

Elementare Zahlentheorie

– Vorlesung –

Modul: CSI-B3 – Angewandte Mathematik

– Version: Wintersemester 2024/2025 –

Dozent: Prof. Dr. Max Krüger

Fakultät Informatik

Technische Hochschule Ingolstadt (THI)



Der vorliegende Foliensatz ist ausschließlich für den persönlichen, vorlesungsinternen Gebrauch im Rahmen der Vorlesung „Diskrete Mathematik – Elementare Zahlentheorie“ an der Fakultät Informatik der Technischen Hochschule Ingolstadt (THI) bestimmt.

Der Foliensatz wird kontinuierlich korrigiert, aktualisiert und erweitert.

– Urheberrechtlich geschütztes Material –

Die Weitergabe an Dritte sowie Veröffentlichungen in jeglicher Form (insb. Hochladen ins Internet, Social Media, Videoplattformen, etc.) sind u.a. aus urheberrechtlichen Gründen in keinem Fall gestattet.

Wie unfair ist das denn ...



Herkunftsnnachweis



Das Vorgehen und die Inhalte dieses Veranstaltungsteils orientieren sich in den ersten drei Kapiteln – sofern nicht abweichend vermerkt – an den ausgewählten Abschnitten der Vorlesung

„Elementare Zahlentheorie mit Maple (Kurs 01202)“ [1]

die jährlich an der Fakultät für Informatik und Mathematik der FernUniversität in Hagen gehalten werden.

Elementare Zahlentheorie

Einführung und Übersicht

– Version: Wintersemester 2024/2025 –

Dozent: Prof. Dr. Max Krüger

Fakultät Informatik

Technische Hochschule Ingolstadt (THI)

5

Begriffseinordnung (vgl. [1])



Elementare Zahlentheorie ...

- ... ist ein Teilgebiet Zahlentheorie (aus der reinen Mathematik)
- ... greift nur auf mathematische Grundlagen (z. B. Mengenlehre, Arithmetik, etc.) und nicht wesentlich auf andere (fortgeschrittene) mathematische Disziplinen zurück.
- ... hat weit zurückreichende Wurzeln.
- ... hat bedeutende Anwendungen in
 - Kryptographie
 - Computeralgebra
 - u. a. .
- ... kann weiterentwickelt werden in
 - Analytischen Zahlentheorie (Input aus der Analysis)
 - Algebraischen Zahlentheorie (Input aus der Algebra)
 - Algorithmischen Zahlentheorie (Input aus der Informatik).



Einführung und Übersicht

Kapitel 01: Grundlagen, Teilbarkeit und Vielfache

Kapitel 02: Primzahlen

Kapitel 03: Kongruenzen und die Sätze von Fermat

Kapitel 04: Einführung in die Kryptologie

Literaturverzeichnis



Technische Hochschule
Ingolstadt

Elementare Zahlentheorie

Kapitel 01: Grundlagen, Teilbarkeit und Vielfache

– Version: Wintersemester 2024/2025 –

Dozent: Prof. Dr. Max Krüger

Fakultät Informatik

Technische Hochschule Ingolstadt (THI)



Kapitel 01: Grundlagen, Teilbarkeit und Vielfache

1.1 Zahlenmengen

- 1.2 Maxima CAS – ein Computer Algebra System
- 1.3 Division mit Rest
- 1.4 Größter gemeinsamer Teiler (ggT)
- 1.5 Kleinstes gemeinsames Vielfaches (kgV)
- 1.6 Lineare Diophantische Gleichungen

Mengen der natürlichen und ganzen Zahlen



Definition (1.1.1): Menge der Natürlichen Zahlen

(1) Die **Menge der natürlichen Zahlen** \mathbb{N} ist definiert durch

$$\mathbb{N} := \{1, 2, 3, 4, 5, \dots\}.$$

(2) Die **Menge der natürlichen Zahlen** \mathbb{N}_0 mit Null ist definiert durch

$$\mathbb{N}_0 := \{0, 1, 2, 3, 4, 5, \dots\}.$$

(3) Die **Menge der ganzen Zahlen** \mathbb{Z} ist definiert durch

$$\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \dots\}.$$

□



Definition(1.1.2): Einschränkungen bekannter Zahlenmengen

Für $z, z_u, z_o \in \mathbb{Z}$ wird definiert:

- $\mathbb{N}_{\leq z} := \{i \in \mathbb{N} \mid i \leq z\} = \{1, \dots, z\}.$
- $\mathbb{N}_{\neq z} := \{i \in \mathbb{N} \mid i \neq z\} = \{1, \dots, z-1, z+1, z+2, z+3, \dots\}.$
- $\mathbb{N}_{0 \leq z} := \{i \in \mathbb{N}_0 \mid i \leq z\} = \{0, 1, \dots, z\}.$
- $\mathbb{Z}_{\neq z} := \{i \in \mathbb{Z} \mid i \neq z\} = \{\dots, z-2, z-1, z+1, z+2, z+3, \dots\}.$
- $\mathbb{Z}_{z_u \leq z_o} := \{i \in \mathbb{Z} \mid z_u \leq i \leq z_o\} = \{z_u, z_u+1, \dots, z_o-1, z_o\}.$
- etc. .

□

Beispiele:

- $\mathbb{N}_{\leq 5} = \{1, 2, 3, 4, 5\}$
- $\mathbb{Z}_{-4 \leq 2} = \{-4, -3, -2, -1, 0, 1, 2\}.$

Inhaltsverzeichnis Kapitel 01



Kapitel 01: Grundlagen, Teilbarkeit und Vielfache

1.1 Zahlenmengen

1.2 Maxima CAS – ein Computer Algebra System

1.3 Division mit Rest

1.4 Größter gemeinsamer Teiler (ggT)

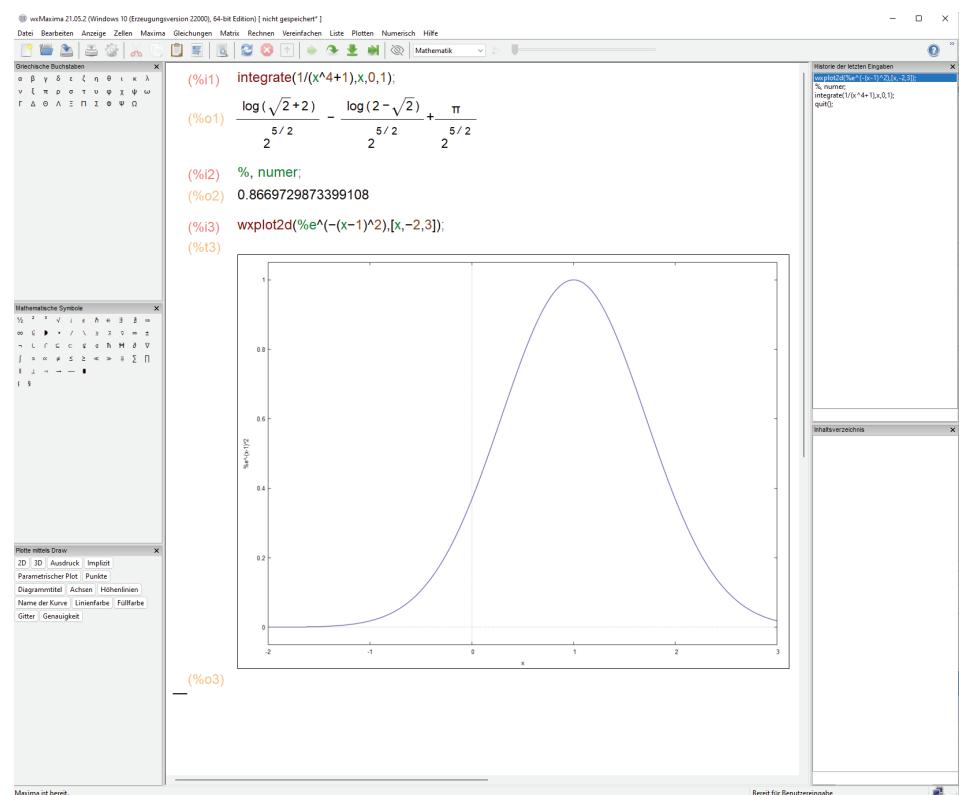
1.5 Kleinstes gemeinsames Vielfaches (kgV)

1.6 Lineare Diophantische Gleichungen



Bild: <https://de.wikipedia.org/wiki/Datei:Maximalogo.png> (download:20.052022)

- Open-Source-Projekt unter der GNU General Public License (GPL) („freie Software“)
- Graphische Benutzeroberfläche wxMaxima
 - vereinfachte Bedienung
 - graphischen Formelausgabe
- Download unter:
<http://maxima.sourceforge.net/>



Computeralgebra



Computeralgebra:

„Die Computeralgebra ist ein Wissenschaftsgebiet, das sich mit Methoden zum Lösen mathematisch formulierter Probleme durch symbolische Algorithmen und deren Umsetzung in Soft- und Hardware beschäftigt. [...]“¹⁾

Computeralgebra-System:

Ein Computeralgebra-System (CAS) ist ein Anwendungsprogramm zur Lösung mathematisch formulierter Probleme mit den Methoden der Computeralgebra.

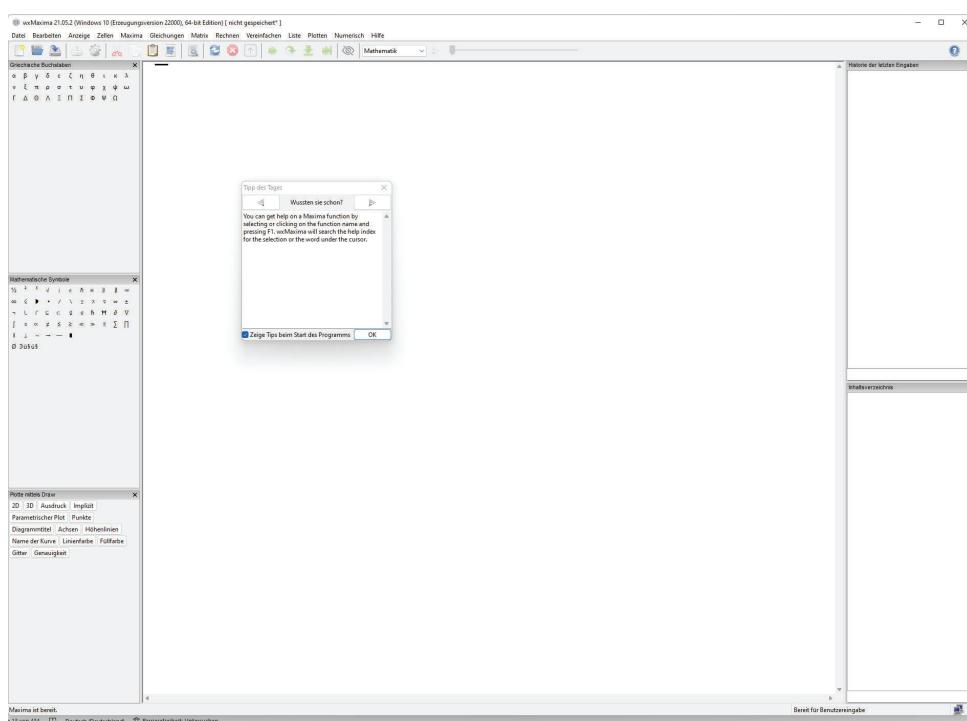
Bemerkung: Wir verwenden stellvertretend das Computeralgebra-System **Maxima**, das vielen anderen Computeralgebra-Systemen ähnelt.

1) Quelle: <http://www.fachgruppe-computeralgebra.de/cms/tiki-index.php?page=Allgemeines> (abgerufen am 07.11.2012).

Begrüßungsbildschirm von **wxMaxima**



Starten Sie **wxMaxima** ...



Computeralgebra- vs. Computernumerik-System (2)



Stärken von Computeralgebra-Systemen:

- Rechnen mit reellen Zahlen ohne Rundungsfehler
- Symbolisches Rechnen mit Variablen (Termumformungen)
- Exakte Lösungen, z.B. für die Gleichung $x^4 + 3x^3 + x^2 + x = 0$
- Dem menschlichen Rechnen nachempfunden.

Stärken von Computernumerik-Systemen:

- Berechnung einer Näherungslösung, auch wenn
 - kein Algorithmus zur exakten Lösung bekannt ist.
 - keine Darstellung der exakten Lösung existiert, z.B. für die Lösung der Gleichung $x + e^x = 0$.

Viele Computeralgebra-Systeme haben auch eine Computernumerik-Komponente und umgekehrt.

Buchhinweis [2]



Haager, Wilhelm:
Computeralgebra mit Maxima –
Grundlagen der Anwendung und
Programmierung

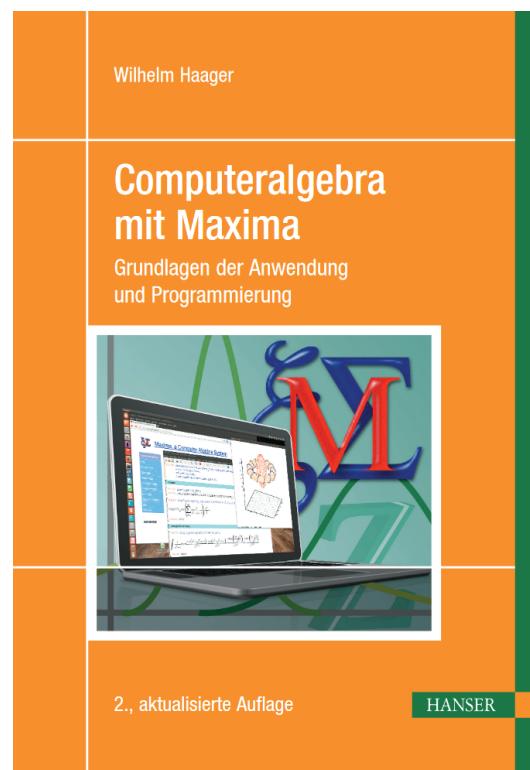
2., aktualisierte Auflage

München : Carl Hanser Verlag, [2019].

Druckausgabe: 978-3-446-44868-1

eBook: ISBN: 978-3-446-46095-9

Hinweis: Das Buch ist als eBook in der
THI-Bibliothek verfügbar.



Inhaltsverzeichnis Kapitel 01



Kapitel 01: Grundlagen, Teilbarkeit und Vielfache

- 1.1 Zahlenmengen
- 1.2 Maxima CAS – ein Computer Algebra System
- 1.3 Division mit Rest
- 1.4 Größter gemeinsamer Teiler (ggT)
- 1.5 Kleinstes gemeinsames Vielfaches (kgV)
- 1.6 Lineare Diophantische Gleichungen

Definition (1.3.1): Teiler ([1])

Seien $a, b \in \mathbb{Z}$ mit $a \neq 0$, dann heißt a **Teiler von b** genau dann, wenn es ein $x \in \mathbb{Z}$ mit $a \cdot x = b$ gibt. \square

Notation (1.3.2): Teiler ([1])

Sei $a, b \in \mathbb{Z}$ mit $a \neq 0$.

