

# Vorlesung Diskrete Strukturen

## Gruppe und Ring

Bernhard Ganter

Institut für Algebra  
TU Dresden  
D-01062 Dresden  
bernhard.ganter@tu-dresden.de

WS 2009/10

# Dividieren modulo $n$ ?

Eine *Division* modulo  $n$  kann man nicht ohne erhebliche Einschränkungen erfinden, falls  $n$  keine Primzahl ist.

Das zeigt ein einfaches Beispiel: das Rechnen modulo 6.

Wenn es möglich wäre, eine Division durch 2 modulo 6 zu erfinden, dann sollte doch jedenfalls 2 geteilt durch 2 das Ergebnis 1 und 0 geteilt durch 2 das Ergebnis Null liefern.

Daraus erhält man die widersprüchliche Gleichung

$$3 \equiv 3 \cdot 1 \equiv 3 \cdot \frac{2}{2} \equiv \frac{3 \cdot 2}{2} \equiv \frac{0}{2} \equiv 0 \pmod{6}.$$

So geht es also nicht!

# Nullteiler

Man kann dieses Beispiel verallgemeinern.

Man nennt eine Zahl  $a \neq 0$  (in einem Ring) einen **Nullteiler**, wenn es eine Zahl  $b \neq 0$  mit  $a \cdot b = 0$  gibt.

Im Ring  $\mathbb{Z}_6$  ist diese Bedingung für  $a = 2$  und  $b = 3$  erfüllt:  
2 ist also ein Nullteiler in  $\mathbb{Z}_6$ .

Die Argumentation der vorigen Seite zeigt:

*eine Division durch Nullteiler  
kann nicht sinnvoll definiert werden.*

# Einheiten

Eine Zahl  $a$  in einem Ring ist eine **Einheit**, wenn es eine Zahl  $b$  mit  $a \cdot b = 1$  gibt.

Durch Einheiten kann man „dividieren“, denn  $b$  verhält sich ja wie ein Kehrwert zu  $a$ .

Man sagt,  $b$  sei *multiplikativ invers* zu  $a$ .

Man dividiert durch  $a$ , indem man mit  $b$  multipliziert.

# Welche Zahlen sind Einheiten mod $n$ ?

Durch Einheiten kann man dividieren, durch Nullteiler nicht.

# Welche Zahlen sind Einheiten mod $n$ ?

Durch Einheiten kann man dividieren, durch Nullteiler nicht.  
Es bleibt die Frage, wie man Einheiten und Nullteiler erkennt.

# Welche Zahlen sind Einheiten mod $n$ ?

Durch Einheiten kann man dividieren, durch Nullteiler nicht.  
Es bleibt die Frage, wie man Einheiten und Nullteiler erkennt.  
Modulo  $n$  ist das einfach:

## Hilfssatz

*Eine Zahl  $a \in \{1, \dots, n-1\}$  ist genau dann eine Einheit modulo  $n$ , wenn  $a$  zu  $n$  teilerfremd ist.*

*Ist  $a$  keine Einheit, dann ist  $a$  ein Nullteiler modulo  $n$ .*

# Welche Zahlen sind Einheiten mod $n$ ?

Durch Einheiten kann man dividieren, durch Nullteiler nicht.  
Es bleibt die Frage, wie man Einheiten und Nullteiler erkennt.  
Modulo  $n$  ist das einfach:

## Hilfssatz

*Eine Zahl  $a \in \{1, \dots, n-1\}$  ist genau dann eine Einheit modulo  $n$ , wenn  $a$  zu  $n$  teilerfremd ist.*

*Ist  $a$  keine Einheit, dann ist  $a$  ein Nullteiler modulo  $n$ .*

## Beweis.

Wenn  $\text{ggT}(a, n) = 1$  ist, dann existieren ganze Zahlen  $\alpha, \beta$  mit  $1 \equiv \alpha \cdot a + \beta \cdot n \pmod{n}$ .  $\alpha \pmod{n}$  ist dann multiplikativ invers zu  $a$ . Wenn  $\text{ggT}(a, n) > 1$  ist, dann ist  $b := n / \text{ggT}(a, n) \in \mathbb{Z}_n$  eine Zahl mit  $a \cdot b \pmod{n} = 0$ . Also ist  $a$  dann ein Nullteiler.  $\square$

# Die Einheiten bilden eine Gruppe

Die Menge der Einheiten modulo  $n$  bildet mit der Multiplikation eine Gruppe:

- Sind nämlich  $a$  und  $b$  Einheiten und sind  $a^{-1}$  und  $b^{-1}$  die dazu multiplikativ inversen Elemente, dann ist  $b^{-1} \cdot a^{-1}$  multiplikativ invers zu  $a \cdot b$ , denn

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = 1.$$

- Ist  $a$  eine Einheit mit multiplikativ Inversem  $a^{-1}$ , dann ist natürlich auch  $a^{-1}$  eine Einheit, weil  $a$  dazu invers ist.

