

# ELEMENTARE ZAHLENTHEORIE

PROF. DR. CHRISTINA BIRKENHAKE

## INHALTSVERZEICHNIS

1. Minimum, Maximum und vollständige Induktion	3
1.1. Zahlen	3
2. Teilbarkeit	8
2.1. Teilbarkeitsrelation	8
2.2. Eigenschaften	10
2.3. Teilmengen	13
2.4. Ordnungsrelation: Teilbarkeit und Hassediagramme	15
3. Primzahlen	16
3.1. Einführung der Primzahlen in der Schule	16
3.2. Wieviele Primzahlen gibt es?	18
3.3. Sieb des Eratosthenes	20
3.4. Wie sind die Primzahlen innerhalb der natürlichen Zahlen verteilt?	21
3.5. Primzahlformeln	23
3.6. Primfaktorzerlegung	27
3.7. Folgerungen aus dem Hauptsatz	31
3.8. Primzahlkriterium und das Lemma von Euklid	32
4. Größter gemeinsamer Teiler ( $ggT$ ) und kleinstes gemeinsames Vielfaches ( $kgV$ )	33
4.1. $ggT$ und Teilmengen	33
4.2. Euklidischer Algorithmus	36
4.3. Vielfache des $ggT$ und Linearkombinationen	42
4.4. Lineare Diophantische Gleichungen	44
4.5. $kgV$ und Vielfachenmengen	49
5. Kongruenzen und Restklassen	54
5.1. Die Kongruenzrelation $\mod m$	54
5.2. Kongruenz als Äquivalenzrelation	59
5.3. Algebraische Struktur von $\mathbb{Z}/m\mathbb{Z}$ - Rechnen im System $\mathbb{Z}/m\mathbb{Z}$	62

5.4. Die Sätze von Euler, Fermat und der Chinesische Restsatz	71
6. Stellenwertsysteme	78
6.1. Verschiedene Stellenwertsysteme	78
6.2. Prinzip des Stellenwertsystems	82
6.3. Zahlen in verschiedenen Zahlssystemen	84
7. Dezimalbrüche	87
7.1. Gemeine Brüche und Dezimalbrüche	87
7.2. Kettenbrüche	96
8. Teilbarkeitsregeln	99
8.1. Endstellenregeln	100
8.2. Quersummenregeln	103
8.3. Weitere Teilbarkeitsregeln für Primzahlen	106
9. Vollkommene Zahlen	109
9.1. Beispiele und Definition	109
10. Fibonaccizahlen, Goldener Schnitt und Irrationalität	113
10.1. Das regelmäßige 5-Eck - Goldener Schnitt	115
10.2. Aperiodische Plasterungen	118
10.3. DIN-Norm für Papier	118
11. <b>EAN, ISBN, PZN und IBAN</b>	122
11.1. EAN im Supermarkt	122
11.2. <b>ISBN</b>	126
11.3. Die Pharmazentralnummer <b>PZN</b>	128
11.4. IBAN, Verfahren Modulo 97-10 (ISO 7064)	129
12. Kryptographie	132
12.1. Monoalphabetische Substitution	132
12.2. Polyalphabetische Substitution	135
13. RSA-Verschlüsselungssystem	136

## 1. MINIMUM, MAXIMUM UND VOLLSTÄNDIGE INDUKTION

## 1.1. Zahlen.

**Natürliche Zahlen - Peano - Axiome (1889)**

Giuseppe Peano (1858-1932)

(1) 1 ist eine natürliche Zahl.  $(1 \in \mathbb{N})$ (2) Jeder natürlichen Zahl  $n$  ist genau eine natürliche Zahl  $n'$  zugeordnet, die *Nachfolger* von  $n$  genannt wird.

$$(n' = n + 1)$$

(3) 1 ist kein Nachfolger.  $(n' = 1 \Rightarrow \text{falsch})$ (4) Sind  $n$  und  $m$  verschiedene natürliche Zahlen, so sind auch ihre Nachfolger  $n'$  und  $m'$  verschieden.

$$(n \neq m \Rightarrow n + 1 \neq m + 1)$$

(5) Enthält eine Menge  $M$  natürlicher Zahlen 1 und folgt aus  $n \in M$  stets  $n' \in M$ , so besteht  $M$  aus *allen* natürlichen Zahlen.  $(M = \mathbb{N})$ **Uneinheitliche Notation: natürliche Zahlen mit oder ohne Null?**

$$\mathbb{N} = \{1, 2, 3, \dots\} \quad \text{oder} \quad \mathbb{N} = \{0, 1, 2, 3, \dots\}$$

In mathematischen Abhandlungen je nach Vereinbarung!In der Schule:X Quadrat-Zeichenlegende:  $\mathbb{N}$  = Menge der natürlichen Zahlen $\mathbb{N}_0$  = Menge der nat. Zahlen einschließlich Null.

bsv, Mathematische Formeln kompakt:

$$\mathbb{N} = \{0, 1, 2, 3, \dots\} \quad \text{und} \quad \mathbb{N}^* = \mathbb{N} \setminus \{0\} = \{1, 2, 3, \dots\}.$$



Eine binäre Relation  $<$  auf einer Menge  $M$  heißt *Ordnung* (oder alternativ *Halbordnung*), wenn für alle  $x, y, z \in M$  gilt:

- (1) es gilt niemals  $x < x$ , (irreflexiv)
- (2) aus  $x < y$  folgt  $y \not< x$ , (Asymmetrie)
- (3) aus  $x < y$  und  $y < z$  folgt, daß  $x < z$ . (Transitivität)

Gilt darüber hinaus, daß

- (4) immer entweder  $x < y$  oder  $y < x$ ,

so heißt  $<$  *totale Ordnung*.

Gilt darüber hinaus, daß

- (5) jede nichtleere Teilmenge  $N \subset M$  ein kleinstes Element besitzt, d.h. es gibt ein  $x \in N$  mit  $x < y$  für alle  $y \in N \setminus \{x\}$ ,

so heißt  $<$  *Wohlordnung*.

**Satz 1.1** (Kleinstes Element - Wohlordnungsprinzip). *Jede nicht leere Teilmenge  $T$  von  $\mathbb{N}$  enthält eine kleinste Zahl  $m$ . Das heißt, für alle  $t \in T$  gilt:  $m \leq t$ .*

**Beweis:**

Da  $T$  nicht leer ist, gibt es ein Element  $n \in T$ . Das erste (= kleinste) Element der geordneten Menge  $\{(0), 1, 2, \dots, n-1, n\}$ , daß auch in  $T$  enthalten ist, ist das gesuchte kleinste Element.  $\square$

**Satz 1.2** (Induktion). *Ist eine Aussage über eine natürliche Zahl wahr für 1)  $n = 0$  (bzw.  $n_0 \in \mathbb{N}$ ) und wenn 2) die Wahrheit der Aussage für alle  $a < n$  die Wahrheit für  $n$  selber zur Folge hat, dann ist die Aussage für alle  $n \in \mathbb{N}$  wahr.*

**Beweis:**

Es sei  $T$  die Menge der natürlichen Zahlen ( $> n_0$ ), für die die Aussage falsch ist. Nach 1) gilt  $0 \notin T$  ( $n_0 \notin T$ ). Wenn  $T = \emptyset$ , haben wir nichts zu zeigen. Wenn aber  $T$  nicht leer ist, so hat es nach 1.1 ein kleinstes Element  $n > 0$  ( $n > n_0$ ). Da dann aber die Aussage für alle natürlichen Zahlen  $(0), 1, \dots, n-1$  (bzw.  $n_0, \dots, n-1$ ) (also für alle  $a < n$ ) gilt, so ist sie nach Voraussetzung 2) auch für  $n$ , damit würde folgen:  $n \notin T$ .  $\square$

Daraus ergibt sich die Beweismethode der *Vollständigen Induktion*:

Es sei  $A(n)$  eine Aussage (abhängig von einer natürlichen Zahl  $n \in \mathbb{N}$ ). Es ist zu zeigen, daß  $A(n)$  für alle natürlichen Zahlen  $n$  ab einem gewissen Anfangswert  $n_0$  gilt (d.h. für alle  $n \geq n_0$ ). Dazu zeigt man:



- (1) *Induktionsanfang*: Die Aussage  $A(n_0)$  ist wahr.  
 (2) *Induktionsschritt*: Man zeigt, daß aus der Gültigkeit von  $A(n)$  für irgendein  $n \in \mathbb{N}$  auch die Gültigkeit der Aussage für den Nachfolger  $n+1$  von  $n$  folgt. (Aus  $A(n)$  ist wahr, folgt  $A(n+1)$  ist wahr!)

**Beispiel:** Beweise die *Summenformel* mit vollständiger Induktion:

$$\sum_{i=1}^n i = 1 + 2 + 3 + \cdots + n = \frac{n \cdot (n+1)}{2} \quad \forall \quad n \in \mathbb{N} \quad (1)$$

**Beweis:**

**Induktionsanfang:** Zu Zeigen: *Die Aussage (1) ist für  $n = 1$  richtig:*

$$\frac{n \cdot (n+1)}{2} \stackrel{n=1}{=} \frac{1 \cdot (1+1)}{2} = 1 \quad \checkmark$$

**Induktionsschritt:** Zu Zeigen: *Aus der Gültigkeit von (1) für  $n$  folgt die für  $n+1$ :* Angenommen es gilt  $1 + 2 + 3 + \cdots + n = \frac{n \cdot (n+1)}{2}$  für ein  $n \in \mathbb{N}$ .

Induktionsvoraussetzung

Dann folgt:

$$\begin{aligned} \frac{[n+1] \cdot ([n+1] + 1)}{2} &= \frac{(n+1) \cdot (n+2)}{2} = \frac{(n+1) \cdot n + (n+1) \cdot 2}{2} \\ &= \frac{n \cdot (n+1)}{2} + (n+1) \quad (\text{mit Ind. Voraussetzung}) \\ &= 1 + 2 + 3 + \cdots + n + (n+1) \quad \square \end{aligned}$$

**Satz 1.3** (Maximumsprinzip). *In jeder nicht leeren endlichen Menge reeller Zahlen gibt es eine größte Zahl.*

(Beachte: hier ist das Wort endlich wichtig! Gegenbeispiel: das offene Intervall  $]0, 1[$  hat weder ein kleinstes noch ein größtes Element.)

**Beweis:**

Eine nicht leere endliche Menge reeller Zahlen hat notwendiger Weise die Form  $\{a_1, \dots, a_n\}$  mit einem  $n \in \mathbb{N}$ .

Sei  $T$  die Menge natürlicher Zahlen  $n \geq 1$  mit der Eigenschaft:

*Jede  $n$ -elementige Menge reeller Zahlen hat ein größtes Element:*

$$T = \{n \in \mathbb{N} \mid \text{ist } M \subset \mathbb{R} \text{ mit } \#M = n \Rightarrow M \text{ hat ein größtes Element}\}$$

Klar:  $1 \in T$ , denn jede Menge  $\{a_1\}$ , mit  $a_1 \in \mathbb{R}$ , hat ein größtes Element!

Angenommen  $n \in T$ , das heißt: jede  $n$ -elementige Menge ( $\subset \mathbb{R}$ ) besitzt ein Maximum. Ist nun  $M = \{a_1, \dots, a_n, a_{n+1}\} \subset \mathbb{R}$ , so hat die Teilmenge  $\{a_1, \dots, a_n\}$



ein größtes Element, OE  $a_n$  ist dieses Element. Da die reellen Zahlen total geordnet sind, gilt entweder  $a_{n+1} > a_n$ ,  $a_{n+1} = a_n$  oder  $a_{n+1} < a_n$ . Gleichheit geht nicht, also ist im Fall  $a_{n+1} > a_n$  die Zahl  $a_{n+1}$  das größte Element von  $M$  oder im Fall  $a_{n+1} < a_n$  ist es  $a_n$ . Damit hat  $M$  in jedem Fall ein größtes Element und folglich gilt  $n + 1 \in T$ . Induktiv folgt, daß  $T = \mathbb{N}$ , und damit die Behauptung.  $\square$

### Natürliche Zahlen - Addition

Den Schülern bewußt machen, daß man die natürlichen Zahlen additiv erzeugen kann:

$$n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ Summanden}}.$$

Die Addition ordnet stets zwei natürlichen Zahlen eine dritte zu:

$$n, m \in \mathbb{N} \Rightarrow n + m = k \in \mathbb{N}.$$

Subtraktion ist Gegenoperation zur Addition:

$$k - m = n \quad \text{genau dann, wenn} \quad n + m = k.$$

Insbesondere:

$$(n + m) - m = n.$$

Subtraktion *hebt die Addition auf*.

**Problem**, Subtraktion geht nicht immer

$$m - n \notin \mathbb{N} \text{ falls } n > m \quad \nrightarrow \Rightarrow \text{Erweiterung auf } \mathbb{Z}$$

## Natürliche Zahlen - Von der Addition zur Multiplikation

Wiederholte Addition der gleichen Zahl:

$$n \cdot m = \underbrace{m + m + \cdots + m}_{n \text{ Summanden}}.$$

Formulierung:  **$n$  mal  $m$**

**Problem** Wo ist die Betonung?

$n$  mal  $m$

$n$  mal  $m$

$$\underbrace{m + m + \cdots + m}_{n \text{ Summanden}}$$

oder

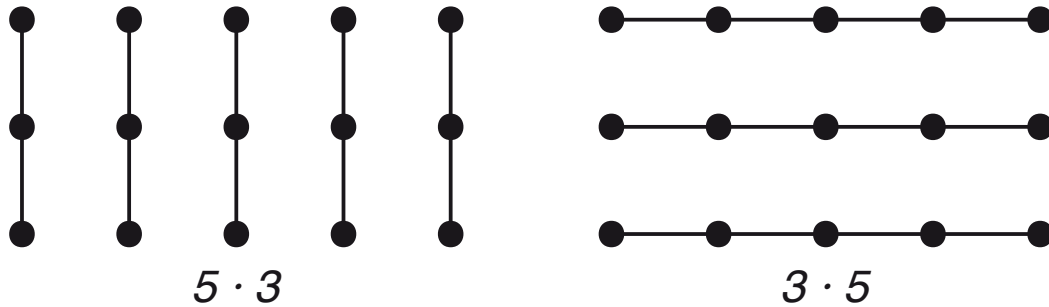
$$\underbrace{n + n + \cdots + n}_{m \text{ Summanden}}$$

Umgangssprache

Operatorauffassung :

$$n \xrightarrow{\cdot m} n \cdot m$$

Das wegen der **Kommutativität** der Multiplikation beides gleich ist, hilft den Schülern wenig. Man muss es durch Übung und Beispiele klar machen. z.B. so:



Natürliche Zahlen - Kommutativität der Multiplikation

Umkehroperation?  $\Rightarrow$  neue Relation: **Teilerrelation**

## 2. TEILBARKEIT

## 2.1. Teilbarkeitsrelation.

**Definition 2.1.** Eine natürliche Zahl  $a$  ist genau dann Teiler der natürlichen Zahl  $b$ , wenn eine natürliche Zahl  $q$  existiert, so daß

$$a \cdot q = b.$$

**Schreibweise:**  $a \mid b$  ( $a$  teilt  $b$ )      sonst  $a \nmid b$  ( $a$  teilt nicht  $b$ )

**Beispiele:**

$$2 \cdot 3 = 6 \qquad \Rightarrow 2 \mid 6 \text{ und } 3 \mid 6$$

$$10 \cdot 7 = 70 \qquad \Rightarrow 10 \mid 70 \text{ und } 7 \mid 70$$

$$\text{aber } 5 \nmid 21 \qquad \text{denn } 4 \cdot 5 = 20 \text{ und } 5 \cdot 5 = 25$$

$$\begin{array}{ccc} \text{und} & & 20 < 21 < 25 \\ & & | & & | \\ & & 5 & & 5 \end{array}$$

Die letzte Begründung wird sicherlich von Schülern akzeptiert.

Wie kann man das aber beweisen?

Das wird mit Korollar 2 möglich sein!



**Bemerkung 2.1.** (1) Null: Vorsicht bei Teilbarkeit:

- $0 \nmid b$  für alle  $b \in \mathbb{N} \setminus \{0\}$ , denn  $q \cdot 0 = 0$  für alle  $q \in \mathbb{N}$
- $0 \mid b$  impliziert  $\Rightarrow b = 0$ !!! **Null ist nur Teiler von Null!**
- $a \mid 0$  für alle  $a \in \mathbb{N}$ , denn  $0 \cdot a = 0$  für alle  $a \in \mathbb{N}$
- $0 \mid 0$ , denn  $q \cdot 0 = 0$  für z.B.  $q = 1$  (und alle  $q \in \mathbb{N}$ !)

Um diese Ausnahmen nicht immer gesondert auszuschließen, beschränkt man sich auf  $\mathbb{N} = \{1, 2, 3, \dots\}$  bei Teilbarkeitsuntersuchungen (ohne dies immer zu erwähnen!).

(2)  $0 \mid 0$  aber !!!  $0 : 0$  !!! ist nicht definiert!

(3) Teilbarkeit wird mittels Multiplikation definiert (nicht via Division wie bei G8)

- Vorteilhaft beim Beweisen
- Multiplikation (bei Schülern) einfacher als Division.
- Zusammenhang Teiler und Vielfache transparenter.
- Problem mit Division durch Null entfällt, keine Fallunterscheidungen nötig!

(4) Teilen versus Dividieren:

- Beim Dividieren können von Null verschiedene Reste auftreten:  
 $3 : 2 = 1 + \frac{1}{2}$
- Bei der Teilerfrage nicht:  $2 \nmid 3$  aber  $2 \mid 6$  weil  $2 \cdot 3 = 6$   
und damit  $\Rightarrow 6 : 2 = 3$
- $\Rightarrow$  Teilen ist eine Spezialfall des Dividierens!
- Die gesuchte Information ist verschieden:

**Teilen:** Frage ob eine Zahl (multiplikativ) in einer anderen Zahl enthalten ist.

**Dividieren:** Frage wie oft eine Zahl in einer anderen enthalten ist.

(5) Teilbarkeitsbetrachtungen können auch auf die ganzen Zahlen

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  erweitert werden. Ersetze  $\mathbb{N}$  durch  $\mathbb{Z}$  in Definition 1 ( und etwas mit der Null aufpassen).

**Definition 2.2.** Die Zahl  $b \in \mathbb{N}$  ist genau dann ein **Vielfaches** der Zahl  $a \in \mathbb{N}$ , wenn es ein  $q \in \mathbb{N}$  gibt mit

$$q \cdot a = b \quad \text{bzw.} \quad a \mid b$$

**Bezeichnung:**  $a \mid b$  kann auch als  $b$  ist Vielfaches von  $a$  gelesen werden.



**Bemerkung 2.2.**  $a$  ist genau dann Teiler von  $b$ , wenn  $b$  Vielfaches von  $a$  ist.

## 2.2. Eigenschaften.

**Satz 2.3** (Teilbarkeitseigenschaften). Für  $a, b, c, d \in \mathbb{Z}$  gilt:

- |  |                                       |
|--|---------------------------------------|
| (1) $a \mid b$ und $b \mid c \Rightarrow a \mid c$                 | (Transitivität)                       |
| (2) $a \mid b$ und $b \mid a \Rightarrow  a  =  b $                | ( $_{\mathbb{N}}$ : (Anti-)Symmetrie) |
| (3) $a \mid b$ und $c \mid d \Rightarrow a \cdot c \mid b \cdot d$ |                                       |

**Beweis:**

$$(1) \quad a \mid b \Rightarrow a \cdot q_1 = b \quad \text{und} \quad b \mid c \Rightarrow b \cdot q_2 = c \quad \text{für} \quad q_1, q_2 \in \mathbb{Z} \\ \Rightarrow c = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2) \quad \Rightarrow a \mid c$$

$$(2) \quad \text{Es gibt } q_1, q_2 \in \mathbb{Z} \text{ mit 1.) } a \cdot q_1 = b \text{ und 2.) } b \cdot q_2 = a. \\ 2.) \text{ in 1.): } b = a \cdot q_1 = (b \cdot q_2) \cdot q_1 = b \cdot q_2 q_1 \stackrel{!}{=} b$$

$$\textbf{Fall: } b \neq 0 \Rightarrow q_2 q_1 = 1$$

$$\text{Da } q_1, q_2 \in \mathbb{Z} \Rightarrow |q_1| = |q_2| = 1 \\ \Rightarrow a = \pm b \Leftrightarrow |a| = |b|.$$

$$\textbf{Fall: } b = 0$$

$$\Rightarrow a \mid 0 \text{ (sowieso)} \text{ und } 0 \mid a \Rightarrow a = 0 \text{ (Bem. 2.1: Null teilt nur Null)}$$

$$(3) \quad a \cdot q_1 = b \text{ und } c \cdot q_2 = d \Rightarrow a \cdot c \cdot (q_1 \cdot q_2) = b \cdot d$$

□

**Korollar 2.4.** Für  $a, b \in \mathbb{Z}$ ,  $a \neq 0$  gilt:

- (1)  $a \mid b \Rightarrow a \mid b \cdot d$  für alle  $d \in \mathbb{Z}$   
 (2)  $a \mid b \Rightarrow a \cdot d \mid b \cdot d$  für alle  $d \in \mathbb{Z}$

**Beweis:**

Folgt aus dem Satz 2.3 (3) mit  $c = 1$  (für 1.) und  $c = d$  (für 2.).  $\square$

Satz 2.3 (3) hat kein additives Analogon, denn

$$2 \mid 6 \quad \text{und} \quad 3 \mid 15 \\ \text{aber} \Rightarrow (2 + 3) = 5 \nmid 21 = (6 + 15)$$

**Satz 2.5** (Teilen von Linearkombinationen). Für  $a, b, c \in \mathbb{Z}$  gilt:

$$a \mid b \quad \text{und} \quad a \mid c \quad \Rightarrow \quad a \mid (rb + sc)$$

für alle  $r, s \in \mathbb{Z}$ . (d.h.  $a$  teilt jede ganzzahlige Linearkombination von  $b$  und  $c$ .)

**Beweis:**

Korollar  $\Rightarrow a \mid r \cdot b$  und  $a \mid s \cdot c$  für alle  $r, s \in \mathbb{Z}$ .

Also  $a \cdot q_1 = r \cdot b$  und  $a \cdot q_2 = s \cdot c$  für  $q_1, q_2 \in \mathbb{Z}$ .

$$\Rightarrow a \cdot (q_1 + q_2) = a \cdot q_1 + a \cdot q_2 = r \cdot b + s \cdot c$$

$\Rightarrow$  Beh.  $\square$

Der Satz ist nicht umkehrbar, denn:

$$2 \mid (2 \cdot 3 + 4 \cdot 5) \quad \text{aber} \quad 2 \nmid 3 \quad \text{und} \quad 2 \nmid 5$$

Aber:

**Korollar 2.6.** Für  $a, b, c \in \mathbb{Z}$  gilt:

$$a \mid b \quad \text{und} \quad a \mid c \quad \Rightarrow \quad a \mid b \pm c$$

Nachtrag zum Beispiel aus Abschnitt 2.1:

**Wie beweist man das Nicht Teiler Sein?**

$$5 \nmid 21 \quad \text{warum?}$$

**Beweis:**

Z.B. durch Widerspruch: Annahme:  $5 \mid 21$

Es gilt sicher auch:  $5 \mid 20$ , denn  $5 \cdot 4 = 20$ .

$$\text{Korollar 2.6} \Rightarrow 5 \mid (21 - 20) = 1 \quad \nmid \quad \square$$



**Satz 2.7.** Für  $a, b \in \mathbb{Z}$  gilt:

$$a \mid b \Leftrightarrow |a| \mid |b|$$

**Beweis:**

$$a = \text{sign}(a) \cdot |a| \text{ und } b = \text{sign}(b) \cdot |b|$$

$$a \mid b \Leftrightarrow a \cdot q = b$$

$$\Leftrightarrow \text{sign}(a) \cdot |a| \cdot q = \text{sign}(b) \cdot |b| \quad (\cdot \text{sign}(b))$$

$$\Leftrightarrow |a| \cdot (q \cdot \text{sign}(a) \cdot \text{sign}(b)) = |b|$$

$$\Leftrightarrow |a| \mid |b|$$

□

**Anwendung:**  $\sqrt{2}$  ist keine rationale Zahl.

**Beweis:**

Angenommen,  $\sqrt{2}$  ist rational, also ein Bruch. Sei  $T$  die Menge der natürlichen Zahlen  $n$ , so daß  $n \cdot \sqrt{2} \in \mathbb{N}$ . Nach dem Satz über das kleinste Element (Wohlordnungsprinzip Satz 1.1) hat  $T$  ein kleinstes Element  $n_0$ , also  $n_0 \cdot \sqrt{2} \in \mathbb{N}$ . Dann:

$$\text{weil: } 1 < 2 < 4 \quad (\text{Wurzel ziehen})$$

$$1 < \sqrt{2} < 2 \quad | \cdot n_0$$

$$n_0 < n_0 \cdot \sqrt{2} < 2n_0 \quad | - n_0$$

$$0 < \underbrace{n_0 \cdot \sqrt{2} - n_0}_{\in \mathbb{N}} < n_0 \quad | \cdot \sqrt{2}$$

$$0 < \underbrace{(n_0 \cdot \sqrt{2} - n_0)}_{< n_0} \cdot \sqrt{2} = \underbrace{2n_0 - n_0 \cdot \sqrt{2}}_{\in \mathbb{N}} < n_0 \cdot \sqrt{2}$$

Also ist  $(n_0 \cdot \sqrt{2} - n_0) < n_0$  ein weiteres Element von  $T$ , das widerspricht der Minimalität von  $n_0$ . Also ist  $T = \emptyset$  und damit  $\sqrt{2}$  irrational! □

## 2.3. Teilmengen.

**Definition 2.3.** Für eine natürliche Zahl  $a$  sei:

$$T_a = T(a) = \{x \in \mathbb{N} \mid x \text{ teilt } a\}$$

die Menge aller Teiler von  $a$ .

**Beispiele**

$$T_{15} = \{1, 3, 5, 15\}$$

$$T_{17} = \{1, 17\}$$

Wegen  $1 \mid a$  und  $a \mid a \Rightarrow \{1, a\} \subseteq T_a$ .

$T_a$  hat also immer mindestens 2 Elemente (für  $a > 1$ ):  $\#T_a \geq 2$ .

**Definition 2.4.**

- (1) Natürliche Zahlen, die genau 2 Teiler haben, heißen Primzahlen.
- (2) Natürliche Zahlen, die mindestens 3 Teiler haben, heißen zusammengesetzte Zahlen.

**Satz 2.8.**

$$a \in \mathbb{N}, a \neq 0 \Rightarrow \#T_a \leq a$$

( $a$  hat also höchstens  $a$  Teiler!)

**Beweis:**

Sei  $b \in T_a$ , (also  $b \mid a$ ).

$\Rightarrow b \cdot q = a$  für ein  $q \in \mathbb{N}$ .

insbesondere  $b, q \geq 1$  (da  $b, q \in \mathbb{N} \setminus \{0\}$ )

$$\Rightarrow 1 \leq b = b \cdot 1 \leq b \cdot q = a$$

Kurz  $1 \leq b \leq a \Rightarrow \text{Beh.}$  □

**Bemerkung 2.9.** Für  $a = 0$  gilt der Satz nicht, denn  $b \cdot 0 = 0$  für alle  $b \in \mathbb{N}$

$$\Rightarrow \#T(0) = \infty$$

Sei  $a \in \mathbb{N}$  mit  $\#T(a) > 2$ .

(also keine Primzahl)

$\Rightarrow$  es gibt Teiler:  $b \mid a$ ,  $b \neq 1$  und  $b \neq a$

$\Rightarrow$  es gibt  $q \in \mathbb{N}$  mit  $b \cdot q = a$

( $q \neq 1, q \neq a$ )

Erlaubt ist auch:  $q = b$

Wegen  $b \cdot q = a$  nennt man  $a$  auch zusammengesetzte Zahl.



**Bemerkung 2.10.** • Die kleinste zusammengesetzte Zahl ist:  $4 = 2 \cdot 2$

$$T_4 = \{1, 2, 4\}.$$

- Die Zahl 1 ist weder Primzahl noch zusammengesetzte Zahl.

### Wie findet man Teilmengen einer Zahl?

Nutze: - Teiler treten in Paaren auf:  $b \cdot q = a$  Paar:  $(b, q)$

- Bei Quadratzahlen:  $b^2 = a$  Paar:  $(b, b)$

### Beispiele:

$$a = 12:$$

$$\begin{array}{c|ccc|c} b & 1 & 2 & 3 & 4 \\ \hline q & 12 & 6 & 4 & 3 \end{array} \Rightarrow T_{12} = \{1, 2, 3, 4, 6, 12\} \Rightarrow \#T_{12} = 6$$

$$a = 21:$$

$$\begin{array}{c|cc|c} b & 1 & 3 & 7 \\ \hline q & 21 & 7 & 3 \end{array} \Rightarrow T_{21} = \{1, 3, 7, 21\} \Rightarrow \#T_{21} = 4$$

$$a = 16:$$

$$\begin{array}{c|ccc} b & 1 & 2 & 4 \\ \hline q & 16 & 8 & 4 \end{array} \Rightarrow T_{16} = \{1, 2, 4, 8, 16\} \Rightarrow \#T_{16} = 5$$

**Bemerkung 2.11.** Quadratzahlen haben eine ungerade Anzahl von Teilern.

Nicht-Quadratzahlen haben eine gerade Anzahl von Teilern.