- $a | b$ bedeutet a ist ein Teiler von b .
- $a \nmid b$ bedeutet a ist kein Teiler von b . \square

Beispiele:

- $2 | 6$ und $3 | 6$
- $2 \nmid 9$ und $1 | 9$
- $5 | 0$ und $0 \nmid 5$

Rechenregeln für Teilbarkeit**Satz (1.3.3): Rechenregeln für Teilbarkeit ([1])**

Seien $a, b, c \in \mathbb{Z}$, dann gelten die folgenden Rechenregeln für Teilbarkeit:

- (1) $a | b, b | c \Rightarrow a | c$.
- (2) $a | b, a | c \Rightarrow a | b + c$.
- (3) $a | b \Rightarrow a | b \cdot c$.
- (4) $a \cdot b = a \cdot c, a \neq 0 \Rightarrow b = c$.

Beweis: Siehe Literatur bzw. Tafel. \square

Beispiele:

- a) Wegen $13 | 26$ und $26 | 442$ folgt $13 | 442$ nach (1).
- b) Wegen $13 | 26$ und $13 | 39$ folgt $13 | 65 (= 26 + 39)$ nach (2).
- c) Wegen $13 | 26$ folgt $13 | 78 (= 26 \cdot 3)$ nach (3).
- d) Wegen $4 \cdot 3 = 2 \cdot 6$ folgt $2 \cdot 3 = 6$ nach (4).
- e) Wegen $3 | 9$ und $3 | 27$ folgt $3 | (9 \cdot 4 + 27 \cdot 5)$ nach (2) und (3).



Beweis: Rechenregeln für Teilbarkeit ([1])



Division mit Rest



Satz (1.3.4): Division mit Rest ([1])

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$, dann gibt es eindeutige ganze Zahlen $q, r \in \mathbb{Z}$, so dass gilt:

$$a = q \cdot b + r \quad \text{mit} \quad 0 \leq r < |b|.$$

Die Zahl q heißt dann **Quotient** und die Zahl r heißt **Rest** der Division von a durch b . Der Rest r wird auch als $a \bmod b := r$ (lies: „ a modulo b “) bezeichnet.

Beweis: Siehe Literatur. □

Beispiele:

- a) Für $a = 17$ und $b = 5$ gilt $17 = 3 \cdot 5 + 2$.
- b) Für $a = -17$ und $b = 5$ gilt $-17 = (-4) \cdot 5 + 3$.
- c) Für $a = 17$ und $b = -5$ gilt $17 = (-3) \cdot (-5) + 2$.
- d) Für $a = -17$ und $b = -5$ gilt $-17 = 4 \cdot (-5) + 3$.
- e) Für $a = -12$ und $b = 3$ gilt $-12 = (-4) \cdot 3 + 0$.



Kapitel 01: Grundlagen, Teilbarkeit und Vielfache

- 1.1 Zahlenmengen
- 1.2 Maxima CAS – ein Computer Algebra System
- 1.3 Division mit Rest
- 1.4 Größter gemeinsamer Teiler (ggT)**
- 1.5 Kleinstes gemeinsames Vielfaches (kgV)
- 1.6 Lineare Diophantische Gleichungen

Gemeinsame Teiler



Definition (1.4.1): Gemeinsame Teiler ([1])

Eine Zahl $d \in \mathbb{Z}_{\neq 0}$ heißt ein **gemeinsamer Teiler von** $a \in \mathbb{Z}$ **und** $b \in \mathbb{Z}$ genau dann, wenn $d | a$ und $d | b$ gilt. □

Beispiele:

- $-3 | 6$ und $-3 | -9$
- $1 | 3$ und $1 | 4$

Definition (1.4.2): Teilerfremde Zahlen ([1])

Die Zahlen $a, b \in \mathbb{Z}$ heißen **teilerfremde Zahlen** genau dann, wenn $d = +1$ und $d = -1$ die einzigen gemeinsamen Teiler von a und b sind. □

Beispiel: 4 und 9 sind teilerfremde Zahlen.



Definition (1.4.3): Größter gemeinsamer Teiler ([1])

Seien die Zahlen $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ gegeben, dann wird der **größte gemeinsamer Teiler** $\text{ggT}(a, b) \in \mathbb{N}$ von a und b definiert durch

$$\text{ggT}(a, b) := \max \{x \in \mathbb{Z} \mid x \mid a \text{ und } x \mid b\}.$$

□

Beispiele:

- $\text{ggT}(-9, 18) = 9$
- $\text{ggT}(-4, -16) = 4$
- $\text{ggT}(7, 9) = 1$

Korollar (1.4.4): Eigenschaften des größten gemeinsamen Teilers ([1])

- (1) Für $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ gilt immer $\text{ggT}(a, b) \geq 1$.
- (2) Für $a \in \mathbb{Z}_{\neq 0}$ gilt $\text{ggT}(a, 0) = |a|$.
- (3) $\text{ggT}(0, 0)$ ist nicht definiert.

Beweis: Siehe Literatur.

□

Rechenregeln für größte gemeinsame Teiler



Satz (1.4.5): Rechenregeln für größte gemeinsame Teiler ([1])

Seien $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$, dann gelten die folgenden Rechenregeln:

- (1) $\text{ggT}(a, b) = \text{ggT}(b, a)$
- (2) $\text{ggT}(a, b) = \text{ggT}(-a, b)$
- (3) $\text{ggT}(a, b) = \text{ggT}(a - b, b)$
- (4) $\text{ggT}\left(\frac{a}{\text{ggT}(a, b)}, \frac{b}{\text{ggT}(a, b)}\right) = 1$
- (5) $\text{ggT}(a, b) = \text{ggT}(r, b)$ für $b \neq 0$ und Rest $r = a \bmod b$ bei Division von a durch b .

Beweis: Siehe Literatur bzw. Tafel.

□



Beweis: Rechenregeln für größte gemeinsame Teiler ([1])

Größter Gemeinsamer Teiler bei Division mit Rest



Satz (1.4.6): Größter gemeinsamer Teiler bei Division mit Rest ([1])

Seien $a, b \in \mathbb{N}$ gegeben und $q, r \in \mathbb{N}_0$ die eindeutigen ganzen Zahlen mit $a = q \cdot b + r$ und $0 \leq r < b$, dann gilt:

$$\text{ggT}(a, b) = \text{ggT}(b, r).$$

Beweis: Siehe Literatur bzw. Tafel.



Beweis: Größter Gemeinsamer Teiler bei Division mit Rest



Beweis: Größter Gemeinsamer Teiler bei Division mit Rest ([1])



Beispiel: Größter Gemeinsamer Teiler bei Division mit Rest



Aufgabe: Anwendung [1]

Wenden Sie den Satz vom größten gemeinsamen Teiler bei Division mit Rest wiederholt auf $\text{ggT}(5767, 4453)$ an, bis sich der Rest Null ergibt. Interpretieren Sie das Ergebnis.



Algorithmus (1.4.7): Euklidischer Algorithmus ([1])

Input: $a, b \in \mathbb{N}$

Output: $\text{ggT}(a, b) \in \mathbb{N}$

Algorithm:

```

1:   procedure EuclidsAlgorithm(a,b)
2:      $x := a; y := b;$            // ▶ Initialisierung
3:     while ( $y \neq 0$ ) do        // ▶ Iteriere für  $y > 0$  :
4:        $r := x \bmod y;$          //  $\text{ggT}(x, y) := \text{ggT}(y, x \bmod y)$ 
5:        $x := y; y := r;$ 
6:     end while;
7:     return x;                // ▶ Rückgabewert:  $x = \text{ggT}(a, b)$ 
8:   end procedure.

```

Beweis:

Die Korrektheit des Algorithmus ergibt sich gemäß Satz zum „Größter gemeinsamer Teiler bei Division mit Rest“. □

Beispiel: Euklidischer Algorithmus



Aufgabe: Berechnung des ggT [1]

Berechnen Sie $\text{ggT}(299, 247) = ?$ $\text{ggT}(578, -442) = ?$.



Satz (1.4.8): Erweiterter Euklidischer Algorithmus ([1])

Seien $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$, dann existieren $s, t \in \mathbb{Z}$ mit

$$\text{ggT}(a, b) = s \cdot a + t \cdot b.$$

Die algorithmische Umsetzung des Vorgehens im Beweis heißt **erweiterter Euklidischer Algorithmus**.

Beweis: Siehe Literatur bzw. Tafel. □

Beweis: Erweiterter Euklidischer Algorithmus



Beweis: Erweiterter Euklidischer Algorithmus ([1])

Die Sonderfälle $a = 0$ bzw. $b = 0$ ergeben direkt $t = \pm 1$ bzw. $s = \pm 1$.

Für $|a|, |b| \neq 0$ gilt:

$$\begin{array}{lll}
 a = q_1 b + r_1 & 0 < r_1 < b & r_1 = a - q_1 b \\
 b = q_2 r_1 + r_2 & 0 < r_2 < r_1 & r_2 = b - q_2 r_1 \\
 r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 & r_3 = r_1 - q_3 r_2 \\
 \dots & \dots & \text{d. h.} \quad \dots \\
 r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} & r_n = r_{n-2} - q_n r_{n-1} \\
 r_{n-1} = q_{n+1} r_n & &
 \end{array}$$

Sukzessives Einsetzen von r_1 in r_2 , r_2 in r_3, \dots, r_{n-1} in r_n ergibt mit $\text{ggT}(a, b) = r_n$ die Darstellung $\text{ggT}(a, b) = \text{ggT}(|a|, |b|) = r_n = s \cdot |a| + t \cdot |b| = \pm s \cdot a \pm t \cdot b$. □



Euklidischer Algorithmus mit $a_i = q_i \cdot b_i + r_i$					$ggT(a, b) = s_i a_i + t_i b_i$	
Iteration i	a_i	b_i	q_i	r_i	s_i	t_i
1	$a_1 := a$	$b_1 := b$	q_1	r_1	$s := s_1 := t_2$	$t := t_1 := s_2 - q_1 \cdot t_2$
2	$a_2 := b_1$	$b_2 := r_1$	q_2	r_2	$s_2 := t_3$	$t_2 := s_3 - q_2 \cdot t_3$
3	$a_3 := b_2$	$b_3 := r_2$	q_3	r_3	$s_3 := t_4$	$t_3 := s_4 - q_3 \cdot t_4$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
i	$a_i := b_{i-1}$	$b_i := r_{i-1}$	q_i	r_i	$s_i := t_{i+1}$	$t_i := s_{i+1} - q_i \cdot t_{i+1}$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
$n-1$	$a_{n-1} := b_{n-2}$	$b_{n-1} := r_{n-2}$	q_{n-1}	r_{n-1}	$s_{n-1} := t_n$	$t_{n-1} := s_n - q_{n-1} \cdot t_n$
n	$ggT(a, b) := b_{n-1}$	0			$s_n := 1$	$t_n := 0$ (oder $t_n \in \mathbb{Z}$)

Invariante im rekursiven Erweiterten Euklidischen Algorithmus



Das Rekursiven Rechenschema 1.4.9 des erweiterten Euklidischen Algorithmus verwendet die **Invariante** $ggT(a, b) = s_i a_i + t_i b_i$ für jede Iteration $i = 1, \dots, n$ (mit den dort geltenden Bezeichnungen). Deren Gültigkeit folgt mit (Rückwärts-)Induktion:

I.A. ($i = n$): Es gilt $ggT(a, b) = a_n = 1 \cdot a_n + t_n \cdot 0 = s_n \cdot a_n + t_n \cdot b_n$.

I.S. ($i + 1 \Rightarrow i$): Nach Induktionsvoraussetzung gilt für ein $i = 1, \dots, n - 1$

$$\begin{aligned}
 ggT(a, b) &= s_{i+1} \cdot a_{i+1} + t_{i+1} \cdot b_{i+1} \\
 &= (t_i + q_i \cdot t_{i+1}) \cdot a_{i+1} + s_i \cdot b_{i+1} \quad (\text{nach Def. von } t_i \text{ und } s_i) \\
 &= (t_i + q_i \cdot s_i) \cdot b_i + s_i \cdot r_i \quad (\text{nach Def. von } s_i, a_{i+1} \text{ und } b_{i+1}) \\
 &= t_i \cdot b_i + s_i \cdot (q_i \cdot b_i + r_i) \\
 &= s_i \cdot a_i + t_i \cdot b_i \quad (\text{nach Schema des Euklidischen Algorithmus}),
 \end{aligned}$$

d.h. die Invariante $ggT(a, b) = s_i a_i + t_i b_i$ gilt für jede Iteration $i = 1, \dots, n$. Für $i = 1$ mit $a_1 := a$ und $b_1 := b$ folgt somit die Darstellung $ggT(a, b) = s_1 \cdot a + t_1 \cdot b$.

□

Beispiel: Erweiterter Euklidischer Algorithmus



Aufgabe: Durchführung des erweiterten Euklidischen Algorithmus [1]

Berechnen Sie $s, t \in \mathbb{Z}$ mit $\text{ggT}(5767, 4453) = s \cdot 5767 + t \cdot 4453$.

(Lösung zur Kontrolle: $s = 17$ und $t = -22$)

Inhaltsverzeichnis Kapitel 01



Kapitel 01: Grundlagen, Teilbarkeit und Vielfache

1.1 Zahlenmengen

1.2 Maxima CAS – ein Computer Algebra System

1.3 Division mit Rest

1.4 Größter gemeinsamer Teiler (ggT)

1.5 Kleinstes gemeinsames Vielfaches (kgV)

1.6 Lineare Diophantische Gleichungen



Definition (1.5.1): Kleinstes gemeinsames Vielfaches ([1])

Seien die Zahlen $a, b \in \mathbb{Z}_{\neq 0}$ gegeben, dann wird das **kleinste gemeinsame Vielfache** $\text{kgV}(a, b) \in \mathbb{N}$ **von** a und b definiert durch

$$\text{kgV}(a, b) := \min \{x \in \mathbb{N} \mid a \mid x \text{ und } b \mid x\}.$$

□

Beispiele:

- $\text{kgV}(4, -16) = 16$
- $\text{kgV}(18, 12) = 36$
- $\text{kgV}(-7, -9) = 63$

Rechenregeln für kleinste gemeinsame Vielfache



Satz (1.5.2): Rechenregeln kleinstes gemeinsames Vielfaches ([1])

Seien $a, b \in \mathbb{Z}_{\neq 0}$ und $m \in \mathbb{N}$ gegeben, dann gelten die folgenden Rechenregeln:

- (1) $\text{kgV}(m \cdot a, m \cdot b) = m \cdot \text{kgV}(a, b)$
- (2) $\text{ggT}(a, b) \cdot \text{kgV}(a, b) = |a| \cdot |b|$.

