

# Einführung in die Zahlentheorie 1

Prof. Dr. Josef F. Bürgler

Studiengang Informatik  
Hochschule Luzern, Informatik

I.BA\_DMATH

## Die StudentIn

- versteht die Division mit Rest und kann diese anwenden
- versteht den (erweiterten) Euklidischen Algorithmus und kann diesen effizient anwenden um Diophantische Gleichungen zu lösen oder das modulare (multiplikative) Inverse zu berechnen.
- versteht den chinesischen Restesatz und kann diesen in der Praxis anwenden.
- versteht die Eulersche  $\phi$ -Funktion und kann diese im Alltag anwenden.
- versteht was Primzahlen sind, kennt deren Verteilung und versteht die speziellen Mersenne-Primzahlen.
- kennt den kleinen Satz von Fermat, den Satz von Euler und den Satz von Wilson im Zusammenhang mit Primzahlen.

- 1 Division mit Rest (Se)
- 2 Kongruenz modulo  $n$  (Se)
- 3 Der Euklidsche Algorithmus (Se)
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

## Satz

Für beliebige  $a, n \in \mathbb{Z}$  mit  $n \neq 0$  existieren eindeutig bestimmte Zahlen  $q \in \mathbb{Z}$  (genannt Quotient) und  $r \in \mathbb{Z}$  (genannt Rest) mit

$$a = q \cdot n + r \quad \text{und} \quad 0 \leq r < |n|$$

Man nennt  $a$  den **Dividend** und  $n$  den **Divisor**. Oft schreibt man auch  $r = R_n(a) = a \bmod n$  (Rest von  $a$  bei Division durch  $n$ ).

## Example

Berechnen Sie  $R_5(13)$ ,  $R_5(-13)$  und  $R_{-5}(13)$ .

Lösung:  $R_5(13) = 13 \bmod 5 = 3$  : Rest wenn man 13 durch 5 teilt.

**Beachte:** der Rest ist immer größer gleich Null und kleiner als  $n$ .

$$R_5(-13) = -13 \bmod 5 = 2 ; \quad R_{-5}(13) = 3 \text{ denn } 13 = (-2)(-5) + 3 .$$

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

# Kongruenz modulo $n$

## Definition

Seien  $a, b \in \mathbb{Z}$  und  $n \in \mathbb{Z}^+$ . Dann ist  $a$  **kongruent zu  $b$  modulo  $n$** , falls  $n$  ein Teiler von  $a - b$  ist, kurz:  $n|(a - b)$ . Wir schreiben dann kurz:

$$a \equiv b \pmod{n}$$

## Satz

$$\begin{aligned} a \equiv b \pmod{n} &\iff n|(a - b) \\ &\iff \exists q : a - b = q \cdot n \\ &\iff \exists q : a = b + q \cdot n \end{aligned}$$

Der Abstand von  $a$  und  $b$  ist ein Vielfaches von  $n$ .



# Kongruenz modulo $n$ (Fort.)

Achtung:

Unterscheiden Sie stets zwischen den Aussagen

- $a \equiv b \pmod{n}$  oder  $b \equiv a \pmod{n}$  (die Differenz aus  $a$  und  $b$  ist durch  $n$  teilbar) und
- $r = a \text{ mod } n$  ( $r$  ist der eindeutig bestimmte Rest bei Division von  $a$  durch  $n$ )

Beachten Sie, dass  $0 \leq r \leq |n|$ !

## Example

Zeigen Sie, dass  $R_{13}(5) = R_{13}(18) = R_{13}(31) = R_{13}(-8)$  gilt.

Lösung:  $R_{13}(5) = 5 ; R_{13}(18) = 5 ; R_{13}(31) = 5$

denn  $5 = 0 \cdot 13 + 5 ; 18 = 1 \cdot 13 + 5 ; 31 = 2 \cdot 13 + 5$

und schliesslich:  $R_{13}(-8) = 5$

denn  $-8 = (-1) \cdot 13 + 5$

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 **Der Euklidische Algorithmus**
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

## Definition

Seien  $a, b \in \mathbb{Z}$  (nicht beide gleich 0). Der **grösste gemeinsame Teiler**  $\text{ggT}(a, b)$  ist die grösste ganze Zahl, die sowohl  $a$  als auch  $b$  teilt.

