + 15$$

$$39 = 2 \cdot 15 + 9$$

$$15 = 1 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

Wir erkennen in der letzten Zeile die Abbruchbedingung „Division geht auf“:

$$6 = 2 \cdot 3 + 0.$$

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

$$93 = 2 \cdot 39 + 15$$

$$39 = 2 \cdot 15 + 9$$

$$15 = 1 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

In den beiden letzten Zeilen sehen wir den größten gemeinsamen Teiler von 93 und 39.

$$\text{ggT}(93, 39) = 3.$$

# Das RSA-Verfahren

## Erweiterter euklidischer Algorithmus (EEA)

### Beispiel

Es seien die Zahlen 93 und 39 gegeben. Wir demonstrieren den erweiterten euklidischen Algorithmus und bestimmen zunächst  $\text{ggT}(93, 39)$ :

$$93 = 2 \cdot 39 + 15$$

$$39 = 2 \cdot 15 + 9$$

$$15 = 1 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + \boxed{3}$$

$$6 = 2 \cdot \boxed{3} + \boxed{0}$$

Wir erkennen in der letzten Zeile die Abbruchbedingung „Division geht auf“:

$$6 = 2 \cdot 3 + \boxed{0}.$$

In den beiden letzten Zeilen sehen wir den größten gemeinsamen Teiler von 93 und 39.

$$\text{ggT}(93, 39) = \boxed{3}.$$

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel – Probe

Wir prüfen von Hand nach, dass das Ergebnis  $\text{ggT}(93, 39) = 3$ , das uns der euklidische Algorithmus geliefert hat, richtig ist:

$$1 \cdot 93 = 93 = 3 \cdot 31$$

$$1 \cdot 39 = 39 = 3 \cdot 13.$$

Die gemeinsamen Teiler von 93 und 39 sind 1 und 3, der größte gemeinsame Teiler ist somit 3.

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel – Vielfachsummandarstellung von $\text{ggT}(93, 39)$ :

Mit der **Erweiterung** des euklidischen Algorithmus' verschaffen wir uns nun eine Darstellung der Form

$$\text{ggT}(93, 39) = 3 = a \cdot 93 + b \cdot 39 :$$

# Das RSA-Verfahren

## Erweiterter euklidischer Algorithmus (EEA)

### Beispiel – Vielfachsummandarstellung von $\text{ggT}(93, 39)$ :

Mit der **Erweiterung** des euklidischen Algorithmus' verschaffen wir uns nun eine Darstellung der Form

$$\text{ggT}(93, 39) = 3 = a \cdot 93 + b \cdot 39 :$$

Wir stellen hierzu zunächst die vorletzte Zeile  $9 = 1 \cdot 6 + 3$  unserer vorherigen Rechnung um:

$$3 = 9 - 1 \cdot 6 \quad (1)$$



# Das RSA-Verfahren

## Erweiterter euklidischer Algorithmus (EEA)

### Beispiel – Vielfachsummendarstellung von $\text{ggT}(93, 39)$ :

Mit der **Erweiterung** des euklidischen Algorithmus' verschaffen wir uns nun eine Darstellung der Form

$$\text{ggT}(93, 39) = 3 = a \cdot 93 + b \cdot 39 :$$

Wir stellen hierzu zunächst die vorletzte Zeile  $9 = 1 \cdot 6 + 3$  unserer vorherigen Rechnung um:

$$3 = 9 - 1 \cdot 6 \quad (1)$$

Dies ist bereits eine Vielfachsummendarstellung von 3, allerdings nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 9 und 6. Wir gehen nun schrittweise rückwärts vor:

# Das RSA-Verfahren

## Erweiterter euklidischer Algorithmus (EEA)

### Beispiel – Vielfachsummendarstellung von $\text{ggT}(93, 39)$ :

Mit der **Erweiterung** des euklidischen Algorithmus' verschaffen wir uns nun eine Darstellung der Form

$$\text{ggT}(93, 39) = 3 = a \cdot 93 + b \cdot 39 :$$

Wir stellen hierzu zunächst die vorletzte Zeile  $9 = 1 \cdot 6 + 3$  unserer vorherigen Rechnung um:

$$3 = 9 - 1 \cdot 6 \quad (1)$$

Dies ist bereits eine Vielfachsummendarstellung von 3, allerdings nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 9 und 6. Wir gehen nun schrittweise rückwärts vor: Aus der **drittletzten** Zeile  $15 = 1 \cdot 9 + 6$  erhalten wir eine Darstellung für 6, nämlich  $6 = 15 - 1 \cdot 9$ , die wir in Gleichung (1) einsetzen:

$$3 = 9 - 1 \cdot \underbrace{(15 - 1 \cdot 9)}_6 = -1 \cdot 15 + 2 \cdot 9 \quad (2)$$

# Das RSA-Verfahren

## Erweiterter euklidischer Algorithmus (EEA)

### Beispiel – Vielfachsummendarstellung von $\text{ggT}(93, 39)$ :

Mit der **Erweiterung** des euklidischen Algorithmus' verschaffen wir uns nun eine Darstellung der Form

$$\text{ggT}(93, 39) = 3 = a \cdot 93 + b \cdot 39 :$$

Wir stellen hierzu zunächst die vorletzte Zeile  $9 = 1 \cdot 6 + 3$  unserer vorherigen Rechnung um:

$$3 = 9 - 1 \cdot 6 \quad (1)$$

Dies ist bereits eine Vielfachsummendarstellung von 3, allerdings nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 9 und 6. Wir gehen nun schrittweise rückwärts vor: Aus der **drittletzten** Zeile  $15 = 1 \cdot 9 + 6$  erhalten wir eine Darstellung für 6, nämlich  $6 = 15 - 1 \cdot 9$ , die wir in Gleichung (1) einsetzen:

$$3 = 9 - 1 \cdot \underbrace{(15 - 1 \cdot 9)}_6 = -1 \cdot 15 + 2 \cdot 9 \quad (2)$$

Aus der **viertletzten** Zeile  $39 = 2 \cdot 15 + 9$  erhalten wir eine Darstellung für 9, nämlich  $9 = 39 - 2 \cdot 15$ , die wir in Gleichung (2) einsetzen:

$$3 = -1 \cdot 15 + 2 \cdot \underbrace{(39 - 2 \cdot 15)}_9 = -5 \cdot 15 + 2 \cdot 39 \quad (3)$$

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

**Beispiel – Vielfachsummendarstellung von  $\text{ggT}(93, 39)$ :**

Zwischenergebnis:

$$3 = -5 \cdot 15 + 2 \cdot 39 \quad (3)$$

# Das RSA-Verfahren

Erweiterter euklidischer Algorithmus (EEA)

## Beispiel – Vielfachsummendarstellung von $\text{ggT}(93, 39)$ :

Zwischenergebnis:

$$3 = -5 \cdot 15 + 2 \cdot 39 \quad (3)$$

Auch dies ist eine Vielfachsummendarstellung von 3, allerdings noch immer nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 15 und 39. Wir müssen also die Zahl 15 noch ersetzen.

# Das RSA-Verfahren

## Erweiterter euklidischer Algorithmus (EEA)

### Beispiel – Vielfachsummandarstellung von $\text{ggT}(93, 39)$ :

Zwischenergebnis:

$$3 = -5 \cdot 15 + 2 \cdot 39 \quad (3)$$

Auch dies ist eine Vielfachsummandarstellung von 3, allerdings noch immer nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 15 und 39. Wir müssen also die Zahl 15 noch ersetzen.

Aus der **fünftletzten** Zeile  $93 = 2 \cdot 39 + 15$  erhalten wir eine Darstellung für 15, nämlich  $15 = 93 - 2 \cdot 39$ , die wir in Gleichung (3) einsetzen:

$$3 = -5 \cdot 15 + 2 \cdot 39 = -5 \cdot \underbrace{(93 - 2 \cdot 39)}_{15} + 2 \cdot 39 = -5 \cdot 93 + 12 \cdot 39 \quad (4)$$

# Das RSA-Verfahren

## Erweiterter euklidischer Algorithmus (EEA)

### Beispiel – Vielfachsummandarstellung von $\text{ggT}(93, 39)$ :

Zwischenergebnis:

$$3 = -5 \cdot 15 + 2 \cdot 39 \quad (3)$$

Auch dies ist eine Vielfachsummandarstellung von 3, allerdings noch immer nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 15 und 39. Wir müssen also die Zahl 15 noch ersetzen.

Aus der **fünftletzten** Zeile  $93 = 2 \cdot 39 + 15$  erhalten wir eine Darstellung für 15, nämlich  $15 = 93 - 2 \cdot 39$ , die wir in Gleichung (3) einsetzen:

$$3 = -5 \cdot 15 + 2 \cdot 39 = -5 \cdot \underbrace{(93 - 2 \cdot 39)}_{15} + 2 \cdot 39 = -5 \cdot 93 + 12 \cdot 39 \quad (4)$$

Auf der rechten Seite der Gleichung  $3 = -5 \cdot 93 + 12 \cdot 39$  steht nun die gesuchte Vielfachsummandarstellung von  $3 = \text{ggT}(93, 39)$  in Abhängigkeit von 93 und 39.

# Das RSA-Verfahren

## Erweiterter euklidischer Algorithmus (EEA)

### Beispiel – Vielfachsummendarstellung von $\text{ggT}(93, 39)$ :

Zwischenergebnis:

$$3 = -5 \cdot 15 + 2 \cdot 39 \quad (3)$$

Auch dies ist eine Vielfachsummendarstellung von 3, allerdings noch immer nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 15 und 39. Wir müssen also die Zahl 15 noch ersetzen.

Aus der **fünftletzten** Zeile  $93 = 2 \cdot 39 + 15$  erhalten wir eine Darstellung für 15, nämlich  $15 = 93 - 2 \cdot 39$ , die wir in Gleichung (3) einsetzen:

$$3 = -5 \cdot 15 + 2 \cdot 39 = -5 \cdot \underbrace{(93 - 2 \cdot 39)}_{15} + 2 \cdot 39 = -5 \cdot 93 + 12 \cdot 39 \quad (4)$$

Auf der rechten Seite der Gleichung  $3 = -5 \cdot 93 + 12 \cdot 39$  steht nun die gesuchte Vielfachsummendarstellung von  $3 = \text{ggT}(93, 39)$  in Abhängigkeit von 93 und 39.

### Probe

$$-5 \cdot 93 + 12 \cdot 39 = -465 + 468 = 3$$



# Das RSA-Verfahren

## Erweiterter euklidischer Algorithmus (EEA)

### Beispiel – Vielfachsummandarstellung von $\text{ggT}(93, 39)$ :

Zwischenergebnis:

$$3 = -5 \cdot 15 + 2 \cdot 39 \quad (3)$$

Auch dies ist eine Vielfachsummandarstellung von 3, allerdings noch immer nicht in Abhängigkeit von 93 und 39, sondern in Abhängigkeit von 15 und 39. Wir müssen also die Zahl 15 noch ersetzen.

Aus der **fünftletzten** Zeile  $93 = 2 \cdot 39 + 15$  erhalten wir eine Darstellung für 15, nämlich  $15 = 93 - 2 \cdot 39$ , die wir in Gleichung (3) einsetzen:

$$3 = -5 \cdot 15 + 2 \cdot 39 = -5 \cdot \underbrace{(93 - 2 \cdot 39)}_{15} + 2 \cdot 39 = -5 \cdot 93 + 12 \cdot 39 \quad (4)$$

Auf der rechten Seite der Gleichung  $3 = -5 \cdot 93 + 12 \cdot 39$  steht nun die gesuchte Vielfachsummandarstellung von  $3 = \text{ggT}(93, 39)$  in Abhängigkeit von 93 und 39.

### Probe

$$-5 \cdot 93 + 12 \cdot 39 = -465 + 468 = 3 \quad \checkmark$$

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### RSA-Demonstrationsbeispiel – Fortsetzung und Schluss

Wir verwenden nun den EEA zur Bestimmung des Entschlüsselungsexponenten  $d$  in unserem Demo-Beispiel mit

$$n = 13 \cdot 17, \varphi(n) = 12 \cdot 16 = 192, e = 5 :$$

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### RSA-Demonstrationsbeispiel – Fortsetzung und Schluss

Wir verwenden nun den EEA zur Bestimmung des Entschlüsselungsexponenten  $d$  in unserem Demo-Beispiel mit

$$n = 13 \cdot 17, \varphi(n) = 12 \cdot 16 = 192, e = 5 :$$

- Schritt 1: Euklidischer Algorithmus

$$192 = 38 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0.$$

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### RSA-Demonstrationsbeispiel – Fortsetzung und Schluss

Wir verwenden nun den EEA zur Bestimmung des Entschlüsselungsexponenten  $d$  in unserem Demo-Beispiel mit

$$n = 13 \cdot 17, \varphi(n) = 12 \cdot 16 = 192, e = 5 :$$

- Schritt 1: Euklidischer Algorithmus

$$192 = 38 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + \boxed{1}$$

$$2 = 2 \cdot \boxed{1} + 0.$$

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### RSA-Demonstrationsbeispiel – Fortsetzung und Schluss

Wir verwenden nun den EEA zur Bestimmung des Entschlüsselungsexponenten  $d$  in unserem Demo-Beispiel mit

$$n = 13 \cdot 17, \varphi(n) = 12 \cdot 16 = 192, e = 5 :$$

- Schritt 1: Euklidischer Algorithmus

$$192 = 38 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + \boxed{1}$$

$$2 = 2 \cdot \boxed{1} + 0.$$

- Schritt 2: Erweiterung zur Bestimmung der Vielfachsummendarstellung von  $\boxed{1 = \text{ggT}(192, 5)}$ :

$$1 = 5 - 2 \cdot 2$$

$$\rightsquigarrow 1 = 5 - 2 \cdot \underbrace{(192 - 38 \cdot 5)}_2$$

$$\rightsquigarrow 1 = -2 \cdot 192 + 77 \cdot 5$$

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### RSA-Demonstrationsbeispiel – Fortsetzung und Schluss

Wir verwenden nun den EEA zur Bestimmung des Entschlüsselungsexponenten  $d$  in unserem Demo-Beispiel mit

$$n = 13 \cdot 17, \varphi(n) = 12 \cdot 16 = 192, e = 5 :$$

- Schritt 1: Euklidischer Algorithmus

$$192 = 38 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + \boxed{1}$$

$$2 = 2 \cdot \boxed{1} + 0.$$

- Schritt 2: Erweiterung zur Bestimmung der Vielfachsummendarstellung von  $\boxed{1 = \text{ggT}(192, 5)}$ :

$$1 = 5 - 2 \cdot 2$$

$$\leadsto 1 = 5 - 2 \cdot \underbrace{(192 - 38 \cdot 5)}_2$$

$$\leadsto 1 = -2 \cdot 192 + 77 \cdot 5$$

Hieraus folgt  $77 \cdot 5 = 2 \cdot 192 + 1$  bzw.  $77 \cdot 5 \equiv_{192} 1$ . Somit ist  $d = 77$  die gesuchte modulare Inverse von  $e = 5$ .