Beweis: Siehe Literatur.

□

Bemerkungen (1.5.3): Kleinstes gemeinsames Vielfaches ([1])

Die Berechnung des $\text{kgV}(a, b) \in \mathbb{N}$ für $a, b \in \mathbb{Z}_{\neq 0}$ kann wegen (2) sehr einfach mit dem Euklidischen Algorithmus erfolgen.

□

Aufgabe: [1]

Berechnen Sie $\text{kgV}(299, 247) = ?$

(Lösung zur Kontrolle: $\text{kgV}(299, 247) = 5681$).



Kapitel 01: Grundlagen, Teilbarkeit und Vielfache

- 1.1 Zahlenmengen
- 1.2 Maxima CAS – ein Computer Algebra System
- 1.3 Division mit Rest
- 1.4 Größter gemeinsamer Teiler (ggT)
- 1.5 Kleinstes gemeinsames Vielfaches (kgV)
- 1.6 Lineare Diophantische Gleichungen

Lineare Diophantische Gleichungen



Definition (1.6.1): Lineare Diophantische Gleichungen ([1])

Seien die Zahlen $a, b, c \in \mathbb{Z}$ gegeben, dann heißt die Gleichung

$$(G): \quad a \cdot X + b \cdot Y = c$$

eine **lineare Diophantische Gleichung**.

Ein Zahlenpaar $(x, y) \in \mathbb{Z}^2$ mit $a \cdot x + b \cdot y = c$ heißt eine **Lösung** der linearen Diophantischen Gleichung (G). □

Fragen:

- Wann ist eine lineare Diophantische Gleichung lösbar?
- Wie kann man alle Lösungen berechnen?



Definition (1.6.2): Reduzierte lineare Diophantische Gleichungen ([1])

Für die Zahlen $a, b, c \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ sei die lineare Diophantische Gleichung

$$(G): \quad a \cdot X + b \cdot Y = c$$

gegeben und gilt $\text{ggT}(a, b)|c$, dann heißt die Gleichung

$$(G_r): \quad \frac{a}{\text{ggT}(a, b)} \cdot X + \frac{b}{\text{ggT}(a, b)} \cdot Y = \frac{c}{\text{ggT}(a, b)}$$

die zu (G) gehörige reduzierte lineare Diophantische Gleichung. □

Korollar (1.6.3): Reduzierte lineare Diophantische Gleichungen ([1])

Eine lineare Diophantische Gleichung (G) sowie im Fall der Existenz ihre zugehörige reduzierte lineare Diophantische Gleichung (G_r) haben dieselben Lösungen.

Beweis: Siehe Literatur. □

Lösbarkeit linearer Diophantischer Gleichungen



Satz (1.6.4): Lösbarkeit linearer Diophantischer Gleichungen ([1])

Seien $a, b, c \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ gegeben, dann existiert eine Lösung der linearen Diophantischen Gleichung $a \cdot X + b \cdot Y = c$ genau dann, wenn $\text{ggT}(a, b)|c$ gilt.

Beweis: Siehe Literatur bzw. Tafel. □



Algorithmus: Lösungsmenge Diophantischer Gleichungen



Algorithmus (1.6.5): Lösungsmenge Diophantischer Gleichungen ([1])

Input: Lösbare reduzierte Diophantische Gleichung (G): $a \cdot X + b \cdot Y = c$
mit $a, b, c \in \mathbb{Z}$, $(a, b) \neq (0, 0)$ und $\text{ggT}(a, b) = 1$

Output: Lösungsmenge \mathbb{L}_G der Diophantischen Gleichung (G): $a \cdot X + b \cdot Y = c$

(Meta-)Algorithm:

metaprocedure DiophantineSolutions(a,b,c):

 1.Schritt: Konstruiere $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot b = 1$ ($= \text{ggT}(a, b)$),
 z. B. mit dem erweiterten Euklidischen Algorithmus.

 2.Schritt: Berechne eine Lösung $(x_0, y_0) := (s \cdot c, t \cdot c)$.

 3. Schritt: Berechnung der Lösungsmenge:

$$\mathbb{L}_G := \{(x_0 + b \cdot t, y_0 - a \cdot t) \in \mathbb{Z}^2 \mid t \in \mathbb{Z}\}.$$

end metaprocedure.

Beweis: Siehe Literatur. □

Beispiel: Lösungsmenge Diophantischer Gleichungen



Aufgabe: Lösungsmenge Diophantischer Gleichungen [1]

Finden Sie alle Lösungen von (G): $2 \cdot X + 6 \cdot Y = 20$.

(Lösung zur Kontrolle: $\mathbb{L}_G := \{(1 + 3 \cdot t, 3 - t) \in \mathbb{Z} \mid t \in \mathbb{Z}\}$.)

Aufgabe: Restaurant mit Festpreisen [1]

Familie Schmidt betreibt ein Restaurant mit Festpreisen: 11 Euro für Erwachsene, 7 Euro für Kinder. Am Ende eines Tages befinden sich 657 Euro in der Kasse. Wie viele Personen haben an diesem Tag mindestens im Restaurant gegessen?

(Quelle: Einsendeaufgaben zu [1])

(Lösung zur Kontrolle: Mögliche Kundenzahl: 63, 67, 71,... oder 91.)



Technische Hochschule
Ingolstadt

Elementare Zahlentheorie

Kapitel 02: Primzahlen

– Version: Wintersemester 2024/2025 –

Dozent: Prof. Dr. Max Krüger

Fakultät Informatik

Technische Hochschule Ingolstadt (THI)



Kapitel 02: Primzahlen

2.1 Definition und grundlegende Eigenschaften von Primzahlen

- 2.2 Das Sieb des Eratosthenes
- 2.3 Verteilung von Primzahlen
- 2.4 Mersennesche Primzahlen
- 2.5 Primfaktorzerlegung

Primzahlen



Definition (2.1.1): Primzahlen ([1])

Eine natürliche Zahl $p \in \mathbb{N}_{>1}$ größer als 1 heißt **Primzahl** genau dann, wenn $\pm p$ und ± 1 die einzigen ganzzahligen Teiler von p in \mathbb{Z} sind. Die **Menge aller Primzahlen** wird mit \mathbb{P} bezeichnet. Ein natürliche Zahl $n \in \mathbb{N}_{>1}$ größer 1 heißt **zusammengesetzte Zahl** genau dann, wenn n keine Primzahl ist. \square

Beispiele:

- 2, 3, 5, 7, 11, 13 sind Primzahlen
- $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$, $10 = 2 \cdot 5$, $12 = 2 \cdot 6$ und $14 = 2 \cdot 7$ sind zusammengesetzte Zahlen.
- 1 ist weder Primzahl noch zusammengesetzte Zahl.

Definition (2.1.2): Primteiler ([1])

Eine Primzahl $p \in \mathbb{P}$ heißt **Primteiler von $n \in \mathbb{Z}$** genau dann, wenn p Teiler von n ist.

□

Beispiele:

- 2, 3, 7 sind Primteiler von 42.
- 5, 11, 13 sind keine Primteiler von 42.
- 6, 14, 21 sind keine Primteiler von 42.

Grundlegende Eigenschaften von Primzahlen

**Satz (2.1.3):** Grundlegende Eigenschaften von Primzahlen ([1])

- (1) Jede natürliche Zahl $n \in \mathbb{N}_{>1}$ größer als 1 besitzt einen Primteiler.
- (2) Es gibt unendlich viele Primzahlen, d.h. $|\mathbb{P}| = \infty$.

Beweis: Siehe Literatur bzw. Tafel.

□



Inhaltsverzeichnis Kapitel 02



Kapitel 02: Primzahlen

2.1 Definition und grundlegende Eigenschaften von Primzahlen

2.2 Das Sieb des Eratosthenes

2.3 Verteilung von Primzahlen

2.4 Mersennesche Primzahlen

2.5 Primfaktorzerlegung



Satz (2.2.1): Eigenschaften von zusammengesetzten Zahlen ([1])

- (1) Eine zusammengesetzte Zahl $n \in \mathbb{N}_{>1}$ hat einen Teiler $d \in \mathbb{N}_{>1}$ mit $1 < d \leq \sqrt{n}$.
- (2) Eine zusammengesetzte Zahl $n \in \mathbb{N}_{>1}$ hat einen Primteiler $p \in \mathbb{P}$ mit $1 < p \leq \sqrt{n}$.

Beweis: Siehe Literatur bzw. Tafel. □

Beweis: Eigenschaften von zusammengesetzten Zahlen





Algorithmus (2.2.2): Sieb des Eratosthenes ([1])

Input: $n \in \mathbb{N}_{>1}$

Output: Liste L aller Primzahlen $\mathbb{P}_{\leq n}$ kleiner oder gleich n .

Algorithm:

procedure Eratosthenes(n):

 1. Schritt: Initialisiere $L := [2, 3, \dots, n]$ und $i := 1$.

 // (Zugriff auf das j -te Element mit $L[j]$)

 2. Schritt: Wenn $L[i] > \sqrt{n}$ gilt, dann gehe zum 5. Schritt.

 3. Schritt: Streiche alle Vielfachen $2 \cdot L[i], 3 \cdot L[i], \dots, \left\lfloor \frac{n}{L[i]} \right\rfloor \cdot L[i]$ aus L .

 4. Schritt: Setze $i := i + 1$ und gehe zum 2. Schritt.

 5. Schritt: Return L .

end procedure.

Beweis: Siehe Literatur. □

Beispiel: Sieb des Eratosthenes



Aufgabe: Sieb des Eratosthenes [1]

Bestimme alle Primzahlen kleiner oder gleich 51 mit dem Sieb des Erathosthenes.



Kapitel 02: Primzahlen

- 2.1 Definition und grundlegende Eigenschaften von Primzahlen
- 2.2 Das Sieb des Eratosthenes
- 2.3 Verteilung von Primzahlen**
- 2.4 Mersennesche Primzahlen
- 2.5 Primfaktorzerlegung

Primzahlfunktion



Definition (2.3.1): Primzahlfunktion ([1])

Die Funktion $\pi : \mathbb{R} \rightarrow \mathbb{N}_0$ mit $\pi(x) := |\{p \in \mathbb{P} \mid p \leq x\}|$ heißt **Primzahlfunktion**.

Der Wert $\pi(x)$ der Primzahlfunktion ist die Anzahl der Primzahlen kleiner gleich $x \in \mathbb{R}$.

□

Beispiele:

- $\pi(0) = 0, \pi(1) = 0, \pi(2) = 1.$
- $\pi(-5) = 0, \pi(1.99) = 0, \pi(3.5) = 2.$
- $\pi(10) = 4, \pi(11.5) = 5, \pi(13.1) = 6.$



Aufgabe: Sieb des Eratosthenes [1]

Bestimmen Sie die Werte $\pi(x)$ der Primzahlfunktion für $x = 0, 1, 2, \dots, 51$.

(Hinweis: Lösung zur Aufgabe zum Sieb des Eratosthenes.)

Primzahlsatz



Satz (2.3.2): Primzahlsatz ([4])

Sei die Primzahlfunktion $\pi : \mathbb{R} \rightarrow \mathbb{N}_0$ mit $\pi(x) := |\{p \in \mathbb{P} \mid p \leq x\}|$ gegeben, dann gilt $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\left(\frac{x}{\ln(x)}\right)} = 1$, d.h. für sehr große $x \in \mathbb{R}$ gilt die Näherung $\pi(x) \approx \frac{x}{\ln(x)}$ für die Anzahl der Primzahlen bis x .

Beweis: Siehe Literatur.

□

Bemerkung:

Für die Integralsinus-Funktion $\text{Li} : \mathbb{R}_{\geq 2} \rightarrow \mathbb{R}$ mit $\text{Li}(x) := \int_2^x \frac{1}{\ln(t)} dt$ gilt ebenfalls $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\text{Li}(x)} = 1$.¹⁾ Sie liefert eine bessere Approximation $\pi(x) \approx \text{Li}(x)$,¹⁾ ist allerdings komplizierter zu berechnen, da $\frac{1}{\ln(x)}$ keine elementar darstellbare Stammfunktion besitzt.

1) Quelle: <https://de.wikipedia.org/wiki/Primzahlsatz> (abgerufen am 17.12.2023).