**Satz 2.12.** Für  $a, b \in \mathbb{N}$  gilt:

$$a \mid b \Leftrightarrow T_a \subseteq T_b$$

### Beweis:

” $\Rightarrow$ ” Transitivität der Teilerrelation (Satz 2.3 (1))

$\Rightarrow c \mid a$  und  $a \mid b \Rightarrow c \mid b \Rightarrow T_a \subseteq T_b$ .

” $\Leftarrow$ ”  $a \in T_a \subseteq T_b \Rightarrow a \mid b$ . □

### Teilbarkeitsregeln



Beispiele: Teiler Bedingung

- |       |  |
|-------|--|
| 2     | gerade Zahl bzw. letzte Ziffer ist gerade            |
| 3     | $3 \mid$ Quersumme                                   |
| 5     | letzte Ziffer 0 oder 5                               |
| 9     | $9 \mid$ Quersumme                                   |
| $2^n$ | Zahl der letzten $n$ Ziffern ist durch $2^n$ teilbar |
| $5^n$ | Zahl der letzten $n$ Ziffern ist durch $5^n$ teilbar |

Das und mehr wird in einem späteren Abschnitt ausführlich behandelt!

## 2.4. Ordnungsrelation: Teilbarkeit und Hassediagramme.

**Satz 2.13.** Die Teilbarkeitsrelation über  $\mathbb{N}$  ist eine Ordnungsrelation, d.h. sie ist:

- reflexiv** :  $a$  teilt  $a$  ( $a \mid a$ ) für alle  $a \in \mathbb{N}$ .  
**transitiv** : aus  $a \mid b$  und  $b \mid c$  folgt  $a \mid c$ , für  $a, b, c \in \mathbb{N}$ .  
**antisymmetrisch** : aus  $a \mid b$  und  $b \mid a$  folgt  $a = b$ .



**Beweis:**

- Reflexivität ist klar
- Transitivität war Inhalt von Satz 2.3 (1)
- (Anti-)Symmetrie: folgt aus Satz 2.3 (2):  $a \mid b$  und  $b \mid a \Rightarrow |a| = |b|$   
mit  $\mathbb{N}$  statt  $\mathbb{Z}$  gilt:  $a = b$

□

Hassediagramme veranschaulichen Teilbarkeitszusammenhänge in Zahlenmengen:

**Beispiele**

- |   |  |                             |  |
|---|--|-----------------------------|--|
| (1) $M = \{1, 2, 3, 4, 5\}$                   | <pre>       4      / \     2   3   5      \ /       1 </pre> | (2) $T_8 = \{1, 2, 4, 8\}$  | <pre>       8               4               2               1 </pre> |
| (3) $T_{21} = \{1, 3, 7, 21\}$                | <pre>       21      /  \     3    7      \  /       1 </pre> | (4) $T_{25} = \{1, 5, 25\}$ | <pre>       25               5               1 </pre>                |
| (5) $M = \{1, 3, 5, 9, 45\}$                  |  |                             |  |
| (6) $T_{70} = \{1, 2, 5, 7, 10, 14, 35, 70\}$ |  |                             |  |



## 3. PRIMZAHLEN

## 3.1. Einführung der Primzahlen in der Schule.

**Methode: Vervielfachungsmaschinen**

Michael hat viele Vervielfachungsmaschinen:

$$\boxed{\cdot 2}, \quad \boxed{\cdot 3}, \quad \boxed{\cdot 4}, \dots$$

Diese *Maschinen* verdoppeln, verdreifachen, vervierfachen etc..

**Aufgabe:** Michael soll 100 große Zahlen versechsfachen!

*Problem:* Maschine  $\boxed{\cdot 6}$  ist defekt.

**Lösung:** Freund Andreas schlägt vor, die Maschinen  $\boxed{\cdot 2}$  und  $\boxed{\cdot 3}$  zu benutzen.

*Frage 1* Warum?

*Frage 2* Gibt es noch mehr überflüssige Maschinen? 

*Frage 3* Welche Maschinen sind unentbehrlich?

**Methode: Rechtecke Legen**

Gegeben: 12 gleichgroße quadratische Plättchen.

**Frage:** Wie viele verschiedene Rechtecke können damit gelegt werden?

**Variationen:** Dabei müssen 1) alle Plättchen genutzt werden oder 2) nicht! 

Wie ist das bei 13, 15 oder 20 Plättchen?

Gibt es auch Plättchenmengen, aus denen (wenn alle Teile benutzt werden sollen) keine Rechtecke gebildet werden können?



**Methode: Gefängniszellen**

Ein Tyrann hat ein Gefängnis mit 1000 Einzelzellen und 1000 Wärtern.

Einmal im Jahr werden im Rahmen einer Amnestie Gefangene entlassen. Dabei werden die Gefangenen nach folgender Methode ausgewählt:

*Wärter 1* macht an jeder Tür ein Kreuz

*Wärter 2* macht an jeder 2ten Tür ein Kreuz

*Wärter 3* macht an jeder 3ten Tür ein Kreuz

⋮

Die Gefangenen hinter den Türen mit genau 2 Kreuzen werden entlassen. Welche Zelltüren werden geöffnet?



$w \backslash z$	1	2	3	4	5	6	7	8	9	10	11
1	×	×	×	×	×	×	×	×	×	×	×
2		×		×		×		×		×	
3			×			×			×		
4				×				×			
5					×					×	
6						×					
7							×				
8								×			
9									×		
2 Kreuze:		↑	↑		↑		↑				↑

**Vergleich der Zugänge:**

**Vervielfachungsmaschinen:** Betont die Eigenschaft der Primzahlen, 1) (multiplikative) Bausteine aller natürlicher Zahlen zu sein und 2) Unzerlegbar zu sein.


**Rechtecke Legen:** Darstellung natürlicher Zahlen als Produkt von 2 Zahlen, enaktiv (durch Handlung), Zerlegbarkeit von Zahlen.

**Gefängnis:** Vielfache, Teilbarkeit, Anzahl der Teiler, Ergänzende Frage:

*Wieviele und welche Wärter machen ein Kreuz an Tür Nummer  $n$ ?*



**Charakteristika von Primzahlen:**

- Primzahlen sind unzerlegbar
- Primzahlen sind die Bausteine der natürlichen Zahlen 
- Primzahlen haben genau 2 Teiler

**Sonderfall:** Die Zahl  $\underline{1}$  ist keine Primzahl! und natürlich auch nicht zerlegbar!!

**Achtung:** Die Begriffe Teilbarkeit und Primzahlen betreffen die Verknüpfung: Multiplikation

Bzgl. Addition gibt es in  $\mathbb{N}$  nur ein unzerlegbares Element: die Zahl 1.

Aber es gibt  $\infty$ -viele unzerlegbare Elemente in  $\mathbb{N}$  bzgl. der Multiplikation  
 $\Rightarrow$  die  $\infty$ -vielen Primzahlen.

**3.2. Wieviele Primzahlen gibt es?**

**Satz 3.1.** *Der kleinste von 1 verschiedene Teiler einer natürlichen Zahl  $a > 1$  ist eine Primzahl.*

**Beweis:**

**Fall 1:**  $a$  ist Primzahl

$\Rightarrow T_a = \{1, a\} \Rightarrow$  der kleinste Teiler  $\neq 1$  ist  $a \Rightarrow$  Beh.

**Fall 2:**  $a$  ist zerlegbar

$\Rightarrow \{1, a\} \subsetneq T_a$

Sei  $b \in T_a \setminus \{1, a\}$  der kleinste Teiler. (vgl. Satz 1.1)

Z.z.  $b$  ist Primzahl.

Klar, wegen der Transitivität der Teilbarkeitsrelation:

Wäre  $b$  keine Primzahl  $\Rightarrow \exists t \neq 1, b$  mit  $t|b \Rightarrow 1 < t < b$

$$t|b \text{ und } b|a \Rightarrow t|a \quad \nexists$$

□



**Satz 3.2** (Euklid (um -3.Jh.)). *Es gibt unendlich viele Primzahlen.*

**Beweis:**

Annahme es gibt endlich viele Primzahlen:

$$p_1, p_2, p_3, \dots, p_n$$

Sei  $a := p_1 \cdot p_2 \cdot \dots \cdot p_n + 1 \quad (\in \mathbb{N})$

$\Rightarrow a$  ist keine Primzahl, da größer als jede Primzahl,  $a > 1$  und:

(\*)  $p_i \nmid a$  für alle  $i = 1, \dots, n$  (weil Rest  $\frac{1}{p_i}$ )

Sei  $p \in T_a$  der kleinste Teiler  $\neq 1$

Aus (\*)  $\Rightarrow p \neq p_i, \quad i = 1, \dots, n$

Aber: Satz 3.1  $\Rightarrow p$  ist Primzahl  $\nmid$

□

**Folgerung** *Zu jeder großen Primzahl gibt es stets eine noch größere - es gibt keine größte Primzahl.*

**Jagd nach großen Primzahlen:** Viele Internetseiten (z.B. [www.primzahlen.de](http://www.primzahlen.de)),

Bücher (Ribenoim,...), Strategien, Primzahlen zu erzeugen:

z.B. Mersennezahlen:  $2^n - 1$



### 3.3. Sieb des Eratosthenes.

Erathosthenes (\* um 273 v. Chr. in Kyrene, † um 194 v. Chr. in Alexandria)  
Mathematiker, Geograph, Astronom, Historiker, Philosoph, leitete die Bibliothek von Alexandria.

Berechnete unter anderem den Erdumfang und die Schiefe der Ekliptik.

#### Siebmethode, 10 Spalten

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
⋮									

- (1) Streiche Zahl 1, da keine Primzahl
- (2) nächste Zahl ist 2, PZ, streiche alle Vielfachen von 2.
- (3) nächste Zahl ist 3, PZ, streiche alle Vielfachen.
- (4) nächste Zahl ist 5, PZ, streiche alle Vielfachen.
- ⋮

#### Siebmethode, 1 + 6 Spalten

<del>1</del>	<u>2</u>	<u>3</u>	<del>4</del>	<u>5</u>	<del>6</del>	<u>7</u>
<del>8</del>	<del>9</del>	<del>10</del>	<u>11</u>	<del>12</del>	<u>13</u>	
<del>14</del>	<del>15</del>	<del>16</del>	<u>17</u>	<del>18</del>	<u>19</u>	
<del>20</del>	<del>21</del>	<del>22</del>	<u>23</u>	<del>24</del>	<del>25</del>	
<del>26</del>	<del>27</del>	<del>28</del>	<u>29</u>	<del>30</del>	<u>31</u>	
<del>32</del>	<del>33</del>	<del>34</del>	<del>35</del>	<del>36</del>	<u>37</u>	
<del>38</del>	<u>39</u>	<del>40</del>	<u>41</u>	<del>42</del>	<u>43</u>	
<del>44</del>	<del>45</del>	<del>46</del>	<u>47</u>	<del>48</del>	<del>49</del>	
⋮						

**Satz 3.3.** Die Primzahlen  $> 3$  sind von der Form  $6n \pm 1$  mit  $n \in \mathbb{N}$ .

**Satz 3.4.** Beim Sieben der natürlichen Zahlen  $\leq n$  nach Eratosthenes reicht es, die Vielfachen der Primzahlen  $\leq \sqrt{n}$  zu streichen.



### 3.4. Wie sind die Primzahlen innerhalb der natürlichen Zahlen verteilt?

Primzahlen  $p$  und  $q$  mit Abstand  $|p - q| = 2$  heißen Primzahlzwillinge.

Weitere Beispiele für Primzahlzwillinge:

$$\begin{array}{c} (9929, 9931), \quad \underbrace{(156 \cdot 5^{202} - 1, 156 \cdot 5^{202} + 1)}_{\text{haben 144 Ziffern}} \\ 2007: \quad \underbrace{(2.003.663.613 \cdot 2^{195.000} \pm 1)}_{\text{haben 58.711 Ziffern}} \end{array}$$

Sei 2300 Jahren bekannt: Es gibt  $\infty$ -viele Primzahlen.

Offen (nicht bekannt): ob es endlich oder unendlich viele Primzahlzwillinge gibt.

#### Primzahltrillings:

$(3, 5, 7)$  sind die einzigen Primzahltrillings der Form  $(p, p + 2, p + 4)$

#### Beweis:

Annahme  $3 < p, p + 2, p + 4$  sind Primzahlen.

Da  $p$  prim  $\Rightarrow p = 6m \pm 1$

$$\text{Wenn } p = 6m + 1 \Rightarrow p + 2 = 6m + 3 \Rightarrow 3|p + 2 \nmid$$

$$\text{Wenn } p = 6m - 1 \Rightarrow p + 4 = 6m + 3 \Rightarrow 3|p + 4 \nmid \quad \square$$

Primzahlfolgen der Form  $p, p + 2, p + 6$  heißen Primzahltrillings.



## Beispiele

(41, 43, 47)

(107, 109, 113)

(10.014.491, 10.014.493, 10.014.497)

Es gibt bei großen Zahlen nicht nur immer wieder Primzahlhäufungen (wie die Beispiele zeigen), aber auch beliebig lange Lücken:

**Satz 3.5.** Für alle  $n \in \mathbb{N}$  gibt es eine Primzahlücke der Länge  $\geq n$ .

(m.a.W.: für jedes  $n$  gibt es eine Folge von  $n$  aufeinanderfolgenden zusammengesetzten Zahlen.)

**Beweis:**

$$\left. \begin{array}{lll} (n+1)! + 2 & = 2 \cdot 3 \cdot 4 \cdots (n+1) + 2 & \text{hat Teiler } 2 \\ (n+1)! + 3 & = 2 \cdot 3 \cdot 4 \cdots (n+1) + 3 & \text{hat Teiler } 3 \\ \vdots & & \\ (n+1)! + (n+1) & = 2 \cdots (n+1) + (n+1) & \text{hat Teiler } (n+1) \end{array} \right\} n \text{ Zahlen}$$

Das sind insbesondere  $n$  aufeinanderfolgende zusammengesetzte Zahlen  $\Rightarrow$  Beh. □

**Satz 3.6.** Für  $n \geq 3$  liegt zwischen  $n$  und  $n!$  mindestens eine Primzahl.

**Beweis:**

$$\text{Sei } n \in \mathbb{N}, n \geq 3 \quad \Rightarrow \quad n! - 1 \geq 3! - 1 = 2 \cdot 3 - 1 = 5 > 1$$

$\Rightarrow$  kleinster Teiler  $p \neq 1$  von  $n! - 1$  ist eine Primzahl (vgl. Satz 3.1) □

$$\text{Dann: } p \leq n! - 1 < n!$$

Wir haben also eine Primzahl  $p < n!$  gefunden.

Es gilt aber auch  $n < p$ , denn:

$$2, 3, 4, \dots, n \in T_{n!} \quad \Rightarrow \quad 2, 3, 4, \dots, n \notin T_{n!-1}$$

$$\Rightarrow p \neq 2, 3, 4, \dots, n \quad \Rightarrow \quad n < p \quad \Rightarrow \text{Beh.} \quad \square$$

*Euler* (1737): Neuer Beweis für die Unendlichkeit der Primzahlen mittels harmonischer Reihe.

**Wdh.: Harmonische Reihe/Folge:**  $\sum_{i=1}^n \frac{1}{i}$  divergiert für  $n \rightarrow \infty$ .

**Satz 3.7** (Euler).

$$\lim_{n \rightarrow \infty} \frac{\sum_{PZ: p \leq n} \frac{1}{p}}{\ln(\ln(n))} = 1$$

d.h. Zähler- und Nennerfunktion verhalten sich asymptotisch gleich!



Folgerung:

**Satz 3.8** (Euler, um 1740).  $\sum_{PZ: p \leq n} \frac{1}{p}$  divergiert für  $n \rightarrow \infty$ .

$$\Pi(x) := \#\{\text{Primzahlen } p \leq x\}, \text{ für } x \in \mathbb{R}$$

$$\text{z.B. } \Pi(1) = 0, \quad \Pi(2) = 1, \quad \Pi(3) = 2, \quad \Pi(10) = 4, \quad \Pi(17,3) = \Pi(17) = 7$$

Legendre (1752-1833) stellte aufgrund empirischer Untersuchungen die Vermutung auf, daß:

$$\Pi(x) \text{ verhält sich asymptotisch gleich } \frac{x}{\ln x}$$

**Satz 3.9** (Primzahlsatz). (Hadamard und unabhängig Ch. de la Vallée Poussin, 1896)

$$\lim_{x \rightarrow \infty} \frac{\Pi(x)}{\frac{x}{\ln x}} = 1$$

### 3.5. Primzahlformeln.



Das Polynom

$$p(x) = x^2 - 79x + 1601$$

$$p(39) = p(40) = 41, \quad p(38) = p(41) = 43,$$

$$p(37) = p(42) = 47, \quad p(36) = p(43) = 53$$

$$p(35) = p(50) = 151 \quad \dots \text{alles Primzahlen?}$$

**Satz 3.10.** Kein Polynom  $p(x) = a_n x^n + \dots + a_1 x + a_0$  vom Grad  $\geq 1$ ,  $a_i \in \mathbb{Z}$ , erfüllt

$$p(m) \text{ ist Primzahl für alle } m \in \mathbb{Z}.$$

**Beweis:**

Sei  $p(x) = a_n x^n + \dots$  ein Polynom vom Grad  $n$  mit ganzzahligen Koeffizienten.

Z.z.:  $\exists m \in \mathbb{Z}$  mit  $p(m)$  ist zusammengesetzte Zahl!

Wenn  $a_0$  zusammengesetzte Zahl  $\Rightarrow p(0) = a_0$  zusammengesetzt. ✓

Also Annahme:  $a_0$  PZ.



$\Rightarrow \forall m \in \mathbb{N}$  gilt:

$$\begin{aligned} p(a_0 \cdot m) &= a_n(a_0 \cdot m)^n + a_{n-1}(a_0 \cdot m)^{n-1} + \cdots + a_1(a_0 \cdot m) + a_0 \\ &= a_0 \underbrace{(a_n a_0^{n-1} m^n + \cdots + a_1 m + 1)}_{=: A(m) \in \mathbb{Z}} \\ &= a_0 (A(m) + 1) \end{aligned}$$

Genauer:

$$A(m) = a_n a_0^{n-1} m^n + a_{n-1} a_0^{n-2} m^{n-1} + \cdots + a_1 m$$

$A(m)$  ist also ein Polynom vom Grad  $n$  in der Variablen  $m$ .

$\Rightarrow A(m)$  hat höchstens  $n$  Nullstellen.

Also  $\exists m_0 \in \mathbb{N}$  (bzw. in  $\mathbb{Z}$ ) mit  $A(m_0) \neq 0$

$$\Rightarrow p(m_0 \cdot a_0) = a_0 \underbrace{(A(m_0) + 1)}_{\neq 1} \text{ ist zusammengesetzte Zahl}$$

□

**Satz 3.11.** Seien  $a, b \in \mathbb{N}$  mit  $\text{ggT}(a, b) > 1$  und  $a \neq 0$ , so kann für  $x \in \mathbb{Z}$  das lineare Polynom  $p(x) = ax + b$  höchstens einen Primzahlwert annehmen.



**Bemerkung 3.12.** Vorgriff:  $\text{ggT}$  wird erst im nächsten Abschnitt definiert!

Wir haben gesehen, daß alle Primzahlen  $> 3$  von der Form  $6n \pm 1$  sind! Das widerspricht nicht dem Satz, denn  $\text{ggT}(6, 1) = 1$

**Beweis:**

Sei  $c := \text{ggT}(a, b)$ , nach Voraussetzung:  $c \neq 1$

$$\Rightarrow a = c \cdot a_1 \text{ und } b = c \cdot b_1 \text{ mit } a_1, b_1 \in \mathbb{N} \text{ und } a_1 \geq 1.$$

$$\Rightarrow \forall z \in \mathbb{Z} \quad p(z) = az + b = ca_1z + cb_1 = c(a_1z + b_1)$$

Das ist nur dann eine Primzahl, wenn  $a_1z + b_1 = 1$  und  $c$  eine Primzahl ist.

Da bleiben die folgenden Möglichkeiten:

$$(1) \quad b_1 = 0 \Rightarrow a_1 \cdot z = 1 \Rightarrow a_1 = z = 1 \text{ und } p(1) = c \text{ PZ,}$$

$$(2) \quad b_1 = 1 \Rightarrow b = c \Rightarrow p(0) = b = c \text{ PZ,}$$

$$(3) \quad b_1 \geq 2 \Rightarrow -1 \leq b_1 - 1 = -a_1z \Rightarrow z \text{ negativ und } a_1 \mid b_1 - 1. \text{ Sei } a_1 \cdot q = b_1 - 1 \Rightarrow p(-q) = c(-a_1q + b_1) = c(1 - b_1 + b_1) = c \text{ PZ.}$$

Die 3 Fälle schliessen sich offensichtlich aus und jeweils gibt es genau den einen angegebenen Primzahlwert. □

**Beispiele**

- $p(x) = 3x$  (also  $b = 0$  und  $a = c \text{ PZ}$ ) hat Primzahlwert:  $p(1) = 3$





- $p(x) = 12x + 4 = 4(3x + 1)$  hat nie Primzahlwerte ( $/\mathbb{N}$ ), denn  $c \neq \text{PZ}$
- $p(x) = 12x + 3 = 3(4x + 1)$  hat den Primzahlwert:  $p(0) = 3$
- $p(x) = 6x + 15 = 3(2x + 5)$  hat den Primzahlwert:  $p(-2) = 3$

Was ist, wenn  $\text{ggT}(a, b) = 1$ ?

**Satz 3.13** (Dirichletscher Primzahlsatz). *Zu jeder natürlichen Zahl  $b$  gibt es unendlich viele Primzahlen der Form*

$$p \equiv a \pmod{b}, \quad \text{mit } \text{ggT}(a, b) = 1$$

**Alternative Formulierung** Sind  $a, b \in \mathbb{N}$  mit  $\text{ggT}(a, b) = 1$ , so gibt es  $\infty$ -viele Primzahlen der Form

$$a \pm nb, \quad n \in \mathbb{N}$$

Zum Beweis benötigt man Begriffe wie Dirichlet-Charakter, Zeta-Funktion und L-Reihen  $\Rightarrow$  übersteigt Möglichkeiten der Elementaren Zahlentheorie.



**Spezialfälle:** a)  $a = 1, b = 2$

$\exists \infty$  – viele Primzahlen:  $p = 1 \pmod{2}$

$\Leftrightarrow \exists \infty$  – viele Primzahlen:  $p = 1 + 2n$

**Klar:** jede Primzahl  $\neq 2$  ist von dieser Form.

b) In Satz 3.3 haben wir gesehen: Jede Primzahl  $> 3$  ist von der Form:

$$6n \pm 1 \quad \text{mit } n \in \mathbb{N}$$

$\Rightarrow$  Fall  $a = 1, b = 6$ :  $p = 1 + 6n$

Aber:  $6n - 1 = 6(n - 1) + 6 - 1 = 6(n - 1) + 5$

$\Rightarrow$  Satz 3.3 beinhaltet also die beiden Fälle:  $(a, b) = (1, 6)$  und  $(a, b) = (5, 6)$ .

### Offene Primzahlprobleme

Goldbach'sche Vermutung: Jede gerade Zahl  $> 2$  lässt sich als Summe von zwei Primzahlen darstellen. (Nachgewiesen für alle  $n \leq 4 \cdot 10^{17}$ .)

Äquivalent (Euler): Jede natürliche Zahl  $> 5$  ist Summe von drei Primzahlen.

**Beweis:**

**"Goldbach  $\Rightarrow$  Euler":**

Wenn  $n > 5$  eine gerade Zahl ist  $\Rightarrow n - 2 > 3 > 2$  ebenfalls gerade und nach der Goldbach'schen Vermutung Summe von 2 Primzahlen:

$$n - 2 = p_1 + p_2 \quad \Rightarrow \quad n = 2 + p_1 + p_2$$

Wenn  $n > 5$  eine ungerade Zahl ist  $\Rightarrow n - 3 > 2$  ist eine gerade Zahl und ebenso nach Goldbach Summe von zwei Primzahlen:

$$n - 3 = p_1 + p_2 \quad \Rightarrow \quad n = 3 + p_1 + p_2 \quad \checkmark$$

**"Goldbach  $\Leftarrow$  Euler":** Sei  $n > 2$  gerade.

Wenn  $n = 4$ ,  $\Rightarrow n = 4 = 2 + 2$ , also Summe von 2 Primzahlen.

Wenn  $n = 6$ ,  $\Rightarrow n = 6 = 3 + 3$ , also Summe von 2 Primzahlen.

Allgemein: mit  $n$  ist  $n + 2 \geq 5$  ebenfalls gerade und nach Euler:

$$n + 2 = p_1 + p_2 + p_3 \text{ mit Primzahlen } p_i.$$

Wären  $p_1, p_2, p_3 > 2$ , so wären alle drei Primzahlen ungerade und dann auch ihre Summe.

$\Rightarrow$  OE  $p_1 = 2$ ,  $\Rightarrow n + 2 = 2 + p_2 + p_3 \Rightarrow n = p_2 + p_3$  ist Summe von 2 Primzahlen.  $\square$



### 3.6. Primfaktorzerlegung.

#### Beispiele

- Bei sehr hohen Zahlen ist das sehr mühselig:  
z.B.  $a = 286.378.465$   
Finde PFZ, ist diese auch eindeutig?  
In der Praxis heute ohne Rechnereinsatz kaum denkbar.
- **Viererwelt:**

$$V := \{1, 4, 8, 12, 16, \dots, 4n, \dots\} = 4\mathbb{N} \cup \{1\}$$

$V$  ist abgeschlossen bzgl. Multiplikation

$\Rightarrow$  Teilbarkeitsuntersuchungen möglich:

Def: Für  $a, b \in V$ ,  $a \mid_4 b$  ( $a$  ist  $V$ -Teiler von  $b$ ) genau dann, wenn  $a \cdot q = b$  für ein  $q \in V$ .

Dann

$$\underbrace{1 \mid_4 32}_{1 \cdot 32 = 32}, \quad \underbrace{4 \mid_4 32, \quad 8 \mid_4 32}_{4 \cdot 8 = 32}, \quad \underbrace{16 \not\mid_4 32}_{16 \cdot 2 = 32, 2 \notin V}, \quad \underbrace{32 \mid_4 32}_{32 \cdot 1 = 32}$$

$\Rightarrow V$ -Primzahlen möglich zu definieren:

Def.: Eine Zahl  $p \in V$  heißt  $V$ -Primzahl, wenn sie genau 2  $V$ -Teiler hat: 1 und  $p$ .

Dann:

$$T_{\mathbb{N}}(4) = \{(1, 4), \underbrace{(2, 4)}_{\notin V}\}$$

$$T_V(4) = \{1, 4\} \Rightarrow V - PZ$$

$$T_{\mathbb{N}}(8) = \{(1, 8), \underbrace{(2, 4)}_{\notin V}\}$$

$$T_V(8) = \{1, 8\} \Rightarrow V - PZ$$

(da  $4 \cdot 2 = 8$  und  $2 \notin V$  ist 4 kein  $V$ -Teiler von 8)

$$T_{\mathbb{N}}(12) = \{(1, 12), \underbrace{(3, 4)}_{\notin V}, \underbrace{(2, 6)}_{\notin V}\}$$

$$T_V(12) = \{1, 12\} \Rightarrow V - PZ$$

(da  $4 \cdot 3 = 12$  ist 4 kein  $V$ -Teiler von 12)

$$T_{\mathbb{N}}(24) = \{(1, 24), \underbrace{(2, 12)}_{\notin V}, \underbrace{(3, 8)}_{\notin V}, \underbrace{(4, 6)}_{\notin V}\}$$

$$T_V(24) = \{1, 24\} \Rightarrow V - PZ$$

$\Rightarrow$  Primfaktorzerlegung in  $V$ :

**Beispiel:**  $a = 96$  eindeutige PFZ in  $V$ ??



$$\begin{aligned}
T_{\mathbb{N}}(96) &= \{(1, 96), (2, 48), (3, 32), (4, 24), (6, 16), (8, 12)\} \\
T_V(96) &= \{(1, 96), (4, 24), (8, 12)\} \\
\Rightarrow 96 &= 8 \cdot 12 = 4 \cdot 24
\end{aligned}$$

Da 4, 8, 12, 24 V-Primzahlen, hat 96 also 2 Primfaktorzerlegungen !!??  
Eindeutigkeit???

**Satz 3.14** (Existenz). *Jede natürliche Zahl  $a \neq 1$  besitzt eine Primfaktorzerlegung (PFZ):*

$$a = p_1 \cdots p_s \quad \text{mit Primzahlen } p_i, i = 1, \dots, s, \quad s \geq 1$$

**Beweis:**

**Fall 1:**  $a$  ist Primzahl  $\Rightarrow a = a$  ist PFZ. ✓

**Fall 2:**  $a$  zusammengesetzte Zahl: sei  $p_1|a$  der kleinste Teiler  $\neq 1$ .

Satz 3.1  $\Rightarrow p_1$  ist Primzahl.

Klar:  $1 < p_1 < a$  und  $p_1 \cdot n_1 = a$  mit einem  $n_1 \in \mathbb{N}$ ,  $1 < n_1 < a$ .