# Das RSA-Verfahren

## Berechnung des Entschlüsselungsexponenten

### Hörsaalübung

Nehmen Sie an, dass für den öffentlichen RSA-Schlüssel  $(n, e) = (247, 7)$  gewählt wurde. Bestimmen Sie

- die Faktorisierung  $247 = p \cdot q$ ,
- den Wert  $\varphi(247)$ ,
- den Entschlüsselungsexponenten  $d$  mithilfe des erweiterten euklidischen Algorithmus.

# Faktorisierung von Restklassenringen

## Einführung:

- In unserem Demonstrationsbeispiel mussten wir u.a.

$c = 10^5 \bmod 221$  und  $m' = 108^{77} \bmod 221$  berechnen.



# Faktorisierung von Restklassenringen

## Einführung:

- In unserem Demonstrationsbeispiel mussten wir u.a.

$$c = 10^5 \bmod 221 \quad \text{und} \quad m' = 108^{77} \bmod 221 \quad \text{berechnen.}$$

- Wir nutzen hierzu nun die folgende Korrespondenz:

$$10^2 \leftrightarrow ([100 \bmod 13]_{13}, [100 \bmod 17]_{17}) = ([9]_{13}, [15]_{17}) \equiv ([9]_{13}, [-2]_{17})$$

# Faktorisierung von Restklassenringen

## Einführung:

- In unserem Demonstrationsbeispiel mussten wir u.a.

$$c = 10^5 \bmod 221 \quad \text{und} \quad m' = 108^{77} \bmod 221 \quad \text{berechnen.}$$

- Wir nutzen hierzu nun die folgende Korrespondenz:

$$10^2 \leftrightarrow ([100 \bmod 13]_{13}, [100 \bmod 17]_{17}) = ([9]_{13}, [15]_{17}) \equiv ([9]_{13}, [-2]_{17})$$

- und rechnen hiermit weiter:

$$10^4 = (10^2)^2 \leftrightarrow ([9^2 \bmod 13]_{13}, [(-2)^2 \bmod 17]_{17}) = ([3]_{13}, [4]_{17}).$$

# Faktorisierung von Restklassenringen

## Einführung:

- In unserem Demonstrationsbeispiel mussten wir u.a.

$$c = 10^5 \bmod 221 \quad \text{und} \quad m' = 108^{77} \bmod 221 \quad \text{berechnen.}$$

- Wir nutzen hierzu nun die folgende Korrespondenz:

$$10^2 \leftrightarrow ([100 \bmod 13]_{13}, [100 \bmod 17]_{17}) = ([9]_{13}, [15]_{17}) \equiv ([9]_{13}, [-2]_{17})$$

- und rechnen hiermit weiter:

$$10^4 = (10^2)^2 \leftrightarrow ([9^2 \bmod 13]_{13}, [(-2)^2 \bmod 17]_{17}) = ([3]_{13}, [4]_{17}).$$

- Somit gilt

$$10^5 = 10^4 \cdot 10 \leftrightarrow ([3 \cdot 10 \bmod 13]_{13}, [4 \cdot 10 \bmod 17]_{17}) = ([30]_{13}, [40]_{17}) \equiv ([4]_{13}, [6]_{17}).$$

# Faktorisierung von Restklassenringen

## Einführung:

- In unserem Demonstrationsbeispiel mussten wir u.a.

$$c = 10^5 \bmod 221 \quad \text{und} \quad m' = 108^{77} \bmod 221 \quad \text{berechnen.}$$

- Wir nutzen hierzu nun die folgende Korrespondenz:

$$10^2 \leftrightarrow ([100 \bmod 13]_{13}, [100 \bmod 17]_{17}) = ([9]_{13}, [15]_{17}) \equiv ([9]_{13}, [-2]_{17})$$

- und rechnen hiermit weiter:

$$10^4 = (10^2)^2 \leftrightarrow ([9^2 \bmod 13]_{13}, [(-2)^2 \bmod 17]_{17}) = ([3]_{13}, [4]_{17}).$$

- Somit gilt

$$10^5 = 10^4 \cdot 10 \leftrightarrow ([3 \cdot 10 \bmod 13]_{13}, [4 \cdot 10 \bmod 17]_{17}) = ([30]_{13}, [40]_{17}) \equiv ([4]_{13}, [6]_{17}).$$

- Wir müssen nun noch die Zahl  $x$  bestimmen, welche die folgenden Bedingungen erfüllt:

$$x \equiv 4 \pmod{13} \quad \text{und} \quad x \equiv 6 \pmod{17}.$$

# Faktorisierung von Restklassenringen

## Einführung:

- In unserem Demonstrationsbeispiel mussten wir u.a.

$$c = 10^5 \bmod 221 \quad \text{und} \quad m' = 108^{77} \bmod 221 \quad \text{berechnen.}$$

- Wir nutzen hierzu nun die folgende Korrespondenz:

$$10^2 \leftrightarrow ([100 \bmod 13]_{13}, [100 \bmod 17]_{17}) = ([9]_{13}, [15]_{17}) \equiv ([9]_{13}, [-2]_{17})$$

- und rechnen hiermit weiter:

$$10^4 = (10^2)^2 \leftrightarrow ([9^2 \bmod 13]_{13}, [(-2)^2 \bmod 17]_{17}) = ([3]_{13}, [4]_{17}).$$

- Somit gilt

$$10^5 = 10^4 \cdot 10 \leftrightarrow ([3 \cdot 10 \bmod 13]_{13}, [4 \cdot 10 \bmod 17]_{17}) = ([30]_{13}, [40]_{17}) \equiv ([4]_{13}, [6]_{17}).$$

- Wir müssen nun noch die Zahl  $x$  bestimmen, welche die folgenden Bedingungen erfüllt:

$$x \equiv 4 \pmod{13} \quad \text{und} \quad x \equiv 6 \pmod{17}.$$

- Hierzu kann man ganz „bodenständig“ Listen von Elementen in den beiden Restklassen  $[4]_{13}$  bzw.  $[6]_{17}$  vergleichen und das gemeinsame Element identifizieren.

# Faktorisierung von Restklassenringen

## Isomorphie

- 1 Der Ring  $\mathbb{Z}_n$  ist isomorph zum Ring  $\mathbb{Z}/n\mathbb{Z}$ .
- 2 Falls die natürlichen Zahlen  $n_1, n_2, \dots, n_r$  paarweise teilerfremd sind, ist der Ring  $\mathbb{Z}/(n_1 \cdot n_2 \dots n_r)\mathbb{Z}$  isomorph zum Ring

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \dots \mathbb{Z}/n_r\mathbb{Z}.$$

# Faktorisierung von Restklassenringen

## Isomorphie

- 1 Der Ring  $\mathbb{Z}_n$  ist isomorph zum Ring  $\mathbb{Z}/n\mathbb{Z}$ .
- 2 Falls die natürlichen Zahlen  $n_1, n_2, \dots, n_r$  paarweise teilerfremd sind, ist der Ring  $\mathbb{Z}/(n_1 \cdot n_2 \dots n_r)\mathbb{Z}$  isomorph zum Ring

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \dots \mathbb{Z}/n_r\mathbb{Z}.$$

## Beispiele

Der Ring  $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/(2 \cdot 3)\mathbb{Z}$  ist isomorph zum Ring  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . Wir werden dies auf der folgenden Beispiele ausführlich diskutieren.

# Faktorisierung von Restklassenringen

## Isomorphie

Wir betrachten die Abbildung

$$f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 : \bar{x} \mapsto (x \bmod 2, x \bmod 3) :$$

$$\bar{0} \mapsto (0, 0)$$

$$\bar{1} \mapsto (1, 1)$$

$$\bar{2} \mapsto (0, 2)$$

$$\bar{3} \mapsto (1, 0)$$

$$\bar{4} \mapsto (0, 1)$$

$$\bar{5} \mapsto (1, 2)$$



# Faktorisierung von Restklassenringen

## Isomorphie

Wir betrachten die Abbildung

$$f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 : \bar{x} \mapsto (x \bmod 2, x \bmod 3) :$$

$$\bar{0} \mapsto (0, 0)$$

$$\bar{1} \mapsto (1, 1)$$

$$\bar{2} \mapsto (0, 2)$$

$$\bar{3} \mapsto (1, 0)$$

$$\bar{4} \mapsto (0, 1)$$

$$\bar{5} \mapsto (1, 2)$$

## Umkehrabbildung

Um zu einem gegebenen Element  $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$  das Element  $\bar{x} \in \mathbb{Z}_6$  mit  $f(\bar{x}) = (a, b)$  zu finden, ist jeweils ein System simultaner Kongruenzen zu lösen:

$$x \bmod 2 = a \quad x \bmod 3 = b.$$

# Faktorisierung von Restklassenringen

## Umkehrabbildung

Wir präsentieren zu jedem Element  $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$  die Zahl  $x$  mit  $\bar{x} \in \mathbb{Z}_6$ , welche Lösung des entsprechenden Systems simultaner Kongruenzen  $x \bmod 2 = a \wedge x \bmod 3 = b$  ist:

# Faktorisierung von Restklassenringen

## Umkehrabbildung

Wir präsentieren zu jedem Element  $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$  die Zahl  $x$  mit  $\bar{x} \in \mathbb{Z}_6$ , welche Lösung des entsprechenden Systems simultaner Kongruenzen  $x \bmod 2 = a \wedge x \bmod 3 = b$  ist:

$$(0, 0) : x \bmod 2 = 0 \wedge x \bmod 3 = 0 \rightsquigarrow x = 0$$

$$(0, 1) : x \bmod 2 = 0 \wedge x \bmod 3 = 1 \rightsquigarrow x = 4$$

$$(0, 2) : x \bmod 2 = 0 \wedge x \bmod 3 = 2 \rightsquigarrow x = 2$$

$$(1, 0) : x \bmod 2 = 1 \wedge x \bmod 3 = 0 \rightsquigarrow x = 3$$

$$(1, 1) : x \bmod 2 = 1 \wedge x \bmod 3 = 1 \rightsquigarrow x = 1$$

$$(1, 2) : x \bmod 2 = 1 \wedge x \bmod 3 = 2 \rightsquigarrow x = 5$$

# Faktorisierung von Restklassenringen

## Umkehrabbildung

Wir präsentieren zu jedem Element  $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$  die Zahl  $x$  mit  $\bar{x} \in \mathbb{Z}_6$ , welche Lösung des entsprechenden Systems simultaner Kongruenzen  $x \bmod 2 = a \wedge x \bmod 3 = b$  ist:

$$(0, 0) : x \bmod 2 = 0 \wedge x \bmod 3 = 0 \rightsquigarrow x = 0$$

$$(0, 1) : x \bmod 2 = 0 \wedge x \bmod 3 = 1 \rightsquigarrow x = 4$$

$$(0, 2) : x \bmod 2 = 0 \wedge x \bmod 3 = 2 \rightsquigarrow x = 2$$

$$(1, 0) : x \bmod 2 = 1 \wedge x \bmod 3 = 0 \rightsquigarrow x = 3$$

$$(1, 1) : x \bmod 2 = 1 \wedge x \bmod 3 = 1 \rightsquigarrow x = 1$$

$$(1, 2) : x \bmod 2 = 1 \wedge x \bmod 3 = 2 \rightsquigarrow x = 5$$

## Bemerkung zur Lösbarkeit simultaner Kongruenzen

Falls zwei Zahlen  $n_1$  und  $n_2$  teilerfremd sind, ist jede simultane Kongruenz der Form  $x \bmod n_1 = a \wedge x \bmod n_2 = b$  lösbar, und die Lösung<sup>a</sup> ist wie folgt gegeben:

<sup>a</sup>Eine ausführliche Diskussion der Theorie simultaner Kongruenzen findet sich etwa in *Elementare und algebraische Zahlentheorie* von S. Müller-Stach und J. Piontkowski, vieweg.

# Faktorisierung von Restklassenringen

## Umkehrabbildung

Wir präsentieren zu jedem Element  $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$  die Zahl  $x$  mit  $\bar{x} \in \mathbb{Z}_6$ , welche Lösung des entsprechenden Systems simultaner Kongruenzen  $x \bmod 2 = a \wedge x \bmod 3 = b$  ist:

$$(0, 0) : x \bmod 2 = 0 \wedge x \bmod 3 = 0 \rightsquigarrow x = 0$$

$$(0, 1) : x \bmod 2 = 0 \wedge x \bmod 3 = 1 \rightsquigarrow x = 4$$

$$(0, 2) : x \bmod 2 = 0 \wedge x \bmod 3 = 2 \rightsquigarrow x = 2$$

$$(1, 0) : x \bmod 2 = 1 \wedge x \bmod 3 = 0 \rightsquigarrow x = 3$$

$$(1, 1) : x \bmod 2 = 1 \wedge x \bmod 3 = 1 \rightsquigarrow x = 1$$

$$(1, 2) : x \bmod 2 = 1 \wedge x \bmod 3 = 2 \rightsquigarrow x = 5$$

## Bemerkung zur Lösbarkeit simultaner Kongruenzen

Falls zwei Zahlen  $n_1$  und  $n_2$  teilerfremd sind, ist jede simultane Kongruenz der Form  $x \bmod n_1 = a \wedge x \bmod n_2 = b$  lösbar, und die Lösung<sup>a</sup> ist wie folgt gegeben: Seien  $y_1$  und  $y_2$  (etwa mit dem erweiterten euklidischen Algorithmus) so bestimmt, dass  $y_1 \cdot n_1 + y_2 \cdot n_2 = 1$  gilt. Dann ist  $x = [a - y_1 \cdot n_1 \cdot (a - b)] \bmod (n_1 \cdot n_2)$ .

<sup>a</sup>Eine ausführliche Diskussion der Theorie simultaner Kongruenzen findet sich etwa in *Elementare und algebraische Zahlentheorie* von S. Müller-Stach und J. Piontkowski, vieweg.

# Faktorisierung von Restklassenringen

## Chinesischer Restsatz – Lösung simultaner Kongruenzen

### Chinesischer Restsatz – allgemeine Fassung

Falls die natürlichen Zahlen  $m$  und  $n$  den größten gemeinsamen Teiler  $d: = \text{ggT}(m, n)$  besitzen, so ergeben sich mit dem erweiterten euklidischen Algorithmus Zahlen  $y$  und  $z$  mit  $d = ym + zn$ .