Beispiele für die Approximation der Primzahlfunktion $\pi(x)$



x	$\pi(x)$	$\frac{x}{\ln(x)} \approx$	$\pi(x) - \frac{x}{\ln(x)} \approx$	$\frac{\pi(x)}{\frac{x}{\ln(x)}} \approx$	$\text{Li}(x) := \int_2^x \frac{dt}{\ln t} \approx$	$\text{Li}(x) - \pi(x) \approx$
10	4	4		0,921034	6	2
10^2	25	22		3,151293	30	5
10^3	168	145		23,160503	178	10
10^4	1.229	1.086		143,131951	1.246	17
10^5	9.592	8.686		906,104320	9.630	38
10^6	78.498	72.382		6.116,1084490	78.628	130
10^7	664.579	620.421		44.158,1071175	664.918	339
10^8	5.761.455	5.428.681		332.774,1061299	5.762.209	754
10^9	50.847.534	48.254.942		2.592.592,1053727	50.849.235	1.701
10^{10}	455.052.511	434.294.482		20.758.029,1047797	455.055.615	3.104
10^{11}	4.118.054.813	3.948.131.654		169.923.159,1043039	4.118.066.401	11.588
10^{12}	37.607.912.018	36.191.206.825		1.416.705.193,1039145	37.607.950.281	38.263
10^{13}	346.065.536.839	334.072.678.387		11.992.858.452,1035899	346.065.645.810	108.971
10^{14}	3.204.941.750.802	3.102.103.442.166		102.838.308.636,1033151	3.204.942.065.692	314.890
10^{15}	29.844.570.422.669	28.952.965.460.217		891.604.962.452,1030795	29.844.571.475.288	1.052.619
10^{16}	279.238.341.033.925	271.434.051.189.532		7.804.289.844.393,1028752	279.238.344.248.557	3.214.632
10^{17}	2.623.557.157.654.233	2.554.673.422.960.305		68.883.734.693.281,1026964	2.623.557.165.610.822	7.956.589
10^{18}	24.739.954.287.740.860	24.127.471.216.847.324		612.483.070.893.536,1025385	24.739.954.309.690.415	21.949.555
10^{19}	234.057.667.276.344.607	228.576.043.106.974.646		5.481.624.169.369.960,1023982	234.057.667.376.222.382	99.877.775
10^{20}	2.220.819.602.560.918.840	2.171.472.409.516.259.138		49.347.193.044.659.701,1022725	2.220.819.602.783.663.484	222.744.644
10^{21}	21.127.269.486.018.731.928	20.680.689.614.440.563.221		446.579.871.578.168.707,1021594	21.127.269.486.616.126.182	597.394.254
10^{22}	201.467.286.689.315.906.290	197.406.582.683.296.285.296		4.060.704.006.019.620.994,1020570	201.467.286.691.248.261.498	1.932.355.208
10^{23}	1.925.320.391.606.803.968.923	1.888.236.877.840.225.337.614		37.083.513.766.578.631.309,1019639	1.925.320.391.614.054.155.139	7.250.186.216
10^{24}	18.435.599.767.349.200.867.866	18.095.603.412.635.492.818.797		339.996.354.713.708.049.069,1018789	18.435.599.767.366.347.775.144	17.146.907.278
10^{25}	176.846.309.399.143.769.411.680	173.717.792.761.300.731.060.452		3.128.516.637.843.038.351.228,1018009	176.846.309.399.198.930.392.619	55.160.980.939
10^{26}	1.699.246.750.872.437.141.327.603	1.670.363.391.935.583.952.504.342		28.883.358.936.853.188.823.261,1017292	1.699.246.750.872.593.033.005.724	155.891.678.121
10^{27}	16.352.460.426.841.680.446.427.399	16.084.980.811.231.549.172.264.034		267.479.615.610.131.274.163.365,1016629	16.352.460.426.842.189.113.085.405	508.666.658.006
10^{28}	157.589.269.275.973.410.412.739.598	155.105.172.108.304.224.161.117.471		2.484.097.167.669.186.251.622.127,1016016	157.589.269.275.974.838.158.399.972	1.427.745.660.374
10^{29}	1.520.698.109.714.272.166.094.258.063	1.497.567.178.976.730.440.176.306.617		23.130.930.737.541.725.917.951.446,1015446	1.520.698.109.714.276.717.287.880.527	4.551.193.622.464
OEIS	Folge A006880 in OEIS	Folge A057834 in OEIS	Folge A057835 in OEIS	Folge A057754 in OEIS	Folge A057752 in OEIS	

Quelle: <https://de.wikipedia.org/wiki/Primzahlsatz> (abgerufen am 17.12.2023).

Primzahlzwillinge und Primzahldrillinge



Definition (2.3.3): Primzahlzwillinge und Primzahldrillinge ([1])

Sei $p \in \mathbb{P}$ eine Primzahl.

- (1) Das Paar $(p, p + 2)$ heißt ein **Primzahlwilling** genau dann, wenn $p + 2$ ebenfalls eine Primzahl ist.
- (2) Das Tripel $(p, p + 2, p + 4)$ heißt ein **Primzahldrilling** genau dann, wenn $p + 2$ und $p + 4$ ebenfalls beide Primzahlen sind. \square

Beispiele:

- $(3, 5), (5, 7), (11, 13), (17, 19)$ sind Primzahlzwillinge.
- $(3, 5, 7)$ ist ein Primzahldrilling.

Bemerkung: Es ist ungeklärt, ob es unendlich viele Primzahlzwillinge gibt.



Satz (2.3.4): Primzahllöcher beliebiger Länge ([1])

Sei $k \in \mathbb{N}$ gegeben, dann gibt es eine natürliche Zahl $n \in \mathbb{N}$, so dass die aufeinander folgenden k Zahlen $n + 1, n + 2, \dots, n + k \notin \mathbb{P}$ keine Primzahlen sind. Es existieren also Primzahllöcher beliebiger Länge.

Beweis: Siehe Literatur bzw. Tafel. □

Beweis: Primzahllöcher beliebiger Länge





Kapitel 02: Primzahlen

- 2.1 Definition und grundlegende Eigenschaften von Primzahlen
- 2.2 Das Sieb des Eratosthenes
- 2.3 Verteilung von Primzahlen
- 2.4 Mersennesche Primzahlen**
- 2.5 Primfaktorzerlegung

Mersennesche Primzahlen



Definition 2.4.3: Mersennesche Primzahlen ([1])

Für $n \in \mathbb{N}$ heißt $M_n := 2^n - 1$ die n -te **Mersennesche Zahl** und ist M_n zusätzlich eine Primzahl, so heißt M_n **Mersennesche Primzahl**. □

Beispiele:

- $2^2 - 1 = 3, 2^3 - 1 = 7, 2^4 - 1 = 15, 2^5 - 1 = 31, 2^6 - 1 = 63, \dots$
sind Mersennesche Zahlen.
- $2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 31, 2^7 - 1 = 127$, u.v.m.
sind Mersennesche Primzahlen.
- $2^{11} - 1 = 2047 = 23 \cdot 89$ ist die kleinste Mersennesche Zahl mit Primzahlexponent die selbst keine Primzahl ist.



Satz (2.4.1): Primzahlen und Vorgänger von Potenzen ([1])

Seien $a, n \in \mathbb{N}$ mit $n \geq 2$ gegeben, dann gilt:

- (1) Wenn $a^n - 1$ Primzahl ist, dann muss $a = 2$ gelten.
- (2) Wenn $2^n - 1$ Primzahl ist, dann ist n ebenfalls Primzahl.

Beweis: Siehe Literatur bzw. Tafel. □

Korollar (2.4.2): Vorgänger von Potenzen ([1])

Für alle $a, n \in \mathbb{N}$ mit $a \geq 3$ und $n \geq 2$ ist $a^n - 1$ eine zusammengesetzte Zahl.

Beweis: Anwendung des Satzes (2.4.1) „Primzahlen und Vorgänger von Potenzen (1)“ . □

Beweis: Primzahlen und Vorgänger von Potenzen



Beweis: Primzahlen und Vorgänger von Potenzen ([1])



Kapitel 02: Primzahlen

- 2.1 Definition und grundlegende Eigenschaften von Primzahlen
- 2.2 Das Sieb des Eratosthenes
- 2.3 Verteilung von Primzahlen
- 2.4 Mersennesche Primzahlen
- 2.5 Primfaktorzerlegung**

Primfaktorzerlegungen



Definition (2.5.1): Primfaktorzerlegungen ganzer Zahlen ([1])

Für eine ganze Zahl $n \in \mathbb{Z}_{\neq 0}$ heißt das Produkt $n = \pm p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ mit Primzahlen $p_1, \dots, p_r \in \mathbb{P}$, Exponenten $e_1, \dots, e_r \in \mathbb{N}_0$ und $r \in \mathbb{N}$ eine **Primfaktorzerlegung**. □

Beispiel:

$-1234567890 = -2^1 \cdot 5^1 \cdot 7^0 \cdot 3^2 \cdot 11^0 \cdot 3607^1 \cdot 13^0 \cdot 3803^1$ ist eine Primfaktordarstellung von -1234567890 .



Satz und Definition (2.5.2): Eindeutige Primfaktorzerlegung ganzer Zahlen ([1])

Alle ganzen Zahlen $n \in \mathbb{Z} \setminus \{0, +1, -1\}$ lassen sich eindeutig als **kanonische Primfaktorzerlegung** $n = \pm p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ mit Primzahlen $p_1, \dots, p_r \in \mathbb{P}$ und Exponenten $e_1, \dots, e_r \in \mathbb{N}$ schreiben, wobei $p_1 < \dots < p_r$ und $r \in \mathbb{N}$ gilt.

Beweis: Siehe Literatur. □

Beispiel:

$$-1234567890 = -2 \cdot 3^2 \cdot 5 \cdot 3803 \cdot 3607$$

Aufgabe:

a) Bestimmen Sie die kanonische Primfaktorzerlegung von $n = 415800$.

b) Warum widerspricht die mehrdeutige Zerlegung

$$2^2 \cdot 3 \cdot 7 \cdot 1183 \cdot 3607 = 358434804 = 2^2 \cdot 3 \cdot 13 \cdot 637 \cdot 3607$$

dem Satz von der eindeutigen Primfaktorzerlegung nicht?

Berechnung von ggT und kgV mittels Primfaktorzerlegungen



Satz (2.5.3): Berechnung von ggT und kgV mittels Primfaktorzerlegungen ([1])

Seien die Zahlen $a, b \in \mathbb{N}$ mit Primfaktorzerlegungen $a = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ und $b = p_1^{f_1} \cdot \dots \cdot p_r^{f_r}$ für Primzahlen $p_1, \dots, p_r \in \mathbb{P}$, Exponenten $e_1, \dots, e_r, f_1, \dots, f_r \in \mathbb{N}_0$ und $r \in \mathbb{N}$ gegeben, dann gilt:

$$(1) \quad \text{ggT}(a, b) = p_1^{\min(e_1, f_1)} \cdot \dots \cdot p_r^{\min(e_r, f_r)} \quad \text{und}$$

$$(2) \quad \text{kgV}(a, b) = p_1^{\max(e_1, f_1)} \cdot \dots \cdot p_r^{\max(e_r, f_r)}.$$

Beweis: Siehe Literatur. □

Aufgabe:

Berechnen Sie ggT(9100,3850) und kgV(9100,3850) mittels Primfaktorzerlegung.

Elementare Zahlentheorie

Kapitel 03: Kongruenzen und die Sätze von Fermat

– Version: Wintersemester 2024/2025 –

Dozent: Prof. Dr. Max Krüger
Fakultät Informatik
Technische Hochschule Ingolstadt (THI)

75

Inhaltsverzeichnis Kapitel 03



Kapitel 03: Kongruenzen und die Sätze von Fermat

- 3.1 Definition und grundlegende Eigenschaften von Kongruenzen
- 3.2 Lineare Kongruenzen und der Chinesische Restsatz
- 3.3 Kleiner Satz von Fermat und Satz von Wilson
- 3.4 Fermat's Last Theorem – Großer Satz von Fermat



Definition und Satz (3.1.1): Modulo, Kongruenzen und ihre Charakterisierung ([1])

Seien ganze Zahlen $a, b \in \mathbb{Z}$ und eine natürliche Zahl $m \in \mathbb{N}$ gegeben.

- (1) Gilt die Teilbarkeitsrelation $m|a - b$, so heißt a **kongruent zu b modulo m** , symbolisch notiert als $a \equiv_m b$ oder $a \equiv b \pmod{m}$.
- (2) Der ganzzahlige Rest $r \in \{0, 1, \dots, m - 1\}$ bei Division von a durch m wird mit $(a \bmod m) := r$ bezeichnet.
- (3) Es gilt $a \equiv_m b$ genau dann, wenn $a \bmod m = b \bmod m$ gilt.

Beweis: Siehe Literatur bzw. Tafel. □

Beispiele:

- $8 \equiv_4 16$
- $13391 \equiv_{773} -19075$, weil $773|13391 - (-19575)$ bzw.
 $(13391 \bmod 773) = 250 = (-19075 \bmod 773)$ gilt.



Beweis: Kongruenzen und ihre Charakterisierung

Beweis: Kongruenzen und ihre Charakterisierung ([1])



Satz (3.1.2): Rechenregeln für Modulo und Kongruenzen ([1])

Seien ganze Zahlen $a, b, c \in \mathbb{Z}$ und $m, n, d \in \mathbb{N}_{>1}$ gegeben, dann gilt:

- (1) $(a + b) \equiv_m (a \text{ mod } m) + (b \text{ mod } m),$
- (2) $(a \cdot b) \equiv_m (a \text{ mod } m) \cdot (b \text{ mod } m),$
- (3) $a \equiv_m a,$
- (4) $a \equiv_m b \Leftrightarrow b \equiv_m a,$
- (5) $a \equiv_m b, b \equiv_m c \Rightarrow a \equiv_m c,$
- (6) $a \equiv_m b \Rightarrow (a + c) \equiv_m (b + c),$
- (7) $a \equiv_m b \Rightarrow (a \cdot c) \equiv_m (b \cdot c),$
- (8) $a \cdot c \equiv_m b \cdot c, \text{ ggT}(c, m) = 1 \Rightarrow a \equiv_m b,$
- (9) $a \cdot c \equiv_m b \cdot c, \text{ ggT}(c, m) = d \Rightarrow a \equiv_{\frac{m}{d}} b,$
- (10) $a \equiv_m b \Rightarrow a^n \equiv_m b^n \text{ und}$
- (11) $a \equiv_m b, a \equiv_n b, \text{ ggT}(m, n) = 1 \Rightarrow a \equiv_{m \cdot n} b.$

Beweis: Siehe Literatur. □

Inhaltsverzeichnis Kapitel 03



Kapitel 03: Kongruenzen und die Sätze von Fermat

- 3.1 Definition und grundlegende Eigenschaften von Kongruenzen
- 3.2 Lineare Kongruenzen und der Chinesische Restsatz
- 3.3 Kleiner Satz von Fermat und Satz von Wilson
- 3.4 Fermat's Last Theorem – Großer Satz von Fermat



Definition (3.2.1): Lineare Kongruenzen ([1])

Seien ganze Zahlen $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}_{>1}$ gegeben, dann heißt der Ausdruck $a \cdot X \equiv_m b$ eine **lineare Kongruenz in X** . Eine Zahl $x_0 \in \{0, 1, \dots, m - 1\}$ heißt **Lösung der linearen Kongruenz** $a \cdot X \equiv_m b$ genau dann, wenn $a \cdot x_0 \equiv_m b$ gilt.

□

Beispiel:

- Die lineare Kongruenz $2 \cdot X \equiv_6 4$ hat die zwei Lösungen $x_{01} = 2$ und $x_{02} = 5$.
- Die lineare Kongruenz $2 \cdot X \equiv_4 1$ hat keine Lösung.

Fragen:

- Wann ist eine lineare Kongruenz lösbar?
- Wie viele Lösungen hat eine lösbare lineare Kongruenz?
- Wie kann man alle Lösungen berechnen?

Lösbarkeit und Lösungen lineare Kongruenzen



Satz (3.2.2): Lösbarkeit und Lösungen lineare Kongruenzen ([1])

Sei die lineare Kongruenz $a \cdot X \equiv_m b$ in X mit $a, b \in \mathbb{Z}, m \in \mathbb{N}_{>1}$ gegeben.