## Eigenschaften von $\text{ggT}(a, b)$

- $\text{ggT}(a, 0) = |a|$
- $\forall a, b \in \mathbb{Z} (\text{ ggT}(a, b) = \text{ggT}(\pm a, \pm b) )$
- $\text{ggT}(a, b) = \text{ggT}(a + k \cdot b, b)$
- $\text{ggT}(a, b) = \text{ggT}(b, R_b(a))$  (**Euklid'sche ggT-Relation**)

*Rest von a, wenn man durch b teilt.*

Insbesondere die letzte Eigenschaft liefert uns ein effizientes Verfahren zur Bestimmung des grössten gemeinsamen Teilers von zwei natürlichen Zahlen.

# Der Euklidsche Algorithmus (ein Beispiel)

Berechnen Sie mit Hilfe des Euklid'schen Algorithmus den grössten gemeinsamen Teiler der Zahlen 963 und 218.

$$963 = \dots \cdot 218 + \text{ggT}(963, 218) = \text{ggT}(218, \dots)$$

$$218 =$$

*Rest von 963, wenn man durch 218 teilt*

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

# Lösung linearer Diophantischer Gleichungen

## Satz (Bezout)

Für  $n, n_1, n_2 \in \mathbb{Z}$  hat die lineare Diophantische Gleichung

$$n_1 \cdot x + n_2 \cdot y = n$$

z.B.

$$\begin{aligned} 3x + 4y &= 7 \\ \text{ggT}(3,4) &\stackrel{?}{=} 1, \quad 1 \mid 7 \\ \text{LÖS. } x=1, y=1 \end{aligned}$$

genau dann ganzzahlige Lösungen  $x, y \in \mathbb{Z}$ , falls  $\text{ggT}(n_1, n_2) | n$ , d.h. falls  $\text{ggT}(n_1, n_2)$  ein Teiler von  $n$  ist.

Wir werden uns auf den Fall  $n = 1$  einschränken, also nach ganzzahligen Lösungen von linearen Diophantischen Gleichungen  $n_1 \cdot x + n_2 \cdot y = 1$  suchen. Nach dem Satz von Bezout existieren solche Lösungen, wenn  $\text{ggT}(n_1, n_2) | 1$  ist, d.h.  $\text{ggT}(n_1, n_2) = 1$ !

$n_1 x + n_2 y = 1$  hat genau dann ganzzahlige Ls.  $x$  u.  $y$  falls  $n_1$  u.  $n_2$  klfremd sind, d.h.  $\text{ggT}(n_1, n_2) = 1$ .

## Bemerkung

Die Lösungen  $x$  und  $y$  der diophantischen Gleichung  $n_1 \cdot x + n_2 \cdot y = 1$  sind nicht eindeutig, denn für jede ganze Zahl  $k$  gilt:

$$n_1 \cdot (\underbrace{x + k \cdot n_2}_{x'}) + n_2 \cdot (\underbrace{y - k \cdot n_1}_{y'}) = 1$$

$$\cancel{n_1 x + k n_1 n_2} + \cancel{n_2 y - k n_1 n_2} = n_1 x + n_2 y = 1$$

Am Bsp.:  $3x + 4y = 1$   
 LÖN.  $x = 3, y = -2$   
 $x' = 3 + 1 \cdot 4 = 7$   
 $y' = -2 - 1 \cdot 3 = -5$   
 $\checkmark (k=1)$

## Example

Es gilt  $\underbrace{963}_{n_1} \cdot \underbrace{(-103)}_x + \underbrace{218}_{n_2} \cdot \underbrace{(455)}_y = 1$  und somit gelten z.B. auch:

$$\underbrace{963}_{n_1} \cdot \underbrace{(-103 + 1 \cdot 218)}_{x+1 \cdot n_2 = 115} + \underbrace{218}_{n_2} \cdot \underbrace{(455 - 1 \cdot 963)}_{y - 1 \cdot n_1 = -508} = 1$$

$$\underbrace{963}_{n_1} \cdot \underbrace{(-103 + 2 \cdot 218)}_{= 333} + \underbrace{218}_{n_2} \cdot \underbrace{(455 - 2 \cdot 963)}_{= -1471} = 1$$

# Modulare Inverse

Die lineare Diophantische Gleichung  $n_1 \cdot x + n_2 \cdot y = 1$  kann wie folgt umgeformt werden:

- $$\begin{aligned} n_1 \cdot x + n_2 \cdot y &= 1 \\ \Leftrightarrow n_1 \cdot x &= 1 - n_2 \cdot y \\ \Rightarrow n_1 \cdot x &\equiv 1 \pmod{n_2} \end{aligned}$$

$$\begin{aligned} 3 \cdot 3 + 4 \cdot (-2) &= 1 \\ 3 \cdot 3 &= 1 - 4 \cdot (-2) \\ 3 \cdot 3 &\equiv 1 \pmod{4} \\ \text{Das modulare Inverse von } 3 \text{ ist } 3 \end{aligned}$$

d.h. wenn wir modulo  $n_2$  denken, ist  $n_1 \cdot x = 1$ . Wir bezeichnen deshalb  $x$  als ein **modulares Inverses** von  $n_1$  modulo  $n_2$ .