# Was ist das, eine Gruppe?

Eine **Gruppe** ist eine Algebra  $(G; \circ, ^{-1}, e)$  vom Typ  $(2, 1, 0)$  mit folgenden Eigenschaften:

- Es gilt  $a \circ (b \circ c) = (a \circ b) \circ c$  für alle  $a, b, c \in G$ ,
- es gilt  $g \circ e = g = e \circ g$  für alle  $g \in G$  und
- es gilt  $g \circ g^{-1} = g^{-1} \circ g = e$  für alle  $g \in G$ .

# Was ist das, eine Gruppe?

Eine **Gruppe** ist eine Algebra  $(G; \circ, ^{-1}, e)$  vom Typ  $(2, 1, 0)$  mit folgenden Eigenschaften:

- Es gilt  $a \circ (b \circ c) = (a \circ b) \circ c$  für alle  $a, b, c \in G$ ,
- es gilt  $g \circ e = g = e \circ g$  für alle  $g \in G$  und
- es gilt  $g \circ g^{-1} = g^{-1} \circ g = e$  für alle  $g \in G$ .

Dabei ist  $G$  die **Trägermenge** der Gruppe,  $\circ$ ,  $^{-1}$  und  $e$  sind die Symbole für die **fundamentalen Operationen**, und der **Typ**  $(2, 1, 0)$  gibt an, dass  $\circ$  eine zweistellige Operation bezeichnet,  $^{-1}$  eine einstellige und  $e$  eine nullstellige Operation.

# Was ist das, eine Gruppe?

Eine **Gruppe** ist eine Algebra  $(G; \circ, ^{-1}, e)$  vom Typ  $(2, 1, 0)$  mit folgenden Eigenschaften:

- Es gilt  $a \circ (b \circ c) = (a \circ b) \circ c$  für alle  $a, b, c \in G$ ,
- es gilt  $g \circ e = g = e \circ g$  für alle  $g \in G$  und
- es gilt  $g \circ g^{-1} = g^{-1} \circ g = e$  für alle  $g \in G$ .

Dabei ist  $G$  die **Trägermenge** der Gruppe,  $\circ$ ,  $^{-1}$  und  $e$  sind die Symbole für die **fundamentalen Operationen**, und der **Typ**  $(2, 1, 0)$  gibt an, dass  $\circ$  eine zweistellige Operation bezeichnet,  $^{-1}$  eine einstellige und  $e$  eine nullstellige Operation.

Man nennt  $e$  das **neutrale Element** der Gruppe und  $g^{-1}$  das zu  $g$  **inverse Element**.

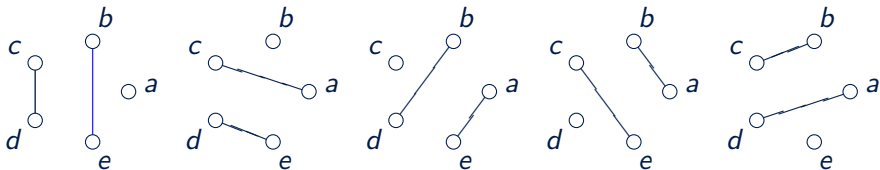
# Es kommt nicht auf die Symbole an!

Die Gestalt der Operationssymbole ist nebensächlich, oft werden z.B. auch die Symbole  $+$ ,  $-$ ,  $0$  benutzt.

Auch auf die Namen der Gruppenelemente kommt es nicht immer an. Zwei Gruppen, die sich durch Umbenennen der Elemente und der Operationssymbole ineinander überführen lassen, nennt man **isomorph**.