# Faktorisierung von Restklassenringen

## Chinesischer Restsatz – Lösung simultaner Kongruenzen

### Chinesischer Restsatz – allgemeine Fassung

Falls die natürliche Zahlen  $m$  und  $n$  den größten gemeinsamen Teiler  $d: = \text{ggT}(m, n)$  besitzen, so ergeben sich mit dem erweiterten euklidischen Algorithmus Zahlen  $y$  und  $z$  mit  $d = ym + zn$ . Das System simultaner Kongruenzen

$$x \equiv_m a, \quad x \equiv_n b$$

ist genau dann lösbar, wenn

$$a \equiv_d b$$

gilt. In diesem Fall<sup>a</sup> erfüllt jede Lösung  $x \in \mathbb{Z}$  des Systems die einfache Kongruenz

$$x \equiv_{\frac{m \cdot n}{d}} b - z \cdot n \cdot \frac{b-a}{d}.$$

<sup>a</sup>Vgl. z.B. *Elementare und algebraische Zahlentheorie* von S. Müller-Stach und J. Piontkowski, vieweg.

# Faktorisierung von Restklassenringen

## Chinesischer Restsatz – Lösung simultaner Kongruenzen

### Chinesischer Restsatz – speziellere Fassung

Falls zwei natürliche Zahlen  $m$  und  $n$  teilerfremd sind (d.h.  $\text{ggT}(m, n) = 1$ ), so ist das System simultaner Kongruenzen

$$x \equiv_m a, \quad x \equiv_n b$$

**für beliebige Werte**  $a \in \mathbb{Z}$  und  $b \in \mathbb{Z}$  lösbar.



# Faktorisierung von Restklassenringen

## Chinesischer Restsatz – Lösung simultaner Kongruenzen

### Chinesischer Restsatz – speziellere Fassung

Falls zwei natürliche Zahlen  $m$  und  $n$  teilerfremd sind (d.h.  $\text{ggT}(m, n) = 1$ ), so ist das System simultaner Kongruenzen

$$x \equiv_m a, \quad x \equiv_n b$$

**für beliebige Werte**  $a \in \mathbb{Z}$  und  $b \in \mathbb{Z}$  lösbar. Seien  $y \in \mathbb{Z}$  und  $z \in \mathbb{Z}$  (etwa mit dem EEA) so bestimmt, dass  $y \cdot m + z \cdot n = 1$  gilt. Dann erfüllt jede Lösung  $x$  des Systems die einfache Kongruenz

$$x \equiv_{m \cdot n} b - z \cdot n \cdot (b - a)$$

bzw.

$$x \equiv_{m \cdot n} a - y \cdot m \cdot (a - b)$$

# Faktorisierung von Restklassenringen

Anwendung auf die modulare Berechnung von Potenzen

## Rückkehr zum RSA-Demonstrationsbeispiel: Vereinfachte Verschlüsselung

Wir hatten auf Folie 53 im Rahmen unseres RSA-Demonstrationsbeispiels für die Verschlüsselung den Wert des Ausdrucks  $10^5 \bmod 221$  zu berechnen. Derlei Rechnungen lassen sich unter Verwendung von Faktorisierungen stark vereinfachen.

# Faktorisierung von Restklassenringen

Anwendung auf die modulare Berechnung von Potenzen

## Rückkehr zum RSA-Demonstrationsbeispiel: Vereinfachte Verschlüsselung

Wir hatten auf Folie 53 im Rahmen unseres RSA-Demonstrationsbeispiels für die Verschlüsselung den Wert des Ausdrucks  $10^5 \bmod 221$  zu berechnen. Derlei Rechnungen lassen sich unter Verwendung von Faktorisierungen stark vereinfachen.

Aus  $221 = 13 \cdot 17$  folgt

$$\mathbb{Z}/221\mathbb{Z} \cong \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \cong \mathbb{Z}_{13} \times \mathbb{Z}_{17}.$$

Zur Bestimmung des Wertes von  $10^5 \bmod 221$  rechnen wir im Ring  $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$  wie folgt:

# Faktorisierung von Restklassenringen

Anwendung auf die modulare Berechnung von Potenzen

## Rückkehr zum RSA-Demonstrationsbeispiel: Vereinfachte Verschlüsselung

Wir hatten auf Folie 53 im Rahmen unseres RSA-Demonstrationsbeispiels für die Verschlüsselung den Wert des Ausdrucks  $10^5 \bmod 221$  zu berechnen. Derlei Rechnungen lassen sich unter Verwendung von Faktorisierungen stark vereinfachen.

Aus  $221 = 13 \cdot 17$  folgt

$$\mathbb{Z}/221\mathbb{Z} \cong \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \cong \mathbb{Z}_{13} \times \mathbb{Z}_{17}.$$

Zur Bestimmung des Wertes von  $10^5 \bmod 221$  rechnen wir im Ring  $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$  wie folgt:

$$10^2 = 100 \mapsto (100 \bmod 13, 100 \bmod 17) = (9, 15)$$

$$10^4 = (10^2)^2 \mapsto (9^2 \bmod 13, 15^2 \bmod 17) = (81 \bmod 13, 225 \bmod 17) = (3, 4)$$

$$10^5 = 10 \cdot 10^4 \mapsto (10 \cdot 3 \bmod 13, 10 \cdot 4 \bmod 17) = (30 \bmod 13, 40 \bmod 17) = (4, 6)$$

# Faktorisierung von Restklassenringen

Anwendung auf die modulare Berechnung von Potenzen

## Rückkehr zum RSA-Demonstrationsbeispiel: Vereinfachte Verschlüsselung

Wir hatten auf Folie 53 im Rahmen unseres RSA-Demonstrationsbeispiels für die Verschlüsselung den Wert des Ausdrucks  $10^5 \bmod 221$  zu berechnen. Derlei Rechnungen lassen sich unter Verwendung von Faktorisierungen stark vereinfachen.

Aus  $221 = 13 \cdot 17$  folgt

$$\mathbb{Z}/221\mathbb{Z} \cong \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \cong \mathbb{Z}_{13} \times \mathbb{Z}_{17}.$$

Zur Bestimmung des Wertes von  $10^5 \bmod 221$  rechnen wir im Ring  $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$  wie folgt:

$$10^2 = 100 \mapsto (100 \bmod 13, 100 \bmod 17) = (9, 15)$$

$$10^4 = (10^2)^2 \mapsto (9^2 \bmod 13, 15^2 \bmod 17) = (81 \bmod 13, 225 \bmod 17) = (3, 4)$$

$$10^5 = 10 \cdot 10^4 \mapsto (10 \cdot 3 \bmod 13, 10 \cdot 4 \bmod 17) = (30 \bmod 13, 40 \bmod 17) = (4, 6)$$

Es verbleibt nun noch das Problem, diejenige ganze Zahl  $x < 221$  zu finden, für die  $x \bmod 13 = 4$  und  $x \bmod 17 = 6$  gilt.

# Faktorisierung von Restklassenringen

Anwendung auf die modulare Berechnung von Potenzen

## Rückkehr zum RSA-Demonstrationsbeispiel: Vereinfachte Verschlüsselung

Wir hatten auf Folie 53 im Rahmen unseres RSA-Demonstrationsbeispiels für die Verschlüsselung den Wert des Ausdrucks  $10^5 \bmod 221$  zu berechnen. Derlei Rechnungen lassen sich unter Verwendung von Faktorisierungen stark vereinfachen.

Aus  $221 = 13 \cdot 17$  folgt

$$\mathbb{Z}/221\mathbb{Z} \cong \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \cong \mathbb{Z}_{13} \times \mathbb{Z}_{17}.$$

Zur Bestimmung des Wertes von  $10^5 \bmod 221$  rechnen wir im Ring  $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$  wie folgt:

$$10^2 = 100 \mapsto (100 \bmod 13, 100 \bmod 17) = (9, 15)$$

$$10^4 = (10^2)^2 \mapsto (9^2 \bmod 13, 15^2 \bmod 17) = (81 \bmod 13, 225 \bmod 17) = (3, 4)$$

$$10^5 = 10 \cdot 10^4 \mapsto (10 \cdot 3 \bmod 13, 10 \cdot 4 \bmod 17) = (30 \bmod 13, 40 \bmod 17) = (4, 6)$$

Es verbleibt nun noch das Problem, diejenige ganze Zahl  $x < 221$  zu finden, für die  $x \bmod 13 = 4$  und  $x \bmod 17 = 6$  gilt.

Vergleich der Zahlenreihen 4, 17, 30, 43, 56, 69, 82, 95, 108, ... und 6, 23, 40, 57, 74, 91, 108, ... ergibt als Ergebnis  $x = 108$ .

# Faktorisierung von Restklassenringen

Anwendung auf die modulare Berechnung von Potenzen

## Rückkehr zum RSA-Demonstrationsbeispiel: Vereinfachte Verschlüsselung

Wir hatten auf Folie 53 im Rahmen unseres RSA-Demonstrationsbeispiels für die Verschlüsselung den Wert des Ausdrucks  $10^5 \bmod 221$  zu berechnen. Derlei Rechnungen lassen sich unter Verwendung von Faktorisierungen stark vereinfachen.

Aus  $221 = 13 \cdot 17$  folgt

$$\mathbb{Z}/221\mathbb{Z} \cong \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \cong \mathbb{Z}_{13} \times \mathbb{Z}_{17}.$$

Zur Bestimmung des Wertes von  $10^5 \bmod 221$  rechnen wir im Ring  $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$  wie folgt:

$$10^2 = 100 \mapsto (100 \bmod 13, 100 \bmod 17) = (9, 15)$$

$$10^4 = (10^2)^2 \mapsto (9^2 \bmod 13, 15^2 \bmod 17) = (81 \bmod 13, 225 \bmod 17) = (3, 4)$$

$$10^5 = 10 \cdot 10^4 \mapsto (10 \cdot 3 \bmod 13, 10 \cdot 4 \bmod 17) = (30 \bmod 13, 40 \bmod 17) = (4, 6)$$

Es verbleibt nun noch das Problem, diejenige ganze Zahl  $x < 221$  zu finden, für die  $x \bmod 13 = 4$  und  $x \bmod 17 = 6$  gilt.

Vergleich der Zahlenreihen 4, 17, 30, 43, 56, 69, 82, 95, 108, ... und 6, 23, 40, 57, 74, 91, 108, ... ergibt als Ergebnis  $x = 108$ .

Alternativ hierzu verwenden wir die Lösungsformel von Folie 68 sowie die Darstellung  $1 = 4 \cdot 13 - 3 \cdot 17$ :

$$x = [4 - 4 \cdot 13 \cdot (-2)] \bmod 221 = 108.$$

# Faktorisierung von Restklassenringen

Anwendung auf die modulare Berechnung von Potenzen

## Hausübung

Auf unseren Folien 54 bis 56 wurde im Rahmen unseres RSA-Demonstrationsbeispiels zur Entschlüsselung die (recht aufwändige) Auswertung des Ausdrucks  $108^{77} \bmod 221$  vorgeführt. Nutzen Sie den Ring  $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$ , um diesen Wert möglichst durch Kopfrechnung zu bestimmen.



# Faktorisierung von Restklassenringen

Anwendung auf die modulare Berechnung von Potenzen

## Hausübung

Auf unseren Folien 54 bis 56 wurde im Rahmen unseres RSA-Demonstrationsbeispiels zur Entschlüsselung die (recht aufwändige) Auswertung des Ausdrucks  $108^{77} \bmod 221$  vorgeführt. Nutzen Sie den Ring  $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$ , um diesen Wert möglichst durch Kopfrechnung zu bestimmen.

## Starthilfe

$$108 = 8 \cdot 13 + 4 \rightsquigarrow 108 \bmod 13 = 4$$

$$108 = 6 \cdot 17 + 6 \rightsquigarrow 108 \bmod 17 = 6$$

# Faktorisierung von Restklassenringen

Anwendung auf die modulare Berechnung von Potenzen

## Fazit

Die Rechnungen bei der Verschlüsselung und auch Entschlüsselung  $\text{mod } (p \cdot q)$  vereinfachen sich durch die Faktorisierung und Rechnung im Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$ , weil dadurch mit weitaus kleineren Zahlen hantiert werden kann.

Der Preis hierfür ist, dass man am Ende eine simultane Kongruenz lösen und hierzu u.U. zunächst mit dem EEA eine Darstellung der 1 als Linearkombination der beiden Primzahlen  $p$  und  $q$  bestimmen muss.

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Was ist noch zu tun?

Wir weisen nach, dass bei Verwendung der korrekten RSA-Schlüssel das Dechiffrieren eines Chiffrats  $c := m^e \bmod n$  durch die Operation  $m' = c^d \bmod n$  immer die ursprüngliche Nachricht  $m' = m$  ergibt.

Das heißt: Wenn  $p$  und  $q$  voneinander verschiedene Primzahlen sind und  $n = p \cdot q$  gilt und wenn die ganzen Zahlen  $e$  und  $d$  die Gleichung  $e \cdot d \equiv 1 \pmod{\varphi(n)}$  erfüllen, so gilt für jede ganze Zahl  $m$  die Beziehung

$$(m^e)^d = m^{e \cdot d} \equiv m \pmod{n}.$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Was ist noch zu tun?

Wir weisen nach, dass bei Verwendung der korrekten RSA-Schlüssel das Dechiffrieren eines Chiffrats  $c := m^e \bmod n$  durch die Operation  $m' = c^d \bmod n$  immer die ursprüngliche Nachricht  $m' = m$  ergibt.

Das heißt: Wenn  $p$  und  $q$  voneinander verschiedene Primzahlen sind und  $n = p \cdot q$  gilt und wenn die ganzen Zahlen  $e$  und  $d$  die Gleichung  $e \cdot d \equiv 1 \pmod{\varphi(n)}$  erfüllen, so gilt für jede ganze Zahl  $m$  die Beziehung

$$(m^e)^d = m^{e \cdot d} \equiv m.$$

### Folgerung

Aus  $e \cdot d \equiv 1 \pmod{\varphi(n)}$  folgt  $e \cdot d = k \cdot \varphi(n) + 1$  mit  $k \in \mathbb{Z}$ . Die Gleichung  $m^{e \cdot d} \equiv m \pmod{n}$  ist somit erfüllt, wenn

$$m^{k \cdot \varphi(n) + 1} = m^{\varphi(n) \cdot k} \cdot m = \left(m^{\varphi(n)}\right)^k \cdot m \equiv m \pmod{n} \quad \text{für beliebige } k \in \mathbb{Z} \text{ gilt.}$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Was haben wir zu erwarten?