Analog:

- $$\begin{aligned} n_1 \cdot x + n_2 \cdot y &= 1 \\ \Leftrightarrow n_2 \cdot y &= 1 - n_1 \cdot x \\ \Rightarrow n_2 \cdot y &\equiv 1 \pmod{n_1} \end{aligned}$$

$$\begin{aligned} 4 \cdot (-2) &= 1 - 3 \cdot 3 \\ 4 \cdot (-2) &\equiv 1 \pmod{3} \\ \text{oder } 1 \cdot 1 &\equiv 1 \pmod{3} \end{aligned}$$

d.h. wenn wir modulo  $n_1$  denken, ist  $n_2 \cdot y = 1$ . Wir bezeichnen deshalb  $y$  als ein **modulares Inverses** von  $n_2$  modulo  $n_1$ .

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

# Der erweiterte Euklidische Algorithmus

Lösung durch den **erweiterten Euklidischen Algorithmus**:

## Example

Finde  $x, y \in \mathbb{Z}$  mit  $211 \cdot x + 13 \cdot y = 1$ .

- Führe den (normalen) Euklidischen Algorithmus mit den beiden Zahlen  $n_1$  und  $n_2$  durch.

*Wegen  $\text{ggT}(211, 13) = 1$   
gibt es Lösungen!*

$$\begin{aligned} 211 &= 16 \cdot 13 + 3 \\ 13 &= 4 \cdot 3 + 1 \quad \text{ggT}(211, 13) \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

- Nutze diese Gleichungen in umgekehrter Reihenfolge, um jeweils *störende Terme* zu eliminieren.

$$\begin{aligned} \text{ggT}(211, 13) &= 1 = 1 \cdot 13 - 4 \cdot 3 && \text{letzte Gleichung} \\ &= 1 \cdot 13 - 4 \cdot (211 - 16 \cdot 13) && \text{letzte mit vorletzter Gleichung} \\ &= 1 \cdot 13 - 4 \cdot 211 + 64 \cdot 13 \\ &= \underbrace{-4}_{x} \cdot 211 + \underbrace{65}_{y} \cdot 13 \end{aligned}$$

- ① Bestimmen Sie mit Hilfe des erweiterten Euklidischen Algorithmus den grössten gemeinsamen Teiler der Zahlen
  - ① 345 und 124
  - ② 129 und 456
- ② Finden Sie  $x, y \in \mathbb{Z}$  mit  $963 \cdot x + 218 \cdot y = 1$ .
- ③ Finden Sie ein modulares Inverses von 963 modulo 218.
- ④ Finden Sie ein modulares Inverses von 218 modulo 963.
- ⑤ Lösen Sie die Relation  $963 \cdot x \equiv 1 \pmod{218}$ .

Wandtafel!

Löse die Diophantinische Gln.  $67 \cdot x + 24 \cdot y = 1$  und berechne  
damit  $24^{-1} \bmod 67$ .

Lösung:

Vergleich liefert:  $x = -5$  u.  $y = 14$

eukl. Alg.

$$\begin{aligned} 67 &= 2 \cdot 24 + 19 \\ 24 &= 1 \cdot 19 + 5 \\ 19 &= 3 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \quad = ggT(67, 24) \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

erm. eukl. Alg.

$$\begin{aligned} 1 &= 4 \cdot 24 - 5(67 - 2 \cdot 24) = -5 \cdot 67 + 14 \cdot 24 \\ 1 &= -1 \cdot 19 + 4(24 - 1 \cdot 19) = 4 \cdot 24 - 5 \cdot 19 \\ 1 &= 5 - 1(19 - 3 \cdot 5) = -1 \cdot 19 + 4 \cdot 5 \\ 1 &= 5 - 1 \cdot 4 \end{aligned}$$

Effiziente Tabellenform des eras. eukl. Algorithmus:

67	-	1	-	0
24	-	0	-	1
19	1	1	-2	
5	3	-1	3	
4	1	4	-11	
1		-5	14	

Man liest aus dieser Tabelle:

$$1 = -5 \cdot 67 + 14 \cdot 24$$

Auf beiden Seiten mod 67 rechnen:

$$1 = 14 \cdot 24 \bmod 67$$

oder

$$14 \cdot \overbrace{24}^{14^{-1}} = 1 \bmod 67$$

$$\underbrace{24^{-1}}_{\text{not } 24^{-1}} \neq \frac{1}{24}$$

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 **Der chinesische Restsatz**
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

# Der chinesische Restsatz

Welche Zahl(en)  $x$  ergeben bei der Division durch 5 den Rest 3, bei der Division durch 7 den Rest 2 und bei der Division durch 9 den Rest 4?

Diese Frage beantwortet der

Satz (Sun Tsu Suan-Ching, 4. Jh. v.C.)

Seien  $m_1, m_2, \dots, m_k \in \mathbb{N}^+$  paarweise teilerfremde Zahlen und  $m := m_1 \cdot m_2 \cdots m_k$ . Dann besitzt das System von  $k$  simultanen Kongruenzen

$$x \equiv r_1 \pmod{m_1}$$

$$x \equiv r_2 \pmod{m_2}$$

⋮

$$x \equiv r_k \pmod{m_k}$$

eine eindeutige Lösung  $x \pmod{m}$ .

Input ?

Bsp : Es gilt

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$x \equiv 4 \pmod{9}$$

gesucht  $x$ . Es gibt  
eine eindeutige Lös.

$$\text{modulo } m = 5 \cdot 7 \cdot 9 = 315$$

# Der chinesische Restsatz (Konstruktionsrezept)

Wir wollen das Konstruktionsrezept einer solchen Lösung angeben:

- Wir definieren für alle  $i = 1, 2, \dots, k$ :

$$M_i = \frac{m}{m_i}$$

$$m = m_1 m_2 \cdots m_k$$

$$m = 5 \cdot 7 \cdot 9 = 315$$

$$M_1 = \frac{m}{m_1} = \frac{315}{5} = 63$$

$$M_2 = 45; M_3 = 35.$$

Sicher gilt dann  $\text{ggT}(m_i, M_i) = 1$ , denn die  $m_i$  sind nach Voraussetzung paarweise teilerfremd.

- Für  $i = 1, 2, \dots, k$  hat  $M_i$  ein modulares Inverses (berechnen mit dem erweiterten Euklidischen Algorithmus)  $y_i$  modulo  $m_i$ , d.h.

$$M_i \cdot y_i \equiv 1 \pmod{m_i}$$

$$63 \cdot y_1 \equiv 1 \pmod{5}$$

$\Rightarrow y_1 = 2$  (durch Ausprobieren gefunden)

$$45 \cdot y_2 \equiv 1 \pmod{7}$$

$\Rightarrow y_2 = 5$

$$35 \cdot y_3 \equiv 1 \pmod{9}$$

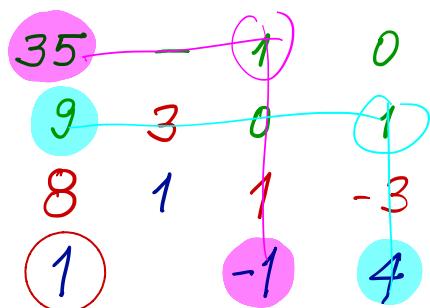
$\Rightarrow y_3 = 8$  (eeA)

- Die simultane Lösung der Kongruenzen ist dann

$$x = \sum_{i=1}^k r_i \cdot M_i \cdot y_i$$

$$x = 3 \cdot 63 \cdot 2 + 2 \cdot 45 \cdot 5 + 4 \cdot 35 \cdot 8 = 1948 = 58 \pmod{315}$$

Lösung mit dem erw. eukl. Algo:



Daraus folgt  $1 = (-1) \cdot 35 + 4 \cdot 9$ . Auf beiden Seiten modulo 9 rechnen

$$1 = (-1) \cdot 35 \pmod{9}$$

oder

$$8 \cdot 35 \equiv 1 \pmod{9}$$

-1 und 8 liegen  
in der selben Rest-  
klasse!