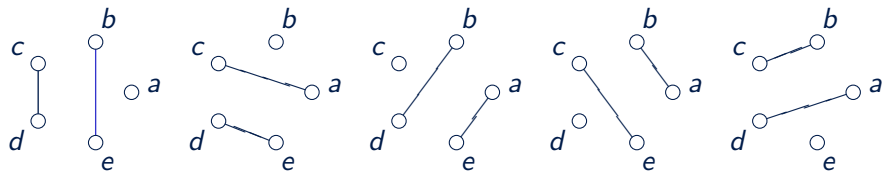
Der Begriff der Isomorphie wird später noch präzisiert. Er wird nicht nur für Gruppen, sondern für beliebige Strukturen benutzt. Für den Moment soll ein Beispiel genügen.

## Tischtennisturniermultiplikation



$$x \circ y := \begin{cases} x & \text{falls } x = y, \\ \text{der Spieler, der aussetzt,} & \\ \text{wenn } x \text{ gegen } y \text{ spielt} & \text{falls } x \neq y. \end{cases}$$

## Tischtennisturniermultiplikationstafel



○	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>a</i>	<i>d</i>	<i>b</i>	<i>e</i>	<i>c</i>
<i>b</i>	<i>d</i>	<i>b</i>	<i>e</i>	<i>c</i>	<i>a</i>
<i>c</i>	<i>b</i>	<i>e</i>	<i>c</i>	<i>a</i>	<i>d</i>
<i>d</i>	<i>e</i>	<i>c</i>	<i>a</i>	<i>d</i>	<i>b</i>
<i>e</i>	<i>c</i>	<i>a</i>	<i>d</i>	<i>b</i>	<i>e</i>

# Tischtennis mod 5

Die Tischtennismultiplikation erweist sich als isomorph zur Operation

$$a \bullet b := 3(a + b) \bmod 5$$

## Tischtennis mod 5

Die Tischtennismultiplikation erweist sich als isomorph zur Operation

$$a \bullet b := 3(a + b) \bmod 5 = \frac{a + b}{2} \bmod 5,$$

dem Mittelwert modulo 5.

○	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>a</i>	<i>d</i>	<i>b</i>	<i>e</i>	<i>c</i>
<i>b</i>	<i>d</i>	<i>b</i>	<i>e</i>	<i>c</i>	<i>a</i>
<i>c</i>	<i>b</i>	<i>e</i>	<i>c</i>	<i>a</i>	<i>d</i>
<i>d</i>	<i>e</i>	<i>c</i>	<i>a</i>	<i>d</i>	<i>b</i>
<i>e</i>	<i>c</i>	<i>a</i>	<i>d</i>	<i>b</i>	<i>e</i>

≅

●	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

# Eine alternative Definition des Gruppenbegriffs

Durch die zweistellige Operation sind die anderen fundamentalen Operationen einer Gruppe eindeutig bestimmt. Manche Autoren definieren deshalb eine Gruppe als eine Algebra  $(G; \circ)$  vom Typ (2), die folgenden Gesetzen genügt:

- Die Operation  $\circ$  ist assoziativ.
- Es gibt ein Element  $e \in G$ , so dass für alle  $g \in G$  die Gleichung  $e \circ g = g \circ e = g$  gilt.
- Zu jedem Element  $g \in G$  existiert ein Element  $g^{-1} \in G$  mit  $g \circ g^{-1} = g^{-1} \circ g = e$ .

Wir bevorzugen die erste Definition, weil sie logisch etwas einfacher ist, denn alle Bedingungen sind Gleichungen.

# Beispiele von Gruppen

Gruppen tauchen vielfältig in der Algebra auf:

- die ganzen Zahlen,
- die rationalen Zahlen,
- die reellen Zahlen und
- die komplexen Zahlen

bilden jeweils mit der Addition eine Gruppe,

- die von Null verschiedenen rationalen Zahlen,
- die von Null verschiedenen reellen Zahlen bzw.
- die von Null verschiedenen komplexen Zahlen

mit der Multiplikation als zweistellige Operation bilden ebenfalls eine Gruppe.

## Beispiele von Gruppen (2)

All diese Gruppen sind **abelsch**, was das gleiche bedeutet wie kommutativ. Diese Eigenschaft haben auch die Gruppen  $\underline{\mathbb{Z}}_n := (\{0, 1, \dots, n-1\}; + \text{ mod } n)$  der ganzen Zahlen modulo  $n$ .

Nichtabelsche Gruppen spielen ebenfalls eine große Rolle. Die Menge alle bijektiven Abbildungen einer Menge  $S$  auf sich ist, mit der Hintereinanderausführung von Abbildungen als Operation, eine Gruppe. Sie wird die **symmetrische Gruppe** auf  $S$  genannt. Hat  $S$  mehr als zwei Elemente, dann ist die symmetrische Gruppe nicht abelsch.