Falls  $n_1$  PZ ✓

Falls  $n_1$  keine PZ: Sei  $p_2|n_1$  kleinster Teiler  $\neq 1$

$\Rightarrow p_2$  PZ und  $n_1 = p_2 \cdot n_2$  mit  $n_2 \in \mathbb{N}$ ,  $1 < n_2 < n_1$ .

$$\Rightarrow a = p_1 \cdot n_1 = p_1 \cdot p_2 \cdot n_2, \quad 1 < n_2 < n_1 < a$$

Nun wieder  $n_2$  entweder Primzahl  $\geq 2$  (und damit wären wir fertig) oder zusammengesetzt ...

Algorithmus muß abbrechen (d.h.  $n_{s-1}$  ist Primzahl  $\geq 2$  für ein  $s$ ), denn es gibt nur endlich viele natürliche Zahlen zwischen 1 und  $a$ .

$$\text{Also} \quad a = p_1 \cdot p_2 \cdot \dots \cdot p_{s-1} \cdot \underbrace{n_{s-1}}_{PZ}$$

Mit  $n_{s-1} =: p_s \Rightarrow a = p_1 \cdots p_s$  □

**Satz 3.15** (Hauptsatz der elementaren Zahlentheorie, Eindeutigkeit). *Jede natürliche Zahl  $a \neq 1$  besitzt genau eine (bis auf die Reihenfolge (b.a.R.) eindeutige) Primfaktorzerlegung.*

**Beweis:**

**Annahme:** Es gibt ein  $n \in \mathbb{N}$  mit 2 Primfaktorzerlegungen.

Sei  $n$  die kleinste natürliche Zahl mit dieser Eigenschaft (vgl. Wohlordnungsprinzip 1.1), dann gilt:

Alle natürlichen Zahlen kleiner  $n$  haben eine (b.a.R.) eindeutige PFZ. (2)

Sei  $p_1 | n$  kleinster Teiler  $\neq 1$

Wie im Beweis von Satz 3.14 gibt es zu  $p_1$  eine PFZ:

$$n = p_1 \cdot p_2 \cdots p_s \quad (3)$$

Nach Annahme gibt es noch eine weitere PFZ:

$$n = q_1 \cdot q_2 \cdots q_t \quad (4)$$

**Zwischenbehauptung:** Die Mengen  $\{p_1, p_2, p_3, \dots, p_s\}$  und  $\{q_1, \dots, q_t\}$  sind disjunkt:

Wäre z.B.  $p_i \in \{q_1, \dots, q_t\}$ , z.B.  $p_i = q_r$ , dann

$$p_1 \cdot p_2 \cdots \overset{\vee}{p_i} \cdots p_s = \frac{n}{p_i} = \frac{q_1 \cdot q_2 \cdots q_t}{q_r} = \underbrace{q_1 \cdot q_2 \cdots \overset{\vee}{q_r} \cdots q_t}_{\text{hat eindeutige PFZ}} < n$$

$\Rightarrow$  nach (2) müssten die beiden (äußeren) PFZ'en übereinstimmen  $\Rightarrow$

$$\begin{aligned} \{p_1, p_2, \dots, \overset{\vee}{p_i}, \dots, p_s\} &= \{q_1, q_2, \dots, \overset{\vee}{q_r}, \dots, q_t\} & (p_i = q_r \text{ hinzufügen:}) \\ \Rightarrow \{p_1, p_2, p_3, \dots, p_s\} &= \{q_1, q_2, \dots, q_r, \dots, q_t\} & \nexists \end{aligned}$$

Widerspruch zur Annahme, daß die PFZ'en (3)  $\neq$  (4).

$\Rightarrow$  Zwischenbehauptung!

$\Rightarrow$  insbesondere gilt:  $p_1 \notin \{q_1, \dots, q_t\}$ .

Setze

$$n = p_1 \cdot \underbrace{p_2 \cdots p_s}_{=:a} = p_1 \cdot a$$

$$n = q_1 \cdot \underbrace{q_2 \cdots q_t}_{=:b} = q_1 \cdot b \quad (\text{dabei gilt } b > 1, \text{ denn sonst wäre } n = q_1 \text{ PZ})$$

$$\Rightarrow z := n - p_1 \cdot b \quad (\Rightarrow z < n)$$

$$\Rightarrow z = p_1 \cdot a - p_1 \cdot b = p_1 \cdot (a - b) \quad \Rightarrow p_1 | z \quad (*)$$

$$z = q_1 \cdot b - p_1 \cdot b = (q_1 - p_1) \cdot b \quad (**)$$

Da  $p_1 \neq q_1$  kleinster Teiler von  $n \Rightarrow p_1 < q_1 \Rightarrow 1 \leq q_1 - p_1$  und es folgt:



$$z = \underbrace{(q_1 - p_1)}_{\geq 1} \cdot \underbrace{b}_{> 1} > 1 \quad \Rightarrow \quad 1 < z < n$$

$\Rightarrow$  PFZ von  $z$  ist eindeutig!

(\*) und (\*\*)  $\Rightarrow p_1$  Teiler von  $z = (q_1 - p_1) \cdot b = (q_1 - p_1) \cdot q_2 \cdots q_t$

Da  $p_1 \notin \{q_1, \dots, q_t\}$  (nach der Zwischenbehauptung)  $\Rightarrow p_1 \mid (q_1 - p_1)$

Da trivialerweise  $p_1 \mid p_1 \Rightarrow$  (mit Satz 2.5)  $p_1 \mid (q_1 - p_1) + p_1 = q_1 \quad \nmid \quad \square$

**Bemerkung 3.16.** (1) Warum funktioniert der Satz nicht in der Viererwelt  $V$ ?

In der letzten Zeile des Beweises, beim Widerspruch:

$$p_1 \mid (q_1 - p_1) + p_1 = q_1 \quad \nmid$$

wird die Summenregel aus Satz 2.5 benutzt:

$$a \mid b \quad \text{und} \quad a \mid c \quad \Rightarrow \quad a \mid b + c \quad !$$

Diese Regel gilt nicht in  $V$ , denn z.B.:

$$4 \mid_4 4 \quad \text{und} \quad 4 \mid_4 4 \quad \text{aber} \quad 4 \nmid_4 (4 + 4) = 8 = 2 \cdot 4$$

(2) Die Primzahlen in einer Primfaktorzerlegung sind im Allgemeinen nicht verschieden:

$$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$$

Es ist üblich (wenn möglich), die Primzahlen der Größe nach zu ordnen und Potenzschreibweise zu benutzen:

$$2^3 \cdot 3^2 \cdot 5 \cdot 11^2 = 42.560$$

$\Rightarrow$  normierte Primfaktorzerlegung!

**Schreibweise für Primfaktorzerlegungen:**

$$a = \prod_{i=1}^{\infty} p_i^{n_i}$$

meint ein Produkt, das formal über alle Primzahlen  $p_i$ , mit

$$p_1 < p_2 < p_3 < \cdots$$

läuft, beim dem aber nur endlich viele der natürlichen Zahlen  $n_i \neq 0$  sind.

Damit handelt es sich also um ein endliches Produkt! z.B.:

$$12 = 2^2 \cdot 3 = \prod_{i=1}^{\infty} p_i^{n_i} = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdots \quad \text{alle } n_i = 0 \text{ für } i \geq 3$$



Oft schreibt man aber auch direkt:

$$a = \prod_{i=1}^s p_i^{n_i}$$

Ob als obere Grenze  $\infty$  oder  $s$  geschrieben wird, hängt vom Zusammenhang ab. In beiden Fällen ist das Produkt aber immer endlich!

### 3.7. Folgerungen aus dem Hauptsatz.

**Satz 3.17** (Teilbarkeitskriterium). Für natürliche Zahlen  $a, b$  mit PFZ:

$a = \prod_{i=1}^{\infty} p_i^{n_i}$  und  $b = \prod_{i=1}^{\infty} p_i^{m_i}$  gilt:

$$a|b \quad \Leftrightarrow \quad n_i \leq m_i \quad \forall i \in \mathbb{N}$$

**Beweis:**

” $\Rightarrow$ ”:

Es gibt  $c \in \mathbb{N}$  mit  $a \cdot c = b$ .

PFZ:  $c = \prod_{i=1}^{\infty} p_i^{k_i}$  mit  $k_i \geq 0$

$$\Rightarrow \quad a \cdot c = \prod_{i=1}^{\infty} p_i^{n_i} \cdot \prod_{i=1}^{\infty} p_i^{k_i} = \prod_{i=1}^{\infty} p_i^{n_i+k_i} \stackrel{!}{=} \prod_{i=1}^{\infty} p_i^{m_i} = b$$

Aus der Eindeutigkeit der PFZ folgt die Gleichheit der Exponenten:

$$\begin{array}{ccc} n_i & \leq & n_i + k_i = m_i \quad \forall i \quad \checkmark \\ \uparrow & & \\ k_i \geq 0 & & \end{array}$$

” $\Leftarrow$ ”

$$n_i \leq m_i \quad \forall i \quad \Leftrightarrow \quad k_i := m_i - n_i \geq 0 \quad \forall i$$

dabei sind nur endlich viele  $k_i \neq 0$ , weil das für  $n_i$  und  $m_i$  gilt.

Sei  $c := \prod_{i=1}^{\infty} p_i^{k_i}$

$$\Rightarrow \quad a \cdot c = b \quad \Rightarrow \quad a|b$$

□

**Korollar 3.18.** Jeder Teiler  $a$  von  $b = \prod_{i=1}^s p_i^{m_i}$  ist von der Form:

$$a = \prod_{i=1}^s p_i^{n_i} \quad \text{mit} \quad 0 \leq n_i \leq m_i \quad \forall i$$

**Satz 3.19.** Die Anzahl der Teiler der natürlichen Zahl  $a = p_1^{m_1} \cdots p_s^{m_s}$  lautet:

$$\#T_a = (m_1 + 1) \cdots (m_s + 1)$$



**Beispiel**  $a = 70 = 2 \cdot 5 \cdot 7$  muß nach Satz 3.19  $2 \cdot 2 \cdot 2 = 8$  Teiler haben:

$$T_{70} = \{1, 2, 5, 7, 10, 14, 35, 70\}$$

$$\begin{array}{ccccccc} & & & & \uparrow & \uparrow & \uparrow & \uparrow \\ & & & & 2 \cdot 5 & 2 \cdot 7 & 5 \cdot 7 & 2 \cdot 5 \cdot 7 \end{array}$$

$$a = 108 = 4 \cdot 27 = 2^2 \cdot 3^3 \Rightarrow \#T_{108} = (2+1) \cdot (3+1) = 12$$

$$T_{108} = \{1, 2, 3, \underbrace{4, 6, 9}_{2 \text{ Faktoren}}, \underbrace{12, 18, 27}_{3 \text{ Faktoren}}, \underbrace{36, 54}_{4 \text{ Faktoren}}, \underbrace{108}_{5 \text{ Faktoren}}\}$$

**Beweis:**

Es gibt  $m_i + 1$  Zahlen  $0 \leq n_i \leq m_i$ . □

### 3.8. Primzahlkriterium und das Lemma von Euklid.

**Satz 3.20** (Primzahlkriterium). *Eine natürliche Zahl  $p > 1$  ist genau dann eine Primzahl, wenn für alle  $a, b \in \mathbb{N}$  gilt:*

$$\text{Aus } p \mid a \cdot b \text{ folgt } p \mid a \text{ oder } p \mid b \quad (5)$$

**Beweis:**

PZ  $\Rightarrow$  (5):

Sei  $p > 1$  Primzahl und es gelte  $p \mid a \cdot b$

$\Rightarrow p$  kommt in der PFZ von  $a \cdot b$  vor.

Wegen der Eindeutigkeit der PFZ kommt  $p$  in der PFZ von  $a$  oder  $b$  oder von beiden vor.

$\Rightarrow p \mid a$  oder  $p \mid b$ .

(5)  $\Rightarrow$  PZ: Es gelte (5) für  $p$ , d.h. falls  $p \mid a \cdot b$  für irgendwelche  $a, b \in \mathbb{N}$ , so folgt:  $p \mid a$  oder  $p \mid b$

z.Z.:  $p$  ist Primzahl

Wäre  $p$  zusammengesetzte Zahl (nicht PZ)  $\Rightarrow p = a \cdot b$  mit natürlichen Zahlen  $1 < a, b < p$

$$\Rightarrow p \mid a \cdot b \stackrel{(5)}{\Rightarrow} p \mid a \text{ oder } p \mid b \quad \text{Widerspruch zu } a, b < p \quad \square$$

**Bemerkung 3.21.** Das Primzahlkriterium gilt nicht in der Viererwelt  $V$ :  
Gegenbeispiel:

$$4 \text{ ist } V\text{-Primzahl}$$

$$4 \mid 96 = \underbrace{8 \cdot 12}_{\text{Zerlegung in } V}$$

$$\text{aber } 4 \nmid 8 \text{ und } 4 \nmid 12$$

Die Implikation  $\Rightarrow$  vom Primzahlkriterium hat einen Namen:





**Satz 3.22** (Lemma von Euklid).

$$p \text{ Primzahl und } p \mid a \cdot b \Rightarrow p \mid a \text{ oder } p \mid b$$

**Bemerkung 3.23.** Wir haben das Lemma von Euklid (bzw. das Primzahlkriterium) aus dem Hauptsatz der elementaren Zahlentheorie gefolgert. Aber es gilt sogar:

$$\text{Hauptsatz der elementaren Zahlentheorie} \Leftrightarrow \text{Lemma von Euklid}$$

#### 4. GRÖSSTER GEMEINSAMER TEILER ( $ggT$ ) UND KLEINSTES GEMEINSAMES VIELFACHES ( $kgV$ )

##### 4.1. $ggT$ und Teilmengen.

Einführung des  $ggT$  über Teilmengen:

**Beispiel**

$$T_{18} = \{1, 2, 3, 6, 9, 18\}$$

$$T_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

$$T_{18} \cap T_{24} = \{1, 2, 3, 6\} = \{\text{gemeinsame Teiler von 18 und 24}\}$$

$$\stackrel{!}{=} T_6$$

Offenbar ist der Durchschnitt dieser Teilmengen wieder eine Teilermenge. Gilt das auch für die Vereinigung?

$$T_{18} \cup T_{24} = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$$

Das ist offenbar keine Teilermenge, da z. B.  $18 \nmid 24$ .

Wir werden im Folgenden sehen, daß das allgemein so gilt.

**Definition 4.1.** Für zwei natürliche Zahlen  $a$  und  $b$  ist der größte gemeinsame Teiler

$$ggT(a, b)$$

das Maximum der Schnittmenge  $T_a \cap T_b$ .

**Bemerkung 4.1.** (1) Der Name größter gemeinsamer Teiler ist selbsterklärend.

(2) Macht diese Definition Sinn?

Ja! Mit  $T_a$  und  $T_b$  ist auch die Schnittmenge  $T_a \cap T_b$  endlich. Außerdem ist  $T_a \cap T_b \neq \emptyset$ , da  $1 \in T_a \cap T_b$ . Nach dem Maximumsprinzip



(Satz 2.5) hat jede endliche, nichtleere Menge ein größtes Element. Es gibt also immer einen  $ggT$ .

(3) Da  $1 \in T_a$  für alle  $a \in \mathbb{N}$ , gilt:

$$\text{Aus } \#T_a \cap T_b = 1 \Rightarrow \text{folgt } T_a \cap T_b = \{1\}$$

In diesem Fall:  $ggT(a, b) = 1$  und man sagt:  $a$  und  $b$  sind teilerfremd.

(4) Analog läßt sich der  $ggT$  von drei, vier oder mehr natürlichen Zahlen definieren:  $a_1, a_2, \dots, a_s \in \mathbb{N}$ :

$$ggT(a_1, a_2, \dots, a_s) := \text{größtes Element von } T_{a_1} \cap T_{a_2} \cap \dots \cap T_{a_s}$$

(5) Erweiterung des Begriffs auf die ganzen Zahlen:

Seien  $a, b \in \mathbb{Z}$ ,  $(a, b) \neq (0, 0)$  (nicht beide gleichzeitig gleich 0).

Sei " $d$ " die größte ganze Zahl mit  $d|a$  und  $d|b$ . 

Dann heißt/ist  $d = ggT(a, b)$ .

Klar:  $d \in \mathbb{N}$ , denn mit  $d|a$  auch  $-d|a$  und  $\max(\pm d) \in \mathbb{N}$ !

Klar:  $ggT(a, b) = ggT(|a|, |b|)$

Insbesondere:  $ggT \geq 1$ .

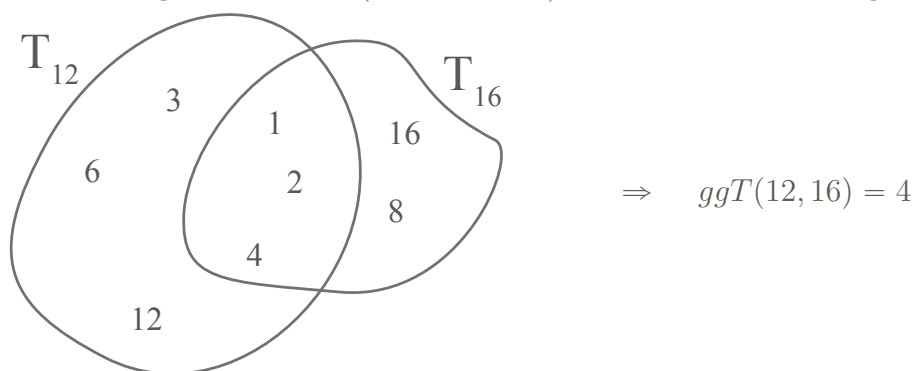
**Satz 4.2.** Für alle  $a, b \in \mathbb{N}$  gilt:

(1)  $ggT(1, a) = 1$

(2) Aus  $a|b$  folgt  $ggT(a, b) = a$  


Wie findet man den  $ggT$ ?

Bei nicht zu großen Zahlen (in der Schule) z.B. mittels Venn-Diagrammen:



**$ggT$  in Schulbüchern:** Hier Aufgabe aus [XQuadrat (5), p.219]:



Miriam besucht ihren Onkel, der ist Fliesenleger. Der muß einen großen rechteckigen Saal der Größe  $252\text{ dm} \times 98\text{ dm}$  mit quadratischen Fliesen einer Größe auslegen. Zur Wahl stehen die Fliesengrößen 

$$15 \times 15 \text{ cm}^2$$

$$25 \times 25 \text{ cm}^2$$

$$35 \times 35 \text{ cm}^2$$

$$40 \times 40 \text{ cm}^2$$

Miriam hilft ihrem Onkel bei der Wahl, weil sie gut rechnen kann.

Dazu gibt es keine weitere Anleitung. Sie als Lehrer müssen sich selber ausdenken, was Sie daraus machen. Was würden Sie machen?

Wie bestimmt man den  $ggT$ ?

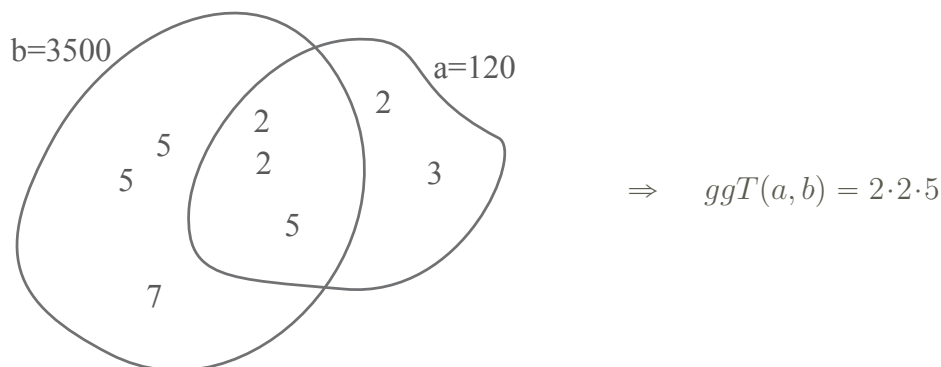
Hilfe: Primfaktorzerlegung:

**Beispiel:**

$$a = 120 = 2 \cdot 60 = 2^2 \cdot 30 = 2^3 \cdot 15 = 2^3 \cdot 3 \cdot 5$$

$$b = 3500 = 35 \cdot 100 = 3 \cdot 7 \cdot 10^2 = 2^2 \cdot 5^3 \cdot 7$$

$$\Rightarrow ggT(a, b) = 2^2 \cdot 5 = 20$$



**Satz 4.3.** Für natürliche Zahlen  $a$  und  $b$  mit Primfaktorzerlegungen

$$a = \prod_{i=1}^{\infty} p_i^{m_i} \quad b = \prod_{i=1}^{\infty} p_i^{n_i} \quad \text{mit} \quad m_i, n_i \in \mathbb{N}$$

ist der größte gemeinsame Teiler: 

$$ggT(a, b) = \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i)}$$

wobei  $\min(m_i, n_i)$  das Minimum der Zahlen  $m_i, n_i$  bezeichnet.



**Beweis:**

Sei  $d := \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i)}$

$$\text{Weil } \left\{ \begin{array}{l} \min(m_i, n_i) \leq m_i \\ \min(m_i, n_i) \leq n_i \end{array} \right. \xRightarrow[\text{(Teilbarkeitskriterium)}]{\text{Satz 3.17}} \left\{ \begin{array}{l} d \mid a \\ d \mid b \end{array} \right.$$

$\Rightarrow d \in T_a \cap T_b$  ist also gemeinsamer Teiler von  $a$  und  $b$ .

Andererseits: für  $c \in T_a \cap T_b$ ,  $c = \prod_{i=1}^{\infty} p_i^{k_i}$  gilt umgekehrt:

$$k_i \leq m_i \quad \text{und} \quad k_i \leq n_i$$

$\Rightarrow k_i \leq \min(m_i, n_i)$  für alle  $i$

$\Rightarrow c \mid d \Rightarrow c \leq d \Rightarrow d$  ist größter gemeinsamer Teiler.  $\square$

**Folgerung:** Für alle  $a, b, n \in \mathbb{N}$  gilt:

$$ggT(n \cdot a, n \cdot b) = n \cdot ggT(a, b)$$

**Spezialfall:** Falls  $a \mid b \Rightarrow ggT(a, b) = a$ .

**Beweis:**

Sei  $a = \prod_{i=1}^{\infty} p_i^{m_i}$ ,  $b = \prod_{i=1}^{\infty} p_i^{n_i}$  und  $n = \prod_{i=1}^{\infty} p_i^{k_i}$ .

Dann gilt  $n \cdot a = \prod_{i=1}^{\infty} p_i^{k_i+m_i}$ ,  $n \cdot b = \prod_{i=1}^{\infty} p_i^{k_i+n_i}$ .

Weil  $\min(k_i + m_i, k_i + n_i) = k_i + \min(m_i, n_i)$  folgt:

$$\begin{aligned} ggT(n \cdot a, n \cdot b) &= \prod_{i=1}^{\infty} p_i^{\min(k_i+m_i, k_i+n_i)} = \prod_{i=1}^{\infty} p_i^{k_i+\min(m_i, n_i)} \\ &= \prod_{i=1}^{\infty} p_i^{k_i} \cdot \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i)} = n \cdot ggT(a, b) \end{aligned}$$

$\square$

**4.2. Euklidischer Algorithmus.**

**Satz 4.4** (Teilen mit Rest). Für natürliche Zahlen  $a, b, b \neq 0$  gibt es eindeutig bestimmte Zahlen  $q, r \in \mathbb{N}_0$ , so daß

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

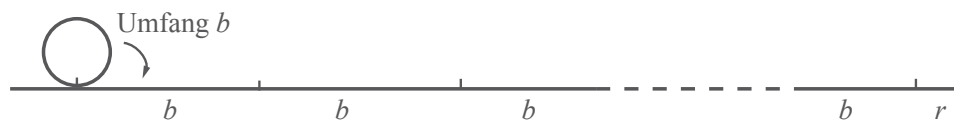
**Beispiele:**

- (1) Sie brauchen mehrere Kabelstücke der gleichen Länge (z.B.  $b = 3$ ). Dazu kaufen Sie eine Kabelrolle mit  $a = 20$  m Kabel. Wieviele Kabelstücke bekommen Sie daraus und wie lang ist der Rest?



$$\begin{array}{ccccccc} 20 & = & 6 & \cdot & 3 & + & 2 \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ a & & q & & b & & r \end{array}$$

(2) Rad abrollen



Wieviele ganze Umdrehungen passen auf eine Strecke der Länge  $a$ , wie groß ist das Reststück  $r$ ?

**Beweis:**

$$V := \{s \cdot b \mid s \cdot b \leq a, s \in \mathbb{N}_0\} = \{n \in \mathbb{N}_0 \mid n \leq a, b \mid n\}$$

sei die Menge aller Vielfachen von  $b$  kleiner gleich  $a$ .

$$0 \in V \Rightarrow V \neq \emptyset$$

$$\text{Klar: } \#V \leq a + 1 < \infty \quad \text{da } V \subset \{0, 1, 2, \dots, a\}$$

(im Fall  $b = 1 \Rightarrow V = \{0, 1, 2, \dots, a\}$ )

Sei  $q \cdot b \in V$  das größte Element.

$$\begin{aligned} \Rightarrow & \quad q \cdot b \leq a < (q+1) \cdot b \\ \Rightarrow & \quad 0 = q \cdot b - q \cdot b \leq \underbrace{a - q \cdot b}_{=: r} < (q+1) \cdot b - q \cdot b = b \\ \Rightarrow & \quad 0 \leq r < b \\ \text{und} & \quad a = q \cdot b + r \end{aligned}$$

Damit ist die **Existenz** von  $q$  und  $r$  nachgewiesen.

**Eindeutigkeit:**

Angenommen es gibt ein zweites solches Paar  $(q', r')$

$$\Rightarrow a = q \cdot b + r = q' \cdot b + r'$$

$$\text{Falls } r = r': \Rightarrow q \cdot b = q' \cdot b \Rightarrow q = q' \quad (\text{da } b \neq 0)$$

$$\text{Falls } r \neq r': \text{ OE } r < r'$$

$$\Rightarrow$$

$$\begin{aligned} 0 &< r' - r &\leq r' &< b \\ 0 &< (a - q'b) - (a - qb) &< b \\ 0 &< qb - q'b &= (q - q')b &< b \\ 0 &< q - q' &\text{ und } q - q' &< 1 \quad \nexists \end{aligned}$$

denn  $q - q'$  ist eine ganze Zahl!

□

Teilen mit Rest gilt auch für negative Zahlen  $a$ :



**Korollar 4.5.** Für ganze Zahlen  $a \in \mathbb{Z}$  und  $b \geq 1$  gibt es eindeutig bestimmte Zahlen  $q, r \in \mathbb{Z}$ , so daß

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

**Beweis:**

Es reicht, den Fall  $a < 0$  zu betrachten: Für  $-a = |a| > 0$  gilt nach Satz 4.4:

$$-a = q' \cdot b + r' \quad \text{mit eindeutigen} \quad 0 \leq r' < b \quad \text{und} \quad q' \in \mathbb{N}.$$

Wenn  $r' = 0$ , dann

$$a = -q' \cdot b = \underbrace{(-q')}_{=:q} \cdot b + \underbrace{0}_{=:r} \quad \checkmark$$

Sonst gilt

$$a = -q' \cdot b - r' = -q' \cdot b - b + b - r' = \underbrace{(-q' - 1)}_{=:q} \cdot b + \underbrace{(b - r')}_{=:r}$$

Klar, wegen  $0 \leq r' < b \Leftrightarrow 0 < b - r' = r < b$  □

Der Satz liefert eine Methode, den  $ggT$  und alle anderen gemeinsamen Teiler ohne PFZ zu finden:

**Beispiel:**  $a = 564, \quad b = 80$

Division mit Rest:  $564 = 7 \cdot 80 + 4$

Sei  $t \in T_{564} \cap T_{80}$  ein beliebiger Teiler

$$\Rightarrow t|564 \text{ und } t|80 \Rightarrow t|(564 - 7 \cdot 80) = 4$$

$$\Rightarrow t|4 \Leftrightarrow t \in T_4 \Rightarrow t \in T_{80} \cap T_4$$

$$\Rightarrow T_{564} \cap T_{80} \subseteq T_{80} \cap T_4 \stackrel{\substack{\uparrow \\ \text{da } T_4 \subseteq T_{80}}}{=} T_4 = \{1, 2, 4\} \quad (*)$$

Die Mengen sind sogar gleich:

$$s \in T_{80} \cap T_4 = T_4$$

$$\text{aus } 564 = 7 \cdot 80 + 4 \Rightarrow s|564$$

$$\Rightarrow T_{80} \cap T_4 \subseteq T_{564}$$

$$\text{klar } T_{80} \cap T_4 \subseteq T_{80}$$

$$\Rightarrow T_{80} \cap T_4 \subseteq T_{564} \cap T_{80}$$

$$\text{aus } (*) \Rightarrow T_{564} \cap T_{80} = T_{80} \cap T_4 = T_4 = \{1, 2, 4\}$$

$$\Rightarrow ggT(564, 80) = 4$$



**Satz 4.6.** Seien  $a, b \in \mathbb{N}$  und  $a = q \cdot b + r$  mit  $q, r \in \mathbb{N}$  und  $0 \leq r < b$ . Dann gilt

$$T_a \cap T_b = T_b \cap T_r$$

**Beweis:**

" $\subseteq$ " Sei  $t \in T_a \cap T_b$

$$\text{Aus } \begin{array}{ccc} a & - & q \cdot b = r \\ \uparrow & & \uparrow \\ t|a & & t|b \end{array} \Rightarrow t|r \Rightarrow t \in T_b \cap T_r$$

" $\supseteq$ " Sei  $s \in T_b \cap T_r$

$$\text{Aus } a = q \cdot b + r \Rightarrow s|a \Rightarrow s \in T_a \cap T_b$$

Folgerung für den  $ggT$ :

**Korollar 4.7.** Für natürliche Zahlen  $a, b$  mit  $a = q \cdot b + r$ ,  $0 \leq r < b$  gilt:

$$ggT(a, b) = ggT(b, r) = ggT(b, a - q \cdot b)$$

**Beispiel:**

$$\begin{aligned} ggT(582, 72) &= ggT(72, 6) & \text{NR: } 582 &= 8 \cdot 72 + 6 \\ &= 6 & 72 &= 12 \cdot 6 \Rightarrow 6|72 \end{aligned}$$

**Satz 4.8** (Euklidischer Algorithmus). Seien  $a, b \in \mathbb{N}$  mit  $a > b$ . Induktiv werde die Division mit Rest durchgeführt:

$$\begin{aligned} \text{Schritt 1} \quad a &= q_1 \cdot b + r_1 \quad \text{mit} \quad 0 \leq r_1 < b \\ \text{Schritt 2} \quad b &= q_2 \cdot r_1 + r_2 \quad \text{mit} \quad 0 \leq r_2 < r_1 \\ \text{Schritt 3} \quad r_1 &= q_3 \cdot r_2 + r_3 \quad \text{mit} \quad 0 \leq r_3 < r_2 \\ &\vdots \\ \text{Schritt } k \quad r_{k-2} &= q_k \cdot r_{k-1} + r_k \quad \text{mit} \quad 0 \leq r_k < r_{k-1} \\ &\vdots \end{aligned}$$

Es gibt einen kleinsten Rest  $\neq 0$ :  $r_n := \min\{r_1, r_2, \dots\}$ , d.h.:

$$\begin{aligned} r_{n-2} &= q_n \cdot r_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} \cdot r_n + 0 \end{aligned}$$

Der Algorithmus bricht also am Schritt  $n+1$  ab ( $r_{n+1} = 0$ ). Insbesondere gilt:

$$T_a \cap T_b = T_{r_n} \quad \text{und} \quad ggT(a, b) = r_n$$



**Beweis:**

Aus Satz 4.4 (Teilen mit Rest) folgt:  $r_1 > r_2 > r_3 > \dots \geq 0$ .