- (1) $a \cdot X \equiv_m b$ ist lösbar genau dann, wenn $\text{ggT}(a, m) | b$ gilt.
- (2) $a \cdot X \equiv_m b$ hat die eindeutige Lösung $x_0 \in \{0, 1, \dots, m - 1\}$ genau dann, wenn $d := \text{ggT}(a, m) = 1$ gilt. Es gilt dann $x_0 := s \cdot b \bmod m$, wobei $s, t \in \mathbb{Z}$ eine Lösung von $s \cdot a + t \cdot m = 1$ gemäß dem erweiterten Euklidischen Algorithmus ist.
- (3) Die lösbare lineare Kongruenz $a \cdot X \equiv_m b$ besitzt genau $\text{ggT}(a, m)$ verschiedene Lösungen $x_i \in \{0, 1, \dots, m - 1\}$ mit $i = 1, \dots, \text{ggT}(a, m)$:

Die eindeutige Lösung von $\frac{a}{\text{ggT}(a, m)} \cdot X \equiv_{(\frac{m}{\text{ggT}(a, m)})} \frac{b}{\text{ggT}(a, m)}$ gemäß (2)
sei x_0 , dann sind $x_i := x_0 + \frac{(i-1) \cdot m}{\text{ggT}(a, m)}$ für $i = 1, \dots, \text{ggT}(a, m)$ alle

Lösungen $x_i \in \{0, 1, \dots, m - 1\}$ der linearen Kongruenz $a \cdot X \equiv_m b$

Beweis: Siehe Literatur.

□



Algorithmus (3.2.3): Lösungsmengen linearer Kongruenzen ([1])

Input: Lösbare lineare Kongruenz (K): $a \cdot X \equiv_m b$ in X
mit $a, b \in \mathbb{Z}$, $m \in \mathbb{N}_{>1}$ und $\text{ggT}(a, m) | b$.

Output: Lösungsmenge \mathbb{L}_K der linearen Kongruenz (K): $a \cdot X \equiv_m b$

(Meta-)Algorithm:

metaprocedure LinearCongruence(a,b,m):

 1.Schritt: Konstruiere $s, t \in \mathbb{Z}$ mit $s \cdot \frac{a}{\text{ggT}(a, m)} + t \cdot \frac{m}{\text{ggT}(a, m)} = 1$,

 z. B. mit dem erweiterten Euklidischen Algorithmus.

 2.Schritt: Berechne eine Lösung $x_0 := s \cdot \frac{b}{\text{ggT}(a, m)} \bmod \left(\frac{m}{\text{ggT}(a, m)} \right)$.

 3. Schritt: Berechnung der Lösungsmenge:

$$\mathbb{L}_K := \left\{ x_0 + \frac{(i-1) \cdot m}{\text{ggT}(a, m)} \in \{0, 1, \dots, m-1\} \mid i = 1, \dots, \text{ggT}(a, m) \right\}.$$

end metaprocedure.

Beweis: Siehe Literatur. □

Beispiel: Lösungsmengen linearer Kongruenzen



Aufgabe: Lineare Kongruenzen [1]

- Bestimme alle Lösungen der linearen Kongruenz $2 \cdot X \equiv_4 1$.
- Bestimme alle Lösungen der linearen Kongruenz $2 \cdot X \equiv_6 4$.

(Lösung zur Kontrolle: $\{\}, \{2,5\}$)

Aufgabe: Lineare Kongruenzen [1]

Bestimme alle Lösungen der linearen Kongruenz $30 \cdot X \equiv_{18} 6$.

(Lösung zur Kontrolle: $\{2, 5, 8, 11, 14, 17\}$)



Definition (3.2.4): Systeme Linearer Kongruenzen (vgl. [1])

Seien ganze Zahlen $a_i, b_i \in \mathbb{Z}$ und $m_i \in \mathbb{N}_{>1}$ für $i = 1, \dots, r$ mit $r \in \mathbb{N}$ gegeben, dann heißt das System

$$(S): \begin{array}{l} a_1 \cdot X \equiv_{m_1} b_1 \\ \vdots \\ a_r \cdot X \equiv_{m_r} b_r \end{array}$$

ein **System linearer Kongruenzen in X** . Eine Zahl $x_0 \in \mathbb{Z}$ heißt **Lösung des Systems (S) linearer Kongruenzen in X** genau dann, wenn alle Kongruenzen gelten:

$$\begin{array}{l} a_1 \cdot x_0 \equiv_{m_1} b_1 \\ \vdots \\ a_r \cdot x_0 \equiv_{m_r} b_r . \end{array}$$

□

Beispiel:

$$X \equiv_3 2$$

$$X \equiv_5 1$$

$$X \equiv_7 6$$

hat die Lösung $x_0 = 41$.

Chinesischer Restsatz



Satz (3.2.5): Chinesischer Restsatz ([1])

Für $i = 1, \dots, r$ mit $r \in \mathbb{N}$ seien $a_i \in \mathbb{Z}$ und paarweise teilerfremde $m_i \in \mathbb{N}_{>1}$ gegeben, d.h. es gilt $\text{ggT}(m_i, m_j) = 1$ für alle $i \in \{1, \dots, r\}$ mit $i \neq j$, dann gilt:

Das System $\begin{pmatrix} X \equiv_{m_1} a_1 \\ \vdots \\ X \equiv_{m_r} a_r \end{pmatrix}$ linearer Kongruenzen in X hat genau eine

nicht-negative Lösung $x_0 \in \mathbb{Z}_{0 \leq m_1 \dots m_r - 1}$ im

Lösungsbereich $\mathbb{Z}_{0 \leq m_1 \dots m_r - 1} := \{0, 1, \dots, m_1 \cdot \dots \cdot m_r - 1\}$.

Beweis: Siehe Literatur.

□



Algorithmus (3.2.6): Lösung des Chinesischen Restsatzes ([1])

Input:

System (S):= $\begin{pmatrix} X \equiv_{m_1} a_1 \\ \vdots \\ X \equiv_{m_r} a_r \end{pmatrix}$ linearer Kongruenzen in X mit

$a_i \in \mathbb{Z}$ und paarweise teilerfremden $m_i \in \mathbb{N}_{>1}$ für $i = 1, \dots, r$ mit $r \in \mathbb{N}$

Output: Lösung $x_0 \in \{0, 1, \dots, m_1 \cdot \dots \cdot m_r\}$ des Systems (S) linearer Kongruenzen

(Meta-)Algorithm:

metaprocedure ChineseRemainder($a_1, \dots, a_r, m_1, \dots, m_r$):

1. Schritt: Berechne $M := m_1 \cdot \dots \cdot m_r$ und $M_i := \frac{M}{m_i}$ für $i = 1, \dots, r$.

2. Schritt: Berechne mit Algorithmus „Lösungsmengen linearer Kongruenzen“ die eindeutigen Lösungen $x_i \in \{0, 1, \dots, m_i - 1\}$ der linearen Kongruenzen $M_i \cdot X \equiv_{m_i} 1$ für $i = 1, \dots, r$.

3. Schritt: Berechne Lösung $x_0 := (a_1 \cdot M_1 \cdot x_1 + \dots + a_r \cdot M_r \cdot x_r) \bmod M$.
end metaprocedure.

Beweis: Siehe Literatur. □

Beispiel: Lösung des Chinesischen Restsatz



Aufgabe: Chinesischer Restsatz [1]

Bestimme die Lösung von $X \equiv_3 2$

$$X \equiv_5 1$$

$$X \equiv_7 6 .$$

(Lösung zur Kontrolle: $x_0 = 41$)

Aufgabe: Marschkapelle [1]

Die Mitglieder einer Marschkapelle sollen so aufgeteilt werden, dass in einer Reihe jeweils 4 Personen laufen. Bei dieser Aufteilung bleibt aber 1 Mitglied über. Der Versuch, 5 Personen in eine Reihe zu stellen, liefert 2 übrig gebliebene Mitglieder. Werden 7 Personen in eine Reihe gestellt, so bleiben 3 über. Wie viele Mitglieder hat die Marschkapelle (im kleinstmöglichen Fall)?

(Lösung zur Kontrolle: 17)



Satz (3.2.7): Ganzzahlige Lösungen des Chinesischen Restsatzes ([1])

Für $i = 1, \dots, r$ mit $r \in \mathbb{N}$ seien $a_i \in \mathbb{Z}$ und paarweise teilerfremde $m_i \in \mathbb{N}_{>1}$

gegeben und das System (S):= $\begin{pmatrix} X \equiv_{m_1} a_1 \\ \vdots \\ X \equiv_{m_r} a_r \end{pmatrix}$ linearer Kongruenzen in X hat eine

ganzzahlige Lösung $x_0 \in \mathbb{Z}$, dann gilt:

Die Zahl $y \in \mathbb{Z}$ ist (weitere) Lösung des Systems (S) linearer Kongruenzen in X genau dann, wenn die Teilbarkeitsbeziehung $m_1 \cdot \dots \cdot m_r | (y - x_0)$ gilt.

Beweis: Siehe Literatur bzw. Tafel

□

Beweis: Ganzzahlige Lösungen des Chinesischen Restsatzes



Beweis: Ganzzahlige Lösungen des Chinesischen Restsatzes ([1])



Aufgabe: Marschkapelle [1]

Die Mitglieder einer Marschkapelle sollen so aufgeteilt werden, dass in einer Reihe jeweils 4 Personen laufen. Bei dieser Aufteilung bleibt aber 1 Mitglied über. Der Versuch, 5 Personen in eine Reihe zu stellen, liefert 2 übrig gebliebene Mitglieder. Werden 7 Personen in eine Reihe gestellt, so bleiben 3 über.

Wie viele Mitglieder könnte die Marschkapelle (theoretisch) noch haben?

(Lösung zur Kontrolle: 17, 157, 297, ...)

Inhaltsverzeichnis Kapitel 03



Kapitel 03: Kongruenzen und die Sätze von Fermat

- 3.1 Definition und grundlegende Eigenschaften von Kongruenzen
- 3.2 Lineare Kongruenzen und der Chinesische Restsatz
- 3.3 Kleiner Satz von Fermat und Satz von Wilson**
- 3.4 Fermat's Last Theorem – Großer Satz von Fermat



Satz (3.3.1): Kleiner Satz von Fermat ([1])

Sei $a \in \mathbb{Z}$ und eine Primzahl $p \in \mathbb{P}$, dann gilt $a^p \equiv_p a$.

Beweis: Siehe Literatur bzw. Tafel. □

Beispiele:

- $2^3 \equiv_3 2$, $2^5 \equiv_5 2$ und $2^7 \equiv_7 2$,
- $3^2 \equiv_2 3$, $3^5 \equiv_5 3$ und $3^7 \equiv_7 3$,
- $4^3 \equiv_3 4$, $6^5 \equiv_5 6$ und $120^7 \equiv_7 120$,
- $2^2 \equiv_2 2$, $3^3 \equiv_3 3$, $4^2 \equiv_2 4$ und $120^5 \equiv_5 120$.

Beweis: Kleiner Satz von Fermat



Beweis: Kleiner Satz von Fermat (Beweisidee gem. [a])



Satz (3.3.2): Kleiner Satz von Fermat – alternative Version ([1])

Sei $a \in \mathbb{Z}$ und eine Primzahl $p \in \mathbb{P}$ mit $\text{ggT}(a, p) = 1$, dann gilt $a^{p-1} \equiv_p 1$.

Beweis: Siehe Literatur bzw. Tafel. □

Beispiele:

- $2^{3-1} \equiv_3 1$, $2^{5-1} \equiv_5 1$ und $2^{7-1} \equiv_7 1$,
- $3^{2-1} \equiv_2 1$, $3^{5-1} \equiv_5 1$ und $3^{7-1} \equiv_7 1$, und
- $4^{3-1} \equiv_3 1$, $6^{5-1} \equiv_5 1$ und $120^{7-1} \equiv_7 1$.

Aufgaben:

- 1) Berechnen Sie (mit Rechenweg oder Begründung) $((10!)^{10} \bmod 11) = \dots$?
- 2) Warum gilt $2^{2-1} \not\equiv_2 1$, $3^{3-1} \not\equiv_3 1$, $4^{2-1} \not\equiv_2 1$ und $120^{5-1} \not\equiv_5 1$ ohne im Widerspruch zum Kleinen Satz von Fermat zu stehen?

Beweis: Kleiner Satz von Fermat – alternative Version



[a] Beweisidee: https://de.wikibooks.org/wiki/Beweisarchiv:_Zahlentheorie:_Elementare_Zahlentheorie:_Kleiner_Satz_von_Fermat, download am 10.12.2023]



Satz (3.3.3): Satz von Wilson ([1])

Die natürliche Zahl $p \in \mathbb{N}_{>1}$ ist genau dann Primzahl, wenn die Kongruenz $(p-1)! \equiv_p -1$ gilt.

Beweis: Siehe Literatur. □

Bemerkungen:

- Aus historischen Gründen schreibt man $(p-1)! \equiv_p -1$ statt $(p-1)! \equiv_p p-1$.
- Für große Zahlen macht die Berechnungskomplexität den Satz von Wilson unbrauchbar.

Beispiele:

- 2, 3, 5, 7 sind Primzahlen und es gilt $1! \equiv_2 1, 2! \equiv_3 2, 4! \equiv_5 4, 6! \equiv_7 6,$
- $36! = 371993326789901217467999448150835200000000 \equiv_{37} 36$, also ist 37 Primzahl.

Aufgaben: Satz von Wilson



Aufgaben:

- 1) Berechnen Sie (mit Rechenweg oder Begründung) $12! \bmod 13 = \dots ?$.
- 2) Prüfen Sie mit dem Satz von Wilson, ob $p=11$ und $p=9$ Primzahlen sind.



Kapitel 03: Kongruenzen und die Sätze von Fermat

- 3.1 Definition und grundlegende Eigenschaften von Kongruenzen
- 3.2 Lineare Kongruenzen und der Chinesische Restsatz
- 3.3 Kleiner Satz von Fermat und Satz von Wilson
- 3.4 Fermat's Last Theorem – Großer Satz von Fermat

Fermat'sche Vermutung – Fermat's Last Theorem



Der französische Mathematiker und Jurist *Pierre de Fermat* (*1607 - †1665) schrieb irgendwann im Zeitraum zwischen 1637 und 1643 in sein Exemplar des Mathematikbuchs *Arithmetica* des *Diophantos von Alexandria* folgende Randnotiz, im Original in Latein:¹⁾

„Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere: cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.“¹⁾ [Pierre de Fermat, Randnotiz in einem Exemplar der *Arithmetica*]

„Es ist nicht möglich, einen Kubus in zwei Kuben oder ein Biquadrat in zwei Biquadrate und allgemein eine Potenz, höher als die zweite, in zwei Potenzen mit demselben Exponenten zu zerlegen. Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch ist der Rand hier zu schmal, um ihn zu fassen.“¹⁾

1) Quelle: https://de.wikipedia.org/wiki/Großer_Fermatscher_Satz (abgerufen am 13.06.2022).



Satz (und Definition) (3.4.1): Großer Satz von Fermat ([1])

Sei $n \in \mathbb{N}_{\geq 2}$ und $X, Y, Z \in \mathbb{Z}$ gegeben.