# Beispiele kleiner Gruppen

Gruppen mit wenigen Elementen kann man gut durch ihre Verknüpfungstafeln angeben. Hier sind zwei (weitere) Beispiele:

1.: Die Gruppe aller Polynome vom Grad  $\leq 1$  mit Koeffizienten aus  $\mathbb{Z}_2$ .

+	0	1	$X$	$X + 1$
0	0	1	$X$	$X + 1$
1	1	0	$X + 1$	$X$
$X$	$X$	$X + 1$	0	1
$X + 1$	$X + 1$	$X$	1	0

Diese Gruppe ist kommutativ. Die Elemente aus  $\{0, 1\}$  bilden eine *Untergruppe*.

# Beispiele kleiner Gruppen

2.: Die Gruppe aller Symmetrien eines gleichseitigen Dreiecks

○	id			$\leftrightarrow$		
id	id			$\leftrightarrow$		
			id		$\leftrightarrow$	
		id				$\leftrightarrow$
$\leftrightarrow$	$\leftrightarrow$			id		
			$\leftrightarrow$		id	
		$\leftrightarrow$				id

	Bedeutung
id	identische Abbildung
	Drehung um $\frac{2}{3}\pi$
	Drehung um $\frac{4}{3}\pi$
$\leftrightarrow$	Spiegelung ( $ab$ )
	Spiegelung ( $ac$ )
	Spiegelung ( $bc$ )

Diese Gruppe ist nicht kommutativ. Die drei Drehungen  $\{\text{id}, \text{clockwise rotation}, \text{counter-clockwise rotation}\}$  bilden eine Untergruppe.

# Beispiele kleiner Gruppen

Die Gruppe aller Symmetrien eines gleichseitigen Dreiecks

○	id	$\begin{pmatrix} abc \\ cab \end{pmatrix}$	$\begin{pmatrix} abc \\ bca \end{pmatrix}$	$\begin{pmatrix} abc \\ bac \end{pmatrix}$	$\begin{pmatrix} abc \\ cba \end{pmatrix}$	$\begin{pmatrix} abc \\ acb \end{pmatrix}$
id	id	$\begin{pmatrix} abc \\ cab \end{pmatrix}$	$\begin{pmatrix} abc \\ bca \end{pmatrix}$	$\begin{pmatrix} abc \\ bac \end{pmatrix}$	$\begin{pmatrix} abc \\ cba \end{pmatrix}$	$\begin{pmatrix} abc \\ acb \end{pmatrix}$
$\begin{pmatrix} abc \\ cab \end{pmatrix}$	$\begin{pmatrix} abc \\ cab \end{pmatrix}$	$\begin{pmatrix} abc \\ bca \end{pmatrix}$	id	$\begin{pmatrix} abc \\ acb \end{pmatrix}$	$\begin{pmatrix} abc \\ bac \end{pmatrix}$	$\begin{pmatrix} abc \\ cba \end{pmatrix}$
$\begin{pmatrix} abc \\ bca \end{pmatrix}$	$\begin{pmatrix} abc \\ bca \end{pmatrix}$	id	$\begin{pmatrix} abc \\ cab \end{pmatrix}$	$\begin{pmatrix} abc \\ cba \end{pmatrix}$	$\begin{pmatrix} abc \\ acb \end{pmatrix}$	$\begin{pmatrix} abc \\ bac \end{pmatrix}$
$\begin{pmatrix} abc \\ bac \end{pmatrix}$	$\begin{pmatrix} abc \\ bac \end{pmatrix}$	$\begin{pmatrix} abc \\ cba \end{pmatrix}$	$\begin{pmatrix} abc \\ acb \end{pmatrix}$	id	$\begin{pmatrix} abc \\ cab \end{pmatrix}$	$\begin{pmatrix} abc \\ bca \end{pmatrix}$
$\begin{pmatrix} abc \\ cba \end{pmatrix}$	$\begin{pmatrix} abc \\ cba \end{pmatrix}$	$\begin{pmatrix} abc \\ acb \end{pmatrix}$	$\begin{pmatrix} abc \\ bac \end{pmatrix}$	$\begin{pmatrix} abc \\ bca \end{pmatrix}$	id	$\begin{pmatrix} abc \\ cab \end{pmatrix}$
$\begin{pmatrix} abc \\ acb \end{pmatrix}$	$\begin{pmatrix} abc \\ acb \end{pmatrix}$	$\begin{pmatrix} abc \\ bac \end{pmatrix}$	$\begin{pmatrix} abc \\ cba \end{pmatrix}$	$\begin{pmatrix} abc \\ cab \end{pmatrix}$	$\begin{pmatrix} abc \\ bca \end{pmatrix}$	id

# Untergruppen

Eine Teilmenge einer Gruppe, die das neutrale Element enthält und die gegen die Operationen  $\circ$  und  $^{-1}$  abgeschlossen ist, nennt man eine **Untergruppe**.