Darum muß irgendwann 0 erreicht werden, sei  $r_n \neq 0$  und  $r_{n+1} = 0$ :

$$\begin{aligned}
 r_{n-1} &= q_{n+1} \cdot r_n + \underbrace{r_{n+1}}_{=0} \\
 \Rightarrow \quad T_a \cap T_b &\stackrel{\text{Satz 4.6}}{=} T_b \cap T_{r_1} & (a = q_1 b + r_1) \\
 &= T_{r_1} \cap T_{r_2} & (b = q_2 r_1 + r_2) \\
 &\vdots \\
 &= T_{r_n} \cap \underbrace{T_{r_{n+1}}}_{=T_0=\mathbb{N}} = T_{r_n} \\
 \Rightarrow \quad ggT(a, b) &= \max(T_{r_n}) = r_n
 \end{aligned}$$

□

**Beispiele**

1)  $a = 1008$  und  $b = 840$

$$1008 = 1 \cdot 840 + 168 \quad (r_1 = 168)$$

$$840 = 5 \cdot 168 + 0 \quad (r_2 = 0)$$

$$ggT(1008, 840) = 168$$

2)  $a = 2940$  und  $b = 1617$

$$2940 = 1 \cdot 1617 + 1323 \quad (r_1 = 1323)$$

$$1617 = 1 \cdot 1323 + 294 \quad (r_2 = 294)$$

$$1323 = 4 \cdot 294 + 147 \quad (r_3 = 147)$$

$$294 = 2 \cdot 147 \quad (\Rightarrow r_4 = 0)$$

$$\Rightarrow \quad ggT(\underbrace{2940}_{20 \cdot 147}, \underbrace{1617}_{11 \cdot 147}) = 147$$

Nun werden auch die Teilmengen-Beziehungen klarer:

**Korollar 4.9.** Für natürliche Zahlen  $a, b$  gilt:  $T_a \cap T_b = T_{ggT(a,b)}$

**Beweis:**

Konsequenz aus dem Euklidischen Algorithmus:

$$T_a \cap T_b = T_{r_n} \quad \begin{array}{c} \stackrel{=}{\uparrow} \\ ggT(a,b)=r_n \end{array} \quad T_{ggT(a,b)}$$







Für Schüler:

**Korollar 4.10.** Jeder Teiler von  $a$  und  $b$  ist auch Teiler von  $ggT(a, b)$ .

$ggT$  von mehr als zwei Zahlen:

**Korollar 4.11.** Für  $a, b, c \in \mathbb{N}$  gilt:

$$ggT(a, b, c) = ggT(ggT(a, b), c)$$



**Beweis:**

Sei  $t$  Teiler von  $a, b$  und  $c$ :

$$\left. \begin{array}{l} t \mid a \\ t \mid b \\ t \mid c \end{array} \right\} \Rightarrow t \mid ggT(a, b) \left. \right\} \Rightarrow t \mid ggT(ggT(a, b), c)$$



**Beispiel**

$$ggT(3792, 5640, 5274) = \dots = ggT(24, 5274) = \dots = 6$$

NR mit TR:

$$\left. \begin{array}{rcl} 5640 & = & 1 \cdot 3792 + 1848 \\ 3792 & = & 2 \cdot 1848 + 96 \\ 1848 & = & 19 \cdot 96 + 24 \\ 96 & = & 4 \cdot 24 + 0 \end{array} \right\} \Rightarrow ggT(3792, 5640) = 24$$

$$\left. \begin{array}{rcl} 5274 & = & 219 \cdot 24 + 18 \\ 24 & = & 1 \cdot 18 + 6 \\ 18 & = & 3 \cdot 6 + 0 \end{array} \right\} \Rightarrow ggT(5274, 24) = 6$$

### 4.3. Vielfache des $ggT$ und Linearkombinationen.

**Ziel:** Den  $ggT$  als Linearkombination darstellen, zum Beispiel:

$$\begin{aligned} ggT(24, 16) &= 8 = 1 \cdot 24 - 1 \cdot 16 \\ ggT(48, 9) &= 3 = 1 \cdot 48 - 5 \cdot 9 \\ ggT(2940, 1617) &= 147 = ??? \end{aligned}$$

**Satz 4.12.** Für  $a, b \in \mathbb{N}$  gibt es ganze Zahlen  $x$  und  $y$  mit:

$$ggT(a, b) = x \cdot a + y \cdot b$$

**Beweis:**

Benutze den Euklidischen Algorithmus: falls  $a > b$ :

$$\begin{aligned} a &= q_1 \cdot b + r_1 & \Rightarrow & \quad r_1 = a - q_1 \cdot b \\ b &= q_2 \cdot r_1 + r_2 & \Rightarrow & \quad r_2 = b - q_2 \cdot r_1 = b - q_2(a - q_1 \cdot b) = -q_2 \cdot a + (q_1 q_2 + 1)b \\ r_1 &= q_3 \cdot r_2 + r_3 & \Rightarrow & \quad r_3 = \underbrace{r_1 - q_3 \cdot r_2}_{\text{LK von } a, b} \\ & & & \quad \quad \quad \uparrow \quad \quad \quad \uparrow \\ & & & \quad \text{LK von } a, b \quad \Rightarrow \quad \text{LK von } a, b \\ & & & \quad \quad \quad \text{LK von } a, b \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n & \Rightarrow & \quad r_n = \underbrace{r_{n-2} - q_n \cdot r_{n-1}}_{\text{LK von } a, b} \\ & & & \quad \quad \quad \uparrow \quad \quad \quad \uparrow \\ & & & \quad ggT \quad \quad \quad \text{LK von } a, b \quad \Rightarrow \quad \text{LK von } a, b \\ & & & \quad \quad \quad \text{LK von } a, b \end{aligned}$$

□

**Bemerkung 4.13.** (1) Satz 4.12 ist eine reine Existenzaussage bzgl.  $x$  und  $y$ , so daß  $ggT(a, b) = xa + yb$ . Diese  $\mathbb{Z}$ -Linearkombination ist nicht eindeutig:

$$\text{z.B.:} \quad ggT(3, 6) = 3 = (-1) \cdot 3 + 1 \cdot 6 = (-3) \cdot 3 + 2 \cdot 6$$

Klar:  $a \cdot x + b \cdot y = \underbrace{ggT(a, b)}_c$  ist eine affine Geradengleichung: jeder Schnittpunkt dieser Geraden mit dem Gitter  $\mathbb{Z}^2$  ergibt eine  $\mathbb{Z}$ -Linearkombination.

(2) Den Satz kann man auf mehr als zwei Zahlen erweitern.

(3) Der Beweis des Satzes ist konstruktiv:

Beispiel:

(vgl. Beispiel oben)

$$ggT(2940, 1617) = 147 = 5 \cdot 2940 - 9 \cdot 1617$$



$$(1) \quad 2940 = 1 \cdot 1617 + 1323$$

$$(2) \quad 1617 = 1 \cdot 1323 + 294$$

$$(3) \quad 1323 = 4 \cdot 294 + 147$$

$$(4) \quad 294 = 2 \cdot 147$$

$$\Rightarrow \quad 147 = 1323 - 4 \cdot 294 \quad (\text{mit (3)})$$

$$= 1323 - 4 \cdot (1617 - 1323) = 5 \cdot 1323 - 4 \cdot 1617 \quad (\text{mit (2)})$$

$$= 5 \cdot (2940 - 1617) - 4 \cdot 1617 \quad (\text{mit (1)})$$

$$= 5 \cdot 2940 - 9 \cdot 1617 \stackrel{\substack{TR \\ \text{Probe}}}{=} 147$$

Sei  $ggT(a, b) = x \cdot a + y \cdot b$  mit  $a, b \in \mathbb{N}, x, y \in \mathbb{Z}$

Dann gilt für alle  $z \in \mathbb{Z}$ :  $z \cdot ggT(a, b) = z \cdot x \cdot a + z \cdot y \cdot b$

D.h. alle Vielfachen von  $ggT(a, b)$  sind auch  $\mathbb{Z}$ -Linearkombinationen von  $a$  und  $b$ . Das gilt auch umgekehrt:

**Satz 4.14.** Jede ganzzahlige Linearkombination von  $a$  und  $b$  ( $a, b \in \mathbb{N}$ ) ist ein  $\mathbb{Z}$ -Vielfaches von  $ggT(a, b)$ , d.h. für alle  $x, y \in \mathbb{Z}$  gibt es ein  $z \in \mathbb{Z}$ , so daß

$$x \cdot a + y \cdot b = z \cdot ggT(a, b)$$

**Beweis:**

Betrachte  $x \cdot a + y \cdot b$  mit  $x, y \in \mathbb{Z}$  beliebig.

Aus  $ggT(a, b) \mid a$  und  $ggT(a, b) \mid b \Rightarrow ggT(a, b) \mid x \cdot a + y \cdot b. \Rightarrow \text{Beh.}$

□

**Satz 4.15.** Für alle natürlichen Zahlen  $a, b$  gibt es ganze Zahlen  $x, y$ , so daß

$$ggT(a, b) = x \cdot a + y \cdot b$$

Hierbei ist  $ggT(a, b)$  die kleinste natürliche Zahl, die sich als  $\mathbb{Z}$ -Linearkombination von  $a$  und  $b$  darstellen läßt. Eine ganze Zahl  $c$  ist genau dann  $\mathbb{Z}$ -Linearkombination von  $a$  und  $b$ , wenn  $c$  Vielfaches/ $\mathbb{Z}$  von  $ggT(a, b)$  ist.

**Beispiel:**

$$ggT(3792, 5640) = 24$$

$\Rightarrow$  es gibt  $x, y \in \mathbb{Z}$  mit  $x \cdot 3792 + y \cdot 5640 = 24$

Aber

$x \cdot 3792 + y \cdot 5640 = \begin{matrix} 25 \\ \text{oder 26 oder 27...} \end{matrix}$  ist über  $\mathbb{Z}$  nicht lösbar.



Spezialfall:  $a$  und  $b$  sind teilerfremd:



**Satz 4.16.** Aus teilerfremden natürlichen Zahlen  $a$  und  $b$  (also  $\text{ggT}(a, b) = 1$ ) läßt sich jede ganze Zahl linearkombinieren, d.h. für alle  $z \in \mathbb{Z}$  gibt es  $x, y \in \mathbb{Z}$  mit

$$x \cdot a + y \cdot b = z$$

**Beispiel:**

$$\begin{aligned} \text{ggT}(5, 3) &= 1 \quad \text{und} \quad 2 \cdot 5 - 3 \cdot 3 = 1 \\ \text{für } z \in \mathbb{Z} \text{ beliebig: } (2z) \cdot 5 - (3z) \cdot 3 &= z \quad !! \end{aligned}$$

#### 4.4. Lineare Diophantische Gleichungen.

(Diophant von Alexandria, ca 250 n. Chr.)

**Beispiel:**

Eine Firma will für 1000 € zwei Sorten von Werbegeschenken kaufen:

Sorte 1: 13,00 € pro Stk.

Sorte 2: 19,00 € pro Stk.

Wieviele Geschenke können damit von jeder Sorte gekauft werden?

**Definition 4.2.** Eine Gleichung  $ax + by = c$  mit  $a, b \in \mathbb{N}$  und  $c \in \mathbb{Z}$  heißt lineare Diophantische Gleichung mit zwei Variablen, falls man als Lösungen nur Elemente  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$  zuläßt.

**Allgemeiner:** Eine Diophantische Gleichung ist eine Gleichung der Form:

$$F(x_1, \dots, x_n) = 0 \tag{6}$$

mit einem Polynom  $F \in \mathbb{Z}[x_1, \dots, x_n]$  und der Frage der Lösbarkeit von (6) über  $\mathbb{Z}$ .

Umformulierung von Satz 4.15 :

**Satz 4.17.** Die lineare diophantische Gleichung  $ax + by = c$  ist genau dann lösbar, wenn  $\text{ggT}(a, b) \mid c$ .

**Beispiel**

Wegen  $\text{ggT}(13, 19) = 1 \Rightarrow x \cdot 13 + y \cdot 19 = 1000$  ist lösbar über  $\mathbb{Z}!!$

Mit Euklidischem Algorithmus:



$$\begin{aligned}
19 &= 1 \cdot 13 + 6 && \Leftrightarrow && \textcolor{red}{6} = 19 - 1 \cdot 13 \\
13 &= 2 \cdot 6 + 1 && \Leftrightarrow && 1 = 13 - 2 \cdot \textcolor{red}{6} \\
6 &= 1 \cdot 6 && && = 13 - 2(\textcolor{red}{19} - \textcolor{red}{13}) = \underline{3} \cdot 13 - \underline{2} \cdot 19
\end{aligned}$$

Also  $(x, y) = (3, -2)$  ist Lösung von  $13x + 19y = 1$ .

$\Rightarrow (3000, -2000)$  ist Lösung von  $13x + 19y = 1000$

$\Rightarrow$  Lösung unbrauchbar - weil eine Zahl negativ!!!

Gibt es Lösungen über  $\mathbb{N}$ ???

Wie finden wir Lösungen über  $\mathbb{N}$ ???

### Ein bisschen Geometrie:

$13x + 19y = 1000$  Geradengleichung!!

Notwendige Voraussetzung für Lösungen über  $\mathbb{N}$ : Gerade muß durch den ersten Quadranten laufen.

Dazu: wie/wo liegt diese Gerade: *Realschule 8te Klasse*: Geraden  $y = mx + t$

Hier:

$$\begin{aligned}
y &= -\frac{13}{19} \cdot x + \frac{1000}{19} && , && t = \frac{1000}{19} \approx 52,63 \\
&&& && m = -\frac{13}{19} \Rightarrow \text{fallend}
\end{aligned}$$

$$\begin{aligned}
\text{Nullstelle: } y = 0 &&& \Rightarrow && 13x + 19 \cdot 0 = 1000 \\
&&& && x = \frac{1000}{13} \approx 76,92
\end{aligned}$$

Wenn es eine Lösung  $(x, y) \in \mathbb{N} \times \mathbb{N}$  gibt, dann:

$$0 \leq x \leq 76, \quad 0 \leq y \leq 52$$

Lösungen z.B. empirisch mit Geogebra suchen:



$$\begin{aligned}
74 \cdot 13 + 2 \cdot 19 &= 1000 && \Rightarrow (74, 2) \\
55 \cdot 13 + 15 \cdot 19 &= 1000 && \Rightarrow (55, 15) \\
36 \cdot 13 + 28 \cdot 19 &= 1000 && \Rightarrow (36, 28)
\end{aligned}$$

Aus einer Lösung auf alle Lösungen schließen:

**Satz 4.18.** Sei  $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$  eine Lösung der diophantischen Gleichung  $ax + by = c$  mit teilerfremden natürlichen Zahlen  $a$  und  $b$ , dann ist jede weitere Lösung von der Form:

$$(x_0 + t \cdot b, y_0 - t \cdot a) \quad \text{mit } t \in \mathbb{Z}$$

**Bemerkung:**

Was, wenn  $a, b$  nicht teilerfremd sind?

Also sei  $ggT(a, b) \neq 1$ !

Wenn  $ax + by = c$  eine Lösung/ $\mathbb{Z}$  hat, dann  $\stackrel{4.17}{\Rightarrow} ggT(a, b) \mid c$ .

$$\Rightarrow \quad a' := \frac{a}{ggT(a, b)}, \quad b' := \frac{b}{ggT(a, b)}, \quad c' := \frac{c}{ggT(a, b)} \in \mathbb{Z}$$

$\Rightarrow \quad ax + by = c$  ist äquivalent zu  $a'x + b'y = c'$  (hat damit die gleichen Lösungen) und das ist eine lineare diophantische Gleichung mit  $a', b'$  teilerfremd,

$\Rightarrow$  mit einer Lösung  $(x_0, y_0)$  sind alle weiteren Lösungen:

$$(x_0 + t \cdot b', y_0 - t \cdot a')$$

**Beweis:**

**Geometrisch:**

$ax + by = c$  ist eine Gerade  $G$  und  $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \in \mathbb{Z}^2$  ein Punkt auf  $G$ :  $\Rightarrow \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \in G \cap \mathbb{Z}^2$

Analytische Geometrie:

$$\text{Parallele Gerade durch Null: } 0 = ax + by = \begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \text{ ist Punkt auf } G: \quad ax_0 + by_0 = c = \begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

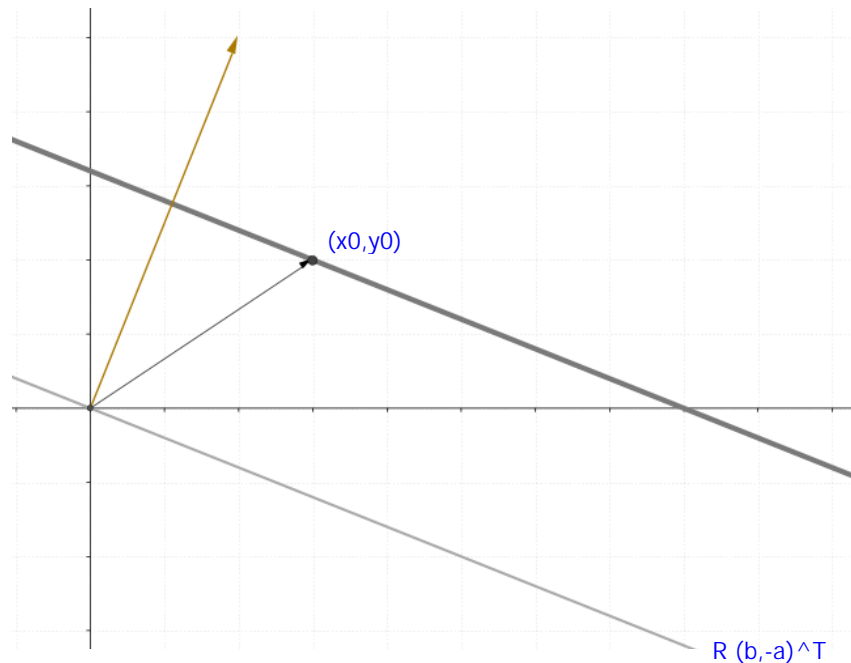
$$\text{Geradengleichung von } G: \quad \begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = c = \begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

$$\Leftrightarrow \quad \begin{pmatrix} a \\ b \end{pmatrix} \cdot \left[ \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \right] = 0$$



$\Rightarrow G$  ist die affine Gerade (orthogonal)  $\perp$  zu  $\underbrace{\begin{pmatrix} a \\ b \end{pmatrix}}_{\mathbb{R} \cdot \begin{pmatrix} b \\ -a \end{pmatrix}}$  und durch den Punkt  $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$

**Beweis:**



Darstellungsweisen der diophantischen Gleichung:

(I, algebraisch):  $ax + by = c$

(II, anal. Geom., Hessesnormalform):

$\{p \in \mathbb{R}^2 \mid \langle (a,b), p \rangle = c\}$

Hyperebene orthogonal zu  $(a,b)$  mit Abstand  $c/|(a,b)|$ .

(III, anal. Geom., parametr. Form):  
mit  $(x_0, y_0)$  Partikularlösung:

$(x_0, y_0) + \mathbb{R}(b, -a)$

$$\begin{aligned} \left\{ \mathbb{R} \begin{pmatrix} b \\ -a \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \right\} \cap \mathbb{Z} \times \mathbb{Z} &= \left\{ \mathbb{Z} \cdot \begin{pmatrix} b \\ -a \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \right\} && (\text{da } a, b, x_0, y_0 \in \mathbb{Z}) \\ &= \left\{ \begin{pmatrix} t \cdot b + x_0 \\ -t \cdot a + y_0 \end{pmatrix} \mid t \in \mathbb{Z} \right\} \end{aligned}$$

**Algebraischer Beweis:**

1) Z.z.:  $(x_0 + tb, y_0 - ta)$  ist für alle  $t \in \mathbb{R}$  eine Lösung!

Überprüfen durch Einsetzen:

$$a(x_0 + tb) + b(y_0 - ta) = \underbrace{ax_0 + by_0}_{=c} + \underbrace{t(ab - ba)}_{=0} = c$$

2) Z.z.: Es gibt keine weitere Lösungen  $\Leftrightarrow$  alle Lösungen sind von der vorgegebenen Form:

Sei also  $(x_1, y_1)$  eine weitere Lösung

$$\Rightarrow ax_1 + by_1 = c$$

Weiterhin gilt aber:  $ax_0 + by_0 = c$



Subtraktion:

$$a(x_1 - x_0) + b(y_1 - y_0) = 0$$

$$a(x_1 - x_0) = b(y_0 - y_1) \quad (*)$$

$$\text{ggT}(a, b) = 1 \Rightarrow a \mid (y_0 - y_1) \Rightarrow a \cdot t = y_0 - y_1$$

$$\Rightarrow y_1 = y_0 - at$$

$$\text{aus } (*) \text{ folgt au\ss erdem: } a(x_1 - x_0) = b \cdot a \cdot t \quad \mid \cdot \frac{1}{a}$$

$$\Leftrightarrow x_1 - x_0 = b \cdot t$$

$$\Leftrightarrow x_1 = x_0 + b \cdot t$$

□

**Zurück zum Werbegeschenk-Beispiel:**

Wir hatten die unbrauchbare Lösung:

$$(3000, -2000) = (x_0, y_0) \text{ von } 13x + 19y = 1000$$

Jede Lösung ist von der Form:

$$(3000 + t \cdot 19, -2000 - t \cdot 13), \quad t \in \mathbb{Z}$$

Damit  $x, y \geq 0$  muß gelten:

$$0 \leq 3000 + t \cdot 19 \Leftrightarrow -3000 \leq 19 \cdot t \Leftrightarrow \underbrace{-\frac{3000}{19}}_{\approx -157,89} \leq t \Leftrightarrow -157 \leq t$$

$$0 \leq -2000 - t \cdot 13 \Leftrightarrow 13 \cdot t \leq -2000 \Leftrightarrow t \leq \underbrace{-\frac{2000}{13}}_{\approx -153,85} \Leftrightarrow t \leq -154$$

$$\Rightarrow -157 \leq t \leq -154 \Rightarrow t = -157, -156, -155, -154$$

$$t = -157 \Rightarrow (3000 - 157 \cdot 19, -2000 + 157 \cdot 13) = (17, 41)$$

$$t = -156 \Rightarrow (3000 - 156 \cdot 19, -2000 + 156 \cdot 13) = (36, 28)$$

$$t = -155 \Rightarrow (3000 - 155 \cdot 19, -2000 + 155 \cdot 13) = (55, 15)$$

$$t = -154 \Rightarrow (3000 - 154 \cdot 19, -2000 + 154 \cdot 13) = (74, 2)$$

Nun wissen wir, daß das alle Lösungen sind.





4.5.  $kgV$  und Vielfachenmengen.

**Definition 4.3.** Für  $a \in \mathbb{N} \setminus \{0\}$  ist die Vielfachenmenge von  $a$  die Menge:

$$V_a = \{ x \in \mathbb{N} \setminus \{0\} \mid a \mid x \}$$



**Beispiel:**

$$V_1 = \{1, 2, 3, \dots\} = \mathbb{N}$$

$$V_2 = \{2, 4, 6, \dots\} = 2\mathbb{N} \quad (\text{Menge der Geraden Zahlen})$$

$$V_3 = \{3, 6, 9, \dots\} \quad (\text{Vielfache von 3})$$

**Bemerkung**

Vielfachenmengen haben stets  $\infty$ -viele Elemente:

$$\#V_a = \infty$$

Dagegen sind die Teilmengen  $T_a$  stets endlich.

**Beispiele**

$$\begin{aligned} V_2 &= \{2, 4, 6, 8, 10, 12, \dots\} & V_3 &= \{3, 6, 9, 12, \dots\} \\ \Rightarrow V_2 \cap V_3 &= \underbrace{\{6, 12, 18, \dots\}}_{\text{gemeinsame Vielfache von 2 und 3}} \end{aligned}$$

**Definition 4.4.** Für  $a, b \in \mathbb{N}$  heißen die Elemente der Schnittmenge

$$V_a \cap V_b = \{ x \in \mathbb{N} \setminus \{0\} \mid a \mid x \text{ und } b \mid x \}$$

gemeinsame Vielfache von  $a$  und  $b$ . Das kleinste Element von  $V_a \cap V_b$  heißt kleinstes gemeinsames Vielfaches:  $kgV(a, b)$ .

**Bemerkungen**

- (1) Zu  $a$  und  $b \in \mathbb{N}$  gibt es immer gemeinsame Vielfache, d.h.  $V_a \cap V_b \neq \emptyset$ , denn

$$a \cdot b \in V_a \cap V_b \quad \Rightarrow \quad V_{a \cdot b} \subseteq V_a \cap V_b \quad (7)$$

Es gibt also sogar  $\infty$ -viele gemeinsame Vielfache.

- (2) Folgerung (7) folgt aus:

$$\text{Aus } v \in V_a \cap V_b \text{ folgt } V_v \subseteq V_a \cap V_b$$

**Denn:** wenn  $v \in V_a \cap V_b$ , gilt 1):  $a \mid v$  und  $b \mid v$ , und 2) gilt für  $x \in V_v$ , daß  $v \mid x$ . Transitivität der Teilerrelation impliziert, daß auch:  $a \mid x$  und  $b \mid x$ . Damit  $x \in V_a \cap V_b$  □



(3) Verallgemeinerung auf drei oder mehr Zahlen: für  $a, b, c, \dots \in \mathbb{N}$  gilt:

$$kgV(a, b, c, \dots) = \min(V_a \cap V_b \cap V_c \cap \dots)$$

**Bsp.:**

$$a = 6, \quad b = 8, \quad c = 15$$

$$V_6 = \{6, 12, 18, \underline{24}, 30, \dots\}$$

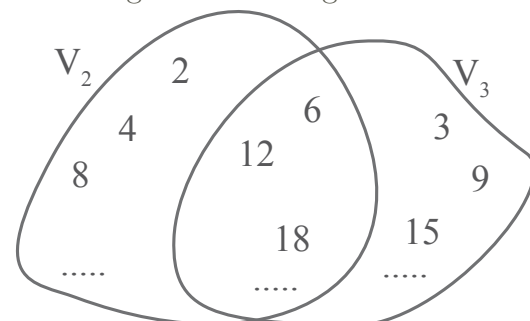
$$V_8 = \{8, 16, \underline{24}, 32, \dots\}$$

$$V_{15} = \{15, 30, 45, 60, 75, 90, 105, \underline{120}, \dots\} \quad (120 = 6 \cdot 20 = 8 \cdot 15)$$

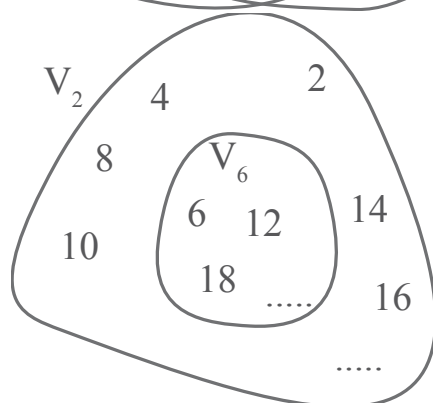
$\begin{matrix} \uparrow & \uparrow \\ 6 & 8 \end{matrix}$

$$kgV(6, 8) = \underline{24} \quad \text{und} \quad kgV(6, 8, 15) = 120$$

(4) Verwendung von Venndiagrammen:



$$\Rightarrow V_2 \cap V_3 = V_6$$



$$\Rightarrow V_6 \subset V_2$$

**Satz 4.19.** Für  $a, b \in \mathbb{N}$  gilt

$$V_a \cap V_b = V_{kgV(a,b)}$$



**Beweis:**

Sei  $k := kgV(a, b)$ .