- Die Gleichung (G): $X^n + Y^n = Z^n$ heißt eine **Fermat'sche Gleichung**.
- Ein ganzzahliges Tripel $(x_0, y_0, z_0) \in \mathbb{Z}^3$ heißt eine **Lösung der Fermat'schen Gleichung** (G): $X^n + Y^n = Z^n$ genau dann, wenn $x_0^n + y_0^n = z_0^n$ gilt.
- Eine Lösung $(x_0, y_0, z_0) \in \mathbb{Z}_{\neq 0}^3$ heißt eine **nicht-triviale Lösung der Fermat'schen Gleichung** (G).

Die Fermat'sche Gleichung (G): $X^n + Y^n = Z^n$ hat ausschließlich im Fall $n = 2$ nicht-triviale Lösungen.

Beweis: Siehe Literatur. □

Bedeutung von Fermat's Last Theorem



Bemerkungen:

- Fermat vermutete also, dass die Gleichung $X^n + Y^n = Z^n$ mit $X, Y, Z \in \mathbb{Z}$ und $n \in \mathbb{N}$ für $n > 2$ nur die trivialen Lösungen mit $X = 0$ oder $Y = 0$ oder $Z = 0$ hat.
- Fermat behauptete einen Beweis zu haben, der aber weder von ihm veröffentlicht wurde noch in seinen Unterlagen gefunden werden konnte.
- Fermat'sche Vermutung wird auch als „Großer Satz von Fermat“ oder im Englischen als „Fermat's Last Theorem“ bezeichnet.
- Der Versuch die Fermat'sche Vermutung zu beweisen oder zu widerlegen hat über 350 Jahre gedauert und – quasi nebenbei – zu Entwicklung einer Vielzahl mathematischer Theorien und Methoden geführt [1].
- Die vollständige Klärung wurde erst im Jahr 1995 durch Andrew Wiles erbracht.
- Vermutlich gibt es weltweit weniger als 10(0) Personen, die die zugehörigen Beweise vollständig verstehen [1].

Definition und Satz(3.4.2): (Primitive) Pythagoreische Tripel ([1])

- (1) Eine nicht-triviale Lösung $(a, b, c) \in \mathbb{Z}_{\neq 0}^3$ der quadratischen Fermat'schen Gleichung $X^2 + Y^2 = Z^2$ heißt **Pythagoreisches Tripel**.
- (2) Ein Pythagoreisches Tripel $(a, b, c) \in \mathbb{Z}_{\neq 0}^3$ heißt **primitives Pythagoreisches Tripel** genau dann, wenn $\text{ggT}(a, b) = 1$ gilt.

Das Tripel $(a, b, c) \in \mathbb{Z}_{\neq 0}^3$ ist ein Pythagoreisches Tripel genau dann, wenn das Tripel $\left(\frac{a}{\text{ggT}(a, b)}, \frac{b}{\text{ggT}(a, b)}, \frac{c}{\text{ggT}(a, b)} \right) \in \mathbb{Z}_{\neq 0}^3$ ein primitives Pythagoreisches Tripel ist.

Beweis: Siehe Literatur bzw. Tafel. □

Beweis: (Primitive) Pythagoreische Tripel



Beweis: (Primitive) Pythagoreische Tripel ([1])



Satz (3.4.3): Euklids Klassifikationssatz für Primitive Pythagoreische Tripel ([1])

Die folgenden Aussagen (1) und (2) sind äquivalent:

- (1) Das Tripel $(a, b, c) \in \mathbb{Z}_{\neq 0}^3$ ist ein primitives Pythagoreisches Tripel mit (o.B.d.A.) $2|a$.
- (2) Es gibt natürliche Zahlen $m, n \in \mathbb{N}$ mit $m > n$, $\text{ggT}(m, n) = 1$ und $m \not\equiv_2 n$ für die $\pm a = 2 \cdot m \cdot n$, $\pm b = m^2 - n^2$ und $\pm c = m^2 + n^2$ gilt.

Beweis: Siehe Literatur. □

Beispiele:

- $(4, 3, 5)$ ist ein primitives Pythagoreisches Tripel mit $4 = 2 \cdot m \cdot n$, $3 = m^2 - n^2$ und $5 = m^2 + n^2$ für $m := 2$ und $n := 1$.
- $(-12, 5, 13)$ ist ein primitives Pythagoreisches Tripel mit $-(-12) = 2 \cdot m \cdot n$, $5 = m^2 - n^2$ und $13 = m^2 + n^2$ für $m := 3$ und $n := 2$.

Bemerkung:

Alle primitiven Pythagoreischen Tripel können mit Euklids Klassifikationssatz durch rekursives Aufzählen von $m, n \in \mathbb{N}$ konstruiert werden.

Lösungsmenge der quadratischen Fermat'schen Gleichung



Satz (3.4.4): Lösungsmenge der quadratischen Fermat'schen Gleichung ([1])

Die Lösungsmenge $\mathbb{L}_F \subset \mathbb{Z}^3$ der quadratischen Fermat'schen Gleichung $X^2 + Y^2 = Z^2$ ergibt sich (bis auf Vertauschung der ersten und zweiten Tripelkomponenten) zu

$$\mathbb{L}_F = T \cup V$$

wobei definiert wird:

- $T := \{(0, 0, 0)\} \cup \{(a, 0, c) \mid a, c \in \mathbb{Z}, |a| = |c|\} \subset \mathbb{Z}^3$ ist die Menge der trivialen Lösungen der quadratischen Fermat'schen Gleichung,
- $P \subset \mathbb{Z}_{\neq 0}^3$ ist die Menge der primitiven Pythagoreischen Tripel, konstruierbar durch rekursive Anwendung von Euklids Klassifikationssatz und
- $V := \{(a \cdot d, b \cdot d, c \cdot d) \mid d \in \mathbb{N}, (a, b, c) \in P\} \subset \mathbb{Z}_{\neq 0}^3$ ist die Menge aller natürlichezahligen Vielfachen der primitiven Pythagoreischen Tripel.

Beweis: Siehe Literatur. □

Elementare Zahlentheorie

Kapitel 04: Einführung in die Kryptologie

– Version: Wintersemester 2024/2025 –

Dozent: Prof. Dr. Max Krüger

Fakultät Informatik

Technische Hochschule Ingolstadt (THI)

107

Begriffseinordnung: Kryptologie



„Die **Kryptologie** (griechisch κρυπτός kryptós 'versteckt, verborgen, geheim' und -logie) ist eine Wissenschaft, die sich mit der Verschlüsselung und Entschlüsselung von Informationen und somit mit der Informationssicherheit beschäftigt. [...]“¹⁾

Die Kryptologie setzt sich üblicherweise aus zwei Teilgebieten zusammen:

- „**Kryptographie** [...] ist ursprünglich die Wissenschaft der Verschlüsselung von Informationen. Heute befasst sie sich auch allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind.“²⁾
- „Die **Kryptoanalyse** [...] bezeichnet im ursprünglichen Sinne das Studium von Methoden und Techniken, um Informationen aus verschlüsselten Texten zu gewinnen. [...] Heutzutage bezeichnet der Begriff Kryptoanalyse allgemeiner die Analyse von kryptographischen Verfahren [...] mit dem Ziel, diese entweder zu „brechen“ [...] oder ihre Sicherheit nachzuweisen und zu quantifizieren.“³⁾

1) Quelle: <https://de.wikipedia.org/wiki/Kryptologie> (abgerufen am 16.12.2023).

2) Quelle: <https://de.wikipedia.org/wiki/Kryptographie> (abgerufen am 16.12.2023).

3) Quelle: <https://de.wikipedia.org/wiki/Kryptoanalyse> (abgerufen am 16.12.2023).



Kapitel 04: Einführung in die Kryptologie

4.1 Ausgewählte Grundlagen der Kryptologie

- 4.2 Erzeugung von Primzahlen und Primzahltests
- 4.3 Asymmetrische Verfahren: RSA-Kryptosystem
- 4.4 Symmetrische Verfahren
- 4.5 Kryptoanalyse und One-Time-Pad

Grundszenar der Kryptographie





Prinzip von Kerckhoff



Prinzip von Kerckhoff [6]

„Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung der Chiffrierungsregel abhängen, sondern darf nur auf der Geheimhaltung des Schlüssels beruhen.“ [6]

Anmerkungen:

- Das Prinzip von Kerckhoff wurde von dem niederländischen Linguisten und Kryptologen Auguste Kerckhoff (*1835 - †1903) im Jahr 1883 in seinem Werk „*La cryptographie militaire*“ als zweiter von sechs Grundsätze zur Konstruktion eines sicheren Verschlüsselungsverfahrens formuliert.¹⁾
- Schlüssel sind i.d.R. im Vergleich zum Kryptosystem viel kürzer und leichter zu ändern.

1) Quelle: https://de.wikipedia.org/wiki/Kerckhoffs'_Prinzip (abgerufen am 28.12.2023).



Inhaltsverzeichnis Kapitel 04



Kapitel 04: Einführung in die Kryptologie

4.1 Ausgewählte Grundlagen der Kryptologie

4.2 Erzeugung von Primzahlen und Primzahltests

4.3 Asymmetrische Verfahren: RSA-Kryptosystem

4.4 Symmetrische Verfahren

4.5 Kryptoanalyse und One-Time-Pad



Bedarf:

In der Kryptographie (z.B. RSA-Verfahren) werden möglichst große zufällige Primzahlen mit 100-1000+ Dezimalziffern benötigt.

Primzahlerzeugung und deterministische Primzahltests:

Primzahlen können mit Hilfe bestimmt werden mit des

- Probedivision mit allen möglichen Teilern bis zur Wurzel des Kandidaten (vgl. Satz (2.2.1)),
- Sieb des Eratosthenes (vgl. Algorithmus (2.2.2)),
- Satz von Willson (Satz 3.3.3).

Herausforderung:

- Die Erzeugungsansätze in a), b) und c) sind für große Primzahlen extrem ineffizient bzw. nicht mehr durchführbar.
- Lösung: Probabilistische Primzahltests liefern mit (relativ) geringem Aufwand Zahlen, die mit (vorher) festgelegter Wahrscheinlichkeit Primzahlen sind.

Anzahl Primzahlen mit vorgegebener Dezimalstellenanzahl



Proposition (4.2.1): Anzahl Primzahlen mit s Dezimalstellen

Sei $s \in \mathbb{N}$ eine vorgegebene Anzahl von Dezimalstellen, dann gilt:

- Mit höchstens s Dezimalziffern lassen sich maximal die $N_{\max}(s) := 10^s$ Zahlen $z \in \mathbb{N}_{0 \leq 10^s - 1}$ darstellen.
- Für $s \geq 2$ gibt es $N_{\text{exact}}(s) := 9 \cdot 10^{s-1}$ Zahlen $z \in \mathbb{N}$ mit genau s Dezimalstellen in der Darstellung: $10^{s-1} \leq z \leq 10^s - 1$.
- Es gibt $N_{\text{prim}}(s) := \pi(10^s - 1) - \pi(10^{s-1} - 1)$ Primzahlen $p \in \mathbb{P}$ mit genau s Dezimalstellen.

Beweis: Siehe Tafel. □

Bemerkungen:

- Die Proposition überträgt sich analog auf Zahlendarstellungen im Binärsystem.
- Näherungsweise gibt es also $N_{\text{prim}}(s) \approx \frac{(10^s - 1)}{\ln(10^s - 1)} - \frac{(10^{s-1} - 1)}{\ln(10^{s-1} - 1)}$ Primzahlen mit s nach dem Primzahlsatz (2.3.2).

Beweis: Anzahl Primzahlen mit s Dezimalstellen



Beweis: Anzahl Primzahlen mit s Dezimalstellen

Beispiele Primzahlanzahlen mit vorgegebener Stellenanzahl



Mit der Formel $N_{\text{prim}}(s) \approx \frac{(10^s - 1)}{\ln(10^s - 1)} - \frac{(10^{s-1} - 1)}{\ln(10^{s-1} - 1)}$ ergibt sich:

Stellenanzahl $s = \dots$	(Ungefähr) Anzahl $N_{\text{prim}}(s) \approx \dots$ Primzahlen mit s Dezimalstellen	(Ungefährer) Anteil $\frac{N_{\text{prim}}(s)}{9 \cdot 10^{s-1}} \approx \dots$ an Primzahlen mit s Dezimalstellen
25	$1.556221893486653 \cdot 10^{23}$	1.729 %
50	$7.799574368874728 \cdot 10^{47}$	0.867 %
100	$3.904263524180749 \cdot 10^{97}$	0.434 %
150	$2.603823739375201 \cdot 10^{147}$	0.289 %
200	$1.953233976399048 \cdot 10^{197}$	0.217 %
250	$1.562762473033388 \cdot 10^{247}$	0.174 %
300	$1.302399282407745 \cdot 10^{297}$	0.145 %



Aufgabe:

Sei $D_{25} \subset \mathbb{N}_0$ die Menge aller natürlichen Zahlen, die mit höchstens 25 Dezimalziffern dargestellt werden können.

- Bestimmen Sie näherungsweise die Anzahl und den Anteil aller Primzahlen in D_{25} .
- Bestimmen Sie näherungsweise die Anzahl und den Anteil aller Primzahlen mit genau 25 Dezimalziffern in ihrer Darstellung.

Aufgabe:

Sei $B_s \subset \mathbb{N}_0$ die Menge aller natürlichen Zahlen, die sich mit höchstens $s \in \mathbb{N}$ Binärziffern als Binärzahl darstellen lassen.

- Welche und wie viele Zahlen (dezimal angegeben) enthält die Menge B_s ?
- Wie viele Binärzahlen mit exakt s Binärziffern gibt es in B_s für ein gegebenes $s \geq 2$?
- Schätzen Sie die Anzahl von Primzahlen die exakt s Binärziffern für ihre Darstellung benötigen.

Hinweis: Nutzen Sie ein zu den Dezimalzahlen analoges Vorgehen.

Kleiner Satz von Fermat – vereinfachte Version



Lemma (4.2.2): Kleiner Satz von Fermat – vereinfachte Version ([6])

Sei eine Primzahl $p \in \mathbb{P}$ und $a \in \mathbb{N}$ mit $1 < a < p$ gegeben, dann gilt $a^{p-1} \equiv_p 1$.

Beweis: Siehe Satz (3.3.2). □

Beispiel:

- für die Primzahl $p = 7$ gilt:

$$2^6 \equiv_7 1, 3^6 \equiv_7 1, 4^6 \equiv_7 1, 5^6 \equiv_7 1, 6^6 \equiv_7 1,$$

aber

- für die zusammengesetzte Zahl $p = 9$ gilt:

$$2^8 \equiv_9 4, 3^8 \equiv_9 0, 4^8 \equiv_9 7, 5^8 \equiv_9 7, 6^8 \equiv_9 0, 7^8 \equiv_9 4, 8^8 \equiv_9 1.$$

Bemerkung:

Das Lemma vereinfacht im Wesentlichen nur die Voraussetzungen des kleinen Satzes von Fermat (in der alternativen Version).