Jede Untergruppe ist also mit den eingeschränkten Operationen selbst eine Gruppe. Genau genommen sollte es besser heißen, dass unter den genannten Bedingungen die Menge  $U$  **Trägermenge** einer Untergruppe ist. Dieser feine Unterschied wird aber oft ignoriert.

Um anzuzeigen, dass  $U$  eine Untergruppe der Gruppe  $G$  ist, schreibt man

$$U \leq G.$$

# Ordnung einer (Unter-)gruppe

Die Anzahl  $|G|$  der Elemente einer Gruppe  $G$  nennt man auch die **Ordnung** von  $G$ .

Die Anzahl  $|U|$  ist dann also die **Ordnung der Untergruppe**  $U$ .

# Erzeugte Untergruppe

Zu jeder Teilmenge  $T$  einer Gruppe gibt es eine kleinste Untergruppe, die  $T$  enthält.

Man nennt sie die von  $T$  **erzeugte Untergruppe**  $\langle T \rangle$ .

$\langle T \rangle$  besteht aus

- dem neutralen Element,
- allen Elementen von  $T$  sowie
- allen Elementen, die man daraus durch wiederholtes Anwenden der Gruppenoperation und der Inversenbildung gewinnen kann.

# Erzeugte Untergruppe

Zu jeder Teilmenge  $T$  einer Gruppe gibt es eine kleinste Untergruppe, die  $T$  enthält.

Man nennt sie die von  $T$  **erzeugte Untergruppe**  $\langle T \rangle$ .

$\langle T \rangle$  besteht aus

- dem neutralen Element,
- allen Elementen von  $T$  sowie
- allen Elementen, die man daraus durch wiederholtes Anwenden der Gruppenoperation und der Inversenbildung gewinnen kann.

Ist  $T = \{a\}$  einelementig, dann schreibt man  $\langle a \rangle$  statt  $\langle \{a\} \rangle$  und sagt,  $\langle a \rangle$  sei von dem Element  $a$  erzeugt.

# Zyklische Gruppen

Eine von einem einzigen Element erzeugte Gruppe nennt man **zyklisch**.

Sie besteht aus den Potenzen dieses erzeugenden Elements (bei additiver Schreibweise aus den Vielfachen).

Ist  $G = \langle a \rangle$  unendlich, dann ist  $G$  isomorph zur Gruppe  $(\mathbb{Z}, +)$  der ganzen Zahlen.

Ist  $G = \langle a \rangle$  endlich, dann gibt es eine kleinste natürliche Zahl  $m$  mit  $a^m = 1$  und es ist

$$G = \{1, a, a^2, \dots, a^{m-1}\}.$$

$G$  ist dann isomorph zur Gruppe  $(\mathbb{Z}_m, +)$ .

# Die Ordnung eines Elements

Als die **Ordnung eines Elements**  $a$  eine Gruppe  $G$  bezeichnet man die Mächtigkeit der von  $a$  erzeugten Untergruppe  $\langle a \rangle$ .

Die Ordnung eines Elementes  $a$  ist also entweder  $\infty$  oder eine natürliche Zahl  $m$ ; in letzterem Fall ist dies auch die kleinste natürliche Zahl mit  $a^m = 1$ .

# Nebenklassen

Ist  $U$  eine Untergruppe der Gruppe  $G$  und  $g$  ein Element von  $G$ , dann nennt man

$$g \circ U := \{g \circ u \mid u \in U\}$$

eine (Links-)Nebenklasse von  $U$  in  $G$ .

**Hilfssatz:** Je zwei Nebenklassen  $a \circ U$  und  $b \circ U$  von  $U$  sind entweder gleich oder disjunkt.

**Beweisskizze:** Ist  $x \in a \circ U \cap b \circ U$ , dann gibt es  $u_1, u_2 \in U$  mit  $x = a \circ u_1 = b \circ u_2$  und deshalb  $a = b \circ (u_2 \circ u_1^{-1})$ , also  $a \in b \circ U$ , und damit für jedes  $u \in U$  auch  $a \circ u \in b \circ U$ , d.h.  $a \circ U \subseteq b \circ U$ .