" $\supseteq$ ": (Folgt auch aus Bemerkung (2)! Hier noch einmal der Vollständigkeit halber.)

Sei  $y \in V_k$  z.z.:  $y \in V_a \cap V_b$



$\Rightarrow k \mid y$ , aber weil  $k = \text{kgV}(a, b)$ , gilt auch  $a \mid k$  und  $b \mid k$

Transitivität der Teilerrelation  $\Rightarrow a \mid y$  und  $b \mid y$  also  $y \in V_a \cap V_b$   
 ” $\subseteq$ “:

Es gilt  $a \mid k$  und  $b \mid k$ . (\*)

Sei  $x \in V_a \cap V_b$ , also ein gemeinsames Vielfaches von  $a$  und  $b$ .

Klar, dann ist  $x \geq k = \text{kgV}(a, b)$ .

Division mit Rest: Es gibt eindeutig bestimmte Zahlen  $q, r \in \mathbb{N}$ ,  $0 \leq r < k$ :

$$x = q \cdot k + r$$

Aus  $x \in V_a \cap V_b \Rightarrow a \mid x$  und  $b \mid x$

Mit (\*)  $\Rightarrow a \mid x - qk = r$  und  $b \mid x - qk = r$

$\Rightarrow r \in V_a \cap V_b \Rightarrow r$  ist ein gemeinsames Vielfaches von  $a$  und  $b$ .

Aber

$$\begin{aligned} r < k = \text{kgV}(a, b) &\Rightarrow r = 0 \\ \Rightarrow x = q \cdot k &\Rightarrow x \in V_{\text{kgV}(a, b)} \end{aligned}$$

□

Der  $\text{kgV}$  kann mit Hilfe der Primfaktorzerlegung gefunden werden:

**Beispiel:**  $\text{kgV}(120, 315) = ?$

$$120 = 10 \cdot 12 = 2 \cdot 5 \cdot 4 \cdot 3 = 2^3 \cdot 3 \cdot 5$$

$$315 = 5 \cdot 63 = 5 \cdot 3 \cdot 21 = 5 \cdot 3 \cdot 3 \cdot 7 = 3^2 \cdot 5 \cdot 7$$

$$\Rightarrow \text{kgV} = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$$

#### Satz 4.20.

(1) Für  $a = \prod_{i=1}^{\infty} p_i^{m_i}$  und  $b = \prod_{i=1}^{\infty} p_i^{n_i}$  gilt:

$$\text{kgV}(a, b) = \prod_{i=1}^{\infty} p_i^{\max(m_i, n_i)}$$

(2) Für  $a, b, n \in \mathbb{N}$  gilt:  $\text{kgV}(n \cdot a, n \cdot b) = n \cdot \text{kgV}(a, b)$ .

#### Beweis:

(1) Sei  $k = \prod_{i=1}^{\infty} p_i^{k_i}$  ein gemeinsames Vielfaches von  $a$  und  $b$ . Da dann  $a$  und  $b$  jeweils Teiler von  $k$  sind, folgt nach Satz 3.17:

$$m_i \leq k_i \quad \text{und} \quad n_i \leq k_i \quad .$$

Die kleinste Zahl mit dieser Eigenschaft ist offensichtlich  $\prod_{i=1}^{\infty} p_i^{\max(m_i, n_i)}$ .



(2) ☞:  $n = p_j$  eine Primzahl, dann

$$p_j \cdot a = p_j^{m_j+1} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{\infty} p_i^{m_i} \quad \text{und} \quad p_j \cdot b = p_j^{n_j+1} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{\infty} p_i^{n_i}$$

Da aber  $\max(m_j + 1, n_j + 1) = \max(m_j, n_j) + 1$  folgt

$$kgV(p_j \cdot a, p_j \cdot b) = p_j^{\max(m_j+1, n_j+1)} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{\infty} p_i^{\max(m_i, n_i)} = p_j \cdot \prod_{i=1}^{\infty} p_i^{\max(m_i, n_i)}$$

□

□

**Beispiel:**

$$\begin{aligned} kgV(\underset{\parallel}{120}, \underset{\parallel}{315}) &= 5 \cdot kgV(2 \cdot 12, 63) = 5 \cdot kgV(2 \cdot 3 \cdot 4, 3 \cdot 21) \\ &= 3 \cdot 5 \cdot kgV(\underset{\uparrow}{2} \cdot \underset{\uparrow}{4}, \underset{\uparrow}{3} \cdot \underset{\uparrow}{7}) \\ &\quad \quad \quad \uparrow \quad \quad \uparrow \\ &\quad \quad \quad \text{teilerfremd} \\ &= 3 \cdot 5 \cdot 2 \cdot 4 \cdot 3 \cdot 7 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520 \end{aligned}$$

**Beispiel zum Zusammenhang von  $kgV$  und  $ggT$ :**

Sei  $a = 4$  und  $b = 12 \Rightarrow 4 \mid 12$

$$\Rightarrow \left. \begin{array}{l} ggT(4, 12) = 4 \\ kgV(4, 12) = 12 \end{array} \right\} \Rightarrow ggT \cdot kgV = 4 \cdot 12 = a \cdot b$$

Allgemeiner:

$$a \mid b \Rightarrow \left. \begin{array}{l} ggT(a, b) = a \\ kgV(a, b) = b \end{array} \right\} \Rightarrow ggT(a, b) \cdot kgV(a, b) = a \cdot b$$

Noch allgemeiner gilt:

**Satz 4.21.** Für  $a, b \in \mathbb{N}$  gilt:  $ggT(a, b) \cdot kgV(a, b) = a \cdot b$ .



**Beweis:**

Sei  $a = \prod_{i=1}^{\infty} p_i^{m_i}$  und  $b = \prod_{i=1}^{\infty} p_i^{n_i}$

$$ggT(a, b) = \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i)}$$

$$kgV(a, b) = \prod_{i=1}^{\infty} p_i^{\max(m_i, n_i)}$$

sicher gilt:  $\min(m_i, n_i) + \max(m_i, n_i) = m_i + n_i$

$$\Rightarrow ggT(a, b) \cdot kgV(a, b) = \prod_{i=1}^{\infty} p_i^{\min+max} = \prod_{i=1}^{\infty} p_i^{m_i+n_i} = a \cdot b$$

□

**Korollar 4.22.** Für teilerfremde  $a, b \in \mathbb{N}$  gilt:  $kgV(a, b) = a \cdot b$

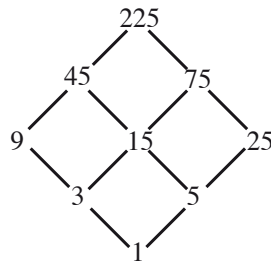
**Bemerkung 4.23.** Mit Hilfe des Euklidischen Algorithmus' kann man den  $ggT$  bestimmen. Zusammen mit Satz 4.21 so auch das  $kgV$ :

$$kgV(a, b) = \frac{a \cdot b}{ggT(a, b)}$$

Hassediagramm eignen sich zur Bestimmung/Darstellung von  $ggT$  und  $kgV$ :

**Beispiele:**

$$a) T_{225} = \left\{ \begin{array}{cccccc} 1, & 3, & 5, & 9, & 15 \\ 225, & 75, & 45, & 25, & 15 \end{array} \right\}$$



$$ggT(45, 75) = 15$$

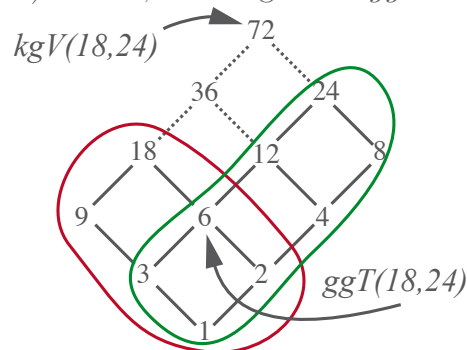
$$T_{45} \cap T_{75} = \{1, 3, 5, 15\}$$

$$kgV(45, 75) = 225$$

$$ggT(25, 45, 75) = 5$$

$$T_{25} \cap T_{45} \cap T_{75} = \{5, 1\}$$

b)  $a = 18, b = 24$  gesucht  $ggT$  und  $kgV$ :



$$T_{18} = \{1, 2, 3, 6, 9, 18\}$$

und

$$T_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$$



## 5. KONGRUENZEN UND RESTKLASSEN

5.1. Die Kongruenzrelation  $\pmod{m}$ .

**Definition 5.1.** Seien  $a$  und  $b$  ganze Zahlen und  $m \in \mathbb{N}$ . Man sagt  $a$  ist kongruent  $b$  modulo  $m$  ( $a \equiv b \pmod{m}$ ) genau dann, wenn  $m \mid a - b$ .  
 Ist  $a$  nicht kongruent  $b$  modulo  $m$ , so sagt man auch  $a$  ist inkongruent  $b$  modulo  $m$  ( $a \not\equiv b \pmod{m}$ ).  
 Die Zahl  $m$  heißt Modul, der Ausdruck  $a \equiv b \pmod{m}$  heißt Kongruenz.

**Beispiel:**  $a = 33, b = 21, m = 6$

Laut Definition:  $a - b = 33 - 21 = 12 = 2 \cdot 6$ ,

also  $6 = m \mid a - b = 33 - 21 = 12 \Rightarrow 33 \equiv 21 \pmod{6}$

## (1) Division mit Rest

$$\left. \begin{array}{rcl} 33 & = & 5 \cdot 6 + 3 \\ 21 & = & 3 \cdot 6 + 3 \end{array} \right\} \Rightarrow \text{Rest}$$

$$33 = 2 \cdot 6 + 21 \Rightarrow 33 \equiv 21 \pmod{6}$$

Frage nach: Was ist der Rest:

$$33 = * \cdot 6 + ? \quad \Leftrightarrow \quad 33 \equiv ? \pmod{6}$$

(2) Um was unterscheiden sich  $a$  und  $b$ ?

$$33 = 21 + 12 = 21 + 2 \cdot 6$$

21 und 33 unterscheiden sich also um ein Vielfaches von 6. Welche Zahlen gehören da noch in dieses Schema:

$$\dots, -3, 3, 9, 15 = 21 - 6, 21, 21 + 6 = 27, 33, = 39, \dots$$

Fragestellung:

$$? = * \cdot 6 + 21 \quad \Leftrightarrow \quad ? \equiv 21 \pmod{6}$$

## (3) Differenz

$$33 - 21 = 12 = 2 \cdot 6$$

$m = 6$  ist ein Teiler der Differenz von  $a = 33$  und  $b = 21$ .

Frage: bezüglich welcher Zahlen sind 33 und 21 kongruent:

$$33 = * \cdot ? + 21 \quad \Leftrightarrow \quad 33 \equiv 21 \pmod{?} \quad \text{💬}$$

**Bemerkung 5.1.** (1) Die Definition folgt dem Zugang (3).



(2) Die Bedingung  $m \in \mathbb{N}$  ist keine Einschränkung, denn

$$m \mid a - b \quad \Leftrightarrow \quad -m \mid a - b$$

Die folgenden Sätze zeigen die Äquivalenz der drei Zugänge.

**Satz 5.2.** Für  $a, b \in \mathbb{Z}$  und  $m \in \mathbb{N}$  gilt:

$$a \equiv b \pmod{m} \Leftrightarrow a \text{ und } b \text{ haben bei Division durch } m \text{ denselben Rest.}$$

**Beweis:**

” $\Rightarrow$ ”: Es gelte also:  $a \equiv b \pmod{m}$

nach Definition  $\Rightarrow m \mid a - b$

Division (durch  $m$ ) mit Rest auf  $a$  und  $b$  anwenden:

Wegen Korollar 4.5 gilt das, egal ob  $a, b$  positiv oder negativ!!

$$a = q_1 \cdot m + r_1 \qquad 0 \leq r_1 < m$$

$$b = q_2 \cdot m + r_2 \qquad 0 \leq r_2 < m$$

mit eindeutigen Zahlen  $r_i, q_i$ .

Subtrahiere die beiden Gleichungen:

$$\begin{aligned} \underbrace{a - b}_m &= \underbrace{(q_1 - q_2) \cdot m}_m + r_1 - r_2 \\ \Rightarrow m \mid \underbrace{(a - b) - (q_1 - q_2) \cdot m}_{=r_1 - r_2} &\Rightarrow m \mid r_1 - r_2 \end{aligned} \quad (*)$$

$$\text{aber } 0 \leq r_i < m \Rightarrow 0 \leq |r_1 - r_2| < m \quad (**)$$

$$(*) \text{ und } (**) \Rightarrow r_1 - r_2 = 0 \Leftrightarrow r_1 = r_2$$

” $\Leftarrow$ ”:

$$\begin{aligned} a &= q_1 \cdot m + r \\ b &= q_2 \cdot m + r \quad \text{mit } q_i \in \mathbb{Z} \text{ und } 0 \leq r < m \\ \Rightarrow a - b &= (q_1 - q_2) \cdot m \Rightarrow m \mid a - b \end{aligned}$$

□

**Satz 5.3.** Für  $a, b \in \mathbb{Z}$  und  $m \in \mathbb{N}$  gilt:

$a \equiv b \pmod{m}$  genau dann, wenn sich  $a$  und  $b$  um ein ganzzahliges Vielfaches von  $m$  unterscheiden (d.h. es gibt ein  $q \in \mathbb{Z}$  mit  $a = b + q \cdot m$ ).



**Beweis:**

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b) \quad (\text{Def. von Kongruenz})$$

$$\Leftrightarrow \text{es gibt ein } q \in \mathbb{Z} \text{ mit } m \cdot q = a - b \quad (\text{Def. von Teiler})$$

$$\Leftrightarrow a = b + m \cdot q \quad \text{für ein } q \in \mathbb{Z}$$

□

**Bemerkung 5.4.** Die in den drei Zugängen dargestellten Wege zur Kongruenz sind damit äquivalent. Das heißt auch für uns, wir können uns im Unterricht für den Weg entscheiden, der am besten in unser Konzept passt!

Wie rechnet man mit Kongruenzen?

**Satz 5.5.** Seien  $a \equiv b \pmod{m}$  und  $c \equiv d \pmod{m}$ . Dann gilt:

$$(1) \ a \pm c \equiv b \pm d \pmod{m}$$

$$(2) \ a \cdot c \equiv b \cdot d \pmod{m}$$

**Beweis:**

Nach Voraussetzung:  $m \mid (a - b)$  und  $m \mid (c - d)$

$$(1) \ m \mid \underbrace{(a - b) \pm (c - d)}_{= a - b \pm c \mp d} = (a \pm c) - (b \pm d)$$

$$\Rightarrow (a \pm c) \equiv (b \pm d) \pmod{m}$$

(2)

$$m \mid (a - b) \Rightarrow m \mid (a - b) \cdot c \Rightarrow m \mid (a - b) \cdot c + (c - d) \cdot b = ac - \cancel{bc} + \cancel{cb} - db = ac - db$$

$$m \mid (c - d) \Rightarrow m \mid (c - d) \cdot b \Rightarrow m \mid (a - b) \cdot c + (c - d) \cdot b = ac - \cancel{bc} + \cancel{cb} - db = ac - db$$

$$\Rightarrow ac \equiv bd \pmod{m}$$

□





## Beispiele

$$\begin{array}{rcll}
& 37 \equiv 17 \pmod{5} & & \\
& 12 \equiv 2 \pmod{5} & & \\
\Rightarrow & \begin{array}{ccc} 49 & \equiv & 19 \\ \uparrow & & \uparrow \\ 37+12 & & 17+2 \end{array} & \pmod{5} & (" + ") \\
\Rightarrow & \begin{array}{ccc} 25 & \equiv & 15 \\ \uparrow & & \uparrow \\ 37-12 & & 17-2 \end{array} & \pmod{5} & (" - ") \\
\Rightarrow & \begin{array}{ccc} 444 & \equiv & 34 \\ \uparrow & & \uparrow \\ 37 \cdot 12 & & 17 \cdot 2 \end{array} & \pmod{5} & (" \cdot ") \\
\text{über Kreuz:} & \begin{array}{ccc} 74 & \equiv & 204 \\ \uparrow & & \uparrow \\ 37 \cdot 2 & & 17 \cdot 12 \end{array} & \pmod{5} & (" \cdot ")
\end{array}$$

Spezialfälle für  $d = c$ :

**Korollar 5.6.** Sei  $a \equiv b \pmod{m}$ . Dann gilt für alle  $c \in \mathbb{Z}$ :

- (1)  $a \pm c \equiv b \pm c \pmod{m}$
- (2)  $a \cdot c \equiv b \cdot c \pmod{m}$

**Beispiel:**

$$\begin{array}{rcll}
& 86 \equiv 60 \pmod{13} & & (\text{denn } 60 + 2 \cdot 13 = 60 + 26 = 86) \\
\stackrel{+100}{\Rightarrow} & 186 \equiv 160 \pmod{13} & & \\
\stackrel{\cdot 3}{\Rightarrow} & 558 \equiv 480 \pmod{13} & & 
\end{array}$$

**Korollar 5.7.** Aus  $a \equiv b \pmod{m}$  folgt  $a^n \equiv b^n \pmod{m}$  für alle  $n \in \mathbb{N}$ .

Hier gilt auch  $n = 0$ , denn trivialerweise:  $a^0 = 1 \stackrel{\text{mod } m}{\equiv} 1 = b^0$ .

**Bemerkung 5.8.** Kongruenzen verhalten sich anscheinend ähnlich wie Gleichungen. Gleichungen sind ein Spezialfall von Kongruenzen: die Kongruenz modulo 0:

$$a \equiv b \pmod{0} \Leftrightarrow 0 \mid a - b \stackrel{!}{\Leftrightarrow} a - b = 0 \Leftrightarrow a = b$$

Konsequenz für das Rechnen mit Kongruenzen: Kongruenzen lassen Äquivalenzumformungen (analog zu den Äquivalenzumformungen von Gleichungen) bzgl. der Verknüpfungen

$$"+", \quad "-", \quad \text{und} \quad "\cdot"$$

zu. Vorsicht ist nur bei der Division  $\div$  geboten:



**Satz 5.9.**

$$z \cdot a \equiv z \cdot b \pmod{m} \quad \Rightarrow \quad a \equiv b \pmod{\frac{m}{\text{ggT}(z, m)}}$$

**Beispiel**

$$\begin{aligned} 88 &\equiv 52 \pmod{12} && (\text{denn } 88 - 52 = 36 = 3 \cdot 12) \\ 4 \cdot 22 &\equiv 4 \cdot 13 \pmod{12} && (| \div 4, \quad \text{ggT}(4, 12) = 4) \\ \Rightarrow 22 &\equiv 13 \pmod{\frac{12}{4} = 3} \\ \text{aber: } 22 &\not\equiv 13 \pmod{12} \end{aligned}$$

**Beweis:**

$$\begin{aligned} z \cdot a &\equiv z \cdot b \pmod{m} \\ \Leftrightarrow m &| (z \cdot a - z \cdot b) = z \cdot (a - b) \\ \Leftrightarrow m \cdot q &= z \cdot (a - b) && (\text{für ein } q \in \mathbb{Z} \quad | \div \underbrace{\text{ggT}(z, m)}_{=:d}) \\ \Leftrightarrow \underbrace{\frac{m}{d}}_{\in \mathbb{Z}} \cdot q &= \underbrace{\frac{z}{d}}_{\in \mathbb{Z}} \cdot (a - b) \\ \Leftrightarrow \frac{m}{d} &| \frac{z}{d} \cdot (a - b) \\ \Rightarrow \frac{m}{d} &| (a - b) && (\text{da } \text{ggT}(\frac{m}{d}, \frac{z}{d}) = 1) \\ \Leftrightarrow a &\equiv b \pmod{\frac{m}{d}} \end{aligned}$$

□

**Korollar 5.10.** Wenn  $\text{ggT}(z, m) = 1$ , dann:

$$z \cdot a \equiv z \cdot b \pmod{m} \quad \Leftrightarrow \quad a \equiv b \pmod{m}$$

**Beispiele**

(1)

$$\begin{aligned} 180 &= 5 \cdot 36 \equiv \underbrace{5 \cdot 24}_{=120} \pmod{12} && (\text{und } \text{ggT}(5, 12) = 1) \\ \Rightarrow 36 &\equiv 24 \pmod{12} \end{aligned}$$



(2) Aber:

$$24 \equiv 6 \pmod{6}$$

$$3 \cdot 8 \equiv 3 \cdot 2 \pmod{6}$$

$$\text{ggT}(3, 6) = 3 \xrightarrow{\text{Satz 5.9}} 8 \equiv 2 \pmod{\frac{6}{3} = 2}$$

$$\text{aber es gilt auch: } 8 \equiv 2 \pmod{6} \quad \text{💬}$$

## 5.2. Kongruenz als Äquivalenzrelation.

**Satz 5.11.** Die Kongruenzrelation modulo  $m$  ist für jeden Modul  $m \in \mathbb{N}$  eine Äquivalenzrelation in  $\mathbb{Z}$ , d.h. für alle  $a, b, c \in \mathbb{Z}$  gilt:

$$(1) \quad a \equiv a \pmod{m} \quad (\text{Reflexivität})$$

$$(2) \quad \text{Aus } a \equiv b \pmod{m} \text{ folgt } b \equiv a \pmod{m} \quad (\text{Symmetrie})$$

$$(3) \quad \text{Aus } a \equiv b \pmod{m} \text{ und } b \equiv c \pmod{m} \text{ folgt } a \equiv c \pmod{m} \quad (\text{Transitivität})$$

**Beweis:**

$$(1) \quad a - a = 0 = m \cdot 0 \quad \Rightarrow \quad m \mid (a - a)$$

(2)

$$\begin{aligned} m \mid (a - b) &\Leftrightarrow m \cdot q = a - b \Leftrightarrow m \cdot (-q) = b - a \\ &\Leftrightarrow m \mid (b - a) \\ &\Leftrightarrow b \equiv a \pmod{m} \end{aligned}$$

$$(3) \quad m \mid (a - b) \text{ und } m \mid (b - c) \Rightarrow m \text{ teilt auch die Summe:}$$

$$\Rightarrow m \mid (a - b) + (b - c) = (a - c) \Leftrightarrow a \equiv c \pmod{m}$$

□

Allgemein: Äquivalenzrelation  $\Rightarrow$  Restklassen(einteilung)

Speziell: Kongruenzrelation modulo  $m$   $\Rightarrow$  Restklassen  $\mathbb{Z}/m\mathbb{Z}$

Sei  $m \in \mathbb{N}$  fest gewählt. Für  $a \in \mathbb{Z}$  sei:

$$\bar{a} := \{ z \in \mathbb{Z} \mid z \equiv a \pmod{m} \} = \{ z = a + n \cdot m \mid n \in \mathbb{Z} \}$$

die Restklasse von  $a$  modulo  $m$ . Die Zahl  $a$  heißt Repräsentant der Restklasse. Der Repräsentant ist nicht eindeutig, es gibt  $\infty$ -viele Repräsentanten einer Restklasse.



**Beispiel:**  $m = 3$ 

$$a = 0 \Rightarrow \bar{0} = \{z \in \mathbb{Z} \mid z \equiv 0 \pmod{3}\} = \{\dots, -6, -3, 0, 3, 6, \dots\} = 3\mathbb{Z}$$

$$a = 1 \Rightarrow \bar{1} = \{z \in \mathbb{Z} \mid z \equiv 1 \pmod{3}\} = \{\dots, -5, -2, 1, 4, 7, \dots\} = 1 + 3\mathbb{Z}$$

$$a = 2 \Rightarrow \bar{2} = \{z \in \mathbb{Z} \mid z \equiv 2 \pmod{3}\} = \{\dots, -4, -1, 2, 5, 8, \dots\} = 2 + 3\mathbb{Z}$$

$$a = 3 \Rightarrow \bar{3} = \{z \in \mathbb{Z} \mid z \equiv 3 \pmod{3}\} = \{\dots, -9, -6, -3, 0, 3, 6, \dots\} = \bar{0}$$

Insbesondere gilt:  $a \in \bar{a}$ **Satz 5.12.** Sei  $m \in \mathbb{N}$ . Für  $a, b \in \mathbb{Z}$  gilt:

$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{m}$$

**Beweis:**"  $\Rightarrow$  ": Es gelte  $\bar{a} = \bar{b}$ Aus  $a \in \bar{a} = \bar{b}$  folgt  $a \in \bar{b} \Rightarrow a \equiv b \pmod{m}$ ."  $\Leftarrow$  ": Sei  $a \equiv b \pmod{m}$ .Z.z.:  $\bar{a} = \bar{b}$  (als Mengen!)Fall:  $\bar{a} \subseteq \bar{b}$ :Sei  $z \in \bar{a} \Rightarrow z \equiv a \pmod{m}$  (nach Def.)Wegen  $a \equiv b \pmod{m}$  und der Transitivität folgt:

$$z \equiv b \pmod{m} \Rightarrow z \in \bar{b} \Rightarrow \bar{a} \subseteq \bar{b}$$

Fall:  $\bar{a} \supseteq \bar{b}$ :Wie oben bei Fall:  $\bar{a} \subseteq \bar{b}$  mit Symmetrie:

$$a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$$

□

**Satz 5.13.**

- (1) Für alle  $a \in \mathbb{Z}$  gilt:  $\bar{a} \neq \emptyset$
- (2) Für alle  $a, b \in \mathbb{Z}$  gilt entweder:  $\bar{a} = \bar{b}$  oder  $\bar{a} \cap \bar{b} = \emptyset$
- (3) Für alle  $z \in \mathbb{Z}$  gibt es ein  $a \in \mathbb{Z}$  mit  $z \in \bar{a}$

**Beweis:**(1) Da  $a \in \bar{a}$  für alle  $a \in \mathbb{Z}$  folgt  $\bar{a} \neq \emptyset \quad \forall a \in \mathbb{Z}$ .(2) Seien  $a, b \in \mathbb{Z}$ :Zwei Fälle:  $a \equiv b \pmod{m}$  oder  $a \not\equiv b \pmod{m}$ Falls  $a \equiv b \pmod{m} \xrightarrow{\text{Satz 5.12}} \bar{a} = \bar{b}$ Falls  $a \not\equiv b \pmod{m}$ : z.z.:  $\bar{a} \cap \bar{b} = \emptyset$  (als Menge)Durch Widerspruch  $\Rightarrow$  Annahme:  $\bar{a} \cap \bar{b} \neq \emptyset$ 

$\Rightarrow$  es gibt ein  $z \in \bar{a} \cap \bar{b}$

Wegen  $z \in \bar{a} \Rightarrow z \equiv a \pmod{m} \xLeftrightarrow{\text{Symmetrie}} a \equiv z \pmod{m}$

Wegen  $z \in \bar{b} \Rightarrow z \equiv b \pmod{m}$

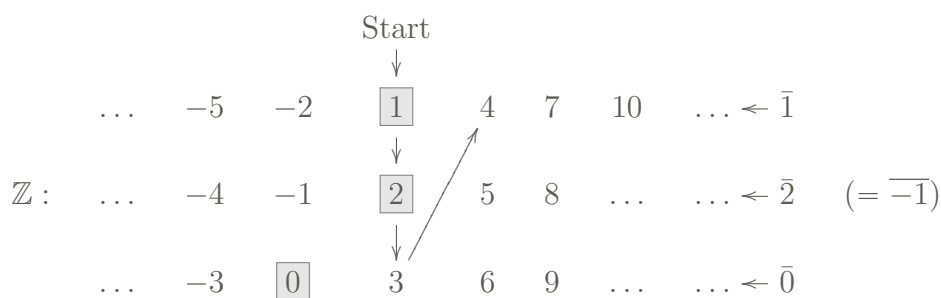
$\xRightarrow{\text{Transitivität}} a \equiv z \equiv b \pmod{m} \quad \nexists$

Also  $\bar{a}$  und  $\bar{b}$  disjunkt.

(3) Klar, wähle z.B.  $z$  selber:  $z \in \bar{z}$  □

**Folgerung:** Die Menge  $\mathbb{Z}$  der ganzen Zahlen wird bei gegebenen Modul  $m$  in disjunkte Teilmengen  $\bar{a}$  zerlegt.

**Beispiel:**  $m = 3$



Die 3 Streifen entsprechen den Restklassen  $\bar{0}$ ,  $\bar{1}$  und  $\bar{2}$ , dabei sind 0, 1 und 2 Repräsentanten.

Wieviele Restklassen modulo  $m$  gibt es?