Definition (4.2.3): Fermatsche Pseudoprimzahlen ([6])

Sei $n \in \mathbb{N}$ eine ungerade zusammengesetzte Zahl und $a \in \{2, 3, \dots, n-1\} \subset \mathbb{N}$, dann heißt n **eine Fermatsche Pseudoprimzahl zur Basis a** , falls $a^{n-1} \equiv_n 1$ gilt.

□

Beispiele:

- $n = 91 = 7 \cdot 13$ ist eine Pseudoprimzahl zur Basis $a = 3$, da $3^{90} \equiv_{91} 1$.
- $n = 91 = 7 \cdot 13$ ist keine Pseudoprimzahl zur Basis $a = 2$, da $2^{90} \equiv_{91} 64$.
- $n = 9 = 3 \cdot 3$ ist eine Pseudoprimzahl zur Basis $a = 8$, da $8^8 \equiv_9 1$.
- $n = 9 = 3 \cdot 3$ ist keine Pseudoprimzahl zur Basis $a = 2, \dots, 7$, da $a^8 \not\equiv_9 1$.

Eigenschaften von Pseudoprimzahlen



Satz (4.2.4): Eigenschaften von Pseudoprimzahlen ([6])

Sei $n \in \mathbb{N}$ eine ungerade zusammengesetzte Zahl, dann gilt entweder

- (1) n ist Fermatische Pseudoprimzahl für alle Basen $a \in \mathbb{N}_{2 \leq n-1}$ oder
- (2) n ist keine Fermatische Pseudoprimzahl für mindestens die Hälfte aller Basen $a \in \mathbb{N}_{2 \leq n-1}$.

Beweis: Siehe Literatur.

□

Beispiel:

Die Zahl $n = 9 = 3 \cdot 3$ ist keine Fermatische Pseudoprimzahl für die Basen $a = 2, 3, 4, 5, 6, 7$ und eine Fermatische Pseudoprimzahl für die Basis $a = 8$.

Definition (4.2.5): Carmichael-Zahlen ([6])

Eine ungerade zusammengesetzte Zahl $n \in \mathbb{N}$, die Fermatsche Pseudoprimzahl für alle Basen $a \in \mathbb{N}_{2 \leq n-1}$ ist, heißt **Carmichael-Zahl** n . \square

Beispiele:

- $n = 561 = 3 \cdot 11 \cdot 17$ ist die kleinste Carmichael-Zahl.
- $n = 1105 = 5 \cdot 13 \cdot 17$ ist die zweitkleinste Carmichael-Zahl.
- $n = 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 46657, 52633$ sind Carmichael-Zahlen zusammengesetzt aus drei verschiedenen Primfaktoren.

Bemerkungen:

- Es gibt nur sehr wenige Carmichael-Zahlen im Verhältnis zu den ungeraden zusammengesetzten Zahlen, aber dennoch sind es unendlich viele.
- Nur 16 Carmichael-Zahlen sind kleiner als 100 000.

Carmichael-Zahlen als Produkt von verschiedenen Primfaktoren


Satz (4.2.6): Carmichael-Zahlen als Produkt von verschiedenen Primfaktoren ([6])

Eine Carmichael-Zahl ist immer das Produkt von mindestens drei verschiedenen Primfaktoren und enthält keinen Primfaktor doppelt.

Beweis: Siehe Literatur. \square

Beispiele:

- $n = 41041 = 7 \cdot 11 \cdot 13 \cdot 41$ ist die kleinste Carmichael-Zahl mit 4 Primfaktoren.
- $n = 62745 = 3 \cdot 5 \cdot 47 \cdot 89$ ist Carmichael-Zahl.
- $n = 63973 = 7 \cdot 13 \cdot 19 \cdot 37$ ist Carmichael-Zahl.
- $n = 75361 = 11 \cdot 13 \cdot 17 \cdot 31$ ist Carmichael-Zahl.

Bemerkung:

Die obigen Beispiele umfassen alle Carmichael-Zahlen die aus vier (oder mehr) Primfaktoren bestehen und kleiner als 100 000 sind.



Satz (4.2.7): Hinreichende Bedingung für Carmichael-Zahlen (Methode von Chernick)¹⁾

Sind für ein $n \in \mathbb{N}$ die Zahlen $6 \cdot m + 1, 12 \cdot m + 1, 18 \cdot m + 1$ Primzahlen, so ist ihr Produkt $(6 \cdot m + 1) \cdot (12 \cdot m + 1) \cdot (18 \cdot m + 1)$ eine Carmichael-Zahl.

Beweis: Siehe Literatur. □

Beispiele:

$n = 1729 = 7 \cdot 13 \cdot 19$ ist Carmichael-Zahl nach der Methode von Chernick mit dem Parameterwert $m = 1$.

Bemerkung:

- Die obigen Beispiele umfassen alle Carmichael-Zahlen die aus vier (oder mehr) Primfaktoren bestehen und kleiner als 100 000 sind.
- Im Jahr 2012 wurde eine Carmichael-Zahl mit mehr als 10 Miliarden Primfaktoren und mehr als 300 Miliarden Dezimalstellen vorgestellt.²⁾

1) Chernick, Jack: „On Fermat's simple theorem“. Bulletin of the American Mathematical Society, 45(4), pp.269-274, 1939.

2) Hayman, Steven und Shallue, Andrew: „Constructing a ten billion factor Carmichael number“. Posterpräsentation auf der ANTS X-Konferenz 2012 in San Diego, San Diego, Juli 2012 (<https://mathweb.ucsd.edu/~kedlaya/ants10/poster-hayman.pdf>, abgerufen am 17.12.2023)

Fermatscher Primzahltest



Algorithmus (4.2.8): Fermatscher Primzahltest ([7])

Input: Ungerade Zahl $n \in \mathbb{N}$ (Primzahlkandidat) mit maximaler Rundenzahl $K \in \mathbb{N}$.

Output: Entscheidung zwischen <COMPOSITE> oder <PROBABLY_PRIME>.

Algorithm:

Procedure FermatPrimalityTest (n, K):

1. Schritt: Initialisiere den Rundenzähler $k := 1$.
2. Schritt: Wähle zufällig eine Test-Basiszahl $a \in \mathbb{N}_{2 \leq n-1} = \{2, 3, \dots, n - 1\}$ gemäß der diskreten Gleichverteilung $U(n - 2)$.
3. Schritt: Falls $a^{n-1} \not\equiv_n 1$ return <COMPOSITE> und STOP.
4. Schritt: Falls $k < K$ setze $k := k + 1$ und weiter mit 2. Schritt.
5. Schritt: Return <PROBABLY_PRIME>.

End Procedure. □



Anmerkungen:

- Der Fermatsche Primzahltest ist ein probabilistischer Primzahltest. Das Ergebnis **<COMPOSITE>** ist in jedem Fall zutreffend, während das Ergebnis **<PROBABLY_PRIME>** nur bis auf eine Irrtumswahrscheinlichkeit richtig ist, sofern es nicht für (die seltenen) Carmichael-Zahlen immer falsch ist.
- Der Fermatsche Primzahltest nutzt im Wesentlichen nur die Potenzbildung modulo $n \in \mathbb{N}$, die aufgrund von Satz (3.1.2(2)) effizient für $a < n$ rekursiv durchgeführt werden kann: $a^n \bmod n = ((a^{n-1} \bmod n) \cdot a) \bmod n$.

Eigenschaften des Fermatschen Primzahltests



Satz (4.2.9): Eigenschaften des Fermatschen Primzahltests ([6], [7])

Seien die ungerade Zahl $n \in \mathbb{N}$ und die maximale Rundenzahl $K \in \mathbb{N}$ der Input für den Fermatschen Primzahltest gemäß Algorithmus (4.2.8), dann gelten (1) und (2):

- (1) Liefert der Algorithmus (4.2.8) den Output **<COMPOSITE>**, so gilt $n \notin \mathbb{P}$, d.h. n ist mit Sicherheit keine Primzahl.
- (2) Liefert der Algorithmus (4.2.8) den Output **<PROBABLY_PRIME>**, so ist n entweder eine (selten auftretende) Carmichael-Zahl oder es gilt $P(n \in \mathbb{P}) \geq 1 - \frac{1}{2^K}$, d.h. n ist mit Wahrscheinlichkeit von mindestens $1 - \frac{1}{2^K}$ eine Primzahl, sofern n keine Carmichael-Zahl ist.

Beweis: Siehe Literatur oder Tafel. □



Beweis:

Verschärfung des Kleinen Satzes von Fermat



Satz (4.2.10): Verschärfung des Kleinen Satzes von Fermat ([8])

Sei die Primzahl $p \in \mathbb{P}$ und die Zahl $a \in \{2, 3, \dots, p-1\} \subset \mathbb{N}$ gegeben und sei der maximale Exponent $s := \max \left\{ r \in \mathbb{N}_0 \mid 2^r \mid (p-1) \right\}$ mit $d := \frac{p-1}{2^s}$ definiert, dessen Zweierpotenz 2^s die Zahl $p-1$ teilt. Dann gilt entweder (1) oder (2):

$$(1) \quad a^d \equiv_p 1$$

oder

$$(2) \quad \text{es gibt einen Zweierpotenzexponenten } r \in \{0, 1, \dots, s-1\} \subset \mathbb{N}_0 \text{ mit } a^{2^r \cdot d} \equiv_p -1, \\ \text{d.h. } \exists r \in \mathbb{N}_0 \leq s-1 : a^{2^r \cdot d} \equiv_p p-1,$$

Beweis: Siehe Literatur oder Tafel. □



Beispiele: Verschärfung des Kleinen Satzes von Fermat



Beispiele:

- 1) Für die Primzahl $n = 563 = 2^1 \cdot 281 + 1$ und die Basis $a = 13$ gilt
 $13^{281} \equiv_{563} 1$ und $13^{2 \cdot 281} \equiv_{563} 1$.
- 2) Für die Carmichael-Zahl $n = 561 = 2^4 \cdot 75 + 1$ und die Basis $a = 13$ gilt
 $13^{75} \equiv_{561} 208$, $13^{1 \cdot 75} \equiv_{561} 67$, $13^{2 \cdot 75} \equiv_{561} 1$ und $13^{3 \cdot 75} \equiv_{561} 1$.
- 3) Für die Primzahl $n = 557 = 2^2 \cdot 139 + 1$ und die Basis $a = 18$ gilt
 $18^{139} \equiv_{557} 439$ und $18^{2 \cdot 139} \equiv_{557} 556 (= -1)$.



Definition (4.2.11): Starke Pseudoprimzahlen ([6])

Sei $n \in \mathbb{N}$ eine ungerade zusammengesetzte Zahl und $a \in \{2, 3, \dots, n-1\} \subset \mathbb{N}$ und seien $s := \max \left\{ r \in \mathbb{N}_0 \mid 2^r \mid (n-1) \right\}$ und $d := \frac{n-1}{2^s}$ definiert, dann heißt die Zahl n **eine Starke Pseudoprimzahl zur Basis a** , falls entweder (1) oder (2) gilt:

$$(1) \quad a^d \equiv_n 1$$

oder

$$(2) \quad \text{es gibt einen Zweierpotenzexponenten } r \in \{0, 1, \dots, s-1\} \subset \mathbb{N}_0 \text{ mit } a^{2^r \cdot d} \equiv_n -1, \\ \text{d.h. } \exists r \in \mathbb{N}_{0 \leq s-1} : a^{2^r \cdot d} \equiv_n n-1.$$

□

Bemerkungen:

- Eine starke Pseudoprimzahl zur Basis a ist immer auch eine Fermatsche Pseudoprimzahl zur Basis a (gem. Def. (4.2.3)). (Warum? Aufgabe: Beweis!)
- Zur Basis 2 gibt es 14884 Fermatsche Pseudoprimzahlen kleiner als 10^{10} aber nur 3291 starke Pseudoprimzahlen.

Eigenschaften von Starken Pseudoprimzahlen



Satz (4.2.12): Eigenschaften von Starken Pseudoprimzahlen ([6], [7], [8])

Sei $n \in \mathbb{N}$ eine ungerade zusammengesetzte Zahl, dann gilt:

- (1) Es gibt mindestens eine Basis $a \in \{2, 3, \dots, n-1\} \subset \mathbb{N}$ zu der die Zahl n keine starke Pseudoprimzahl ist.
- (2) Für höchstens $\frac{1}{4}$ aller Basen aus $a \in \{2, 3, \dots, n-1\} \subset \mathbb{N}$ ist die Zahl n eine starke Pseudoprimzahl.

Beweis: Siehe Literatur.

□

Bemerkungen:

- Es gibt also kein Pendant zu Carmichael-Zahlen, wenn man starke Pseudoprimzahlen anstelle von Carmichael-Zahlen zugrunde legt.
- Meist ist die Anzahl der Basen mit starken Pseudoprimzahlen deutlich geringer als $\frac{1}{4}$.



Algorithmus (4.2.13): Rabin-Miller Primzahltest – Single Round ([7], [8])

Input: Ungerade Zahl $n \in \mathbb{N}$ (Primzahlkandidat).

Output: <COMPOSITE> oder <PROBABLY_PRIME>.

Algorithm:

Procedure RabinMillerPrimalityTestSingleRound (n):

1. Schritt: Berechne $s := \max \left\{ r \in \mathbb{N}_0 \mid 2^r | (n - 1) \right\}$ und $d := \frac{n - 1}{2^s}$.
2. Schritt: Wähle zufällig eine Test-Basiszahl $a \in \mathbb{N}_{2 \leq n-1} = \{2, 3, \dots, n - 1\}$ gemäß der diskreten Gleichverteilung $U(n - 2)$.
3. Schritt: Falls $a^d \equiv_n 1$ return < PROBABLY_PRIME > und STOP.
4. Schritt: Setze $r := 0$.
5. Schritt: Falls $a^{2^r \cdot d} \equiv_n n - 1$ return < PROBABLY_PRIME > und STOP.
6. Schritt: Falls $r < s - 1$ erhöhe $r := r + 1$ und weiter mit 5. Schritt.
7. Schritt: Return < COMPOSITE >.

End Procedure.



Algorithmus (4.2.14): Rabin-Miller Primzahltest – Multiple Round ([7])

Input: Ungerade Zahl $n \in \mathbb{N}$ (Primzahlkandidat) mit maximaler Rundenzahl $K \in \mathbb{N}$.