Zu erfüllen ist die Bedingung

$$m^{k \cdot \varphi(n) + 1} = m^{\varphi(n) \cdot k} \cdot m = \left(m^{\varphi(n)}\right)^k \cdot m \equiv m \pmod{n} \quad \text{für beliebige } k \in \mathbb{Z}.$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Was haben wir zu erwarten?

Zu erfüllen ist die Bedingung

$$m^{k \cdot \varphi(n) + 1} = m^{\varphi(n) \cdot k} \cdot m = \left(m^{\varphi(n)}\right)^k \cdot m \equiv m \pmod{n} \quad \text{für beliebige } k \in \mathbb{Z}.$$

### Möglichkeit 1:

Dies jedenfalls dann der Fall, wenn  $m^{\varphi(n)} \equiv 1 \pmod{n}$  ist, denn dann folgt

$$m^{k \cdot \varphi(n) + 1} = \left(m^{\varphi(n)}\right)^k \cdot m \equiv 1^k \cdot m = m.$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Was haben wir zu erwarten?

Zu erfüllen ist die Bedingung

$$m^{k \cdot \varphi(n) + 1} = m^{\varphi(n) \cdot k} \cdot m = \left(m^{\varphi(n)}\right)^k \cdot m \equiv m \pmod{n} \quad \text{für beliebige } k \in \mathbb{Z}.$$

### Möglichkeit 1:

Dies jedenfalls dann der Fall, wenn  $m^{\varphi(n)} \equiv 1 \pmod{n}$  ist, denn dann folgt

$$m^{k \cdot \varphi(n) + 1} = \left(m^{\varphi(n)}\right)^k \cdot m \equiv 1^k \cdot m = m.$$

### Möglichkeit 2:

Angenommen, es gilt zwar **nicht**  $m^{\varphi(n)} \equiv 1 \pmod{n}$ , aber für alle  $k \in \mathbb{Z}$  sind die Potenzen  $\left(m^{\varphi(n)}\right)^k$  identisch, also  $\left(m^{\varphi(n)}\right)^k = m^{\varphi(n)} =: f$  für alle  $k \in \mathbb{Z}$ .

Wir werden (noch einmal) feststellen, dass auch im Fall  $f \neq 1$  die Gleichung  $f \cdot m \equiv m \pmod{n}$  gelten kann. Dann ist  $\left(m^{\varphi(n)}\right)^k \cdot m \equiv m$  ebenfalls erfüllt.

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Vorgehensweise

Wir untersuchen für verschiedene Moduli  $n$  Potenzen der Form  $a^{\varphi(n)}$  sowie Ausdrücke der Form  $a^{\varphi(n) \cdot k + 1} = (a^{\varphi(n)})^k \cdot a$ .

Da stets  $0^k = 0 \equiv_n 0$  sowie  $a^k \equiv_n 0$ , falls  $n$  gleich  $a$  oder ein Teiler von  $a$  ist, werden diese Fälle im Folgenden nicht gesondert aufgeführt



# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Vorgehensweise

Wir untersuchen für verschiedene Moduli  $n$  Potenzen der Form  $a^{\varphi(n)}$  sowie Ausdrücke der Form  $a^{\varphi(n) \cdot k + 1} = (a^{\varphi(n)})^k \cdot a$ .

Da stets  $0^k = 0 \equiv 0$  sowie  $a^k \equiv 0$ , falls  $n$  gleich  $a$  oder ein Teiler von  $a$  ist, werden diese Fälle im Folgenden nicht gesondert aufgeführt

### Vorausschau:

Es wird sich herausstellen, dass die folgenden drei Fälle unterschiedliche Situationen ergeben:

- 1  $n$  Primzahl,
- 2  $n$  ist Produkt von (paarweise verschiedenen) Primzahlen,
- 3  $n$  ist Produkt von Primzahlpotenzen.

# Das RSA-Verfahren

Satz vom korrekten Dechiffrieren

## Vorgehensweise

Wir beginnen mit dem Beispiel, bei dem  $n$  eine **Primzahl** ist, nämlich  $n = 5$ .

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Vorgehensweise

Wir beginnen mit dem Beispiel, bei dem  $n$  eine **Primzahl** ist, nämlich  $n = 5$ .

### Potenzen modulo 5

Für alle ganzen Zahlen  $a$  mit  $1 \leq a < 5$  gilt  $\text{ggT}(5, a) = 1$ , d.h.  $\varphi(5) = 4$ :

$$\begin{array}{llll} 1^4 = 1 \equiv 1 & \rightsquigarrow 1^5 \equiv 1 \cdot 1 = 1, & \text{und } (1^4)^k \cdot 1 \equiv 1 \cdot 1 = 1 \\ 2^4 = 16 = 1 \equiv 1 & \rightsquigarrow 2^5 \equiv 1 \cdot 2 = 2, & \text{und } (2^4)^k \cdot 2 \equiv 1 \cdot 2 = 2, \\ 3^4 = 81 = 1 \equiv 1 & \rightsquigarrow 3^5 \equiv 1 \cdot 3 = 3, & \text{und } (3^4)^k \cdot 3 \equiv 1 \cdot 3 = 3, \\ 4^4 = 256 = 1 \equiv 1 & \rightsquigarrow 4^5 \equiv 1 \cdot 4 = 4 & \text{und } (4^4)^k \cdot 4 \equiv 1 \cdot 4 = 4. \end{array}$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Potenzen modulo $6 = 2 \cdot 3$

Nur für  $a = 1$  und  $a = 5$  gilt  $1 \leq a < 6$  und  $\text{ggT}(6, a) = 1$ , also ist  $\varphi(6) = 2$ .

$1^2 = 1 \equiv 1$	und	$1^2 \cdot 1 = 1 \equiv 1$
$2^2 = 4 \equiv 4 \neq 1$	aber	$2^2 \cdot 2 = 8 \equiv 2$
$3^2 = 9 \equiv 3 \neq 1$	aber	$3^2 \cdot 3 = 27 \equiv 3$
$4^2 = 16 \equiv 4 \neq 1$	aber	$4^2 \cdot 4 = 64 \equiv 4$
$5^2 = 25 \equiv 1$	und	$5^2 \cdot 5 = 125 \equiv 5$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Potenzen modulo $6 = 2 \cdot 3$

Nur für  $a = 1$  und  $a = 5$  gilt  $1 \leq a < 6$  und  $\text{ggT}(6, a) = 1$ , also ist  $\varphi(6) = 2$ .

$1^2 = 1 \equiv 1$	und	$1^2 \cdot 1 = 1 \equiv 1$
$2^2 = 4 \equiv 4 \neq 1$	aber	$2^2 \cdot 2 = 8 \equiv 2$
$3^2 = 9 \equiv 3 \neq 1$	aber	$3^2 \cdot 3 = 27 \equiv 3$
$4^2 = 16 \equiv 4 \neq 1$	aber	$4^2 \cdot 4 = 64 \equiv 4$
$5^2 = 25 \equiv 1$	und	$5^2 \cdot 5 = 125 \equiv 5$

### Höhere Potenzen von $a^{\varphi(6)} \bmod 6$ :

Wir betrachten nun höhere Potenzen von  $a^{\varphi(6)} \bmod 6$ , also Ausdrücke der Form  $(a^{\varphi(6)})^k \bmod 6$ . Als Hilfsmittel verwenden wir (informell) die Beweistechnik der **vollständigen Induktion**. Bitte recherchieren und studieren Sie diese selbständig, falls sie Ihnen noch nicht vertraut sein sollte.

# Das RSA-Verfahren

Satz vom korrekten Dechiffrieren

Höhere Potenzen von  $a^{\varphi(6)} \bmod 6$  – Beispiele und Induktion:

# Das RSA-Verfahren

Satz vom korrekten Dechiffrieren

Höhere Potenzen von  $a^{\varphi(6)} \bmod 6$  – Beispiele und Induktion:

$$\text{Beispiele: } (2^2)^2 = 16 \equiv_6 4, \quad (2^2)^3 = 4^3 = 64 \equiv_6 4,$$

# Das RSA-Verfahren

Satz vom korrekten Dechiffrieren

## Höhere Potenzen von $a^{\varphi(6)} \bmod 6$ – Beispiele und Induktion:

$$\text{Beispiele: } (2^2)^2 = 16 \equiv_6 4, \quad (2^2)^3 = 4^3 = 64 \equiv_6 4,$$

$$\text{Induktionsschritt: } (2^2)^{k+1} = 4^k \cdot 4 \equiv_6 4 \cdot 4 = 16 \equiv_6 4,$$



# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Höhere Potenzen von $a^{\varphi(6)} \bmod 6$ – Beispiele und Induktion:

$$\text{Beispiele: } (2^2)^2 = 16 \equiv_6 4, \quad (2^2)^3 = 4^3 = 64 \equiv_6 4,$$

$$\text{Induktionsschritt: } (2^2)^{k+1} = 4^k \cdot 4 \equiv_6 4 \cdot 4 = 16 \equiv_6 4,$$

$$\text{Beispiele: } (3^2)^2 = 9^2 = 81 = 13 \cdot 6 + 3 \equiv_6 3, \quad (3^2)^3 = 729 \equiv_6 3,$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Höhere Potenzen von $a^{\varphi(6)} \bmod 6$ – Beispiele und Induktion:

$$\text{Beispiele: } (2^2)^2 = 16 \equiv_6 4, \quad (2^2)^3 = 4^3 = 64 \equiv_6 4,$$

$$\text{Induktionsschritt: } (2^2)^{k+1} = 4^k \cdot 4 \equiv_6 4 \cdot 4 = 16 \equiv_6 4,$$

$$\text{Beispiele: } (3^2)^2 = 9^2 = 81 = 13 \cdot 6 + 3 \equiv_6 3, \quad (3^2)^3 = 729 \equiv_6 3,$$

$$\text{Induktionsschritt: } (3^2)^{k+1} = 9^k \cdot 9 \equiv_6 3 \cdot 9 = 27 \equiv_6 3,$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Höhere Potenzen von $a^{\varphi(6)} \bmod 6$ – Beispiele und Induktion:

$$\text{Beispiele: } (2^2)^2 = 16 \equiv_6 4, \quad (2^2)^3 = 4^3 = 64 \equiv_6 4,$$

$$\text{Induktionsschritt: } (2^2)^{k+1} = 4^k \cdot 4 \equiv_6 4 \cdot 4 = 16 \equiv_6 4,$$

$$\text{Beispiele: } (3^2)^2 = 9^2 = 81 = 13 \cdot 6 + 3 \equiv_6 3, \quad (3^2)^3 = 729 \equiv_6 3,$$

$$\text{Induktionsschritt: } (3^2)^{k+1} = 9^k \cdot 9 \equiv_6 3 \cdot 9 = 27 \equiv_6 3,$$

$$\text{Beispiel: } (4^2)^2 = 16^2 = 256 \equiv_6 4,$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Höhere Potenzen von $a^{\varphi(6)} \bmod 6$ – Beispiele und Induktion:

Beispiele:  $(2^2)^2 = 16 \equiv_6 4$ ,  $(2^2)^3 = 4^3 = 64 \equiv_6 4$ ,

Induktionsschritt:  $(2^2)^{k+1} = 4^k \cdot 4 \equiv_6 4 \cdot 4 = 16 \equiv_6 4$ ,

Beispiele:  $(3^2)^2 = 9^2 = 81 = 13 \cdot 6 + 3 \equiv_6 3$ ,  $(3^2)^3 = 729 \equiv_6 3$ ,

Induktionsschritt:  $(3^2)^{k+1} = 9^k \cdot 9 \equiv_6 3 \cdot 9 = 27 \equiv_6 3$ ,

Beispiel:  $(4^2)^2 = 16^2 = 256 \equiv_6 4$ ,

Induktionsschritt:  $(4^2)^{k+1} = 16^k \cdot 16 \equiv_6 4 \cdot 16 = 64 \equiv_6 4$ ,

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Höhere Potenzen von $a^{\varphi(6)} \bmod 6$ – Beispiele und Induktion:

$$\text{Beispiele: } (2^2)^2 = 16 \equiv_6 4, \quad (2^2)^3 = 4^3 = 64 \equiv_6 4,$$

$$\text{Induktionsschritt: } (2^2)^{k+1} = 4^k \cdot 4 \equiv_6 4 \cdot 4 = 16 \equiv_6 4,$$

$$\text{Beispiele: } (3^2)^2 = 9^2 = 81 = 13 \cdot 6 + 3 \equiv_6 3, \quad (3^2)^3 = 729 \equiv_6 3,$$

$$\text{Induktionsschritt: } (3^2)^{k+1} = 9^k \cdot 9 \equiv_6 3 \cdot 9 = 27 \equiv_6 3,$$

$$\text{Beispiel: } (4^2)^2 = 16^2 = 256 \equiv_6 4,$$

$$\text{Induktionsschritt: } (4^2)^{k+1} = 16^k \cdot 16 \equiv_6 4 \cdot 16 = 64 \equiv_6 4,$$

$$\text{Beispiel: } (5^2)^2 = 25^2 = 625 \equiv_6 1,$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Höhere Potenzen von $a^{\varphi(6)} \bmod 6$ – Beispiele und Induktion:

Beispiele:  $(2^2)^2 = 16 \equiv_6 4$ ,  $(2^2)^3 = 4^3 = 64 \equiv_6 4$ ,

Induktionsschritt:  $(2^2)^{k+1} = 4^k \cdot 4 \equiv_6 4 \cdot 4 = 16 \equiv_6 4$ ,

Beispiele:  $(3^2)^2 = 9^2 = 81 = 13 \cdot 6 + 3 \equiv_6 3$ ,  $(3^2)^3 = 729 \equiv_6 3$ ,

Induktionsschritt:  $(3^2)^{k+1} = 9^k \cdot 9 \equiv_6 3 \cdot 9 = 27 \equiv_6 3$ ,

Beispiel:  $(4^2)^2 = 16^2 = 256 \equiv_6 4$ ,

Induktionsschritt:  $(4^2)^{k+1} = 16^k \cdot 16 \equiv_6 4 \cdot 16 = 64 \equiv_6 4$ ,

Beispiel:  $(5^2)^2 = 25^2 = 625 \equiv_6 1$ ,

Induktionsschritt:  $(5^2)^{k+1} = 25^k \cdot 25 \equiv_6 1 \cdot 1 \equiv_6 1$ .