## Example

Bestimmen Sie alle Lösungen  $x$  des folgenden Systems von Kongruenzen:

$$x \equiv -2 \pmod{5} = 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$x \equiv 4 \pmod{9}$$

Lösung: **Siehe vorne!**

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

# Die Eulersche $\phi$ -Funktion

Die Eulersche  $\phi$ -Funktion ordnet jeder natürlichen Zahl  $n$  die Anzahl der zu ihr teilerfremden natürlichen Zahlen zu, die kleiner als  $n$  sind.

$$n=7:$$

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

$$|\mathbb{Z}_7^*| = 6$$

$$\mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}$$

$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid x > 0 \text{ und } \text{ggT}(x, n) = 1\}$$

$$|\mathbb{Z}_n^*| := \text{Anzahl Elemente in } \mathbb{Z}_n^*$$

$$n=6:$$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$\mathbb{Z}_6^* = \{1, 5\}$$

$$|\mathbb{Z}_6^*| = 2$$

## Definition

Die Eulersche  $\phi$ -Funktion ist gegeben durch:

$$\phi : \mathbb{N} \rightarrow \mathbb{N}, n \mapsto |\mathbb{Z}_n^*| =: \phi(n)$$

$$\phi(6) = |\mathbb{Z}_6^*| = 2$$

$$\phi(7) = |\mathbb{Z}_7^*| = 6$$

$n$	1	2	3	4	5	6	7	8	9	10	$\dots$
$\phi(n)$	0	1	2	2	4	2	6	4	6	4	$\dots$

## Satz

Seien  $p$  und  $q$  zwei verschiedene Primzahlen und  $m = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$  die Primfaktorzerlegung von  $m \in \mathbb{N}$ . Dann gilt

$$\phi(p) = p - 1$$

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

$$\phi(m) = (p_1 - 1) \cdot p_1^{r_1 - 1} \cdot (p_2 - 1) \cdot p_2^{r_2 - 1} \cdots (p_n - 1) \cdot p_n^{r_n - 1}$$

# Die Eulersche $\phi$ -Funktion (Beispiele)

## Example

Berechnen Sie mit Hilfe des letzten Satzes die folgenden Werte der Funktion  $\phi$ .

①  $\phi(6) = \phi(2 \cdot 3)$

②  $\phi(16) = \phi(2^4)$

③  $\phi(693) = \phi(3^2 \cdot 7 \cdot 11)$

④  $\phi(6732) = \phi(2^2 \cdot 3^2 \cdot 11 \cdot 17)$

1)  $\phi(6) = \phi(2 \cdot 3) = (2-1)(3-1) = 1 \cdot 2 = 2$

2)  $\phi(16) = \phi(2^4) = (2-1)2^{(4-1)} = 1 \cdot 2^3 = 8$

3)  $\phi(693) = \phi(3^2 \cdot 7^1 \cdot 11^1) = (3-1)3^{(2-1)} \cdot (7-1)7^{(1-1)} \cdot (11-1)11^{(1-1)}$   
 $= 2 \cdot 3 \cdot 6 \cdot 10 = 360$

4)  $\phi(6732) = \phi(2^2 \cdot 3^2 \cdot 11 \cdot 17) = 1 \cdot 2 \cdot 2 \cdot 3 \cdot 10 \cdot 16 = 1920$

$\downarrow$   
 $(2-1) \cdot 2^1$

Die Eulersche  $\phi$ -Fkt. an der Stelle  $n \in \mathbb{N}$  ist gleich der Anzahl El. in  $\mathbb{Z}_n^*$ .

Bei  $n=9$ :  $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ : Jedes El. in  $\mathbb{Z}_9^*$  hat ein modulare Inverses (in  $\mathbb{Z}_9^*$ )

Multiplikationstabelle

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

$$2 \cdot 5 = 5 \cdot 2 = 1 \pmod{9}$$

$$\Rightarrow 2^{-1} = 5 \pmod{9}$$

$$5^{-1} = 2 \pmod{9}$$

Das modulare  
Inversen von 2 ( $\pmod{9}$ )  
ist 5 und vice versa.

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen**
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

## Definition

Eine natürliche Zahl  $p > 1$  heisst **Primzahl**, wenn sie nur durch 1 und sich selber teilbar ist.