# Index einer Untergruppe

Ist  $G$  eine endliche Gruppe und  $U$  eine Untergruppe von  $G$ , dann bezeichnet  $[G : U]$  die Anzahl der Nebenklassen von  $U$  in  $G$ . Man nennt diese Zahl den **Index** von  $U$  in  $G$ .

Man kann den Index ganz leicht bestimmen, wenn man beachtet, dass jede Nebenklasse von  $U$  die gleiche Mächtigkeit hat wie  $U$ .

Das ist deshalb richtig, weil die Abbildung

$$U \rightarrow g \circ U \quad \text{mit} \quad u \mapsto g \circ u$$

stets bijektiv ist.

Die Nebenklassen von  $U$  zerlegen also die Menge  $G$  in gleichgroße disjunkte Teilmengen.

# Der Satz von Lagrange

**Satz von Lagrange:** Ist  $U$  eine Untergruppe der endlichen Gruppe  $G$ , dann gilt

$$[G : U] = \frac{|G|}{|U|}.$$

Weil  $[G : U]$  ganzzahlig ist, gilt

*Die Ordnung einer Untergruppe teilt stets die Ordnung der Gruppe.*

Eine Gruppe mit beispielsweise 62 Elementen kann also vielleicht Untergruppen der Ordnungen 1, 2, 31 oder 62 haben, aber bestimmt keine mit 3, 4, 5, 6 oder z.B. 33 Elementen.

# Folgerung

## Satz

*Für jedes Element  $a$  einer endlichen Gruppe  $(G, \cdot, ^{-1}, 1)$  gilt: Die Ordnung von  $a$  ist ein Teiler der Anzahl  $|G|$  der Gruppenelemente.*

# Zahlentheoretische Konsequenzen

Aus dem Satz von Lagrange bekommt man ganz leicht ein zahlentheoretisches Ergebnis, das in der *Kryptographie* eine Rolle spielt, nämlich den **Satz von Euler–Fermat**.

Wir stellen hier zuerst einen Spezialfall vor, den sogenannten *kleinen Fermat*. Dazu müssen wir nur drei Beobachtungen kombinieren:

- Die Ordnung eines Elements ist stets ein Teiler der Gruppenordnung.
- Deshalb gilt  $a^{|G|} = 1$  für jedes Gruppenelement  $a$ .
- Ist  $p$  eine Primzahl, dann bilden die Zahlen  $\{1, 2, \dots, p - 1\}$  mit der Multiplikation modulo  $p$  eine Gruppe.

# Ein Lemma von Fermat

**Lemma von Fermat:** Ist  $p$  eine Primzahl, dann gilt für jede ganze Zahl  $a$ , die nicht durch  $p$  teilbar ist

$$a^{p-1} \bmod p = 1.$$

**Anwendungsbeispiel 1:** Man kann leicht Potenzen modulo  $p$  ausrechnen. Ein Beispiel dazu:

$p := 997$  ist eine Primzahl. Deshalb gilt

$$2^{1000} \bmod 997 = 2^{996} \cdot 2^4 \bmod 997 = 16.$$

# Ein ganz schlauer Trick!

**Anwendungsbeispiel 2:** Man kann beweisen, dass eine Zahl *keine* Primzahl ist, ohne einen Teiler anzugeben.

# Ein ganz schlauer Trick!

**Anwendungsbeispiel 2:** Man kann beweisen, dass eine Zahl *keine* Primzahl ist, ohne einen Teiler anzugeben. Ein Beispiel dazu:

Ist 100001 eine Primzahl? Wenn ja, dann muss für jede Zahl  $0 < a < 100001$  folgendes gelten:

$$a^{100000} \bmod 100001 = 1.$$

# Ein ganz schlauer Trick!

**Anwendungsbeispiel 2:** Man kann beweisen, dass eine Zahl *keine* Primzahl ist, ohne einen Teiler anzugeben. Ein Beispiel dazu:

Ist 100001 eine Primzahl? Wenn ja, dann muss für jede Zahl  $0 < a < 100001$  folgendes gelten:

$$a^{100000} \bmod 100001 = 1.$$

Für  $a := 2$  hatten wir diese Rechnung schon mit dem “Square and Multiply”-Trick durchgeführt und ausgerechnet, dass

$$2^{100000} \bmod 100001 = 1024 \neq 1.$$

# Ein ganz schlauer Trick!

**Anwendungsbeispiel 2:** Man kann beweisen, dass eine Zahl *keine* Primzahl ist, ohne einen Teiler anzugeben. Ein Beispiel dazu:

Ist 100001 eine Primzahl? Wenn ja, dann muss für jede Zahl  $0 < a < 100001$  folgendes gelten:

$$a^{100000} \bmod 100001 = 1.$$

Für  $a := 2$  hatten wir diese Rechnung schon mit dem “Square and Multiply”-Trick durchgeführt und ausgerechnet, dass

$$2^{100000} \bmod 100001 = 1024 \neq 1.$$

100001 ist also keine Primzahl! (Na klar:  $100001 = 11 \cdot 9091$ .)

# Verallgemeinerung des Lemmas von Fermat

Das Lemma von Fermat gilt nur für Primzahlen. Im Beweis wurden benutzt, dass die Zahlen  $\{1, 2, \dots, p - 1\}$  bezüglich der Multiplikation mod  $p$  eine Gruppe bilden. Für diese Gruppe wurde der Satz von Lagrange angewendet.

# Verallgemeinerung des Lemmas von Fermat

Das Lemma von Fermat gilt nur für Primzahlen. Im Beweis wurden benutzt, dass die Zahlen  $\{1, 2, \dots, p - 1\}$  bezüglich der Multiplikation mod  $p$  eine Gruppe bilden. Für diese Gruppe wurde der Satz von Lagrange angewendet.

Wenn  $p$  keine Primzahl ist, dann bilden die Zahlen  $\{1, 2, \dots, p - 1\}$  bezüglich der Multiplikation mod  $p$  keine Gruppe, denn dann sind nicht alle dieser Zahlen Einheiten modulo  $p$ .

# Verallgemeinerung des Lemmas von Fermat

Das Lemma von Fermat gilt nur für Primzahlen. Im Beweis wurden benutzt, dass die Zahlen  $\{1, 2, \dots, p - 1\}$  bezüglich der Multiplikation  $\text{mod } p$  eine Gruppe bilden. Für diese Gruppe wurde der Satz von Lagrange angewendet.

Wenn  $p$  keine Primzahl ist, dann bilden die Zahlen  $\{1, 2, \dots, p - 1\}$  bezüglich der Multiplikation  $\text{mod } p$  keine Gruppe, denn dann sind nicht alle dieser Zahlen Einheiten modulo  $p$ .

Aber die Einheiten bilden eine Gruppe! Das Lemma von Fermat lässt sich auf beliebige Zahlen  $n$  verallgemeinern, wenn man es für Einheiten formuliert.

# Das Lemma von Euler-Fermat

## Satz

*Ist  $a$  zu  $n$  teilerfremd, dann gilt*

$$a^{\varphi(n)} \bmod n = 1.$$

# Anwendungsbeispiel

**Aufgabe:** Wie lauten die letzten beiden Ziffern von  $7^{111111}$ ?

# Anwendungsbeispiel

**Aufgabe:** Wie lauten die letzten beiden Ziffern von  $7^{111111}$ ?

Umformuliert: Berechne  $7^{111111} \bmod 100$ .

# Anwendungsbeispiel

**Aufgabe:** Wie lauten die letzten beiden Ziffern von  $7^{111111}$ ?

Umformuliert: Berechne  $7^{111111} \bmod 100$ .

Wegen  $\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$  gilt

$$7^{111111} \equiv 7^{111111 \bmod 40} \equiv 7^{31} \pmod{100}.$$

# Anwendungsbeispiel

**Aufgabe:** Wie lauten die letzten beiden Ziffern von  $7^{111111}$ ?

Umformuliert: Berechne  $7^{111111} \bmod 100$ .

Wegen  $\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$  gilt

$$7^{111111} \equiv 7^{111111 \bmod 40} \equiv 7^{31} \pmod{100}.$$

$$7^{31} = 7^{16+8+4+2+1} = 7^{16} \cdot 7^8 \cdot 7^4 \cdot 7^2 \cdot 7^1 = (((7^2 \cdot 7)^2 \cdot 7)^2 \cdot 7)^2 \cdot 7.$$

Das kann man modulo 100 leicht von Hand auswerten.