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Annäherung an unser Ziel für $n = 6 = 2 \cdot 3$

Wir zeigen nun, dass für alle  $a$  mit  $1 \leq a < 6$  und für beliebige  $k \in \mathbb{N}$  stets die Beziehung  $(a^{\varphi(6)})^k \cdot a = a$  gilt. Hierzu verwenden wir unsere Ergebnisse der vorigen Folie.

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Annäherung an unser Ziel für $n = 6 = 2 \cdot 3$

Wir zeigen nun, dass für alle  $a$  mit  $1 \leq a < 6$  und für beliebige  $k \in \mathbb{N}$  stets die Beziehung  $(a^{\varphi(6)})^k \cdot a = a$  gilt. Hierzu verwenden wir unsere Ergebnisse der vorigen Folie.

### Berechne $(a^{\varphi(6)})^k \cdot a$ für beliebige $k \in \mathbb{N}$ , vgl. Folie 79:

$$\begin{aligned}(1^2)^k \cdot 1 &= 1 \cdot 1 = 1 \equiv_6 1, \\(2^2)^k \cdot 2 &= 4^k \cdot 2 \equiv_6 4 \cdot 2 = 8 \equiv_6 2, \\(3^2)^k \cdot 3 &= 9^k \cdot 3 \equiv_6 3 \cdot 3 = 9 \equiv_6 3, \\(4^2)^k \cdot 4 &= 16^k \cdot 4 \equiv_6 4 \cdot 4 = 16 \equiv_6 4, \\(5^2)^k \cdot 5 &= 25^k \cdot 5 \equiv_6 1 \cdot 5 = 5 \equiv_6 5.\end{aligned}$$



# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Beispiel für Fall 3: $n = 8 = 2^3$

Nur für  $a = 1, a = 3, a = 5$  und  $a = 7$  gilt  $1 \leq a < 8$  und  $\text{ggT}(8, a) = 1$ , d.h.  $\varphi(8) = 4$ .

$1^4 = 1 \equiv_8 1$	und	$1^4 \cdot 1 = 1 \equiv_8 1$
$2^4 = 16 \equiv_8 0 \neq 1$	und	$2^4 \cdot 2 = 32 \equiv_8 0 \neq 2$
$3^4 = 81 \equiv_8 1$	und	$3^4 \cdot 3 = 243 \equiv_8 3$
$4^4 = 256 \equiv_8 0 \neq 1$	und	$4^4 \cdot 4 = 1024 \equiv_8 0 \neq 4$
$5^4 = 625 \equiv_8 1$	und	$5^4 \cdot 5 = 3125 \equiv_8 5$
$6^4 = 1096 \equiv_8 0 \neq 1$	und	$6^4 \cdot 6 = \dots \equiv_8 0 \neq 6$
$7^4 = 2401 \equiv_8 1$	und	$7^4 \cdot 7 = \dots \equiv_8 7.$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Beispiel für Fall 3: $n = 8 = 2^3$

Nur für  $a = 1$ ,  $a = 3$ ,  $a = 5$  und  $a = 7$  gilt  $1 \leq a < 8$  und  $\text{ggT}(8, a) = 1$ , d.h.  $\varphi(8) = 4$ .

$1^4 = 1 \equiv_8 1$	und	$1^4 \cdot 1 = 1 \equiv_8 1$
$2^4 = 16 \equiv_8 0 \neq 1$	und	$2^4 \cdot 2 = 32 \equiv_8 0 \neq 2$
$3^4 = 81 \equiv_8 1$	und	$3^4 \cdot 3 = 243 \equiv_8 3$
$4^4 = 256 \equiv_8 0 \neq 1$	und	$4^4 \cdot 4 = 1024 \equiv_8 0 \neq 4$
$5^4 = 625 \equiv_8 1$	und	$5^4 \cdot 5 = 3125 \equiv_8 5$
$6^4 = 1096 \equiv_8 0 \neq 1$	und	$6^4 \cdot 6 = \dots \equiv_8 0 \neq 6$
$7^4 = 2401 \equiv_8 1$	und	$7^4 \cdot 7 = \dots \equiv_8 7.$

### Bemerkung

Wir stellen fest, dass die Beziehung  $(a^{\varphi(n)})^k \cdot a \equiv_n a$  in diesem Fall **nicht** universell gilt. Dies liegt daran, dass 8 weder eine Primzahl noch ein Produkt von (unterschiedlichen) Primzahlen, sondern eine Primzahlpotenz ist.

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Weiteres Beispiel für Fall 3: $n = 18 = 2^1 \cdot 3^2$

Nur für  $a = 1, a = 5, a = 7, a = 11, a = 13$  und  $a = 17$  gilt  $1 \leq a < 18$  und  $\text{ggT}(a, 18) = 1$ , d.h.  $\varphi(18) = 6$ .

$1^6 = 1 \equiv_{18} 1$	und	$1^6 \cdot 1 = 1 \equiv_{18} 1$
$2^6 = 64 \equiv_{18} 10 \neq 1$	und	$2^6 \cdot 2 = 128 = 7 \cdot 18 + 2 \equiv_{18} 2$
$3^6 = 27^2 \equiv_{18} 9 \neq 1$	und	$3^6 \cdot 3 \equiv_{18} 9 \cdot 3 \equiv_{18} 9 \neq 3$
$4^6 = 64^2 \equiv_{18} 10^2 \equiv_{18} 10 \neq 1$	und	$4^6 \cdot 4 \equiv_{18} 10 \cdot 4 = 40 \equiv_{18} 4$
$5^6 = 125^2 \equiv_{18} (-1)^2 = 1$	und	$5^6 \cdot 5 \equiv_{18} 1 \cdot 5 = 5$
$6^6 = 216^2 \equiv_{18} 0 \neq 1$	und	$6^6 \cdot 6 \equiv_{18} 0 \cdot 6 = 0 \neq 6$
$7^6 = 343^2 \equiv_{18} 1$	und	$7^6 \cdot 7 \equiv_{18} 1 \cdot 7 = 7$
$8^6 = 512^2 \equiv_{18} 8^2 \equiv_{18} 10$	und	$8^6 \cdot 8 = 80 \equiv_{18} 8$
$9^6 = 729^2 \equiv_{18} 9^2 \equiv_{18} 9$	und	$9^6 \cdot 9 = \dots \equiv_{18} 9$
$\vdots$	$\vdots$	$\vdots$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Weiteres Beispiel für Fall 3: $n = 18 = 2^1 \cdot 3^2$

Nur für  $a = 1, a = 5, a = 7, a = 11, a = 13$  und  $a = 17$  gilt  $1 \leq a < 18$  und  $\text{ggT}(a, 18) = 1$ , d.h.  $\varphi(18) = 6$ .

$1^6 = 1 \equiv_{18} 1$	und	$1^6 \cdot 1 = 1 \equiv_{18} 1$
$2^6 = 64 \equiv_{18} 10 \neq 1$	und	$2^6 \cdot 2 = 128 = 7 \cdot 18 + 2 \equiv_{18} 2$
$3^6 = 27^2 \equiv_{18} 9 \neq 1$	und	$3^6 \cdot 3 \equiv_{18} 9 \cdot 3 \equiv_{18} 9 \neq 3$
$4^6 = 64^2 \equiv_{18} 10^2 \equiv_{18} 10 \neq 1$	und	$4^6 \cdot 4 \equiv_{18} 10 \cdot 4 = 40 \equiv_{18} 4$
$5^6 = 125^2 \equiv_{18} (-1)^2 = 1$	und	$5^6 \cdot 5 \equiv_{18} 1 \cdot 5 = 5$
$6^6 = 216^2 \equiv_{18} 0 \neq 1$	und	$6^6 \cdot 6 \equiv_{18} 0 \cdot 6 = 0 \neq 6$
$7^6 = 343^2 \equiv_{18} 1$	und	$7^6 \cdot 7 \equiv_{18} 1 \cdot 7 = 7$
$8^6 = 512^2 \equiv_{18} 8^2 \equiv_{18} 10$	und	$8^6 \cdot 8 = 80 \equiv_{18} 8$
$9^6 = 729^2 \equiv_{18} 9^2 \equiv_{18} 9$	und	$9^6 \cdot 9 = \dots \equiv_{18} 9$
$\vdots$	$\vdots$	$\vdots$

### Bemerkung

Wir stellen fest, dass die Beziehung  $(a^{\varphi(n)})^k \cdot a \equiv_n a$  auch hier **nicht** universell gilt. Dies liegt daran, dass 18 weder eine Primzahl noch ein Produkt von (unterschiedlichen) Primzahlen, sondern ein Produkt von Primzahlpotenzen ist.

# Das RSA-Verfahren

Satz vom korrekten Dechiffrieren

## Werkzeuge aus der Algebra:

Aus der Theorie der Gruppen und Ringe (Algebra) sind einige Theoreme bekannt, die uns bzgl. des Dechiffrierproblems Klärung bringen.

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Werkzeuge aus der Algebra:

Aus der Theorie der Gruppen und Ringe (Algebra) sind einige Theoreme bekannt, die uns bzgl. des Dechiffrierproblems Klärung bringen.

### Der kleine Satz von Fermat

Ist  $p$  eine Primzahl, und ist  $a$  eine ganze Zahl mit  $1 \leq a < p$ , so gilt

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

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Werkzeuge aus der Algebra:

Aus der Theorie der Gruppen und Ringe (Algebra) sind einige Theoreme bekannt, die uns bzgl. des Dechiffrierproblems Klärung bringen.

### Der kleine Satz von Fermat

Ist  $p$  eine Primzahl, und ist  $a$  eine ganze Zahl mit  $1 \leq a < p$ , so gilt

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

### Skizze einer Begründung

Da  $p$  eine Primzahl ist, sind alle ganzen Zahlen  $a$  mit  $1 \leq a < p$  teilerfremd zu  $p$  und somit **Einheiten** im Ring  $Z_p$ . Die Menge (Gruppe) der Einheiten in  $Z_p$  hat somit die Mächtigkeit  $p - 1$ . Nach dem *Satz von Lagrange*<sup>a</sup> gilt in jeder endlichen Gruppe  $G$  mit Neutralelement  $e$  und Mächtigkeit  $|G|$  für jedes Element  $g \in G$  die Gleichung  $g^{|G|} = e$ .

<sup>a</sup>Dieser Satz ist ein wichtiges Resultat aus der Theorie der endlichen Gruppen.

# Das RSA-Verfahren

Satz vom korrekten Dechiffrieren

## Folgerung aus dem kleinen Fermat'schen Satz:

Ist  $p$  eine Primzahl, und ist  $a$  eine ganze Zahl, die kein Vielfaches von  $p$  ist, so gilt

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



# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Folgerung aus dem kleinen Fermat'schen Satz:

Ist  $p$  eine Primzahl, und ist  $a$  eine ganze Zahl, die kein Vielfaches von  $p$  ist, so gilt

$$a^p \equiv a.$$

### Begründung

Da  $a$  kein Vielfaches von  $p$  ist, gilt  $a \bmod p \neq 0$ . Somit folgt  $a^{p-1} \equiv 1 \pmod{p}$  (Fermat) und hieraus  $a^p = a^{p-1} \cdot a \equiv 1 \cdot a = a.$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Folgerung aus dem kleinen Fermat'schen Satz:

Ist  $p$  eine Primzahl, und ist  $a$  eine ganze Zahl, die kein Vielfaches von  $p$  ist, so gilt

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

### Begründung

Da  $a$  kein Vielfaches von  $p$  ist, gilt  $a \bmod p \neq 0$ . Somit folgt  $a^{p-1} \equiv 1 \pmod{p}$  (Fermat) und hieraus  $a^p = a^{p-1} \cdot a \equiv 1 \cdot a = a \pmod{p}$ .

### Bemerkung:

Der kleine Satz von Fermat liefert Aussagen über Ringe mit Primzahlordnung. Beim RSA-Verfahren arbeiten wir jedoch mit Ringen  $\mathbb{Z}_n$ , bei denen  $n$  jeweils **keine** Primzahl, sondern ein Produkt von Primzahlen ist. Die nächste Folie beginnt die Klärung der allgemeineren Situation.

# Das RSA-Verfahren

Satz vom korrekten Dechiffrieren

## Verallgemeinerung: Satz von Euler

Ist  $n > 1$  eine natürliche Zahl und ist  $a$  eine ganze Zahl mit  $\text{ggT}(n, a) = 1$ , so gilt

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

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Verallgemeinerung: Satz von Euler

Ist  $n > 1$  eine natürliche Zahl und ist  $a$  eine ganze Zahl mit  $\text{ggT}(n, a) = 1$ , so gilt

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

### Skizze einer Begründung

Wegen der Voraussetzung  $\text{ggT}(n, a) = 1$  ist  $a \bmod n$  eine **Einheit** im Ring  $\mathbb{Z}_n$ . Die Gruppe der Einheiten in  $\mathbb{Z}_n$  hat die Mächtigkeit  $\varphi(n)$ . Wiederum aus dem *Satz von Lagrange* folgt die Gleichung  $a^{\varphi(n)} = 1$ .

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Verallgemeinerung: Satz von Euler

Ist  $n > 1$  eine natürliche Zahl und ist  $a$  eine ganze Zahl mit  $\text{ggT}(n, a) = 1$ , so gilt

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

### Skizze einer Begründung

Wegen der Voraussetzung  $\text{ggT}(n, a) = 1$  ist  $a \bmod n$  eine **Einheit** im Ring  $\mathbb{Z}_n$ . Die Gruppe der Einheiten in  $\mathbb{Z}_n$  hat die Mächtigkeit  $\varphi(n)$ . Wiederum aus dem *Satz von Lagrange* folgt die Gleichung  $a^{\varphi(n)} = 1$ .

### Bemerkung

Für jede natürliche Zahl  $n > 1$  ist somit klar, dass die Gleichung  $(a^{\varphi(n)})^k \cdot a \equiv 1^k \cdot a = a$  für Einheiten (also für Zahlen  $a$  mit  $\text{ggT}(a, n) = 1$ ) richtig ist. Für **Nichteinheiten** ist dies im Allgemeinen **nicht** der Fall, wie wir auf Folie 81 gesehen haben. Wir wollen nun (hinreichende) Bedingungen benennen, die sicherstellen, dass  $(a^{\varphi(n)})^k \cdot a \equiv a = a$  für alle ganzen Zahlen  $a$  mit  $0 \leq a < n$  gilt.