**Satz 5.14.** Sei  $m \in \mathbb{N}$ . Es gibt genau  $m$  verschiedene Restklassen modulo  $m$ :

$$\bar{0}, \bar{1}, \dots, \overline{m-1}$$

( $=\bar{m}$ )

**Bemerkung 5.15.** (1) Es müssen nicht die Repräsentanten  $0, 1, 2, \dots, m-1$  sein, diese werden aber gerne genommen.

(2) Aus Sätzen 5.13 und 5.14 folgt:

$$\bar{0} \cup \bar{1} \cup \bar{2} \cup \dots \cup \overline{m-1} = \mathbb{Z}$$

**Beweis:**

Von Satz 5.14: Es reicht zu zeigen, daß jede Restklasse modulo  $m$  einen Repräsentanten zwischen 0 und  $m-1$  hat:

Sei  $a \in \mathbb{Z} \Rightarrow$  Restklasse  $\bar{a}$



Euklidischer Algorithmus: es gibt eindeutig bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r$  mit  $0 \leq r < m$ , so daß:

$$\begin{aligned} a &= q \cdot m + r \\ \Rightarrow a &\equiv r \pmod{m} \\ \Leftrightarrow \bar{a} &= \bar{r} \quad \text{mit} \quad r \in \{0, 1, 2, \dots, m-1\} \end{aligned}$$

□

Die Restklassen modulo  $m$  bilden die Menge:

$$\mathbb{Z}/m\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$$

- $\mathbb{Z}/m\mathbb{Z}$  ist eine Menge von Mengen!
- $\mathbb{Z}/m\mathbb{Z}$  wird als Menge der  $m$  "Symbole":  $\bar{0}, \bar{1}, \dots, \overline{m-1}$  aufgefasst. Dabei "vergisst" man, daß  $\bar{0}, \bar{1}, \dots, \overline{m-1}$  Mengen sind, aber nicht ihre Eigenschaften.
- $\mathbb{Z}/m\mathbb{Z}$  wird *Restsystem modulo  $m$*  (oder auch *Restklassenmenge*) genannt.

**Beispiele:**

$$\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\} \quad \text{und} \quad \mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

### 5.3. Algebraische Struktur von $\mathbb{Z}/m\mathbb{Z}$ - Rechnen im System $\mathbb{Z}/m\mathbb{Z}$ .

Wir führen eine Addition  $\oplus$  und eine Multiplikation  $\odot$  in  $\mathbb{Z}/m\mathbb{Z}$  ein:

Für  $\bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$  sei:

$$\bar{a} \oplus \bar{b} := \overline{a+b} \quad \text{Restklassenaddition}$$

$$\bar{a} \odot \bar{b} := \overline{a \cdot b} \quad \text{Restklassenmultiplikation}$$

Warum ist das vernünftig?

**Satz 5.16.** Die Restklassenverknüpfungen  $\oplus$  und  $\odot$  in  $\mathbb{Z}/m\mathbb{Z}$  sind wohldefiniert.

**Beweis:**

1)  $\bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$  bedeutet, daß  $a, b \in \mathbb{Z}$ .

Hier sind Addition  $a + b \in \mathbb{Z}$  und Multiplikation  $a \cdot b \in \mathbb{Z}$  definiert.

Damit gilt für die Restklassen:  $\overline{a+b}, \overline{a \cdot b} \in \mathbb{Z}/m\mathbb{Z}$ .

2) *Unabhängigkeit von der Wahl des Repräsentanten:*

Seien:

$\bar{a} = \bar{a}'$  (also  $a, a' \in \mathbb{Z}$  mit  $a \equiv a' \pmod{m}$ ) und



$\bar{b} = \bar{b}'$  (also  $b, b' \in \mathbb{Z}$  mit  $b \equiv b' \pmod{m}$ ).

Z.z.: (i)  $\bar{a} \oplus \bar{b} = \overline{a' \oplus b'}$  und (ii)  $\bar{a} \odot \bar{b} = \overline{a' \odot b'}$

Aber:  $m \mid a - a'$  und  $m \mid b - b'$  (\*)

$$\Rightarrow m \mid \underbrace{(a - a') + (b - b')}_{=(a+b)-(a'+b')} \Rightarrow a + b \equiv a' + b' \pmod{m}$$

$$\Leftrightarrow \bar{a} \oplus \bar{b} = \overline{a' \oplus b'} \Rightarrow (i)$$

Aus (\*) folgt:  $a = a' + m \cdot q_1$  und  $b = b' + m \cdot q_2$

$$\begin{aligned} \Rightarrow a \cdot b &= (a' + m \cdot q_1) \cdot (b' + m \cdot q_2) \\ &= a' \cdot b' + m \cdot q_1 b' + m q_2 a' + m^2 q_1 q_2 \\ &= a' \cdot b' + m \cdot (*) \end{aligned}$$

$$\Rightarrow a \cdot b \equiv a' \cdot b' \pmod{m}$$

$$\Leftrightarrow \bar{a} \odot \bar{b} = \overline{a' \odot b'} \Rightarrow (ii)$$

□

## Beispiele

in  $\mathbb{Z}/5\mathbb{Z}$  gilt:  $\bar{3} \oplus \bar{4} = \bar{7} = \bar{2}$

$$\bar{3} \odot \bar{4} = \overline{12} = \bar{2}$$

in  $\mathbb{Z}/7\mathbb{Z}$  gilt:  $\bar{3} \oplus \bar{4} = \bar{7} = \bar{0}$

$$\bar{3} \odot \bar{4} = \overline{12} = \bar{5}$$

## Verknüpfungstabellen:

$\mathbb{Z}/5\mathbb{Z}$ :

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	0	1	2	3	4
$\bar{1}$	1	2	3	4	0
$\bar{2}$	2	3	4	0	1
$\bar{3}$	3	4	0	1	2
$\bar{4}$	4	0	1	2	3

und

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	0	0	0	0	0
$\bar{1}$	0	1	2	3	4
$\bar{2}$	0	2	4	1	3
$\bar{3}$	0	3	1	4	2
$\bar{4}$	0	4	3	2	1

symmetrisch, da  $\mathbb{Z}/5\mathbb{Z}$  Ring  
(Addition in Ringen immer kommutativ)

symmetrisch, da  $\mathbb{Z}/5\mathbb{Z}$  kommutativer Ring  
(d.h. Multiplikation kommutativ)



**Die algebraische Struktur der Restklassenmengen:**

**Satz 5.17.**  $(\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$  ist ein kommutativer Ring (mit Einselement).

**Wiederholung/Exkurs:** Sei  $M$  eine Menge und  $+$  :  $M \times M \rightarrow M$  und  $\cdot$  :  $M \times M \rightarrow M$  Verknüpfungen.

**Gruppe:**  $(M, +)$  ist eine Gruppe, wenn gilt:

- (1) es gibt ein neutrales Element  $e = 0$  : ("Nichts" der Addition)  
 $\uparrow$   
 bei +

$$m + e = e + m = m \quad \text{für alle } m \in M$$

- (2) Inverses Element: für alle  $m \in M$  gibt es ein Inverses  $m'$ , d.h.:

$$m + m' = m' + m = e$$

- (3) Assoziativität: für alle  $m, n, p \in M$  gilt  $(m + n) + p = m + (n + p)$ .  
 (macht erst die Schreibweise:  $m + n + p$  möglich!)

Gruppe

Wenn auch noch

- (4) Kommutativität: für alle  $n, m \in M$  gilt:  $n + m = m + n$

gilt, dann heißt  $(M, +)$  kommutative oder abelsche Gruppe.

**Beispiel:**  $(\mathbb{Z}, +)$  ist eine kommutative Gruppe,  $\mathbb{N}$  nein,  $(\mathbb{Z}, \cdot)$  auch nein, weil Inverse fehlen, aber  $(\mathbb{Q}, \cdot)$  ist eine abelsche Gruppe. Rotationsgruppen: endliche abelsche Gruppen, Diedergruppen: endliche nicht abelsche Gruppen.

**Ring:** Ein Ring ist eine Menge  $M$  mit 2 Verknüpfungen (meist  $+$  und  $\cdot$  bezeichnet), also  $(M, +, \cdot)$ , wenn gilt:

- $(M, +)$  ist eine kommutative Gruppe, es gilt also (1)...(4).
- $(M, \cdot)$  hat ein neutrales Element (vgl. (1), bei Multiplikation Einselement 1 genannt) und erfüllt die Assoziativität (3)

und zusätzlich gilt:

- (5) Distributivität: für alle  $m, n, p \in M$  gilt:

$$(m + n) \cdot p = m \cdot p + n \cdot p \quad \text{und} \quad p \cdot (m + n) = p \cdot m + p \cdot n$$

Wenn zusätzlich gilt:

- (6) Kommutativität der Multiplikation: für alle  $n, m \in M$  gilt:

$$n \cdot m = m \cdot n$$



dann heit  $(M, +, \cdot)$  *kommutativer Ring (mit Eins)*.

**Bemerkung:** Es gibt auch Ringe ohne Eins, dann ist  $(M, \cdot)$  eine Halbgruppe, kommt selten vor!!

**Beweis:**

(Von Satz 5.17)

(1) Neutrales Element bzgl.  $\oplus$ :  $\bar{0}$  tuts, denn fr alle  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  gilt:

$$\bar{a} \oplus \bar{0} = \overline{a + 0} = \bar{a} = \overline{0 + a} = \bar{0} \oplus \bar{a}$$

(2) Inverses Element: Sei  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ . Beh:  $\bar{a}' = \overline{-a}$

$$\bar{a} \oplus \bar{a}' = \bar{a} \oplus \overline{-a} = \overline{a + (-a)} = \bar{0}$$

$$\bar{a}' \oplus \bar{a} = \dots = \bar{0}$$

(3) Assoziativitt:  $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/m\mathbb{Z}$ , also  $a, b, c \in \mathbb{Z}$ :

$$(\bar{a} \oplus \bar{b}) \oplus \bar{c} = \overline{a + b} \oplus \bar{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \bar{a} \oplus \overline{b + c} = \bar{a} \oplus (\bar{b} \oplus \bar{c})$$

$\uparrow$   
 Assoziativitt  
 von  $\mathbb{Z}$

(4) Kommutatives Element: folgt aus der Kommutativitt von  $\mathbb{Z}$ :

$$\bar{a} \oplus \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} \oplus \bar{a}$$

Damit ist  $(\mathbb{Z}/m\mathbb{Z}, \oplus)$  eine kommutative Gruppe.

Nun zur Multiplikation  $\odot$ :

Einselement: Beh.:  $\bar{1}$  ist ein Einselement: Fr alle  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  gilt:

$$\bar{1} \odot \bar{a} = \overline{1 \cdot a} = \overline{a \cdot 1} = \bar{a} \odot \bar{1}$$

(5) Distributivitt:  $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/m\mathbb{Z}$ :

$$(\bar{a} \oplus \bar{b}) \odot \bar{c} = \overline{(a + b) \cdot c} = \overline{a \cdot c + b \cdot c} = \bar{a} \odot \bar{c} \oplus \bar{b} \odot \bar{c}$$

(6) Kommutativitt von  $\odot$ :  $\bar{a} \odot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \odot \bar{a}$

□

## Beispiel

(1)  $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

neutrales Element der Addition:  $\bar{0}$  (vgl. Verkn. Tafel)

neutrales Element der Multiplikation:  $\bar{1}$

Kommutativitt von  $\oplus$  und  $\odot$  sehen wir an der Symmetrie der Verknpfungstafel.



Inverse Elemente der Addition:

$$\bar{0}' = \bar{0}$$

$$-\bar{1} = \bar{1}' = \overline{-1} = \bar{4}$$

$$-\bar{2} = \bar{2}' = \overline{-2} = \bar{3}$$

$$\bar{3}' = \overline{-3} = \bar{2}$$

$$\bar{4}' = \overline{-4} = \bar{1}$$

$$\text{denn } \bar{1} \oplus \bar{4} = \bar{5} = \bar{0}$$

Wo sieht man das in der Verknüpfungstafel? Suche Paare, die die  $\bar{0}$  erzeugen!

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Inverse der Multiplikation? Ja, Paare die in der Tafel eine  $\bar{1}$  erzeugen.

$$\bar{1} \odot \bar{1} = \bar{1} \Rightarrow \bar{1}^{-1} = \bar{1}$$

$$\bar{2} \odot \bar{3} = \bar{1} \Rightarrow \bar{2}^{-1} = \bar{3}$$

$$\dots \dots \Rightarrow \bar{3}^{-1} = \bar{2}$$

$$\bar{4} \odot \bar{4} = \bar{1} \Rightarrow \bar{4}^{-1} = \bar{4}$$

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

(2)  $\mathbb{Z}/6\mathbb{Z} \Rightarrow \bar{0}$  neutrales Element der Addition,  $\bar{1}$  Einselement.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Inverse der Addition:

z.B.:  $-\bar{5} = \bar{1}$ , denn  $\bar{5} \oplus \bar{1} = \bar{0}$

und

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Inverse der Multiplikation:

$\bar{1}^{-1} = \bar{1}$ ,  $\bar{5}^{-1} = \bar{5}$

Neu: Nullteiler:

$\bar{3} \odot \bar{2} = \bar{0}$  und  $\bar{4} \odot \bar{3} = \bar{0}$

**Satz 5.18.**  $(\mathbb{Z}/m\mathbb{Z}, \odot)$  enthält genau dann Nullteiler, wenn  $m$  eine zusammengesetzte Zahl ist.

**Beweis:**

" $\Leftarrow$ ": Sei  $m = a \cdot b$  mit  $1 < a < m$  also auch  $1 < b < m$

$\Rightarrow \bar{a} \odot \bar{b} = \overline{a \cdot b} = \bar{m} = \bar{0} \in \mathbb{Z}/m\mathbb{Z}$

" $\Rightarrow$ ": Umgekehrt:  $(\mathbb{Z}/m\mathbb{Z}, \odot)$  enthalte Nullteiler, d.h.

$$\begin{aligned} \exists \bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z} \setminus \{\bar{0}\} \quad \text{mit} \quad \bar{a} \odot \bar{b} = \bar{0} \\ \Leftrightarrow \overline{a \cdot b} = \bar{0} \quad \Leftrightarrow \quad m \mid \underbrace{(a \cdot b - 0)}_{a \cdot b} \quad \Leftrightarrow \quad m \mid a \cdot b \end{aligned}$$

Da  $\bar{a} \neq \bar{0} \Rightarrow m \nmid a - 0 \Rightarrow m \nmid a$

Analog  $m \nmid b$

Also  $m \mid a \cdot b$ , aber  $m \nmid a$  und  $m \nmid b$ . Aus dem Primzahlkriterium 3.20 folgt  $\Rightarrow m$  ist keine Primzahl sondern zusammengesetzte Zahl! (oder  $m = 1!!$ )  $\square$

Ein Ring ohne Nullteiler heißt *Integritätsring*.

**Korollar 5.19.** Für  $m > 1$  gilt:

$\mathbb{Z}/m\mathbb{Z}$  ist Integritätsring  $\Leftrightarrow m$  ist Primzahl

Gibt es auch Inverse der Multiplikation?

**Satz 5.20.**  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  hat genau dann ein multiplikativ Inverses ( $\bar{a}^{-1}$  existiert), wenn  $\text{ggT}(a, m) = 1$ .



**Beweis:**

$$\begin{aligned}
\bar{a}^{-1} \in \mathbb{Z}/m\mathbb{Z} \text{ existiert} &\Leftrightarrow \bar{a}^{-1} = \bar{s} \quad \text{mit } s \in \mathbb{Z}, \quad OE: \quad 1 \leq s < m \\
&\Leftrightarrow \bar{s} \cdot \bar{a} = \bar{1} \quad (\text{mit } \bar{s} \in \mathbb{Z}/m\mathbb{Z}) \\
&\Leftrightarrow s \cdot a \equiv 1 \pmod{m} \quad (\text{mit } s \in \mathbb{Z}) \\
&\Leftrightarrow s \cdot a = 1 + t \cdot m \quad (\text{mit } s, t \in \mathbb{Z}) \\
&\Leftrightarrow s \cdot a - t \cdot m = 1 \quad (\text{mit } s, t \in \mathbb{Z})
\end{aligned}$$

$\Leftrightarrow$  die lineare diophantische Gleichung  $s \cdot a - t \cdot m = 1$  ist lösbar in  $\mathbb{Z}$

$$\begin{aligned}
&\Leftrightarrow ggT(a, m) \mid 1 \quad (\text{vgl. Satz 4.17}) \\
&\Leftrightarrow ggT(a, m) = 1
\end{aligned}$$

□

**Korollar 5.21.** Seien  $a, b \in \mathbb{N}$  mit  $ggT(a, b) = 1$ . Dann ist die Kongruenz  $a \cdot x \equiv 1 \pmod{b}$  lösbar.

Ring  $\rightarrow$  Körper???

Wdh. zu Körpern:  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  sind Körper (mit  $+$  und  $\cdot$ ).

Was brauchen wir noch, um aus einem Ring einen Körper zu machen?

$\Rightarrow$  Wir brauchen noch Inverse der Multiplikation:

Sei wie zuvor:  $(M, +, \cdot)$  ein kommutativer Ring. Es gelte ferner:

- (7) Inverses Element der Multiplikation: für alle  $a \in M \setminus \{0\}$  gibt es ein Inverses  $a^{-1}$ , so daß:

$$a \cdot a^{-1} = 1 \leftarrow \text{Einselement} = \text{neutrales Element der Multiplikation}$$

(Wegen der Kommutativität gilt auch  $a^{-1} \cdot a = 1$ )

Ein kommutativer Ring, der auch (7) erfüllt, heißt Körper.

**Integritätsring  $\Leftrightarrow$  Körper??**

Klar, ein Körper ist immer auch ein Integritätsring, da er keine Nullteiler außer Null selber haben kann. Umgekehrt ist die Eigenschaft, ein Integritätsring zu sein, also keine Nullteiler zu haben, eine notwendige Voraussetzung dafür, ein Körper zu sein. Aber diese Eigenschaft ist nicht hinreichend.

Gegenbeispiel: Die ganzen Zahlen  $\mathbb{Z}$  sind ein Integritätsring, aber kein Element  $\neq 0$  oder  $\pm 1$  ist invertierbar in  $\mathbb{Z}$ .



Bei den Restklassen modulo  $m$  passiert das aber nicht, sobald keine Nullteiler, dann auch sogleich Körper!

Das folgt aus der allgemeineren Tatsache, daß Integritätsringe mit endlich vielen Elementen immer auch Körper sind.

**Satz 5.22.**  $(\mathbb{Z}/p\mathbb{Z}, \oplus, \odot)$  ist genau dann ein Körper, wenn  $p$  eine Primzahl ist.

**Beweis:**

" $\Leftarrow$ ": Sei  $p$  Primzahl.

Korollar 5.19  $\Rightarrow (\mathbb{Z}/p\mathbb{Z}, \oplus, \odot)$  ist Integritätsring.

Z.Z.: (7) jedes von Null verschiedene Element hat ein multiplikativ Inverses!

Sei  $\bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ , also  $a \in \mathbb{Z}$ , OE:  $0 < a < p$

Wir suchen das Inverse:  $\bar{a}^{-1}$

Da  $p$  Primzahl  $\Rightarrow \text{ggT}(a, p) = 1$

Satz 5.20  $\Rightarrow$  das Inverse  $\bar{a}^{-1}$  existiert!

" $\Rightarrow$ ":  $\mathbb{Z}/p\mathbb{Z}$  sei ein Körper. Z.Z.:  $p$  ist Primzahl

$\mathbb{Z}/p\mathbb{Z}$  Körper  $\Rightarrow$  jedes Element  $\bar{a} \neq \bar{0}$  hat ein Inverses.

Satz 5.20: die Zahlen (Repräsentanten der Elemente von  $\mathbb{Z}/p\mathbb{Z}$ )  $1, 2, 3, \dots, p-1$  sind zu  $p$  teilerfremd:

$\text{ggT}(a, p) = 1 \quad \forall \quad a = 1, 2, \dots, p-1 \Rightarrow T_p = \{1, p\} \Rightarrow p$  ist Primzahl.  $\square$

**Bemerkung 5.23.** Das Inverse eines Elementes  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  findet man mit Hilfe des Euklidischen Algorithmus' bzw. durch Lösen der linearen diophantischen Gleichung:

$$x \cdot a + y \cdot m = 1 \quad \Rightarrow \quad \bar{a}^{-1} = \bar{x}$$



**Beispiel:** Bestimme  $\bar{7}^{-1} \in \mathbb{Z}/12\mathbb{Z}$ :  $(\text{ggT}(7, 12) = 1 \Rightarrow \bar{7}^{-1} \text{ existiert})$

$$7 \cdot x \equiv 1 \pmod{12} \Leftrightarrow 7x + 12y = 1$$

$$12 = 1 \cdot 7 + 5 \quad (5 = 12 - 7)$$

$$7 = 1 \cdot 5 + 2 \quad (2 = 7 - 5)$$

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

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

$$= 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7$$

$$= 3 \cdot (12 - 7) - 2 \cdot 7$$

$$= 3 \cdot 12 - 5 \cdot 7$$

$$\Leftrightarrow 7 \cdot (-5) = 1 - 3 \cdot 12$$

$$\Leftrightarrow 7 \cdot (-5) \equiv 1 \pmod{12}$$

$$\Leftrightarrow \bar{7} \odot \overline{(-5)} = \bar{1} \quad (\text{in } \mathbb{Z}/12\mathbb{Z})$$

$$\Rightarrow \bar{7}^{-1} = \overline{-5} = \bar{7} \in \mathbb{Z}/12\mathbb{Z}$$

Klar:  $7 \cdot 7 = 7^2 = 49 = 1 + 48 = 1 + 4 \cdot 12 \equiv 1 \pmod{12}$

□

**Bemerkungen:**

- (1) in  $\mathbb{Z}/p\mathbb{Z}$ , mit einer Primzahl  $p$ , haben alle Elemente  $\neq 0$  ein multiplikatives Inverses  $\Rightarrow \bar{a} \in \mathbb{Z}/p\mathbb{Z}, \bar{a} \neq \bar{0}$  dann existiert  $\bar{a}^{-1} \in \mathbb{Z}/p\mathbb{Z}$ .
- (2) in  $\mathbb{Z}/m\mathbb{Z}$ ,  $m$  beliebig, haben genau die Elemente  $\bar{a} \neq \bar{0}$  mit  $\text{ggT}(a, m) = 1$  ein Inverses  $\bar{a}^{-1}$ .  
(vgl. Multiplikationstafel von  $\mathbb{Z}/6\mathbb{Z}$ : nur 5 ist zu 6 teilerfremd!  $\Rightarrow$  nur  $\bar{5}^{-1} = \bar{5}$  existiert, sogar selbstinvers!)



### 5.4. Die Sätze von Euler, Fermat und der Chinesische Restsatz.

**Eulersche  $\varphi$ -Funktion:**  $\varphi(m) := \#\{x \in \{1, 2, \dots, m\} \mid \text{ggT}(x, m) = 1\}$

$$\begin{array}{ccccc} \underbrace{\varphi(1)}_{\{1\}} = 1, & \underbrace{\varphi(2)}_{\{1\}} = 1, & \underbrace{\varphi(3)}_{\{1,2\}} = 2, & \underbrace{\varphi(4)}_{\{1,3\}} = 2, & \underbrace{\varphi(5)}_{\{1,2,3,4\}} = 4, \\ \underbrace{\varphi(6)}_{\{1,5\}} = 2, & \underbrace{\varphi(7)}_{\{1,2,3,4,5,6\}} = 6, & \underbrace{\varphi(8)}_{\{1,3,5,7\}} = 4, & \underbrace{\varphi(9)}_{\{1,2,4,5,7,8\}} = 6, & \underbrace{\varphi(10)}_{\{1,3,7,9\}} = 4 \end{array}$$

$\Rightarrow$  Offensichtlich gilt für Primzahlen  $p$ :  $\varphi(p) = p - 1$   
(denn  $\{1, 2, \dots, p-1\}$  sind zu  $p$  teilerfremd!)

$\Rightarrow \varphi(m)$  hat was mit der Anzahl der invertierbaren Elemente in  $\mathbb{Z}/m\mathbb{Z}$  zu tun, was?

Klar,  $\varphi(m)$  ist genau die Anzahl der invertierbaren Elemente in  $\mathbb{Z}/m\mathbb{Z}$  (vgl. Satz 5.20)

**Satz 5.24** (Eulerscher Satz). Für alle teilerfremden Zahlen  $a, m \in \mathbb{N}$  gilt:  
 $a^{\varphi(m)} \equiv 1 \pmod{m}$

Äquivalent:

$$\bar{a}^{\varphi(m)} = \bar{1} \quad \text{in } \mathbb{Z}/m\mathbb{Z}$$

**Beispiele (1)**  $m = 7$ , (also  $\varphi(7) = 6$ )  $\Rightarrow$  für alle  $a \in \mathbb{N}$  mit  $\text{ggT}(a, 7) = 1$  gilt

$$a^6 \equiv 1 \pmod{7} \quad \Leftrightarrow \quad 7 \mid a^6 - 1$$

$\Rightarrow$  unendlichviele Teilbarkeitsaussagen:

$$\begin{array}{ccccccc} 7 \mid \underbrace{1^6 - 1}_{=0}, & 7 \mid \underbrace{2^6 - 1}_{=63}, & 7 \mid \underbrace{3^6 - 1}_{=728=7 \cdot 104}, & 7 \mid \underbrace{4^6 - 1}_{=4095=7 \cdot 585}, \\ & 7 \mid \underbrace{5^6 - 1}_{=15.624=7 \cdot 2232}, & 7 \mid 6^6 - 1, & 7 \mid 8^6 - 1, \dots \end{array}$$

**(2)** Frage nach dem Rest: z.B. Was ist der Rest von  $2^{81}$  bei der Division durch 5? Also:  $2^{81} \equiv ? \pmod{5}$  Es gilt:  $\varphi(5) = 4$

$$\begin{aligned} 2^{80} &= 2^{4 \cdot 20} = (2^{20})^4 = (2^{20})^{\varphi(5)} \stackrel{\text{Satz 5.24}}{\equiv} 1 \pmod{5} \quad \text{da } \text{ggT}(2^{20}, 5) = 1 \\ \Rightarrow 2^{81} &= 2 \cdot 2^{80} \equiv 2 \cdot 1 \equiv 2 \pmod{5} \end{aligned}$$



**Beweis:**

Sei  $m \in \mathbb{N}$ . Nach Definition gibt es genau  $\varphi(m)$  zu  $m$  teilerfremde Zahlen  $< m$ :

$$1 \leq r_1 < r_2 < r_3 < \dots < r_{\varphi(m)} < m$$

Ihre Restklassen:

$$\overline{r_1}, \overline{r_2}, \dots, \overline{r_{\varphi(m)}} \in \mathbb{Z}/m\mathbb{Z}$$

sind genau die invertierbaren Elemente von  $\mathbb{Z}/m\mathbb{Z}$ .

Da  $1 \leq r_i < m \Rightarrow$  für alle  $i \neq j$  gilt:

$$1 \leq |r_i - r_j| < m$$

$$\Rightarrow m \nmid r_i - r_j \Rightarrow r_i \not\equiv r_j \pmod{m} \quad \forall i \neq j$$

$$\Rightarrow \overline{r_1}, \overline{r_2}, \dots, \overline{r_{\varphi(m)}} \quad \text{paarweise verschieden}$$

$$\Rightarrow \left\{ \overline{r_1}, \overline{r_2}, \dots, \overline{r_{\varphi(m)}} \right\} = (\mathbb{Z}/m\mathbb{Z})^* = \text{Gruppe der invertierbaren Elemente.}$$

Sei nun  $a \in \mathbb{N}$  teilerfremd zu  $m$ .

Dann gilt

$$(1) \quad ar_i \text{ ist teilerfremd zu } m \text{ für alle } i = 1, \dots, \varphi(m) \Rightarrow \overline{ar_i} \in (\mathbb{Z}/m\mathbb{Z})^*$$

$$(2) \quad \overline{ar_i} \neq \overline{ar_j} \text{ in } (\mathbb{Z}/m\mathbb{Z})^* \text{ für alle } i \neq j,$$

$$\left( \text{denn sonst } m \mid ar_i - ar_j = \begin{array}{ccc} a & (r_i - r_j) & \not\equiv 0 \\ \uparrow & \uparrow & \\ \text{ggT}(a,m)=1 & m \nmid (r_i - r_j) & \end{array} \right)$$

$\Rightarrow \overline{ar_1}, \overline{ar_2}, \dots, \overline{ar_{\varphi(m)}}$  sind paarweise verschiedene invertierbare Elemente von  $(\mathbb{Z}/m\mathbb{Z})^*$

$$\Rightarrow \left\{ \overline{ar_1}, \overline{ar_2}, \dots, \overline{ar_{\varphi(m)}} \right\} = \left\{ \overline{r_1}, \overline{r_2}, \dots, \overline{r_{\varphi(m)}} \right\}$$

$$\Rightarrow \overline{ar_1} \cdot \overline{ar_2} \cdot \dots \cdot \overline{ar_{\varphi(m)}} = \overline{r_1} \cdot \overline{r_2} \cdot \dots \cdot \overline{r_{\varphi(m)}} \quad \text{in } (\mathbb{Z}/m\mathbb{Z})^*$$

$$\Rightarrow (ar_1) \cdot (ar_2) \cdot \dots \cdot (ar_{\varphi(m)}) \equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \pmod{m}$$

$$a^{\varphi(m)} \cdot (r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}) \equiv (r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}) \pmod{m}$$

$$\Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

da  $r_1 \cdot \dots \cdot r_{\varphi(m)}$  teilerfremd zu  $m$ , dürfen wir dadurch teilen, vgl. Korollar 5.10

□

**Satz 5.25** (Kleiner Satz von Fermat). Ist  $a \in \mathbb{N}$  und  $p$  eine Primzahl die  $a$  nicht teilt ( $p \nmid a$  oder  $\text{ggT}(p, a) = 1$ ), so gilt

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

**Beweis:**

Direkte Folgerung aus  $\varphi(p) = p - 1$ .