# RSA: Ein Public-Key-Kryptoverfahren

Man kann das Lemma von Euler-Fermat dazu benutzen,  
Verschlüsselungsverfahren mit öffentlichem Schlüssel zu entwerfen.  
Das bekannteste ist das von Rivest, Shamir und Adleman.

# RSA: Ein Public-Key-Kryptoverfahren

Man kann das Lemma von Euler-Fermat dazu benutzen, Verschlüsselungsverfahren mit öffentlichem Schlüssel zu entwerfen. Das bekannteste ist das von Rivest, Shamir und Adleman.

- Dabei teilt der Empfänger einer zu sendenden Nachricht vorab dem Absender einen „Schlüssel“ öffentlich mit.
- Dieser Schlüssel ist dazu geeignet, Nachrichten zu *verschlüsseln*, nicht aber dazu, verschlüsselte Nachrichten wieder zu *entschlüsseln*.
- Dafür wird ein anderer Schlüssel benötigt, den der Empfänger geheim hält.
- Der Absender kann seine Nachricht mit Hilfe des öffentlichen Schüssels verschlüsseln. Nur der Empfänger kann sie wieder entschlüsseln.

## RSA

- 1 Der Empfänger wählt zwei große Primzahlen  $p, q$ , berechnet  $n := p \cdot q$ , wählt eine zu  $\varphi(n)$  teilerfremde Zahl  $d \in \mathbb{Z}_n$  und berechnet deren multiplikatives Inverses  $e$  modulo  $\varphi(n)$ .
- 2 Er teilt die Zahlen  $n$  und  $e$  (öffentlich) dem Absender mit.
- 3 Der Absender möchte dem Empfänger eine Zahl  $m \in \mathbb{Z}_n$  mitteilen. Zur Vereinfachung wird angenommen, dass  $m$  teilerfremd zu  $n$  ist. Der eigentliche Nachrichtentext wird vorher auf eine vereinbarte Weise in solche Zahlen übersetzt.
- 4 Der Absender berechnet

$$E(m) := m^e \bmod n$$

und sendet diese Zahl an den Empfänger.

## RSA

- 5 Der Empfänger kennt nun  $\tilde{m} := E(m) := m^e \bmod n$ .
- 6 Er berechnet nun

$$D(\tilde{m}) := \tilde{m}^d \bmod n.$$

- 7 Weil  $d$  und  $e$  zueinander invers modulo  $\varphi(n)$  sind, ist  $d \cdot e$  um Eins größer als ein Vielfaches von  $\varphi(n)$ . Es gilt also

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

für eine ganze Zahl  $k$ .

- 8 Damit ist

$$D(\tilde{m}) = D(E(m)) \equiv (m^e)^d = m^{k \cdot \varphi(n) + 1}$$

## RSA

- 9 Nach dem Lemma von Euler-Fermat ist

$$D(\tilde{m}) = m^{k \cdot \varphi(n) + 1} = m^{\varphi(n) \cdot k + 1} = m.$$

Der Empfänger hat die Nachricht damit also entschlüsselt.

- 10 Ein Angreifer kann nicht auf diese Weise entschlüsseln, weil er die Primfaktorzerlegung  $n = p \cdot q$  nicht kennt und deshalb  $\varphi(n)$  nicht berechnen kann.  $\varphi(n)$  bräuchte er aber, um den Exponenten  $d$  zu ermitteln, der zum Entschlüsseln benutzt wird.
- 11 Es ist bis heute kein allgemeines Verfahren bekannt, solche Nachrichten auf anderem Wege zu entschlüsseln, also den „Code zu knacken“.

## RSA

- 9 Nach dem Lemma von Euler-Fermat ist

$$D(\tilde{m}) = m^{k \cdot \varphi(n) + 1} = m^{\varphi(n) \cdot k + 1} = m.$$

Der Empfänger hat die Nachricht damit also entschlüsselt.

- 10 Ein Angreifer kann nicht auf diese Weise entschlüsseln, weil er die Primfaktorzerlegung  $n = p \cdot q$  nicht kennt und deshalb  $\varphi(n)$  nicht berechnen kann.  $\varphi(n)$  bräuchte er aber, um den Exponenten  $d$  zu ermitteln, der zum Entschlüsseln benutzt wird.
- 11 Es ist bis heute kein allgemeines Verfahren bekannt, solche Nachrichten auf anderem Wege zu entschlüsseln, also den „Code zu knacken“.
- 12 Aber Vorsicht: Die Realität ist komplizierter!