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Wiederholung der Formulierung des Satzes

Es seien  $p$  und  $q$  voneinander verschiedene Primzahlen und es sei  $n = p \cdot q$ . Ferner erfüllen die ganzen Zahlen  $e$  und  $d$  die Gleichung  $e \cdot d \equiv 1 \pmod{\varphi(n)}$ , d.h. es gibt eine ganze Zahl  $k$  mit  $e \cdot d = k \cdot \varphi(n) = k \cdot (p-1) \cdot (q-1)$ . Dann gilt für jede ganze Zahl  $m < n$  die Beziehung

$$(m^e)^d \bmod n = (m^{(p-1) \cdot (q-1)})^k \cdot m \bmod n = m.$$

# Das RSA-Verfahren

## Satz vom korrekten Dechiffrieren

### Wiederholung der Formulierung des Satzes

Es seien  $p$  und  $q$  voneinander verschiedene Primzahlen und es sei  $n = p \cdot q$ . Ferner erfüllen die ganzen Zahlen  $e$  und  $d$  die Gleichung  $e \cdot d \equiv 1 \pmod{\varphi(n)}$ , d.h. es gibt eine ganze Zahl  $k$  mit  $e \cdot d = k \cdot \varphi(n) = k \cdot (p-1) \cdot (q-1)$ . Dann gilt für jede ganze Zahl  $m < n$  die Beziehung

$$(m^e)^d \bmod n = (m^{(p-1) \cdot (q-1)})^k \cdot m \bmod n = m.$$

### Beweis später

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

## Ausblick auf den Rest der Wegstrecke:

Auf den folgenden Folien sehen wir uns das Dechiffrierproblem noch einmal unter Zuhilfenahme geeigneter Faktorisierungen an. Wir werden anhand von Beispielen noch einmal sehen, warum Ringe der Form  $\mathbb{Z}_n$  mit  $n = p$  oder  $n = p \cdot q$  oder auch  $n = p_1 \cdot p_2 \cdot \dots \cdot p_r$  geeignet sind, während das Auftreten von **Primzahlpotenzen** in der Primfaktorzerlegung von  $n$  ein Hindernis darstellt.



# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

## Ausblick auf den Rest der Wegstrecke:

Auf den folgenden Folien sehen wir uns das Dechiffrierproblem noch einmal unter Zuhilfenahme geeigneter Faktorisierungen an. Wir werden anhand von Beispielen noch einmal sehen, warum Ringe der Form  $\mathbb{Z}_n$  mit  $n = p$  oder  $n = p \cdot q$  oder auch  $n = p_1 \cdot p_2 \cdot \dots \cdot p_r$  geeignet sind, während das Auftreten von **Primzahlpotenzen** in der Primfaktorzerlegung von  $n$  ein Hindernis darstellt.

## Erinnerung:

Wir haben zu prüfen, ob für alle  $m \in \mathbb{Z}_n$  und alle  $k \in \mathbb{N}$  die Gleichung

$$(m^{\varphi n})^k \cdot m \bmod n = m$$

gilt.

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

## Einheiten

Seien  $p$  und  $q$  Primzahlen. Wir halten ohne Beweis fest, dass die Einheiten im Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$  genau diejenigen Elemente  $(a, b)$  sind, für die  $a \neq 0$  und  $b \neq 0$  gilt.

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem ...

...im Ring  $\mathbb{Z}_6$  mit  $\varphi(6) = 2$ :

Wir betrachten  $(m^2)^k \cdot m$ .

$$(\bar{0}^2)^2 \cdot \bar{0} \mapsto \left( (0^2)^k \bmod 2, (0^2)^k \bmod 3 \right) \cdot (0, 0) = (0 \cdot 0 \bmod 2, 0 \cdot 0 \bmod 3) = (0, 0) \rightsquigarrow \bar{0}$$

$$(\bar{1}^2)^2 \cdot \bar{1} \mapsto \left( (1^2)^k \bmod 2, (1^2)^k \bmod 3 \right) \cdot (1, 1) = (1 \cdot 1 \bmod 2, 1 \cdot 1 \bmod 3) = (1, 1) \rightsquigarrow \bar{1}$$

$$(\bar{2}^2)^2 \cdot \bar{2} \mapsto \left( (0^2)^k \bmod 2, (2^2)^k \bmod 3 \right) \cdot (0, 2) = (0 \cdot 0 \bmod 2, 1 \cdot 2 \bmod 3) = (0, 2) = \rightsquigarrow \bar{2}$$

$$(\bar{3}^2)^2 \cdot \bar{3} \mapsto \left( (1^2)^k \bmod 2, (0^2)^k \bmod 3 \right) \cdot (1, 0) = (1 \cdot 1 \bmod 2, 0 \cdot 0 \bmod 3) = (1, 0) \rightsquigarrow \bar{3}$$

$$(\bar{4}^2)^2 \cdot \bar{4} \mapsto \left( (0^2)^k \bmod 2, (1^2)^k \bmod 3 \right) \cdot (0, 1) = (0 \cdot 0 \bmod 2, 1 \cdot 1 \bmod 3) = (0, 1) \rightsquigarrow \bar{4}$$

$$(\bar{5}^2)^2 \cdot \bar{5} \mapsto \left( (1^2)^k \bmod 2, (2^2)^k \bmod 3 \right) \cdot (1, 2) = (1 \cdot 1 \bmod 2, 1 \cdot 2 \bmod 3) = (1, 2) \rightsquigarrow \bar{5}$$

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

**Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ :**

Wir erinnern an die Abbildung  $f: \mathbb{Z}_{p \cdot q} \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q, x \mapsto (x \bmod p, x \bmod q)$ , welche die Korrespondenz zwischen dem Ring  $\mathbb{Z}_{p \cdot q}$  und dem Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$  herstellt.

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

**Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ :**

Wir erinnern an die Abbildung<sup>a</sup>  $f: \mathbb{Z}_{p \cdot q} \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q, x \mapsto (x \bmod p, x \bmod q)$ , welche die Korrespondenz zwischen dem Ring  $\mathbb{Z}_{p \cdot q}$  und dem Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$  herstellt.

<sup>a</sup>Diese Abbildung ist bijektiv und übersetzt die Ringoperationen richtig. Man sagt auch  $f$  ist ein *Ring-Isomorphismus* und kennzeichnet zueinander isomorphe Ringe durch das Zeichen  $\cong$ .

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

**Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ :**

Wir erinnern an die Abbildung  $f: \mathbb{Z}_{p \cdot q} \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q, x \mapsto (x \bmod p, x \bmod q)$ , welche die Korrespondenz zwischen dem Ring  $\mathbb{Z}_{p \cdot q}$  und dem Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$  herstellt.

## **Einheiten und Nichteinheiten:**

Die Einheiten im Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$  sind genau diejenigen Elemente  $(a, b)$ , für die  $a \neq 0$  und  $b \neq 0$  gilt.

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

**Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ :**

Wir erinnern an die Abbildung  $f: \mathbb{Z}_{p \cdot q} \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q, x \mapsto (x \bmod p, x \bmod q)$ , welche die Korrespondenz zwischen dem Ring  $\mathbb{Z}_{p \cdot q}$  und dem Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$  herstellt.

## Einheiten und Nichteinheiten:

Die Einheiten im Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$  sind genau diejenigen Elemente  $(a, b)$ , für die  $a \neq 0$  und  $b \neq 0$  gilt.

## Begründung:

Ist  $x$  **keine** Einheit in  $\mathbb{Z}_{p \cdot q}$ , gilt also  $\text{ggT}(x, p \cdot q) \neq 1$ , so ist  $x$  durch  $p$  oder durch  $q$  teilbar, d.h. es gilt  $x \bmod p = 0$  oder  $x \bmod q = 0$ . Somit ist  $f(x) = (a, 0)$  oder  $f(x) = (0, b)$ .

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

**Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ :**

Wir erinnern an die Abbildung<sup>a</sup>  $f: \mathbb{Z}_{p \cdot q} \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q, x \mapsto (x \bmod p, x \bmod q)$ , welche die Korrespondenz zwischen dem Ring  $\mathbb{Z}_{p \cdot q}$  und dem Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$  herstellt.

## Einheiten und Nichteinheiten:

Die Einheiten im Ring  $\mathbb{Z}_p \times \mathbb{Z}_q$  sind genau diejenigen Elemente  $(a, b)$ , für die  $a \neq 0$  und  $b \neq 0$  gilt.

## Begründung:

Ist  $x$  **keine** Einheit in  $\mathbb{Z}_{p \cdot q}$ , gilt also  $\text{ggT}(x, p \cdot q) \neq 1$ , so ist  $x$  durch  $p$  oder durch  $q$  teilbar, d.h. es gilt  $x \bmod p = 0$  oder  $x \bmod q = 0$ . Somit ist  $f(x) = (a, 0)$  oder  $f(x) = (0, b)$ .

<sup>a</sup>Diese Abbildung ist bijektiv und übersetzt die Ringoperationen richtig. Man sagt auch  $f$  ist ein *Ring-Isomorphismus* und kennzeichnet zueinander isomorphe Ringe durch das Zeichen  $\cong$ .



# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

**Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 2:**

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 2:

Auswertung des Ausdrucks  $m^{\varphi(n)}$ :

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 2:

Auswertung des Ausdrucks  $m^{\varphi(n)}$ :

Für Einheiten

Falls  $m$  eine Einheit in  $\mathbb{Z}_{p \cdot q}$  ist, so gilt  $m^{\varphi(p \cdot q)} \bmod n = 1$  nach dem Satz von Euler. Wir sehen uns an, wie sich dies im Korrespondenzring  $\mathbb{Z}_p \times \mathbb{Z}_q$  äußert:

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 2:

Auswertung des Ausdrucks  $m^{\varphi(n)}$ :

Für Einheiten

Falls  $m$  eine Einheit in  $\mathbb{Z}_{p \cdot q}$  ist, so gilt  $m^{\varphi(p \cdot q)} \bmod n = 1$  nach dem Satz von Euler. Wir sehen uns an, wie sich dies im Korrespondenzring  $\mathbb{Z}_p \times \mathbb{Z}_q$  äußert:

- Der Ausdruck  $m^{\varphi(n)} \bmod n$  übersetzt sich durch  $f$  in den Ausdruck  $f(m^{\varphi(n)}) = \left( (a^{p-1})^{q-1} \bmod p, (b^{q-1})^{p-1} \bmod q \right)$

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 2:

Auswertung des Ausdrucks  $m^{\varphi(n)}$ :

Für Einheiten

Falls  $m$  eine Einheit in  $\mathbb{Z}_{p \cdot q}$  ist, so gilt  $m^{\varphi(p \cdot q)} \bmod n = 1$  nach dem Satz von Euler. Wir sehen uns an, wie sich dies im Korrespondenzring  $\mathbb{Z}_p \times \mathbb{Z}_q$  äußert:

- Der Ausdruck  $m^{\varphi(n)} \bmod n$  übersetzt sich durch  $f$  in den Ausdruck  $f(m^{\varphi(n)}) = \left( (a^{p-1})^{q-1} \bmod p, (b^{q-1})^{p-1} \bmod q \right)$
- Falls  $m$  Einheit ist, sind beide Komponenten von  $f(m) = (a, b)$  ungleich Null. Nach dem kleinen Satz von Fermat ist dann

$$\begin{aligned} & \left( (a^{p-1})^{q-1} \bmod p, (b^{q-1})^{p-1} \bmod q \right) \\ &= \left( (1)^{q-1} \bmod p, (1)^{p-1} \bmod q \right) \\ &= (1, 1). \end{aligned}$$

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

**Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 3:**

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 3:

Auswertung des Ausdrucks  $m^{\varphi(n)}$ :

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 3:

Auswertung des Ausdrucks  $m^{\varphi(n)}$ :

Für Nicht-Einheiten:



# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 3:

Auswertung des Ausdrucks  $m^{\varphi(n)}$ :

Für Nicht-Einheiten:

- Ist  $m$  **keine** Einheit, so ist die erste oder die zweite Komponente von  $f(m) = (a, b)$  gleich Null. Wir betrachten den Fall, dass  $m \neq 0$  durch  $p$  teilbar ist, dann gilt  $a = 0$  und  $b \neq 0$ :

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 3:

Auswertung des Ausdrucks  $m^{\varphi(n)}$ :

Für Nicht-Einheiten:

- Ist  $m$  **keine** Einheit, so ist die erste oder die zweite Komponente von  $f(m) = (a, b)$  gleich Null. Wir betrachten den Fall, dass  $m \neq 0$  durch  $p$  teilbar ist, dann gilt  $a = 0$  und  $b \neq 0$ :
- Der Ausdruck  $m^{\varphi(n)} \bmod n$  übersetzt sich in diesem Fall durch  $f$  in den Ausdruck

$$\begin{aligned} & \left( (a^{p-1})^{q-1} \bmod p, (b^{q-1})^{p-1} \bmod q \right) \\ &= \left( 0, (1)^{p-1} \bmod q \right) \\ &= (0, 1). \end{aligned}$$

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 3:

Auswertung des Ausdrucks  $m^{\varphi(n)}$ :

Für Nicht-Einheiten:

- Ist  $m$  **keine** Einheit, so ist die erste oder die zweite Komponente von  $f(m) = (a, b)$  gleich Null. Wir betrachten den Fall, dass  $m \neq 0$  durch  $p$  teilbar ist, dann gilt  $a = 0$  und  $b \neq 0$ :
- Der Ausdruck  $m^{\varphi(n)} \bmod n$  übersetzt sich in diesem Fall durch  $f$  in den Ausdruck

$$\begin{aligned} & \left( (a^{p-1})^{q-1} \bmod p, (b^{q-1})^{p-1} \bmod q \right) \\ &= \left( 0, (1)^{p-1} \bmod q \right) \\ &= (0, 1). \end{aligned}$$

- Falls  $m \neq 0$  durch  $q$  teilbar ist, ergibt sich entsprechend  $(1, 0)$  und für  $m = 0$  ist natürlich  $f(m^{\varphi(n)}) = (0, 0)$ .

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

**Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 4:**

Es sei im Folgenden stets  $m \in \mathbb{Z}_{p \cdot q}$ . Wir überzeugen uns davon, dass  $(m^{\varphi(n)})^k \cdot m = m$  gilt, wie es korrekte Dechiffrieren notwendig ist. Hierzu verwenden wir die Korrespondenz  $f(m) = (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$ .

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 4:

Es sei im Folgenden stets  $m \in \mathbb{Z}_{p \cdot q}$ . Wir überzeugen uns davon, dass  $(m^{\varphi(n)})^k \cdot m = m$  gilt, wie es korrekte Dechiffrieren notwendig ist. Hierzu verwenden wir die Korrespondenz  $f(m) = (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$ .

**Auswertung des Ausdrucks  $(m^{\varphi(n)})^k \cdot m$ :**

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 4:

Es sei im Folgenden stets  $m \in \mathbb{Z}_{p \cdot q}$ . Wir überzeugen uns davon, dass  $(m^{\varphi(n)})^k \cdot m = m$  gilt, wie es korrekte Dechiffrieren notwendig ist. Hierzu verwenden wir die Korrespondenz  $f(m) = (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$ .