Zwei wichtige Bemerkungen:

## Satz

*Es gibt unendlich viele Primzahlen (haben wir bereits gesehen).*

## Satz (Fundamentalsatz der Arithmetik)

*Jede positive natürliche Zahl  $n > 1$  kann (bis auf die Reihenfolge) eindeutig als Produkt von Primzahlen  $p_1, p_2, \dots, p_n$  geschrieben werden:*

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}$$

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 **Der kleine Satz von Fermat**
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

## Satz (Kleiner Satz von Fermat)

Sei  $p$  eine Primzahl und  $m$  eine nichtnegative ganze Zahl. Dann gilt

$$m^p \bmod p = m \bmod p$$

$$p=7, m=6$$

$$6^{7-1} \bmod 7 = 1$$

$$6^6 \bmod 7 = 1$$

Daraus folgt falls  $m < p$  gilt:  $m^{p-1} \bmod p = 1$

## Example

Chinesische Mathematiker vermuteten, dass sogar das Folgende gilt: Eine natürliche Zahl  $n$  ist genau dann prim, wenn  $2^{n-1} \bmod n = 1$ . Wäre das richtig, hätten wir einen effizienten Primzahltest gefunden.

Prüfen Sie die Vermutung für die Zahlen  $n = 3, 5, 6, 7$  und  $341$ .

*„M. 31“      Spezialfall kl. Fermat.*

$$2^{341-1} \bmod 341 = 1$$

## Beweisidee

- Induktionsanfang:  $m = 0: 0^p \pmod{p} = 0$
- Induktionsschritt: Sei  $m \geq 0$  und die Behauptung für  $m$  wahr. Dann

$$\begin{aligned}(m+1)^p &= \sum_{k=0}^p \binom{p}{k} m^{p-k} \\ &= m^p + \underbrace{\binom{p}{1} m^{p-1} + \binom{p}{2} m^{p-2} + \cdots + \binom{p}{p-1} m}_{\text{durch } p \text{ teilbar}} + 1\end{aligned}$$

Alle in der letzten Gleichung vorkommenden Binomialkoeffizienten sind durch  $p$  teilbar (Warum?). Damit folgt

$$(m+1)^p \pmod{p} = m^p + 1 \pmod{p} = (m+1) \pmod{p}$$

wobei in der zweiten Umformung die Induktionsvoraussetzung  $m^p \pmod{p} = m \pmod{p}$  verwendet wurde.

Berechne mit Hilfe des kl. Fermat'schen Satzes:

$$3^{302} = 43 \cdot 7 + 1$$

$$3^{302} \pmod{7} = 3^{43 \cdot 7 + 1} \pmod{7}$$

$$= (3^{43})^7 \cdot 3 \pmod{7}$$

$$= (\underbrace{a}_a^7 \pmod{7} \cdot 3 \pmod{7}) \pmod{7}$$

$$= a \cdot 3 \pmod{7}$$

$$= 3^{43} \cdot 3 \pmod{7}$$

$$= (3^6)^7 \cdot 3^2 \pmod{7}$$

$$= (3^6)^7 \pmod{7} \cdot (3^2 \pmod{7}) \pmod{7}$$

$$= 3^6 \cdot 3^2 \pmod{7}$$

$$= 3^7 \cdot 3 \pmod{7}$$

$$= 3 \cdot 3 \pmod{7}$$

$$= 2$$

kl. Fermat. falls  $p$  eine P2,  
dann gilt:

$$a^p \equiv a \pmod{p}, \forall a \geq 0$$

Spezialfall:  $0 \leq a < p$

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

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

## Satz (Primzahltest von Wilson)

Eine natürliche Zahl  $n > 1$  ist genau dann eine Primzahl, wenn  $(n-1)! + 1 = n \cdot (n-1) \cdots 1 + 1$  durch  $n$  teilbar ist.

### Example

$$\begin{aligned} n=2 : \quad (2-1)! + 1 &= 2^1 & (5-1)! + 1 &= 25 \\ n=3 : \quad (3-1)! + 1 &= 3^1 & (6-1)! + 1 &= 121 \rightarrow 121 \text{ ist nicht durch } 6 \\ & (4-1)! + 1 &= 7^1 & \text{teilbar, also ist } 7 \text{ keine} \\ & (7-1)! + 1 &= 721 \end{aligned}$$

721 ist durch 7 teilbar, also ist 7 ein PZ.

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

Ein wichtiges Problem ist die Untersuchung der Verteilung der Primzahlen in der Menge aller natürlichen Zahlen.

Mathematisch kann das wie folgt beschrieben werden: Für jede natürliche Zahl  $n$  sei  $\pi(n)$  die Anzahl der Primzahlen  $p$  mit  $p \leq n$ . Was können wir über die Funktion

$$\pi : \mathbb{N} \longrightarrow \mathbb{N}$$

$$n \longmapsto \underbrace{|\{p \in \mathbb{N} : p \in \mathbb{P}, p \leq n\}|}_{\text{Anzahl aller Primzahlen kleiner oder gleich } n}$$

aussagen?