□





**Korollar 5.26.** Für jede Primzahl  $p$  und  $a \in \mathbb{N}$  gilt:

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

**Beweis:**

Wenn  $\text{ggT}(a, p) = 1$  ist das eine Folgerung aus dem Kleinen Fermat'schen Satz.

Wenn  $\text{ggT}(a, p) \neq 1$ , also  $\text{ggT}(a, p) = p \Rightarrow p \mid a$

$$\Rightarrow a \equiv 0 \pmod{p} \quad \text{und damit auch } a^n \equiv 0 \pmod{p}$$

Also ist in diesem Fall die Aussage trivial!  $\square$

**Satz 5.27.** Für alle natürlichen Zahlen  $n \in \mathbb{N}$  gilt  $\sum_{d \mid n} \varphi(d) = n$ .

**Beweis**

Für jeden Teiler  $d \in T_n$  definiere die Menge

$$C_d := \{ x \in \{1, 2, \dots, n\} \mid \text{ggT}(x, n) = d \}.$$

Damit gilt: wenn  $x \in \{1, \dots, n\}$ , dann  $x \in C_d$  mit  $d := \text{ggT}(x, n)$ .

D.h. jedes  $x \in \{1, \dots, n\}$  ist eindeutig in einem  $C_d$  enthalten.

$$\bigcup_{d \mid n} C_d = \{1, 2, 3, \dots, n\}$$

Zahlenbeispiel:  $n = 12 = 2^2 \cdot 3$ , dann  $T_{12} = \{1, 2, 3, 4, 6, 12\}$  und

$$C_1 = \{1 \leq x \leq 12 \mid \text{ggT}(x, 12) = 1\} = \{1, 5, 7, 11\} \quad \varphi(12) = 4$$

$$C_2 = \{1 \leq x \leq 12 \mid \text{ggT}(x, 12) = 2\} = \{2, 10 = 2 \cdot 5\} \quad \varphi\left(\frac{12}{2} = 6\right) = 2$$

$$C_3 = \{1 \leq x \leq 12 \mid \text{ggT}(x, 12) = 3\} = \{3, 9\} \quad \varphi\left(\frac{12}{3} = 4\right) = 2$$

$$C_4 = \{1 \leq x \leq 12 \mid \text{ggT}(x, 12) = 4\} = \{4, 8 = 2 \cdot 4\} \quad \varphi\left(\frac{12}{4} = 3\right) = 3 - 1 = 2$$

$$C_6 = \{1 \leq x \leq 12 \mid \text{ggT}(x, 12) = 6\} = \{6\} \quad \varphi\left(\frac{12}{6} = 2\right) = 2 - 1 = 1$$

$$C_{12} = \{1 \leq x \leq 12 \mid \text{ggT}(x, 12) = 12\} = \{12\} \quad \varphi(1) = 1$$

Sicherlich sind die Mengen  $C_d$  für verschiedene Teiler  $d$  von  $n$  disjunkt:

$$\bigcup_{d \mid n} C_d = \{1, 2, 3, \dots, n\}$$



Ausserdem gilt

$$\begin{aligned}
 \#C_d &= \#\{ x \in \{1, 2, \dots, n\} \mid ggT(x, n) = d \} \quad (\text{somit } d \mid x \text{ bzw. } x = d \cdot y) \\
 &= \#\{ y \in \{1, 2, \dots, \frac{n}{d}\} \mid \underbrace{ggT(d \cdot y, n) = d}_{ggT(y, \frac{n}{d})=1} \} \quad (\text{da } d \mid n) \\
 &= \varphi\left(\frac{n}{d}\right)
 \end{aligned}$$

Schließlich folgt:

$$n = \#\{1, 2, 3, \dots, n\} = \# \bigcup_{d \mid n} C_d = \sum_{d \mid n} \#C_d = \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) \stackrel{\substack{= \\ \uparrow \\ \text{durch Umsummieren}}}{=} \sum_{d \mid n} \varphi(d)$$

□

**Satz 5.28.** Für jede Primzahl  $p$  und jedes  $n \in \mathbb{N}$  gilt:

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

**Beweis** Nach Satz 5.27 gilt

$$\begin{aligned}
 p^n &= \sum_{d \mid p^n} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^n) \\
 p^{n-1} &= \varphi(1) + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^{n-1}) \\
 \Rightarrow \quad p^n - p^{n-1} &= \varphi(p^n)
 \end{aligned}$$

□

### Handbuch der Arithmetik des Chinesen Sun-Tzu, vor ca. 2000 Jahren:

Es soll eine Anzahl von Dingen gezählt werden. Zählt man sie zu je drei, dann bleiben zwei übrig. Zählt man sie zu je fünf, dann bleiben drei übrig. Zählt man sie zu je sieben, dann bleiben zwei übrig. Wie viele sind es??

Was ist gemeint?

$$x \equiv 2 \pmod{3}$$

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

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

Zur Lösung:

$$x \equiv 2 \pmod{3} \quad \Rightarrow x \in \{\dots, -1, 2, 5, 8, \dots\}$$

$$x \equiv 3 \pmod{5} \quad \Rightarrow x \in \{\dots, -2, 3, 8, 13, \dots\}$$

$$x \equiv 2 \pmod{7} \quad \Rightarrow x \in \{\dots, -5, 2, 9, 16, \dots\}$$

**Satz 5.29** (Chinesischer Restsatz). Seien  $m_1, m_2, \dots, m_k$  paarweise teilerfremde natürliche Zahlen und  $a_1, a_2, \dots, a_k \in \mathbb{Z}$ . Das System linearer Kongruenzen:

$$x \equiv a_1 \pmod{m_1}$$

$$\vdots$$

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

ist lösbar. Alle Lösungen sind kongruent modulo  $m := m_1 \cdot m_2 \cdots m_k$ , d.h. die Restklasse  $\bar{x}$  der Lösung  $x$  ist in  $\mathbb{Z}/m\mathbb{Z}$  eindeutig.

**Beweis** (der Beweis ist konstruktiv!)

Lösbarkeit: Setze:

$$m := m_1 \cdot m_2 \cdots m_k$$

$$q_i := \frac{m}{m_i} = m_1 \cdots \overset{\vee}{m_i} \cdots m_k$$

$$m_i \text{ paarweise teilerfremd} \Rightarrow \text{ggT}(m_i, q_i) = 1 \Leftrightarrow \bar{q}_i \in \mathbb{Z}/m_i\mathbb{Z} \text{ invertierbar}$$



$\Rightarrow q_i \cdot z \equiv 1 \pmod{m_i}$  ist lösbar (vgl. Korollar 5.21)

Sei  $q'_i$  eine Lösung, d.h.  $q'_i$  ist ein Repräsentant von  $\bar{q}_i^{-1} \in \mathbb{Z}/m_i\mathbb{Z}$

$$q_i \cdot q'_i \equiv 1 \pmod{m_i} \quad \text{für } i = 1, 2, \dots, k$$

Sei

$$x := a_1 \cdot q_1 \cdot q'_1 + a_2 \cdot q_2 \cdot q'_2 + \dots + a_k \cdot q_k \cdot q'_k$$

Modulo  $m_i$  gilt:

$$\begin{aligned} x &= a_1 \cdot \underbrace{q_1}_{m_i} \cdot q'_1 + a_2 \cdot \underbrace{q_2}_{m_i} \cdot q'_2 + \dots + a_i \cdot \underbrace{q_i \cdot q'_i}_{\substack{\uparrow \\ \text{ggT}(q_i, m_i)=1}} + \dots + a_k \cdot \underbrace{q_k}_{m_i} \cdot q'_k \\ &\equiv a_i \cdot q_i \cdot q'_i \pmod{m_i} \\ &\equiv a_i \qquad \qquad \qquad \text{da } q_i \cdot q'_i \equiv 1 \end{aligned}$$

Das geht für alle  $i = 1, \dots, k$ , damit ist  $x$  eine Lösung.

Eindeutigkeit:

Sei  $y$  eine weitere Lösung:

$$\begin{aligned} \Rightarrow \quad x &\equiv a_i \pmod{m_i} \quad \text{und} \quad y \equiv a_i \pmod{m_i} \quad (\text{für } i=1, \dots, k) \\ \Rightarrow \quad x &\equiv y \pmod{m_i} \quad (\text{für } i=1, \dots, k) \\ \Rightarrow \quad m_i &\mid (x - y) \quad (\text{für } i=1, \dots, k) \\ \Rightarrow \quad m &\mid (x - y) \quad \text{da die } m_i \text{ paarweise teilerfremd} \\ \Rightarrow \quad x &\equiv y \pmod{m} \\ \Leftrightarrow \quad \bar{x} &= \bar{y} \quad \text{in } \mathbb{Z}/m\mathbb{Z} \end{aligned}$$

□

**Beispiel:** Sei

$$\begin{aligned} x &\equiv 1 \pmod{3} & (i=1) \\ x &\equiv 3 \pmod{7} & (i=2) \\ x &\equiv 5 \pmod{11} & (i=3) \\ \Rightarrow \quad m &= 3 \cdot 7 \cdot 11 = 231 \\ \Rightarrow \quad q_1 &= \overset{\vee}{3} \cdot 7 \cdot 11 = 77, \quad q_2 = 3 \cdot \overset{\vee}{7} \cdot 11 = 33, \quad q_3 = 3 \cdot 7 = 21 \end{aligned}$$



Finde Repräsentanten  $q'_i$  von  $\bar{q}_i^{-1}$  (modulo  $m_i$ ):

$$\begin{aligned} i = 1 : \text{in } \mathbb{Z}/3\mathbb{Z} : \quad \bar{q}_1 &= \overline{77} = \overline{3 \cdot 25 + 2} = \bar{2}, & \text{selbstinvers} &\Rightarrow q'_1 = 2 \\ i = 2 : \text{in } \mathbb{Z}/7\mathbb{Z} : \quad \bar{q}_2 &= \overline{33} = \overline{7 \cdot 4 + 5} = \bar{5}, & \bar{5} \cdot \bar{3} = \overline{15} = \bar{1} &\Rightarrow q'_2 = 3 \\ i = 3 : \text{in } \mathbb{Z}/11\mathbb{Z} : \quad \bar{q}_3 &= \overline{21} = \overline{10}, & \overline{10} \cdot \overline{10} = \overline{99 + 1} = \bar{1} &\Rightarrow q'_3 = 10 \end{aligned}$$

$$\begin{aligned} x &= a_1 \cdot q_1 \cdot q'_1 + \cdots = 1 \cdot \overset{77, \text{ nicht } 2}{\downarrow} 77 \cdot 2 + 3 \cdot 33 \cdot 3 + 5 \cdot 21 \cdot 10 \\ &= 1501 = 6 \cdot 231 + 115 \end{aligned}$$

(in der Formel sind die  $q_i$ 's nicht unabhängig vom Repräsentanten, denn es wird benutzt, daß z. B.  $m_2 = 7$  die Zahl  $q_1 = 77$  teilt, aber  $7 \nmid 2!$  )

$$\Rightarrow \quad \bar{x} = \overline{115} \quad \text{in} \quad \mathbb{Z}/231\mathbb{Z}$$

$$\begin{aligned} \textbf{Probe:} \quad 115 &= 38 \cdot 3 + 1 \equiv 1 \pmod{3} && \checkmark \\ 115 &= 16 \cdot 7 + 3 \equiv 3 \pmod{7} && \checkmark \\ 115 &= 10 \cdot 11 + 5 \equiv 5 \pmod{11} && \checkmark \end{aligned}$$

Zurück zur Euler- $\varphi$ -Funktion:

**Satz 5.30.** Für teilerfremde Zahlen  $n$  und  $m$  gilt:

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

**Beweis:**

Noch ohne Beweis, bei Beweis wird der Chinesische Restsatz benutzt! □

### Beispiel aus der Astronomie

Die drei inneren Planeten unseres Sonnensystems: Merkur, Venus und Erde haben Umlaufzeiten von (gerundet) 88, 225 und 365 Tagen um die Sonne. Angenommen, ein Bahnradius  $R$  wird von Merkur in 15, von der Venus in 43 und von der Erde in 100 Tagen erreicht. Kann es sein, daß sich

- (1) Merkur und Venus,
- (2) Merkur und Erde,
- (3) Venus und Erde
- (4) Merkur, Venus und Erde

irgendwann gleichzeitig auf dem Radius  $R$  befinden? Wenn ja, wann ist das?

**Vgl. Geogebra: Bahnschleifen**

**Zur Lösung dieses Problems:**

Merkur befindet sich immer nach  $15 + n_M \cdot 88$  Tagen auf  $R$ , entsprechend befindet sich Venus immer nach  $43 + n_V \cdot 225$  und die Erde nach  $100 + n_E \cdot$



365 Tagen auf  $R$ . Also müssen zur Lösung von (1)-(4) Systeme von Linearen Kongruenzen gelöst werden:

- (1) Merkur und Venus:  $x \equiv 15 \pmod{88}$  und  $x \equiv 43 \pmod{225}$
- (2) Merkur und Erde:  $x \equiv 15 \pmod{88}$  und  $x \equiv 100 \pmod{365}$
- (3) Venus und Erde:  $x \equiv 43 \pmod{225}$  und  $x \equiv 100 \pmod{365}$
- (4) Merkur, Venus und Erde:  
 $x \equiv 15 \pmod{88}, \quad x \equiv 43 \pmod{225} \quad \text{und} \quad x \equiv 100 \pmod{365}$

Da  $88 = 2^3 \cdot 11$ ,  $225 = 3^2 \cdot 5^2$  und  $365 = 5 \cdot 73$  sind die Moduln 88, 225 bzw. 88 und 365 paarweise teilerfremd.

Zu (1):

$$x \equiv 15 \pmod{88} \quad (\text{i}=1)$$

$$x \equiv 43 \pmod{225} \quad (\text{i}=2)$$

$$\Rightarrow m = 88 \cdot 225 = 19800$$

$$\Rightarrow q_1 = \overset{\vee}{88} \cdot 225 = 225, \quad q_2 = 88 \cdot \overset{\vee}{225} = 88,$$

Repräsentanten  $q'_i$  von  $\bar{q}_i^{-1}$  (modulo  $m_i$ )?

$$9 \cdot 225 - 23 \cdot 88 = 1$$

$$i = 1 : \text{in } \mathbb{Z}/88\mathbb{Z} : \quad \bar{q}_1 = \overline{225}, \quad \bar{9} \cdot \overline{225} = \bar{1} \Rightarrow q'_1 = 9$$

$$i = 2 : \text{in } \mathbb{Z}/225\mathbb{Z} : \quad \bar{q}_2 = \overline{88}, \quad \overline{202} \cdot \overline{88} = \overline{-23} \cdot \overline{88} = \bar{1} \Rightarrow q'_2 = 202$$

$$x = a_1 \cdot q_1 \cdot q'_1 + \dots = 15 \cdot 225 \cdot 9 + 43 \cdot 88 \cdot 202$$

$$= 794\,743 = 40 \cdot 19800 + 2743$$

$$\text{Probe:} \quad 2743 = 31 \cdot 88 + 15$$

$$2743 = 12 \cdot 225 + 43$$

Also in 2743 Tagen ( $\approx 7,5$  Jahre) sind Merkur und Venus auf einem Bahnradius!

## 6. STELLENWERTSYSTEME

### 6.1. Verschiedene Stellenwertsysteme.

**Sumerer im 3ten Jt v.Chr., Babylon im 2ten Jt. v.Chr., Sexagesimal-system:** Stellenwertsystem (Positionssystem) mit Basis 60, die Zahlensymbole in Keilschrift:





Bemerkenswert und innovativ: ein Zeichen für Null! (seit Ptolemaios 150 n.Chr.)  
*Das sexagesimale Positionssystem war außerordentlich leistungsfähig und allen späteren Zahlensystemen der Antike überlegen. Daher wurde es u.a. von den griechisch-hellenistischen Mathematikern dort verwendet, wo viele ausgiebige Rechnungen durchgeführt werden mussten, insbesondere in der Astronomie [Wußing, 6000 Jahre Mathematik, Eine kulturgeschichtliche Zeitreise, Berlin/Heidelberg, (2008), p. 130]*

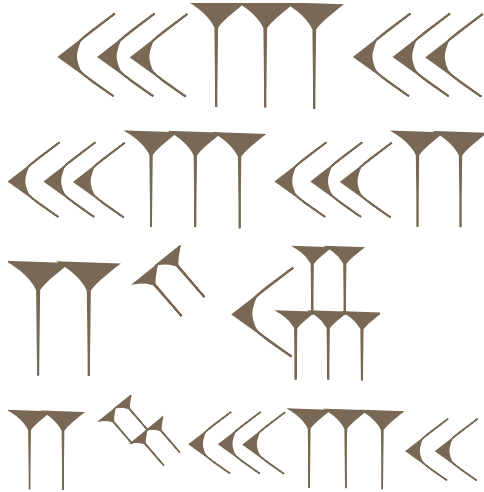
*Die babylonische Schreibweise hatte auch Nachteile. Daß man zwischen 1 und 60 in der Schreibweise keinen Unterschied machen kann, ist für den täglichen Gebrauch nicht allzu schlimm, weil die Größenordnung meistens sowieso bekannt ist (wir wissen ja auch, wenn im Schaufenster die Zahl 30 auf einer Bluse steht, dass es sich nicht um 30 Pfennig handelt); aber bei rein theoretischen Aufgaben kann es doch unangenehm sein. Noch unangenehmer ist es, wenn man in der Schreibweise zwischen 1, 0, 30 und 1,30 nicht unterscheiden konnte, weil die Null nicht existierte. Um diese Schwierigkeit zu beheben, hat man später ein eigenes Zeichen für den leeren Platz zwischen zwei Ziffern eingeführt, zum Beispiel:*

$$\begin{array}{c} \text{triangle} \\ | \end{array} \begin{array}{c} \text{triangle} \\ | \end{array} \begin{array}{c} \text{triangle} \\ | \end{array} = 1, 0, 4 \text{ (60-iger Syst.)} = 3604 \text{ (10-er Syst.)}.$$

*Der Griechische Astronom Ptolemaios (150 n. Chr.), der immer sexagesimal rechnete, braucht das Zeichen 0 für Null, auch am Ende einer Zahl. Das gab dem sexagesimalen Positionssystem den letzten Schliff: dadurch wurde es fast gleichwertig mit unserem dezimalen Positionssystem. Ptolemaios schreibt zwar die ganzen Zahlen dezimal und nur die Brüche sexagesimal, aber das spielt keine große Rolle, da er fast nie große ganze Zahlen braucht. Die starke Überlegenheit der sexagesimalen Bruchrechnung war der Grund, dass die Astronomen*

*immer mit Sexagesimalbrüchen rechneten: daher stammen auch unsere Minuten und Sekunden. [van der Waerden, Erwachende Wissenschaft II, p. 62-63]*

Zahlenbeispiele:



*... haben babylonische Einflüsse mit Langzeitwirkung auf Kulturtraditionen Europas gewirkt. Etliche unserer Maßeinheiten zur Messung der Zeit u.ä. leiten sich vom babylonischen Positionssystem ab:*

- *Sexagesimale Zeitmaße: Die Sexagesimal-Zählung strukturiert die Einteilung des Tagesrhythmus in kleinere Zeiteinheiten: Tag + Nacht ( $24 = 2 \times 6$  bzw.  $2 \times 12$  Stunden), 1 Stunde ( $60 = 6 \times 10$  Minuten), 1 Minute ( $60 = 6 \times 10$  Sekunden).*
- *Sexagesimale Bogen und Winkelmaße: z.B. Gradeinteilung ( $360^\circ = 6 \times 60$  Gradeinheiten).*

[H. Haarmann, Weltgeschichte der Zahlen, C.H.Beck-Wissen (2008), auch für weiteres:]

**Vigesimalsystem:** Zahlssystem mit Basis 20, in der Sprache enthalten z.B. in Asien (Chepang, Ainu, Tschuktschisch), Ozeanien (Drehu, Daga, Mangap-Mbula), Amerika (Zoque, Yukatekisch, Warao, Caribe), Afrika (Igbo, Yoruba, Kana, und die Niger-Kongo-Sprache Diola-Fogny).

**Duales- bzw. Binäres System: Computer!**

**Dezimalsysteme:** Zum erstem mal in Indien im 6. Jhd. n. Chr. nachgewiesen. Auch in Mittelamerika (Bibri, Nahuatl)





8 Jhd. n. Chr.: dezimales System + arabische Ziffern wurde nach Europa eingeführt, es dauerte aber noch einige Jahrhunderte, bis es sich in Europa durchsetzte. Einen wichtigen Beitrag dazu lieferte Adam Ries (1492-1559) mit seinen Rechenbüchern.

### **Vigesimal-dezimales Mischsystem**

In vielen Sprachen, deren Zahlwortsysteme Vigesimal- und Dezimalsystem erkennen lassen, z.B. in Französischen: im Bereich 80 – 99 gilt die 20-er Ordnung, z.B. *quatre-vingt-dix-huit*:  $4 \times 20 + 10 + 8 = 98$ .

**Fünfer-Zwanziger Mischsystem** Mittelamerika: Aztekisch:

## 6.2. Prinzip des Stellenwertsystems.

Stellenwertsystem der Basis  $b$ :

- $b$  Symbole/Ziffern nötig
- Wert einer Ziffer gibt Anzahl der Bündel der betreffenden Mächtigkeit an.
- Stellung/Position der Ziffer gibt an, um welche Mächtigkeit es sich handelt.

Beispiel: Analyse des Dezimalsystems:

- Zehn Ziffern:  $0, 1, 2, \dots, 9$
- Mächtigkeiten: Zehnerpotenzen  $10^n$
- Wert einer Ziffer gibt Anzahl der Bündel der betreffenden Mächtigkeit an.
- Stellung/Position der Ziffer gibt an, um welche Mächtigkeit es sich handelt.

### Beispiele

- (1)  $51037 = 5 \cdot 10^4 + 1 \cdot 10^3 + 0 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$
- (2) 5555 hier bedeutet die Ziffer 5 je nach Position Einer, Zehner, Hunderter oder Tausender!

Hat man das Prinzip verstanden, so läßt es sich leicht auf andere Basen übertragen:

Basis 2:

Dezimalsystem      Dualsystem

$$25_{10} = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 11001_2$$

Algorithmus: suche größte 2er-Potenz, die  $\leq 25$ , hier:  $16 = 2^4 < 25 < 32 = 2^5$ .  
da  $25 = 1 \cdot 16 + 9$  mache nun mit 9 so weiter:  $9 = 8 + 1 = 2^3 + 1$ . etc.

Beachte: im Dualsystem gibt es nur die Ziffern 0 und 1!

### Allgemein:

- Ist die Basis  $b < 10 \Rightarrow$  die Ziffern  $0, 1, \dots, b-1$  reichen für die Darstellung der Zahlen aus. Natürlich können auch neue Ziffern erfunden werden.



- Ist die Basis  $b > 10$ , so brauchen wir neue Symbole, z.B.: im Duodezimalsystem  $\Leftrightarrow$  Basis  $b = 12$ , setze  $z := 10$  und  $e = 11$ :

$$\begin{aligned}
 e\,4\,z\,0\,e_{12} &= 11 \cdot 12^4 + 4 \cdot 12^3 + 10 \cdot 12^2 + 0 \cdot 12^1 + 11 \cdot 12^0 \\
 \begin{array}{ccccc}
 | & | & | & | & | \\
 4 & 3 & 2 & 1 & 0
 \end{array} & \\
 &= 11 \cdot 12^4 + 4 \cdot 12^3 + 10 \cdot 12^2 + 11 = \\
 &= 236459_{10} = 236459
 \end{aligned}$$

Ohne die neuen Ziffern  $z$  und  $e$  ließe sich die Zahl nicht eindeutig schreiben:

$$e\,4\,z\,0\,e_{12} = 11\,4\,12\,0\,11_{12} \stackrel{\text{besser}}{=} (11)\,4\,(12)\,0\,(11)$$

Die Zahl 25 im Duodezimalsystem:

$$25 = 2 \cdot 12 + 1 = 21_{12}$$

### Fragen:

- Warum findet man sehr häufig auf der Welt das Dezimalsystem?  
*Schon immer haben Menschen ihr Zehn Finger als "Taschenrechner" benutzt.*
- Kann man jede natürliche Zahl als Basis für ein Stellenwertsystem benutzen?

Ja, vgl. nächsten Satz.

**Satz 6.1.** Sei  $b \in \mathbb{N} \setminus \{1\}$ . Jede Zahl  $a \in \mathbb{N}$  läßt sich eindeutig in der Form

$$a = k_n b^n + k_{n-1} b^{n-1} + \cdots + k_1 b + k_0$$

mit  $k_i \in \mathbb{N}_0$ ,  $k_n \neq 0$  und  $0 \leq k_i < b$  für  $i = 0, 1, \dots, n$  darstellen.

### Beweis

(Der Beweis ist konstruktiv, vgl. Beispiel am Ende des Kapitels.)

Eindeutigkeit der Division mit Rest impliziert:

$$\begin{aligned}
 a &= q_0 \cdot b + k_0, & 0 \leq k_0 < b, \quad q_0 \in \mathbb{N} \\
 q_0 &= q_1 \cdot b + k_1, & 0 \leq k_1 < b, \quad q_1 \in \mathbb{N} \\
 q_1 &= q_2 \cdot b + k_2 & \vdots \\
 &\vdots & \vdots \\
 \Rightarrow a &> q_0 > q_1 > q_2 \cdots > 0
 \end{aligned}$$

$\Rightarrow$  der Algorithmus muss abbrechen, d.h. es gibt ein  $n \in \mathbb{N}$  mit  $q_n = 0$ .



Die letzten Schritte lauten somit:

$$\begin{aligned} q_{n-2} &= q_{n-1} \cdot b + k_{n-1}, & 0 \leq k_{n-1} < b, \quad q_{n-1} \in \mathbb{N} \\ q_{n-1} &= q_n \cdot b + k_n = k_n \\ &\quad \parallel \\ &\quad 0 \end{aligned}$$

Sukzessives Einsetzen:

$$\begin{aligned} a &= q_0 \cdot b + k_0 \\ &= (q_1 \cdot b + k_1) \cdot b + k_0 = q_1 b^2 + k_1 b + k_0 \\ &= (q_2 b + k_2) b^2 + k_1 b + k_0 = q_2 b^3 + k_2 b^2 + k_1 b + k_0 \\ &\vdots \\ &= q_{n-1} b^n + k_{n-1} b^{n-1} + \cdots + k_1 b + k_0 \\ &\quad \parallel \\ &\quad k_n \end{aligned}$$

□

### Warum Stellenwertsysteme behandeln?

- Unterscheidung Zahl und Zahlwort wird thematisiert.  
Z.B. Bedeutung vermeindlich besonderer Zahlen (z.B. Geburtstage) wird relativiert:

$$20 = 20_{\textcircled{9}} = 2 \cdot 9 + 2 = 22_{\textcircled{9}} = 1 \cdot 11 + 9 = 19_{\textcircled{11}}$$

- Computer arbeiten im Dualsystem: Basis 2
- Verständnis des Babylonischen Sexagezimalsystems und der daraus abgeleiteten Zeit- und Winkelmaße.
- Das Verständnis des Stellenwertsystems fördert auch das Verständnis von Dezimalbrüchen und Teilbarkeitsregeln.
- Polynome mit Koeffizienten aus  $\mathbb{N}$ .

### 6.3. Zahlen in verschiedenen Zahlssystemen.

#### Vorgänger und Nachfolger:

Beispiel: Basis 3:  $N$  = Neuner,  $D$  = Dreier,  $E$  = Einser



Nachfolger:

$$\begin{array}{c|c|c} N & D & E \\ \hline \times & \times & \times \\ \times & & \times \\ 2 & 1 & 2 \end{array} \xrightarrow{+1} \begin{array}{c|c|c} N & D & E \\ \hline \times & \times & \times \\ \times & & \times \\ 2 & 1 & 2+1 \end{array} \xrightarrow{\text{Umbündeln} \approx} \begin{array}{c|c|c} N & D & E \\ \hline \times & \times & \\ \times & \times & \\ 2 & 2 & 0 \end{array}$$

d.h.  $212_{(3)}$  hat den Nachfolger  $220_{(3)}$

Vorgänger:

$$\begin{array}{c|c|c} N & D & E \\ \hline \times & \times & \times \\ \times & & \times \\ 2 & 1 & 2 \end{array} \xrightarrow{-1} \begin{array}{c|c|c} N & D & E \\ \hline \times & \times & \times \\ \times & & \times \\ 2 & 1 & 1 \end{array}$$

hier ist keine Umbündelung nötig.