**Auswertung des Ausdrucks  $(m^{\varphi(n)})^k \cdot m$ :**

**Für Einheiten:**

Ist  $m$  eine Einheit, so übersetzt sich der Ausdruck  $(m^{\varphi(n)})^k \cdot m$  durch  $f$  in den Ausdruck  $(1^k \cdot a \bmod p, 1^k \cdot b \bmod q) = (a, b) \rightsquigarrow m$ .

# Faktorisierung von Restklassenringen

## Anwendung auf das Dechiffrierproblem

Analyse für Ringe der Form  $\mathbb{Z}_{p \cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$  mit Primzahlen  $p$  und  $q$ , Teil 4:

Es sei im Folgenden stets  $m \in \mathbb{Z}_{p \cdot q}$ . Wir überzeugen uns davon, dass  $(m^{\varphi(n)})^k \cdot m = m$  gilt, wie es korrekte Dechiffrieren notwendig ist. Hierzu verwenden wir die Korrespondenz  $f(m) = (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$ .

**Auswertung des Ausdrucks  $(m^{\varphi(n)})^k \cdot m$ :**

**Für Einheiten:**

Ist  $m$  eine Einheit, so übersetzt sich der Ausdruck  $(m^{\varphi(n)})^k \cdot m$  durch  $f$  in den Ausdruck  $(1^k \cdot a \bmod p, 1^k \cdot b \bmod q) = (a, b) \rightsquigarrow m$ .

**Für Nicht-Einheiten:**

Wir betrachten zunächst den Fall, dass  $m \neq 0$  durch  $p$  teilbar ist. Wie gesehen, gilt dann  $f(m) = (0, b)$  mit  $b \neq 0$  und

$$f\left((m^{\varphi(n)})^k \cdot m\right) = (0^k \cdot a \bmod p, 1^k \cdot b \bmod q) = (0, b) \rightsquigarrow m.$$

Fall andererseits  $m \neq 0$  durch  $q$  teilbar ist, so ist  $f(m) = (a, 0)$  mit  $a \neq 0$  und

$$f\left((m^{\varphi(n)})^k \cdot m\right) = (1^k \cdot a \bmod p, 0^k \cdot b \bmod q) = (a, 0) \rightsquigarrow m.$$

# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

## Exemplarische Analyse für den Ring $\mathbb{Z}_{18} = \mathbb{Z}_{2 \cdot 3^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$

Wir werden sehen, dass in diesem Ring die Gleichung  $(m^{\varphi(n)})^k \cdot m = m$  **nicht** für alle Elemente  $m$  gilt. Dies liegt daran, dass schon der Ring  $\mathbb{Z}_9$  Nullteiler besitzt. Die Einheiten in  $\mathbb{Z}_{18}$  sind 1, 5, 7, 11, 13 und 17, und es ist  $\varphi(18) = 6$ .



# Faktorisierung von Restklassenringen

Anwendung auf das Dechiffrierproblem

**Exemplarische Analyse für den Ring  $\mathbb{Z}_{18} = \mathbb{Z}_{2 \cdot 3^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$**

Wir werden sehen, dass in diesem Ring die Gleichung  $(m^{\varphi(n)})^k \cdot m = m$  **nicht** für alle Elemente  $m$  gilt. Dies liegt daran, dass schon der Ring  $\mathbb{Z}_9$  Nullteiler besitzt. Die Einheiten in  $\mathbb{Z}_{18}$  sind 1, 5, 7, 11, 13 und 17, und es ist  $\varphi(18) = 6$ .

**Auswertung des Ausdrucks  $(m^{\varphi(n)})^k \cdot m = (m^6)^k \cdot m$ :**

# Faktorisierung von Restklassenringen

## Anwendung auf das Dechiffrierproblem

### Exemplarische Analyse für den Ring $\mathbb{Z}_{18} = \mathbb{Z}_{2 \cdot 3^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$

Wir werden sehen, dass in diesem Ring die Gleichung  $(m^{\varphi(n)})^k \cdot m = m$  **nicht** für alle Elemente  $m$  gilt. Dies liegt daran, dass schon der Ring  $\mathbb{Z}_9$  Nullteiler besitzt. Die Einheiten in  $\mathbb{Z}_{18}$  sind 1, 5, 7, 11, 13 und 17, und es ist  $\varphi(18) = 6$ .

**Auswertung des Ausdrucks**  $(m^{\varphi(n)})^k \cdot m = (m^6)^k \cdot m$ :

**Für Einheiten:**

Ist  $m$  eine Einheit, so gilt nach dem Satz von Euler  $(m^6)^k \cdot m \bmod 18 = (1)^k \cdot m \bmod 18 = m$ .

# Faktorisierung von Restklassenringen

## Anwendung auf das Dechiffrierproblem

### Exemplarische Analyse für den Ring $\mathbb{Z}_{18} = \mathbb{Z}_{2 \cdot 3^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$

Wir werden sehen, dass in diesem Ring die Gleichung  $(m^{\varphi(n)})^k \cdot m = m$  **nicht** für alle Elemente  $m$  gilt. Dies liegt daran, dass schon der Ring  $\mathbb{Z}_9$  Nullteiler besitzt. Die Einheiten in  $\mathbb{Z}_{18}$  sind 1, 5, 7, 11, 13 und 17, und es ist  $\varphi(18) = 6$ .

### Auswertung des Ausdrucks $(m^{\varphi(n)})^k \cdot m = (m^6)^k \cdot m$ :

#### Für Einheiten:

Ist  $m$  eine Einheit, so gilt nach dem Satz von Euler  $(m^6)^k \cdot m \bmod 18 = (1)^k \cdot m \bmod 18 = m$ .

#### Für Nicht-Einheiten:

Wir betrachten den Ring-Isomorphismus  $f: \mathbb{Z}_{18} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_9, x \mapsto (x \bmod 2, x \bmod 9)$ .

# Faktorisierung von Restklassenringen

## Anwendung auf das Dechiffrierproblem

### Exemplarische Analyse für den Ring $\mathbb{Z}_{18} = \mathbb{Z}_{2 \cdot 3^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$

Wir werden sehen, dass in diesem Ring die Gleichung  $(m^{\varphi(n)})^k \cdot m = m$  **nicht** für alle Elemente  $m$  gilt. Dies liegt daran, dass schon der Ring  $\mathbb{Z}_9$  Nullteiler besitzt. Die Einheiten in  $\mathbb{Z}_{18}$  sind 1, 5, 7, 11, 13 und 17, und es ist  $\varphi(18) = 6$ .

### Auswertung des Ausdrucks $(m^{\varphi(n)})^k \cdot m = (m^6)^k \cdot m$ :

#### Für Einheiten:

Ist  $m$  eine Einheit, so gilt nach dem Satz von Euler  $(m^6)^k \cdot m \bmod 18 = (1)^k \cdot m \bmod 18 = m$ .

#### Für Nicht-Einheiten:

Wir betrachten den Ring-Isomorphismus  $f: \mathbb{Z}_{18} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_9, x \mapsto (x \bmod 2, x \bmod 9)$ .

In  $\mathbb{Z}_{18}$  gibt es, **anders** als in Ringen der Form  $\mathbb{Z}_{p \cdot q}$  mit Primzahlen  $p$  und  $q$ , **Nicht-Einheiten**  $m$ , die durch  $f$  auf ein Paar  $(a, b)$  mit  $a \neq 0$  und  $b \neq 0$  abgebildet werden. So ist

$$\begin{aligned} f(3) &= (3 \bmod 2, 3 \bmod 9) = (1, 3) \\ f(15) &= (15 \bmod 2, 15 \bmod 9) = (1, 6) \end{aligned}$$

# Faktorisierung von Restklassenringen

## Anwendung auf das Dechiffrierproblem

### Exemplarische Analyse für den Ring $\mathbb{Z}_{18} = \mathbb{Z}_{2 \cdot 3^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$

Wir werden sehen, dass in diesem Ring die Gleichung  $(m^{\varphi(n)})^k \cdot m = m$  **nicht** für alle Elemente  $m$  gilt. Dies liegt daran, dass schon der Ring  $\mathbb{Z}_9$  Nullteiler besitzt. Die Einheiten in  $\mathbb{Z}_{18}$  sind 1, 5, 7, 11, 13 und 17, und es ist  $\varphi(18) = 6$ .

### Auswertung des Ausdrucks $(m^{\varphi(n)})^k \cdot m = (m^6)^k \cdot m$ :

#### Für Einheiten:

Ist  $m$  eine Einheit, so gilt nach dem Satz von Euler  $(m^6)^k \cdot m \bmod 18 = (1)^k \cdot m \bmod 18 = m$ .

#### Für Nicht-Einheiten:

Wir betrachten den Ring-Isomorphismus  $f: \mathbb{Z}_{18} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_9, x \mapsto (x \bmod 2, x \bmod 9)$ .

In  $\mathbb{Z}_{18}$  gibt es, **anders** als in Ringen der Form  $\mathbb{Z}_{p \cdot q}$  mit Primzahlen  $p$  und  $q$ , **Nicht-Einheiten**  $m$ , die durch  $f$  auf ein Paar  $(a, b)$  mit  $a \neq 0$  und  $b \neq 0$  abgebildet werden. So ist

$$\begin{aligned} f(3) &= (3 \bmod 2, 3 \bmod 9) = (1, 3) \\ f(15) &= (15 \bmod 2, 15 \bmod 9) = (1, 6) \end{aligned}$$

und es gilt z.B.  $f(3^6 \cdot 3 \bmod 18) = (1^6 \cdot 1 \bmod 2, 3^6 \cdot 3 \bmod 9) = (1, 0) \neq (1, 3)$ .

Man erkennt als Ursache die Tatsache, dass 3 ein Nullteiler in  $\mathbb{Z}_9$  ist.

# Faktorisierung von Restklassenringen

## Anwendung auf das Dechiffrierproblem

### Exemplarische Analyse für den Ring $\mathbb{Z}_{18} = \mathbb{Z}_{2 \cdot 3^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$

Wir werden sehen, dass in diesem Ring die Gleichung  $(m^{\varphi(n)})^k \cdot m = m$  **nicht** für alle Elemente  $m$  gilt. Dies liegt daran, dass schon der Ring  $\mathbb{Z}_9$  Nullteiler besitzt. Die Einheiten in  $\mathbb{Z}_{18}$  sind 1, 5, 7, 11, 13 und 17, und es ist  $\varphi(18) = 6$ .

### Auswertung des Ausdrucks $(m^{\varphi(n)})^k \cdot m = (m^6)^k \cdot m$ :

#### Für Einheiten:

Ist  $m$  eine Einheit, so gilt nach dem Satz von Euler  $(m^6)^k \cdot m \bmod 18 = (1)^k \cdot m \bmod 18 = m$ .

#### Für Nicht-Einheiten:

Wir betrachten den Ring-Isomorphismus  $f: \mathbb{Z}_{18} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_9$ ,  $x \mapsto (x \bmod 2, x \bmod 9)$ .

In  $\mathbb{Z}_{18}$  gibt es, **anders** als in Ringen der Form  $\mathbb{Z}_{p \cdot q}$  mit Primzahlen  $p$  und  $q$ , **Nicht-Einheiten**  $m$ , die durch  $f$  auf ein Paar  $(a, b)$  mit  $a \neq 0$  und  $b \neq 0$  abgebildet werden. So ist

$$\begin{aligned} f(3) &= (3 \bmod 2, 3 \bmod 9) = (1, 3) \\ f(15) &= (15 \bmod 2, 15 \bmod 9) = (1, 6) \end{aligned}$$

und es gilt z.B.  $f(3^6 \cdot 3 \bmod 18) = (1^6 \cdot 1 \bmod 2, 3^6 \cdot 3 \bmod 9) = (1, 0) \neq (1, 3)$ .

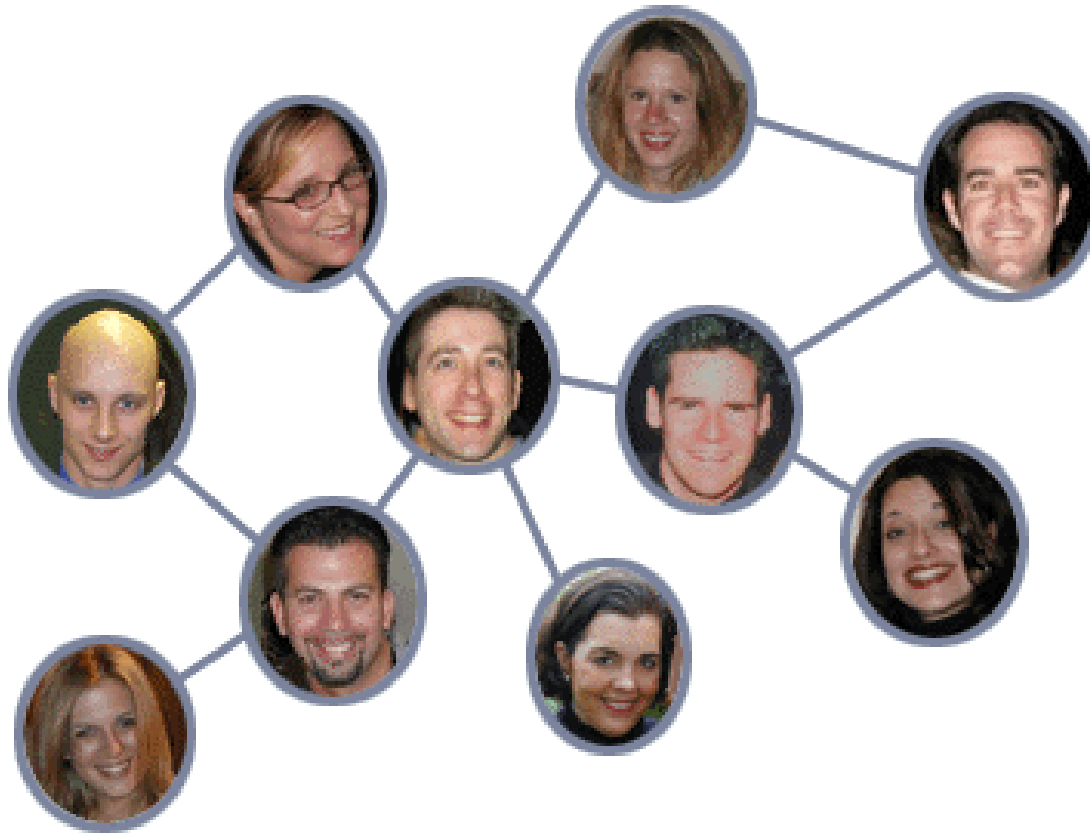
Man erkennt als Ursache die Tatsache, dass 3 ein Nullteiler in  $\mathbb{Z}_9$  ist.