## Example

Berechnen Sie  $\pi(5)$ ,  $\pi(10)$ ,  $\pi(11)$ , ... und  $\pi(21)$ .

# Verteilung der Primzahlen (Fort.)

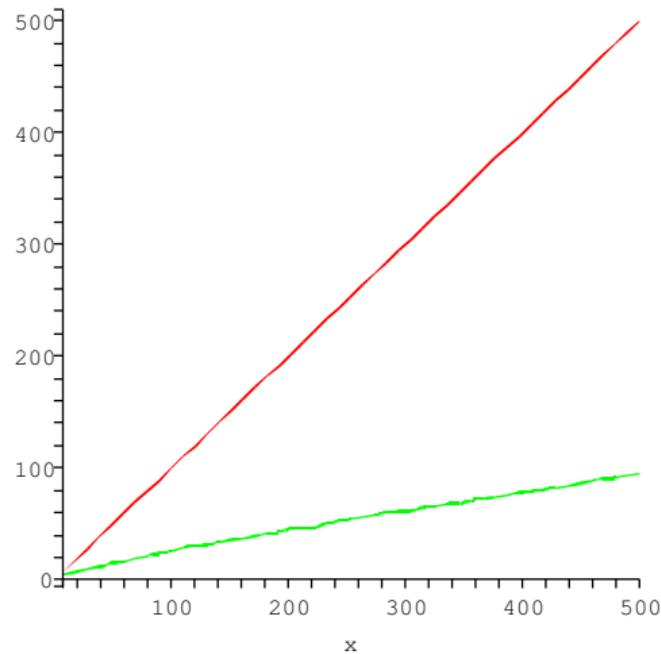


Abbildung: Vergleich zwischen der Identität (rot, oben) und  $\pi$  (grün, unten)

Ein grundlegender Satz der Zahlentheorie sagt, dass die Primzahlen relativ dicht zwischen den natürlichen Zahlen liegen.

## Satz (Primzahlsatz)

Es gilt:

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\frac{n}{\ln(n)}} = 1.$$

Der Satz sagt aus, dass die Anzahl der Primzahlen ungefähr so schnell wächst wie die Funktion  $n/\ln(n)$ . Wir sagen auch, dass die beiden Funktionen  $\pi(n)$  und  $n/\ln(n)$  **asymptotisch äquivalent** sind und bezeichnen das durch

Anzahl Pz  
kleiner gleich n 

$$\pi(n) \sim \frac{n}{\ln(n)}.$$

# Verteilung der Primzahlen (Fort.)

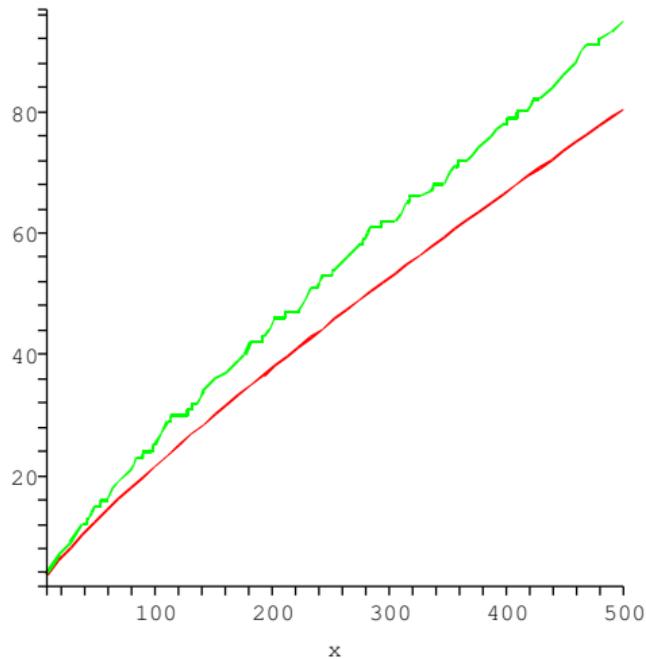


Abbildung: Vergleich zwischen  $\pi$  (grün, oben) und der Funktion  $n / \ln(n)$

# Verteilung der Primzahlen (Fort.)

$$\forall n \geq 67 : \frac{n}{\ln(n)} < \frac{n}{\ln(n) - \frac{1}{2}} < \pi(n) < \frac{n}{\ln(n) - \frac{3}{2}}.$$