Output: <COMPOSITE> oder <PROBABLY_PRIME>.

Algorithm:

Procedure RabinMillerPrimalityTest(n, K):

1. Schritt: Initialisiere den Rundenzähler $k := 1$.
2. Schritt: Falls (RabinMillerPrimalityTestSingleRound (n) == <COMPOSITE>) return <COMPOSITE> und STOP.
3. Schritt: Falls $k < K$ setze $k := k + 1$ und weiter mit 2. Schritt.
4. Schritt: Return <PROBABLY_PRIME>.

End Procedure.





Satz (4.2.15): Eigenschaften des Rabin-Miller Primzahltest ([6], [7])

Seien die ungerade Zahl $n \in \mathbb{N}$ und die maximale Rundenzahl $K \in \mathbb{N}$ der Input für den Rabin-Miller-Primzahltest gemäß Algorithmus (4.2.14), dann gelten (1) und (2):

- (1) Liefert der Algorithmus (4.2.14) den Output <COMPOSITE>, so gilt $n \notin \mathbb{P}$, d.h. n ist mit Sicherheit keine Primzahl.
- (2) Liefert der Algorithmus (4.2.14) den Output <PROBABLY_PRIME>, so ist die Zahl n mit Wahrscheinlichkeit von mindestens $1 - \frac{1}{4^K}$ eine Primzahl, d.h. es gilt:
$$P(n \in \mathbb{P}) \geq 1 - \frac{1}{4^K}$$

Beweis: Siehe Literatur oder Tafel. □

Beweis: Eigenschaften des Rabin-Miller Primzahltests





Anmerkungen:

- Der Rabin-Miller Primzahltest ist (wie der Fermatsche Primzahltest) ein probabilistischer Primzahltest. Das Ergebnis <COMPOSITE> ist in jedem Fall zutreffend, während das Ergebnis <PROBABLY_PRIME> nur bis auf eine Irrtumswahrscheinlichkeit richtig ist.
- Für die seltene Ausnahme der Carmichael-Zahlen beim Fermatschen Primzahltest gibt es beim Rabin-Miller Primzahltest keine Entsprechung.
- Wie der Fermatsche Primzahltest nutzt der Rabin-Miller Primzahltest im Wesentlichen nur die Potenzbildung modulo $n \in \mathbb{N}$, die für $a < n$ aufgrund von Satz (3.1.2(2)) effizient rekursiv auch für große Zahlen durchgeführt werden kann:

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

Aufgaben: Primzahltests und Primzahlerzeugung



Aufgabe:

Finden Sie für die Carmichael-Zahlen $n = 1729, 2465, 2821, 6601, 8911$ Basen, bei deren Wahl der Rabin-Miller Primzahltest die Zahlen als zusammengestetzt erkennen würde. Als was hätte der Fermat Primzahltest diese Zahlen klassifiziert?

Aufgabe:

Geben Sie ein Verfahren zur Erzeugung einer

- ungeraden Zahl und einer
 - Primzahl (bei verbleibender Restunsicherheit von 10^{-10} hinsichtlich der Primalität)
- in Binärdarstellung an, die jeweils genau $s \in \mathbb{N}$ Binärziffern für ihre Darstellung benötigen.



Inhaltsverzeichnis Kapitel 04



Kapitel 04: Einführung in die Kryptologie

- 4.1 Ausgewählte Grundlagen der Kryptologie
- 4.2 Erzeugung von Primzahlen und Primzahltests
- 4.3 Asymmetrische Verfahren: RSA-Kryptosystem
- 4.4 Symmetrische Verfahren
- 4.5 Kryptoanalyse und One-Time-Pad



„[Bei einem] **Asymmetrisches Kryptosystem** [...] handelt sich um ein kryptographisches Verfahren, bei dem [...] die kommunizierenden Parteien keinen gemeinsamen geheimen Schlüssel benötigen. Jeder Benutzer erzeugt sein eigenes Schlüsselpaar, das aus einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher Schlüssel) besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Besitzer des privaten Schlüssels zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Der private Schlüssel ermöglicht es seinem Besitzer, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren.“¹⁾

Anmerkungen:

- Asymmetrische Kryptosysteme reduzieren/lösen das Schlüsselverteilungsproblem.¹⁾
- Asymmetrische Kryptosysteme basieren auf sogenannten Einwegfunktionen deren Werte im Gegensatz zu ihren Umkehrfunktionswerten leicht zu berechnen sind.²⁾

1) Quelle: https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem (abgerufen am 28.12.2023)

2) Quelle: <https://de.wikipedia.org/wiki/Einwegfunktion> (abgerufen am 28.12.2023)

Einwegfunktionen



Definition (4.3.1): Einwegfunktionen ([8])

Eine bijektive Funktion $f: D \rightarrow W$ mit $f: x \mapsto f(x)$ heißt eine **Einwegfunktion**, wenn ihre Funktionswerte mit wenig Aufwand (d.h. insbesondere mit polynomialer Laufzeit) berechnet werden können aber die Werte ihrer Umkehrfunktion $f^{-1}: W \rightarrow D$ praktisch nur mit extrem viel Aufwand oder gar nicht berechenbar sind. □

Anmerkungen: [8]

- Für eine Einwegfunktion $f: D \rightarrow W$ lässt sich i. A. praktisch kein Argument $x \in D$ mit $f(x) = y$ zu einem vorgegebenen $y \in W$ bestimmen.
- Es ist nicht bekannt, ob Einwegfunktionen überhaupt existieren. Es gibt aber Funktionen, die sich – nach derzeitigem Wissenstand – wie Einwegfunktionen verhalten.

Beispiele: [8]

- Multiplikation von Primzahlen (mit der Faktorisierung von Primzahlprodukten)
- Potenzen in endlichen Gruppen (mit der Berechnung von diskreten Logarithmen).

Definition und Algorithmus (4.3.2): RSA – Schlüsselerzeugung ([8])

Erzeugung des öffentlichen und des privaten Schlüssels eines RSA-Kryptosystems:

1. Schritt: Man wähle zwei große Primzahlen $p, q \in \mathbb{P}$, $p \neq q$ und berechne den RSA-Modul $n := p \cdot q$.

2. Schritt: Man bestimme eine zu $(p - 1) \cdot (q - 1)$ teilerfremde ungerade Zahl $e \in \mathbb{N}_{3 \leq (p-1) \cdot (q-1)-1}$ mit $\text{ggT}(e, (p - 1) \cdot (q - 1)) = 1$.

3. Schritt: Man berechne die Zahl $d \in \mathbb{N}_{0 \leq (p-1) \cdot (q-1)-1}$ mit $e \cdot d \equiv_{(p-1) \cdot (q-1)} 1$:

Der erweiterte Euklidische Algorithmus liefert $s, t \in \mathbb{Z}$ als Lösung von

$s \cdot e + t \cdot (p - 1) \cdot (q - 1) = 1$, da $\text{ggT}(e, (p - 1) \cdot (q - 1)) = 1$ gilt.

Das multiplikativ Inverse von e modulo $(p - 1) \cdot (q - 1)$ erhält man dann als $d := s \bmod (p - 1) \cdot (q - 1)$.

Das Paar (n, e) heißt der **öffentliche Schlüssel** und das Paar (n, d) heißt der **private Schlüssel des RSA-Kryptosystems**.

□

Aufgabe: RSA – Schlüsselerzeugung



Aufgabe: [8]

Bestimmen Sie den öffentlichen und den privaten Schlüssel des RSA-Kryptosystems, dass auf den Primzahlen $p = 11$ und $q = 23$ basiert und das das kleinstmögliche e als öffentlichen (Teil-)Schlüssel verwendet.

(Lösung zur Kontrolle: öffentlich: $(n, e) = (253, 3)$; privat $(n, e) = (253, 147)$)



Anmerkungen: (gem.[8])

- Die Zahlen $p, q, (p - 1) \cdot (q - 1)$ müssen geheim bleiben werden aber nach der Schlüsselerzeugung nicht mehr benötigt.
- Zur Vermeidung bestimmter Angriffsschemata muss $2^{16} < e < 2^{64}$ gewählt werden.¹⁾
- Die $p, q \in \mathbb{P}$ sollten $\frac{k}{2}$ -Bit-Primzahlen sein, wobei folgende Mindestgrößen k für den RSA-Modul gelten sollten:²⁾

Schutz bis in(s) ...	Empfohlene ²⁾ Mindestgröße in [Bit]
Jahr 2015	$k=1248$
Jahr 2020	$k=1176$
Jahr 2030	$k=2432$
Jahr 2040	$k=3248$
absehbare Zukunft	$k=15424$

1) Quelle: <https://de.wikipedia.org/wiki/RSA-Kryptosystem> (abgerufen am 28.12.2023).

2) Yearly report on algorithms and keysizes, ICT-2007-216676 ECRYPT II, 2012 (übernommen aus [8])

RSA – Verschlüsselung und Entschlüsselung



Definition und Satz (4.3.3): RSA – Verschlüsselung und Entschlüsselung ([6], [8])

Seien (n, e) der öffentliche und (n, d) der private Schlüssel eines RSA-Kryptosystems, dann gilt:

- (1) **Verschlüsselung:** Der Chiffretext $c \in \mathbb{N}_{0 \leq n-1}$ berechnet sich aus dem Klartext $m \in \mathbb{N}_{0 \leq n-1}$ mittels $c := \text{Enc}(m) := m^e \bmod n$.
- (2) **Entschlüsselung:** Der Klartext $m \in \mathbb{N}_{0 \leq n-1}$ berechnet sich aus dem Chiffretext $c \in \mathbb{N}_{0 \leq n-1}$ mittels $m := \text{Dec}(c) := c^d \bmod n$.

Für die Komposition gilt $\text{Dec} \circ \text{Enc}(m) = (m^e \bmod n)^d \equiv_n m$ für alle $m \in \mathbb{N}_{0 \leq n-1}$.

Beweis: Siehe Literatur oder Tafel. □



Beweis:

Aufgabe: RSA – Verschlüsselung und Entschlüsselung



Aufgabe: [8]

Gegeben ist das RSA-Kryptosystem mit dem öffentlichen Schlüssel $(n, e) = (253, 3)$ und dem privaten Schlüssel $(n, d) = (253, 147)$.

1. Verschlüsseln Sie die folgenden Botschaften:
 - a) $m_1 = 11$
 - b) $m_2 = 111$
 - c) $m_3 = 231$
2. Entschlüsseln Sie die Chiffretexte a), b) und c) aus Aufgabe 1.



Anmerkungen: (gem.[8])

- Das RSA-Verfahren von Rivest, Shamir und Adleman ist das erste veröffentlichte asymmetrische Verschlüsselungsverfahren aus dem Jahr 1977.¹⁾
- Die Sicherheit des RSA-Kryptosystems beruht auf der Annahme (!), dass das RSA-Modul $n := p \cdot q$ sich nicht effizient in seine Primfaktoren $p, q \in \mathbb{P}$ zerlegen lässt.
- Es ist nicht auszuschließen, dass Fortschritte in der Mathematik zukünftig erhebliche Beschleunigungen in Primfaktorzerlegungen ermöglichen.
- Fortschritte im Bau realer Quantencomputer gefährden die Sicherheit des RSA-Verfahrens. Mit dem Shor-Algorithmus¹⁾ ist ein Algorithmus bekannt, der auf Quantencomputern effizient durchführbar ist.
- Die Post-Quanten-Kryptographie beschäftigt sich mit Verfahren die auch bei Verwendung von Quanten-Computern praktisch nicht entschlüsselbar sein sollen.²⁾

1) Quelle: <https://de.wikipedia.org/wiki/RSA-Kryptosystem> (abgerufen am 28.12.2023).

2) Quelle: <https://de.wikipedia.org/wiki/Post-Quanten-Kryptographie> (abgerufen am 28.12.2023).





Kapitel 04: Einführung in die Kryptologie

- 4.1 Ausgewählte Grundlagen der Kryptologie
- 4.2 Erzeugung von Primzahlen und Primzahltests
- 4.3 Asymmetrische Verfahren: RSA-Kryptosystem
- 4.4 Symmetrische Verfahren**
- 4.5 Kryptoanalyse und One-Time-Pad



Prinzipien

Anwendungsszenarien

Vor- und Nachteile

Beispiel-Vervahren



Kapitel 04: Einführung in die Kryptologie

- 4.1 Ausgewählte Grundlagen der Kryptologie
- 4.2 Erzeugung von Primzahlen und Primzahltests
- 4.3 Asymmetrische Verfahren: RSA-Kryptosystem
- 4.4 Symmetrische Verfahren
- 4.5 Kryptoanalyse und One-Time-Pad



Prinzipien

Anwendungsszenarien der Kryptoanalyse

Einfache Beispiele

Beispiel-Verfahren

Absolute Sicherheit

One-Time-Pad

Eigenschaften und Fehler in der Anwendung

One-Time-Pad kombiniert mit Quantenübertragung

Kryptoanalyse:

-> Problemstellung und Anwendungsszenarien

-> Grundsätzliche Herangehensweise

- [1] Hartlieb, Silke und Unger, Luise: *Elementare Zahlentheorie mit Maple* (Sommersemester 2022). FernUniversität in Hagen: Kurstext zur Vorlesung im Modul 01202, 2022.
- [2] Haager, Wilhem: *Computeralgebra mit Maxima – Grundlagen der Anwendung und Programmierung* (2. aktualisierte Auflage). München: Carl Hanser Verlag, 2019. (ISBN-13: 978-3-446-44868-1)
- [3] Wittmann, Gerald: *Grundbegriffe der elementaren Zahlentheorie – Von der Teilerrelation zur Kongruenz modulo m*. Wiesbaden: Springer Spektrum, 2020. (ISBN-13: 978-3-658-31756-0)
- [4] Stroth, Gernot: *Elementare Algebra und Zahlentheorie* (2. Auflage). Wiesbaden: Springer Spektrum, 2020. (ISBN-13: 978-3-658-31756-0)
- [5] Ziegenbalg, Jochen: *Elementare Zahlentheorie – Beispiele, Geschichte, Algorithmen* (2. Auflage). Wiesbaden: Springer Spektrum, 2015. (ISBN-13: 978-3-658-07171-4)
- [6] Hartlieb, Silke und Unger, Luise: *Mathematische Grundlagen der Kryptographie* (Wintersemester 2022/2024). FernUniversität in Hagen: Kurstext zur Vorlesung im Modul 01149, 2023.
- [7] Harchol-Balter, Mor: *Introduction to Probability for Computing*. Cambridge (UK): Cambridge University Press, 2023.
- [8] Buchmann, Johannes: *Einführung in die Kryptographie* (6. Auflage). Wiesbaden: Springer Spektrum, 2016. (ISBN-13: 978-3-642-39775-2)