Rechnet man übrigens direkt in  $\mathbb{Z}_{18}$ , so erhält man

$$3^6 \cdot 3 \bmod 18 = 27^2 \cdot 3 \bmod 18 = 9^2 \cdot 3 \bmod 18 = 3 \cdot 3 \bmod 18 = 9 \neq 3 \quad \text{und} \quad f(9) = (1, 0) \quad \checkmark$$

# Relationen

## Einführung



### Relationen

- Elemente aus Mengen in Beziehung setzen ('Relation' bedeutet Beziehung)
- Elemente mit ähnlichen Eigenschaften zusammenfassen oder anders ausgedrückt: eine Menge in Klassen 'ähnlicher' Beziehungen zerlegen
- Elemente innerhalb einer Menge ordnen  
z.B. lexikographische Ordnung: Alphabet  
z.B. Ordnung von Objekten hinsichtlich ihrer Größe



### Definition

Seien  $M_1, M_2$  beliebige nichtleere Mengen. Eine **Relation**  $R$  auf  $M_1 \times M_2$  ist eine Teilmenge von  $M_1 \times M_2$ .

$$R \subset M_1 \times M_2.$$

### Bemerkung

- $M_1 \times M_2 := \{(x, y) | x \in M_1, y \in M_2\}$  ist das kartesische Produkt zwischen den Mengen  $M_1, M_2$ .
- Sind  $M_1 = M_2 =: M$ , so spricht man von einer **zweistelligen Relation** auf  $M$ .
- Falls  $(x, y) \in R$  gilt, so sagt man „ $x$  steht in Relation  $R$  zu  $y$ “ und schreibt auch  $xRy$ .
- Eine  $n$ -stellige Relation  $R$  auf  $M$  ist eine Teilmenge von  $M^n$ :  $R \subset M^n$ .

### Beispiele

- 1 Sei  $S$  die Menge der Studierenden an der HFU und  $F$  die Menge aller Studiengänge. So ist die Menge  $B = \{(s, f) \mid s \text{ belegt den Studiengang } f\}$  eine Relation auf  $S \times F$

- 5  $M = \{1, 2\}$   
 $R_{100} := \{(1, 1), (1, 2), (2, 2)\}$

### Beispiele

- 1 Sei  $S$  die Menge der Studierenden an der HFU und  $F$  die Menge aller Studiengänge. So ist die Menge  $B = \{(s, f) \mid s \text{ belegt den Studiengang } f\}$  eine Relation auf  $S \times F$
- 2 Alle Vergleichsoperationen  $<, >, \leq, \geq, =, \neq$  sind Relationen auf  $\mathbb{R}$
- 5  $M = \{1, 2\}$   
 $R_{100} := \{(1, 1), (1, 2), (2, 2)\}$

### Beispiele

- 1 Sei  $S$  die Menge der Studierenden an der HFU und  $F$  die Menge aller Studiengänge. So ist die Menge  $B = \{(s, f) \mid s \text{ belegt den Studiengang } f\}$  eine Relation auf  $S \times F$
- 2 Alle Vergleichsoperationen  $<, >, \leq, \geq, =, \neq$  sind Relationen auf  $\mathbb{R}$
- 3  $R_1 := \{(x, y) \in \mathbb{R}^2 \mid x^2 = y\}$
- 5  $M = \{1, 2\}$   
 $R_{100} := \{(1, 1), (1, 2), (2, 2)\}$

### Beispiele

- ① Sei  $S$  die Menge der Studierenden an der HFU und  $F$  die Menge aller Studiengänge. So ist die Menge  $B = \{(s, f) \mid s \text{ belegt den Studiengang } f\}$  eine Relation auf  $S \times F$
- ② Alle Vergleichsoperationen  $<, >, \leq, \geq, =, \neq$  sind Relationen auf  $\mathbb{R}$
- ③  $R_1 := \{(x, y) \in \mathbb{R}^2 \mid x^2 = y\}$
- ④  $R_2 := \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$
- ⑤  $M = \{1, 2\}$   
 $R_{100} := \{(1, 1), (1, 2), (2, 2)\}$

# Relationen

Reflexivität, Symmetrie, Antisymmetrie, Transitivität

## Definition

Seien  $R$  eine Relation auf der Menge  $M$ .  $R$  heißt

- **reflexiv**, wenn für alle  $x$  aus  $M$  gilt :  $xRx$  bzw.  $(x, x) \in R$

# Relationen

Reflexivität, Symmetrie, Antisymmetrie, Transitivität

## Definition

Seien  $R$  eine Relation auf der Menge  $M$ .  $R$  heißt

- **reflexiv**, wenn für alle  $x$  aus  $M$  gilt :  $xRx$  bzw.  $(x, x) \in R$
- **symmetrisch**, wenn für alle  $x, y$  aus  $M$  mit  $xRy$  gilt:  $yRx$  bzw. falls  $(x, y) \in R$ , so auch  $(y, x) \in R$

# Relationen

Reflexivität, Symmetrie, Antisymmetrie, Transitivität

## Definition

Seien  $R$  eine Relation auf der Menge  $M$ .  $R$  heißt

- **reflexiv**, wenn für alle  $x$  aus  $M$  gilt :  $xRx$  bzw.  $(x, x) \in R$
- **symmetrisch**, wenn für alle  $x, y$  aus  $M$  mit  $xRy$  gilt:  $yRx$  bzw. falls  $(x, y) \in R$ , so auch  $(y, x) \in R$
- **antisymmetrisch**, wenn für alle  $x, y$  aus  $M$  mit  $xRy$  und  $yRx$  gilt:  $x = y$  bzw. falls  $(x, y) \in R$  und  $(y, x) \in R$ , so folgt  $x = y$



# Relationen

Reflexivität, Symmetrie, Antisymmetrie, Transitivität

## Definition

Seien  $R$  eine Relation auf der Menge  $M$ .  $R$  heißt

- **reflexiv**, wenn für alle  $x$  aus  $M$  gilt :  $xRx$  bzw.  $(x, x) \in R$
- **symmetrisch**, wenn für alle  $x, y$  aus  $M$  mit  $xRy$  gilt:  $yRx$  bzw. falls  $(x, y) \in R$ , so auch  $(y, x) \in R$
- **antisymmetrisch**, wenn für alle  $x, y$  aus  $M$  mit  $xRy$  und  $yRx$  gilt:  $x = y$  bzw. falls  $(x, y) \in R$  und  $(y, x) \in R$ , so folgt  $x = y$
- **transitiv**, wenn  $\forall x, y, z$  aus  $M$  mit  $xRy$  und  $yRz$  gilt:  $xRz$  bzw. falls  $(x, y) \in R$  und  $(y, z) \in R$ , so folgt  $(x, z) \in R$

# Äquivalenzrelation

## Einführung

Man nennt Objekte äquivalent, wenn sie sich in irgendeiner Eigenschaft gleichen.

### Beispiele:

- PC: Schalter die an sind und Schalter die aus sind.
- Natürliche Zahlen die nach Division durch 2 den gleichen Rest lassen.

# Äquivalenzrelation

## Definition

Eine Relation heißt **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist.

## Bemerkung

Für eine Äquivalenzrelation schreibt man  $\sim$ . Es gilt laut Definition dann:

- i) Für alle  $x \in M$  gilt  $x \sim x$  (reflexiv)
- ii) Für alle  $x, y \in M$  gilt: Ist  $x \sim y$ , so ist  $y \sim x$  (symmetrisch)
- iii) Für alle  $x, y, z \in M$  gilt:  $x \sim y$  und  $y \sim z$ , so ist  $x \sim z$  (transitiv)

# Äquivalenzrelation

## Beispiel

### Beispiele

- Sei die Menge  $M = \mathbb{Z}$ ,  
 $R_5 := \{(x, y) \in \mathbb{Z}^2 \mid (x - y) \text{ ist ohne Rest durch 5 teilbar}\}$ . (Eine Zahl  $a \in \mathbb{Z}$  ist teilbar durch 5, wenn es eine ganze Zahl  $k$  derart gibt, daß  $a = k \cdot 5$ .)
  - Reflexivität  
 $xR_5x$ , denn  $x - x = 0$  ist ohne Rest durch 5 teilbar.
  - Symmetrie  
Sei  $xR_5y$ , d.h. es existiert ein  $k \in \mathbb{Z} : x - y = k \cdot 5$   
somit  $-x + y = -(k \cdot 5)$   
also auch  $y - x = (-k) \cdot 5$ , da  $(-k) \in \mathbb{Z}$  folgt schließlich  $yR_5x$

# Äquivalenzrelationen

## Beispiel

- Transitivität

Sei  $xR_5y$  und  $yR_5z$ , d.h. es existiert ein  $k \in \mathbb{Z}$  und es existiert ein  $l \in \mathbb{Z}$ , so dass  $x - y = 5k$  und  $y - z = 5l$  gilt.

Wir schreiben  $x - z$  als  $x - y + y - z$ :

$$x - y + y - z = 5k + 5l \Leftrightarrow x - z = 5(k + l) \Rightarrow xR_5z, \text{ da } (k + l) \in \mathbb{Z}$$

# Äquivalenzrelationen

## Äquivalenzklasse

### Definition

Sei  $\sim$  eine Äquivalenzrelation auf  $M$  und  $x \in M$  ein beliebiges Element. Dann heißt die Menge

$$[x] = \{y \in M \mid y \sim x\}$$

die **Äquivalenzklasse** von  $x$ . Die Elemente von  $[x]$  heißen die zu  $x$  **äqui-valenten** Elemente.

### Satz:

- Verschiedene Äquivalenzklassen sind disjunkt.
- Die Vereinigung aller Äquivalenzklassen ergibt die ganze Menge  $M$ .

# Äquivalenzrelation

## Äquivalenzklasse - Beispiel

### Beispiel

Sei  $R_5$  wie vorhin definiert und sei

$$[x] := \{y \in \mathbb{Z} \mid y - x \text{ ist ohne Rest durch } 5 \text{ teilbar}\}.$$

$$[0] := \{y \in \mathbb{Z} \mid y - 0 \text{ ist ohne Rest durch } 5 \text{ teilbar}\}$$

$$= \{\dots, -15, -10, -5\} \cup \{0, 5, 10, \dots\}$$

$$[1] := \{y \in \mathbb{Z} \mid y - 1 \text{ ist ohne Rest durch } 5 \text{ teilbar}\}$$

$$= \{\dots, -14, -9, -4\} \cup \{1, 6, 11, \dots\}$$

$$[2] := \{y \in \mathbb{Z} \mid y - 2 \text{ ist ohne Rest durch } 5 \text{ teilbar}\}$$

$$= \{\dots, -13, -8, -3\} \cup \{2, 7, 12, \dots\}$$

$$[3] := \{y \in \mathbb{Z} \mid y - 3 \text{ ist ohne Rest durch } 5 \text{ teilbar}\}$$

$$= \{\dots, -12, -7, -2\} \cup \{3, 8, 13, \dots\}$$

$$[4] := \{y \in \mathbb{Z} \mid y - 4 \text{ ist ohne Rest durch } 5 \text{ teilbar}\}$$

$$= \{\dots, -11, -6, -1\} \cup \{4, 9, 14, \dots\}$$

$$[5] := \{y \in \mathbb{Z} \mid y - 5 \text{ ist ohne Rest durch } 5 \text{ teilbar}\}$$

$$= \{\dots, -15, -10, -5\} \cup \{0, 5, 10, \dots\}$$

# Äquivalenzrelationen

## Äquivalenzklasse – Beispiel

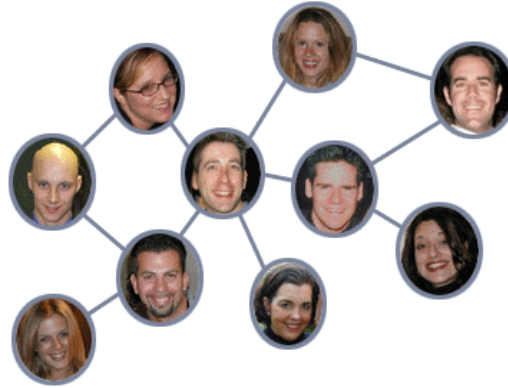
### Beispiel

- Offensichtlich gilt  $[1] = [6] = \dots$  und auch  $[5] = [0] = \dots$  usw.
- Durch die Relation  $R_5$  wurden die ganzen Zahlen in 5 disjunkten Äquivalenzklassen zerlegt. Deren Vereinigung ergibt wieder  $\mathbb{Z}$ .
- $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$



# Äquivalenzrelationen

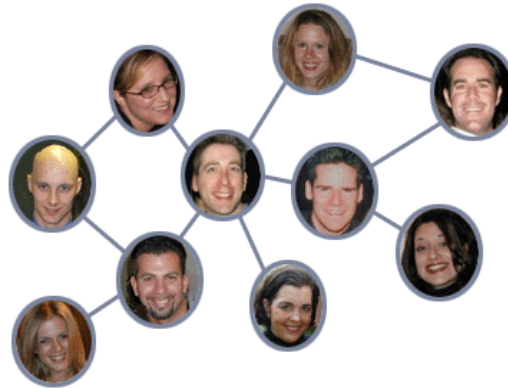
## Beispiel



Es sei der oben abgebildete Freundschaftsgraph gegeben. Die Relation 'Freundschaft' in diesem Graph ist folgendermaßen definiert: wird eine Linie zwischen zwei Personen gezogen, dann sind diese 2 Personen Freunde. Ist die Relation auf dem gesamten Graph:

- reflexiv? nein
- symmetrisch? ja
- transitiv? nein

# Äquivalenzrelationen



## Hausübung

Wie müßte man das Diagramm verändern, damit eine Äquivalenzrelation dargestellt wird?

- Um Reflexivität zu gewährleisten, muss man jede Person auch mit sich selbst verbinden (Schleufe).
- Um Transitivität herzustellen, muss der Graph (ggf. iterativ) so ergänzt werden, dass zu jeder existierenden „Kette“  $A - B - C$  von drei Personen auch die Verbindung  $A - C$  existiert (*transitive Hülle*).
- Skizzieren Sie die transitive Hülle der gegebenen Freundschaftsrelation.

# Äquivalenzrelationen

- Äquivalenzrelation  
gruppiert  
abstrahiert: Elemente innerhalb dessen sind nicht mehr unterscheidbar  
dadurch vergrößerte Gleichheit