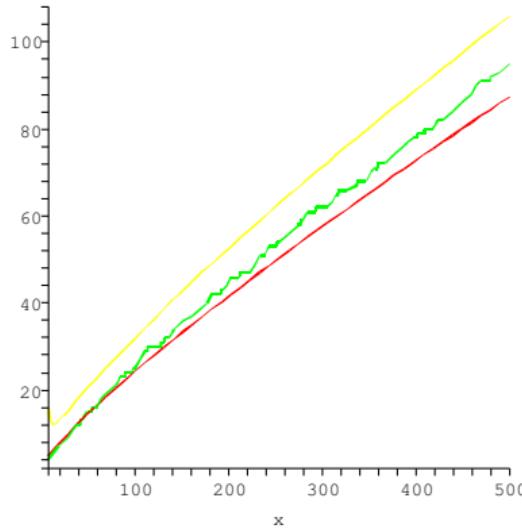


Abbildung: Vergleich zwischen  $\pi$  (grün),  $\frac{n}{\ln(n) - \frac{1}{2}}$  (rot) bzw.  $\frac{n}{\ln(n) - \frac{3}{2}}$  (gelb)

- 1 Division mit Rest
- 2 Kongruenz modulo  $n$
- 3 Der Euklidsche Algorithmus
- 4 Lösung linearer Diophantischer Gleichungen
- 5 Der erweiterte Euklidische Algorithmus
- 6 Der chinesische Restsatz
- 7 Die Eulersche  $\phi$ -Funktion
- 8 Primzahlen
- 9 Der kleine Satz von Fermat
- 10 Der Satz von Wilson
- 11 Verteilung der Primzahlen
- 12 Mersenne-Primzahlen

# Mersenne-Primzahlen

## Definition

Für  $n \in \mathbb{N}$  heisst  $M_n := 2^n - 1$  die  $n$ -te **Mersenne-Zahl**. Ist  $M_n$  eine Primzahl, so heisst sie **Mersenne-Primzahl**.

## Satz

Die Mersenne-Zahlen sind genau die Zahlen, die in Binärschreibweise ausschliesslich aus 1'en bestehen:

$$M_n = 2^n - 1 = 1 \cdot 2^{n-1} + 1 \cdot 2^{n-2} + \dots + 1 \cdot 2^1 + 1 \cdot 2^0 = (11\dots11)_2$$

## Example

$n$		1	2	3	4	5	6	7
$M_n$		1	3	7	15	31	63	127

Berechnen Sie  $M_8, \dots, M_{13}$  und entscheiden Sie, ob diese Zahlen Primzahlen sind.

## Mersenne-Primzahlen (Fort.)

49. bekannte Mersenne P2 :  $2^{74'207'281} - 1$  (22'338'618 Stellen)

### Satz

Ist  $n = r \cdot s$  zusammengesetzt (also keine Primzahl), so ist auch  $M_n$  zusammengesetzt.

Beweis: Für  $n = r \cdot s$  (mit  $1 < r, s < n$ ) gilt:

$$\begin{aligned}M_n &= 2^{r \cdot s} - 1 \\&= (2^r - 1) \cdot (2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1) \\&= (2^s - 1) \cdot (2^{s(r-1)} + 2^{s(r-2)} + \cdots + 2^s + 1)\end{aligned}$$

also ist  $M_n$  auf keinen Fall eine Primzahl. Also kann  $M_n$  höchstens dann eine Primzahl sein, wenn  $n$  eine Primzahl ist!

### Example

Bestätigen Sie die obigen Zerlegungen für die Mersenne-Zahlen  $M_4, M_6, M_8$  und  $M_9$ . Falls die Zerlegung von  $n$  in zwei Faktoren nicht eindeutig ist, überprüfen Sie alle Zerlegungen.

Wir haben folgende Begriffe kennen gelernt, können Sie einordnen und mit Ihnen umgehen.  
Weiter kennen wir einige Anwendungen:

- (Erweiterter) Euklidischer Algorithmus
- Diophantische Gleichungen und ihre Lösungen (+ mod. Inverser)
- Der chinesische Restsatz
- Die Eulersche  $\phi$ -Funktion
- Primzahlen und ihre Eigenschaften
- Der kleine Satz von Fermat
- Der Satz von Wilson
- Mersenne-Primzahlen

Wichtig !

# Fragen ?