Aber beim folgenden Beispiel:

Vorgänger mit Umbündelung:

$$\begin{array}{c|c|c} N & D & E \\ \hline \times & \times & \\ \times & & \\ 2 & 1 & 0 \end{array} \xrightarrow{\text{Umbündeln} \approx} \begin{array}{c|c|c} N & D & E \\ \hline \times & & \times \\ \times & & \times \\ 2 & 0 & 2+1 \end{array} \xrightarrow{-1} \begin{array}{c|c|c} N & D & E \\ \hline \times & & \times \\ \times & & \times \\ 2 & 0 & 2 \end{array}$$

Durch fortgesetzte Nachfolgerbildung, beginnend mit der Zahl 1, erhält man die Zählreihen bezüglich beliebiger Basen:

Basis 2: 1, 10, 11, 100, 101, 110, 111, 1000, 1001, ...

Basis 3: 1, 2, 10, 11, 12, 20, 21, 22, 100, 101, ...

Basis 4: 1, 2, 3, 10, 11, 12, 13, 20, 21, 22, ...

Basis 5: 1, 2, 3, 4, 10, 11, 12, 13, 14, 20, ...

Basis 10: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ...

**Folgerung:** Man muß zwischen einer Zahl und ihrem Zahlwort bzw. Zahlzeichen unterscheiden. Z.B. Anzahl der Finger einer Hand ist **Fünf** als Zahlwort und hat viele Zahlzeichen, beispielsweise:

$$5_{(10)} = 10_{(5)} = 11_{(4)} = 12_{(3)} = 101_{(2)}$$

Wie übersetzt man die Zahlzeichen eines Systems in ein anderes?

**Dezimalsystem  $\Rightarrow b$ -System:** Division mit Rest  $b$ .



Beispiel  $b = 12$ :

$$\begin{array}{ll}
 8924 = 8924_{\text{10}} & (\text{TR: } 8924 \div_{\text{R}} 12 \equiv) \\
 = 743 \cdot 12 + 8 & k_0 = 8 \\
 743 = 61 \cdot 12 + 11 & k_1 = 11 = e \\
 61 = 5 \cdot 12 + 1 & k_2 = 1 \\
 5 = 0 \cdot 12 + 5 & k_3 = 5 \\
 \Downarrow &
 \end{array}$$

Algorithmus bricht ab

$$\begin{aligned}
 & \overbrace{\overbrace{(5 \cdot 12 + 1)}^{61} \cdot 12 + 11}^{743} \cdot 12 + 8 = 5 \cdot 12^3 + 1 \cdot 12^2 + 11 \cdot 12 + 8 \\
 \Rightarrow 8924 &= ((5 \cdot 12 + 1) \cdot 12 + 11) \cdot 12 + 8 = 5 \cdot 12^3 + 1 \cdot 12^2 + 11 \cdot 12 + 8 \\
 &= 5 \, 1 \, (11) \, 8_{\text{12}} \\
 &= 5 \, 1 \, e \, 8_{\text{12}}
 \end{aligned}$$

Alternativ die intuitive Methode: Suche größte 12-er Potenz kleiner-gleich 8924 durch ausprobieren:

$$\begin{array}{ll}
 8924 & 12^3 = 1728 < 8924 < 20736 = 12^4 \\
 = 5 \cdot 12^3 + 284 & 8924 \div 12^3 = 5, \dots \Rightarrow 8924 - 5 \cdot 12^3 = 284 \\
 284 = 1 \cdot 12^2 + 140 & 284 \div 12^2 = 1, \dots \text{ etc.} \\
 140 = 11 \cdot 12 + 8 & \\
 8 = 8 \cdot 12^0 = 8 \cdot 1 &
 \end{array}$$

**b-System**  $\Rightarrow$  **Dezimalsystem** (an Polynome denken)

$$3714_{\text{8}} = 3 \cdot 8^3 + 7 \cdot 8^2 + 1 \cdot 8^1 + 4 \cdot 8^0 = 1996_{\text{10}}$$



## 7. DEZIMALBRÜCHE

7.1. **Gemeine Brüche und Dezimalbrüche.**

Bezeichnungen:  $\frac{7}{8}$  gemeiner Bruch  
0,875 Dezimalbruch

Vorteile gemeiner Brüche:

- (1) Rechnen mit Verhältnissen.
- (2) Bekannt aus dem Sprachgebrauch: Ein Viertel Pfund ..., ein halbes Kilo..., Halb/ Viertel-Finale, dreiviertel 2 Uhr, etc..
- (3) Rechnen mit Wahrscheinlichkeiten,
- (4) Äquivalenzumformungen, Algebra, Einfache Rechenoperationen bei Multiplikation und Division, Ableitungen!
- (5) (Anschauliche) Grundlage für Dezimalbrüche.

Vorteile der Dezimalbrüche:

- (1) Starke Verbreitung im täglichen Leben, z.B. im Umgang mit Geld.
- (2) Enger Zusammenhang der Schreibweise mit den ganzen Zahlen.
- (3) Einfache Rechenoperationen bei Addition, Subtraktion und Größenvergleich.
- (4) Eindeutigkeit der Schreibweise:

$$0,875 = \frac{7}{8} = \frac{35}{40} = \dots$$

Problem:  $0,88 \neq 0,875$

- (5) Einfache Schreibweise bei gewöhnlicher Textverarbeitung.



Umformung gemeiner Brüche in Dezimalbrüche:

Brüche mit Zehnerpotenz im Nenner:

$$\frac{3}{10} = 0,3 \quad ; \quad \frac{53}{100} = 0,53$$

Divisionsalgorithmus:

$$5 \div 8 = 0,625$$

$$\begin{array}{r} 50 \\ 48 \\ \hline 20 \\ 16 \\ \hline 40 \\ 40 \\ \hline 0 \end{array}$$

$$\Rightarrow \frac{5}{8} = 0,625$$

$$5 \div 11 = 0,4545\dots = 0,\overline{45}$$

$$\begin{array}{r} 50 \\ 44 \\ \hline 60 \\ 55 \\ \hline 50 \\ 44 \\ \hline 60 \\ 55 \\ \hline \vdots \end{array}$$

$$\Rightarrow \frac{5}{11} = 0,\overline{45}$$

Stellenwerttafeln:  $E$ =Einer,  $z$ =Zehntel,  $h$ =Hundertstel, etc.

$E$	$z$	$h$	$t$		$E$	$z$	$h$	$t$
5				$\div 8 =$	0	6	2	5
5	0							
4	8							
	2	0						
	1	6						
		4	0					
		4	0					
			0					

Hintergrund: Division mit Rest

$$\begin{array}{lcl} E & 5 & = \boxed{0} \cdot 8 + 5 \\ z & 50 & = 10 \cdot 5 = \boxed{6} \cdot 8 + 2 \\ h & 20 & = 10 \cdot 2 = \boxed{2} \cdot 8 + 4 \\ t & 40 & = 10 \cdot 4 = \boxed{5} \cdot 8 + 0 \end{array} \quad (5 E = 50 z)$$

↑

In der grauen Spalte kann man die Dezimalbruchentwicklung ablesen.





### Weitere Verallgemeinerung dieser Rechnung

$\frac{m}{n}$  sei ein vollständig gekürzter (also  $\text{ggT}(m, n) = 1$ ) echter (also  $1 \leq m < n$ ) Bruch. Wiederholte Division mit Rest:

$$\begin{array}{llll}
 E & m & = & \boxed{0} \cdot n + r_0 & 0 \leq r_0 = m < n \\
 z & 10 \cdot r_0 & = & \boxed{q_1} \cdot n + r_1 & 0 \leq r_1 < n \\
 h & 10 \cdot r_1 & = & \boxed{q_2} \cdot n + r_2 & 0 \leq r_2 < n \\
 t & 10 \cdot r_2 & = & \boxed{q_3} \cdot n + r_3 & 0 \leq r_3 < n \\
 & \vdots & & & \\
 & 10 \cdot r_{k-1} & = & \boxed{q_k} \cdot n + r_k & 0 \leq r_k < n
 \end{array}$$

$\uparrow$

Dabei gilt:  $0 \leq q_i < 10$  für alle  $i$ .

Denn

$$10 \cdot n > 10 \cdot r_{i-1} = q_i \cdot n + r_i \geq q_i \cdot n$$

### Dezimalbruchentwicklung:

$$\begin{aligned}
 m &= 0 \cdot n + r_0 & (r_0 &= \frac{q_1}{10} \cdot n + \frac{r_1}{10}) \\
 &= \frac{q_1}{10} \cdot n + \frac{r_1}{10} & (r_1 &= \frac{q_2}{10} \cdot n + \frac{r_2}{10}) \\
 &= \frac{q_1}{10} \cdot n + \frac{q_2}{10^2} \cdot n + \frac{r_2}{10^2} & (r_2 &= \frac{q_3}{10} \cdot n + \frac{r_3}{10}) \\
 &\vdots \\
 &= \frac{q_1}{10} \cdot n + \frac{q_2}{10^2} \cdot n + \frac{q_3}{10^3} \cdot n + \cdots + \frac{q_k}{10^k} \cdot n + \frac{r_k}{10^k} \\
 \Leftrightarrow \frac{m}{n} &= \frac{q_1}{10} + \frac{q_2}{10^2} + \frac{q_3}{10^3} + \cdots + \frac{q_k}{10^k} + \frac{r_k}{10^k \cdot n} \\
 &\stackrel{!}{=} 0, q_1 q_2 q_3 \cdots q_k \cdots
 \end{aligned}$$

Wegen der Eindeutigkeit der Division mit Rest, ist diese Schreibweise bzw. dieser Dezimalbruch ebenfalls eindeutig!

Die Dezimalbruchentwicklung des echten, vollständig gekürzten Bruches  $\frac{m}{n}$  heißt

- endlich, wenn  $q_i = 0$  für alle  $i \geq i_0$  für ein  $i_0 \in \mathbb{N}$ .
- periodisch, wenn es  $p$  und  $i_0 \in \mathbb{N}$  gibt, so daß für alle  $i \geq i_0$  gilt:  
 $q_{i+p} = q_i$ .

Wenn dabei  $i_0 = 1 \Rightarrow$  reinperiodische Dezimalbruchentwicklung

Wenn dabei  $i_0 > 1 \Rightarrow$  gemischtperiodische Dezimalbruchentwicklung

Im Folgenden entwickeln wir Kriterien dafür, das Dezimalbruchzerlegungen endlich, reinperiodisch oder gemischtperiodisch sind.

**Satz 7.1.** *Der vollständig gekürzte, echte Bruch  $\frac{m}{n}$  hat genau dann eine endliche Dezimalbruchentwicklung, wenn*

$$n = 2^a \cdot 5^b$$

*In diesem Fall hat die Dezimalbruchentwicklung genau  $s = \max(a, b)$  Stellen.*

**Kurz:**  $\frac{m}{n}$  endlich  $\Leftrightarrow n$  hat nur Primfaktoren aus  $\{2, 5\}$

**Beweis:**

” $\Leftarrow$ ”:

$$\frac{m}{n} = \frac{m}{2^a \cdot 5^b} = \frac{2^{s-a} \cdot 5^{s-b} \cdot m}{2^{s-a} \cdot 5^{s-b} \cdot 2^a \cdot 5^b} = \frac{\overbrace{2^{s-a} \cdot 5^{s-b} \cdot m}^{=:z}}{2^s \cdot 5^s} = \frac{z}{10^s}$$

Da  $z \in \mathbb{N}$ , hat  $\frac{z}{10^s}$  eine endliche Dezimalbruchentwicklung.

Diese hat genau  $s = \text{Exponent von } 10^s$  Dezimalstellen, denn nach Voraussetzung und Konstruktion gilt entweder:  $s - a = 0$  oder  $s - b = 0$  und somit  $10 \nmid z$ .

” $\Rightarrow$ ”:

$\frac{m}{n}$  habe eine endliche Dezimalbruchentwicklung der Länge  $s$ :

$$\frac{m}{n} = \underset{\substack{\uparrow \\ \text{da } m < n}}{0}, q_1 q_2 \cdots q_s \quad 0 \leq q_i < 10, q_s \neq 0$$

$$\Rightarrow \frac{m \cdot 10^s}{n} = q_1 q_2 \cdots q_s = \underbrace{q_1 \cdot 10^s + q_2 10^{s-1} + \cdots + q_{s-1} \cdot 10 + q_s}_{\in \mathbb{N}}$$

$$\left. \begin{array}{l} \text{da } \text{ggT}(m, n) = 1 \\ \text{und } \frac{10^s \cdot m}{n} \in \mathbb{N} \end{array} \right\} \Rightarrow n \mid 10^s$$

□



**Beispiel:**

$$\begin{aligned}\frac{1}{1024} &= \frac{1}{2^{10}} && \text{endlicher Dezimalbr. mit 10 Stellen} \\ &= 0,0009765625\end{aligned}$$

$$\begin{aligned}\frac{1}{125} &= \frac{1}{5^3} && \text{endlicher Dezimalbr. mit 3 Stellen} \\ &= 0,008\end{aligned}$$

$$\frac{37}{125} = \frac{37}{5^3} = 0,296 \quad \text{dito}$$

**Bemerkung** Kurzfassung vom letzten Satz:

$\frac{m}{n}$  hat endliche Dezimalbruchentwicklung.  $\Leftrightarrow$  Der Nenner hat nur Primfaktoren aus  $\{2, 5\}$ .

Die Richtung  $\Leftarrow$  gilt auch für ungekürzte Brüche. Allerdings kann man dann aus  $n = 2^a 5^b$  nicht die Anzahl der Dezimalstellen ablesen.

**Satz 7.2.** Sei  $\frac{m}{n}$  ein vollständig gekürzter, echter Bruch. Die Dezimalbruchentwicklung von  $\frac{m}{n}$  ist genau dann reinperiodisch, wenn  $\text{ggT}(n, 10) = 1$ .

**Beweis:**

Wiederholte Division mit Rest, die wie oben zur Dezimalbruchentwicklung führt:

$$\begin{aligned}m &= \boxed{0} \cdot n + r_0 && 0 \leq r_0 = m < n \\ 10 \cdot r_0 &= \boxed{q_1} \cdot n + r_1 && 0 \leq r_1 < n \\ 10 \cdot r_1 &= \boxed{q_2} \cdot n + r_2 && 0 \leq r_2 < n \\ &\vdots \\ 10 \cdot r_{k-1} &= \boxed{q_k} \cdot n + r_k && 0 \leq r_k < n\end{aligned}$$

Annahme:  $\frac{m}{n}$  nicht endlich!

Kann es dann sein, daß  $r_{i_0} = 0$  für einen Index  $i_0$ ?

Wäre  $r_{i_0} = 0$ , so folgte :

$$\begin{aligned}10 \cdot r_{i_0-1} &= q_{i_0} \cdot n + \underbrace{r_{i_0}}_{=0} \\ 10 \cdot 0 &= 10 \cdot r_{i_0} = q_{i_0+1} \cdot n + r_{i_0+1} = 0 \cdot n + 0 \\ \Rightarrow q_{i_0+1} &= 0\end{aligned}$$



damit sind alle folgenden Schritte auch  $= 0$  und die Dezimalbruchentwicklung ist endlich!  $\nmid$  Also gilt:  $0 < r_i < n \quad \forall i$

Also, m.a.W.:  $r_i \in \{1, 2, \dots, n-1\} \quad \forall i$ , also gibt es nur endlich viele Möglichkeiten.  $\Rightarrow$  irgendwann muss eine Zahl ein zweites Mal vorkommen: z.B.:

$$r_{i_0} = r_{p+i_0} \quad \text{für Indices } 1 \leq i_0, p$$

Dabei sei  $i_0$  der kleinste Index mit dieser Eigenschaft!

⊗

Dann sieht der Algorithmus folgendermaßen aus:

$$\begin{array}{rcll} \vdots & & & \\ 10 \cdot r_{i_0-1} & = & q_{i_0} \cdot n + \boxed{r_{i_0}} & (*) \\ 10 \cdot r_{i_0} & = & q_{i_0+1} \cdot n + r_{i_0+1} & \\ \vdots & & & \\ 10 \cdot r_{p+i_0-1} & = & q_{p+i_0} \cdot n + \boxed{r_{p+i_0}} = q_{p+i_0} \cdot n + \boxed{r_{i_0}} & (**) \\ 10 \cdot r_{i_0} & = & \underset{\substack{\uparrow \\ q_{i_0+1}}}{q_{p+i_0+1}} \cdot n + \underset{\substack{\uparrow \\ r_{i_0+1}}}{r_{p+i_0+1}} = q_{i_0+1} \cdot n + r_{i_0+1} & \\ \vdots & & & \end{array}$$

Nach  $p$  Schritten wiederholt sich also alles! Insbesondere wiederholen sich auch die  $q'_i$ s:

$$\begin{aligned} q_{p+i_0+1} &= q_{i_0+1} \\ q_{p+i_0+2} &= q_{i_0+2} \quad \dots \text{etc.} \end{aligned}$$

Es bleibt z.z.:

$$\text{Dezimalbruchzerlegung rein periodisch} \Leftrightarrow ggT(n, 10) = 1$$

" $\Leftarrow$ ":

Dazu betrachte die Differenz der Gleichungen (\*) und (\*\*):

$$\begin{aligned} 10 \cdot (r_{i_0-1} - r_{p+i_0-1}) &= (q_{i_0} - q_{p+i_0}) \cdot n + \underbrace{r_{i_0} - r_{p+i_0}}_{=0} \\ \Rightarrow n &\mid 10 \cdot (r_{i_0-1} - r_{p+i_0-1}) \\ \text{aus: } ggT(n, 10) = 1 &\Rightarrow n \mid (r_{i_0-1} - r_{p+i_0-1}) \\ \text{mit: } 0 < r_{i_0-1}, r_{p+i_0-1} < n &\Rightarrow r_{i_0-1} - r_{p+i_0-1} = 0 \\ &\Leftrightarrow r_{i_0-1} = r_{p+i_0-1} \end{aligned}$$

Nach Voraussetzung ⊗ war aber  $i_0$  der kleinste Index, der sich wiederholt. Also muss  $i_0 = 0$  gelten und schon der erste Rest (und alle folgenden) wiederholt sich, m.a.W.: die Dezimalbruchentwicklung ist reinperiodisch!



" $\Rightarrow$ ": Sei  $\frac{m}{n}$  reinperiodisch:

$$\begin{aligned}
 \frac{m}{n} &= 0,\overline{q_1 q_2 \cdots q_s} \\
 \frac{m}{n} \cdot 10^s &= \underbrace{q_1 q_2 \cdots q_s}_{=:z}, \overline{q_1 q_2 \cdots q_s} \\
 &= z + 0,\overline{q_1 q_2 \cdots q_s} \stackrel{!}{=} z + \frac{m}{n} \\
 \Leftrightarrow \quad \frac{m}{n} \cdot (10^s - 1) &= z \\
 \Leftrightarrow \quad m \cdot (10^s - 1) &= z \cdot n \\
 \Rightarrow \quad n \mid m \cdot (10^s - 1) \\
 \text{weil } \text{ggT}(m, n) = 1 \Rightarrow \quad n \mid (10^s - 1) & \quad (*) \\
 10^s - 1 \text{ ist ungerade} \Rightarrow 2 \nmid 10^s - 1 \\
 \text{ebenfalls gilt sicherlich auch: } 5 \nmid 10^s - 1 \\
 \Rightarrow \quad \text{ggT}(10^s - 1, 10) = 1 \\
 (*) \Rightarrow \quad \text{ggT}(n, 10) = 1
 \end{aligned}$$

□

**Bemerkung 7.3.** Sobald die  $r_i$ 's sich im Algorithmus wiederholen, endet die, bzw. beginnt eine neue Periode, die  $q_i$ 's können sich natürlich zuvor schon wiederholen.

**Satz 7.4.** Die kleinste Zahl  $s \in \mathbb{N}$  mit  $n \mid (10^s - 1)$  ist die Periodenlänge des gekürzten, echten, und reinperiodischen Bruchs  $\frac{m}{n}$ .

**Bemerkung 7.5.** Die Periodenlänge hängt nur vom Nenner, nicht vom Zähler des gekürzten Bruches ab!

**Beweis:**

$\frac{m}{n}$  sei reinperiodisch und  $s \in \mathbb{N}$  die kleinste Zahl mit  $n \mid (10^s - 1)$ . Dann gilt auch  $n \mid m \cdot (10^s - 1)$  und damit:

$$\begin{aligned}
 m \cdot (10^s - 1) &= n \cdot z & (\text{für ein } z \in \mathbb{N}) \\
 \frac{m}{n} \cdot (10^s - 1) &= z \\
 \frac{m}{n} \cdot 10^s &= z + \frac{m}{n}
 \end{aligned}$$

Mit  $\frac{m}{n} = 0, q_1 q_2 \dots$ , ist das äquivalent zu:

$$q_1 q_2 \dots q_s, q_{s+1} q_{s+2} \dots = z, q_1 q_2 \dots$$

$$\Rightarrow q_1 q_2 \dots q_s = z \quad \text{und} \quad q_{s+i} = q_i \quad (\text{für } i \geq 1)$$

□

**Beispiele:**

$$\frac{1}{3} = 0,\overline{3} \quad \text{denn:}$$

$$10^1 - 1 = 9 = 3 \cdot 3$$

Periodenlänge 1

$$\frac{1}{333} = 0,\overline{003} \quad \text{denn:}$$

$$10^3 - 1 = 999 = 333 \cdot 3$$

$$\text{Aber } 333 \nmid 10^2 - 1 = 99$$

Periodenlänge 3

$$\frac{1}{7} = 0,\overline{142857} \quad \text{denn:}$$

$$10^6 - 1 = 142857 \cdot 7$$

$$\text{Aber } 7 \nmid 10^5 - 1$$

Periodenlänge 6

$$\frac{5}{7} = 0,\overline{714285} :$$

ebenfalls Periodenlänge 6

$$1 = \boxed{0} \cdot 3 + \boxed{1}$$

$$10 \cdot 1 = \boxed{3} \cdot 3 + \boxed{1}$$

$$1 = \boxed{0} \cdot 333 + \boxed{1}$$

$$10 \cdot 1 = \boxed{0} \cdot 333 + 10$$

$$10 \cdot 10 = \boxed{0} \cdot 333 + 100$$

$$10 \cdot 100 = \boxed{3} \cdot 333 + \boxed{1}$$

$$1 = \boxed{0} \cdot 7 + \boxed{1}$$

$$10 \cdot 1 = \boxed{1} \cdot 7 + 3$$

$$10 \cdot 3 = \boxed{4} \cdot 7 + 2$$

$$10 \cdot 2 = \boxed{2} \cdot 7 + 6$$

$$10 \cdot 6 = \boxed{8} \cdot 7 + 4$$

$$10 \cdot 4 = \boxed{5} \cdot 7 + 5$$

$$10 \cdot 5 = \boxed{7} \cdot 7 + \boxed{1}$$

$$5 = \boxed{0} \cdot 7 + \boxed{5}$$

$$10 \cdot 5 = \boxed{7} \cdot 7 + 1$$

$$10 \cdot 1 = \boxed{1} \cdot 7 + 3$$

$$10 \cdot 3 = \boxed{4} \cdot 7 + 2$$

$$10 \cdot 2 = \boxed{2} \cdot 7 + 6$$

$$10 \cdot 6 = \boxed{8} \cdot 7 + 4$$

$$10 \cdot 4 = \boxed{5} \cdot 7 + \boxed{5}$$



**Beispiele:** Konstruiere einen Bruch zu vorgegebener Periode und Periodenlänge:

(1) Periode:  $z = 173$  und damit Periodenlänge  $s = 3$ . Nun wie im Beweis:

$$\begin{aligned} \frac{m}{n}(10^3 - 1) &= z = 173 \\ \Leftrightarrow \quad \frac{m}{n} &= \frac{173}{10^3 - 1} = \frac{173}{999} = 0,\overline{173} \end{aligned}$$

(2) Periode:  $z = 173$  aber nun mit Periodenlänge  $s = 4$ .

$$\Leftrightarrow \quad \frac{m}{n} = \frac{173}{10^4 - 1} = \frac{173}{9999} = 0,\overline{0173}$$

(3) Ziffernfolge 3712:

$$\text{Periodenlänge: } s = 4 \Rightarrow \frac{3712}{10^4 - 1} = \frac{3712}{9999} = 0,\overline{3712}$$

$$\text{Periodenlänge: } s = 6 \Rightarrow \frac{3712}{10^6 - 1} = \frac{3712}{999999} = 0,\overline{003712}$$

$$\text{Aber wenn: } s = 2 \Rightarrow \frac{3712}{10^2 - 1} = \frac{3712}{99} = 37,\overline{46}$$

**Wiederholung:**

$\frac{m}{n}$  echter, vollständig gekürzter Bruch (also  $\text{ggT}(m, n) = 1$  und  $m < n$ ).

Wenn: alle Primteiler von  $n$  aus  $\{2, 5\}$   $\frac{m}{n}$  endlich  
 $\text{ggT}(n, 10) = 1$   $\frac{m}{n}$  reinperiodisch

Welcher Fall bleibt übrig?

$n$  hat Teiler aus  $\{2, 5\}$  und noch zusätzlich andere Primteiler:

**Satz 7.6.** Der vollständig gekürzte echte Bruch  $\frac{m}{n}$  besitzt genau dann eine gemischt-periodische Dezimalbruchentwicklung (mit  $t$  Vorziffern), wenn  $n = n_1 \cdot n_2$  mit  $n_1 \mid 10^t$  (dabei ist  $t$  minimal mit dieser Eigenschaft) und  $\text{ggT}(n_2, 10) = 1$ .

Die Periodenlänge von  $\frac{m}{n}$  ist gleich der von  $\frac{1}{n_2}$ .

**Beispiel:**

$$\begin{array}{ll} n = 15 = \underset{\substack{\uparrow \\ n_1}}{5} \cdot \underset{\substack{\uparrow \\ n_2}}{3} & m = 8 \\ n_1 = 5 \mid 10 = 10^1 & t = 1 \quad \text{Vorziffer} \\ n_2 = 3 \mid 10^1 - 1 = 9 & \Rightarrow s = 1 \quad \text{Periodenlänge} \end{array}$$



Dezimalbruchentwicklung:

$$\begin{aligned}
 8 &= 0 \cdot 15 + 8 \\
 10 \cdot 8 &= \boxed{5} \cdot 15 + \boxed{5} \\
 10 \cdot 5 &= \boxed{3} \cdot 15 + \boxed{5} \\
 \Rightarrow \quad \frac{8}{15} &= 0,5\bar{3}
 \end{aligned}$$

**Beweis:**

Aus  $n_1 \mid 10^t$  folgt:  $n_1 \cdot q = 10^t$  für einen Teiler  $q \in \mathbb{N}$  von  $10^t$ .

$$\frac{m}{n} = \frac{m}{n_1 \cdot n_2} = \frac{m \cdot q}{10^t \cdot n_2} = \frac{1}{10^t} \cdot \frac{m \cdot q}{n_2}$$

Aus  $q \in T_{10^t}$  und  $ggT(n_2, 10) = 1$  folgt  $ggT(n_2, q) = 1$

$\Rightarrow \frac{m \cdot q}{n_2}$  ist vollst. gekürzt und hat eine reinperiodische Dezimalbruchentwicklung.

$$\Rightarrow \frac{m \cdot q}{n_2} = q_0, \overline{q_1 q_2 \cdots q_s} \quad (q_0 \in \mathbb{N} \text{ kann aus mehreren Ziffern bestehen})$$

Daraus folgt:

$$\frac{1}{10^t} \cdot \frac{m \cdot q}{n_2} = 0, \underbrace{0 \cdots 0}_t \overline{q_1 q_2 \cdots q_s}$$

Umkehrung ohne Beweis!

□

## 7.2. Kettenbrüche.

**Beispiel**

$$\begin{aligned}
 \frac{31}{14} &= 2 + \frac{3}{14} \\
 &= 2 + \frac{1}{\frac{14}{3}} = 2 + \frac{1}{4 + \frac{2}{3}} \\
 &= 2 + \frac{1}{4 + \frac{1}{\frac{3}{2}}} = 2 + \frac{1}{4 + \frac{1}{1 + \frac{1}{2}}} \\
 \text{und weiter?} \quad &= 2 + \frac{1}{4 + \frac{1}{1 + \frac{1}{\frac{2}{1}}}}} = 2 + \frac{1}{4 + \frac{1}{1 + \frac{1}{\frac{1}{2}}}}}
 \end{aligned}$$

nichts passiert weiter, weil  $\frac{1}{2}$  ein Stammbruch ist.

Der Algorithmus bricht ab, sobald man einen Stammbruch erhält!





Die Kettenbruchdarstellung von  $\frac{31}{14}$  wird zum Teil auch durch die Folge  $[2, 4, 1, 2]$  abgekürzt, man kann also abkürzen:

$$\frac{31}{14} = 2 + \frac{1}{4 + \frac{1}{1 + \frac{1}{2}}} \stackrel{\text{statt}}{=} [2, 4, 1, 2]$$

Der Kettenbruch kann auch mittels des Euklidischen Algorithmus' berechnet werden:

$$\begin{aligned} 31 &= \boxed{2} \cdot 14 + 3 & \left(\frac{31}{14} = 2 + \frac{3}{14}\right) \\ 14 &= \boxed{4} \cdot 3 + 2 & \left(\frac{3}{14} = \frac{1}{\frac{14}{3}} = \frac{1}{4 + \frac{2}{3}}\right) \\ 3 &= \boxed{1} \cdot 2 + 1 & \left(\frac{2}{3} = \frac{1}{\frac{3}{2}} = \frac{1}{1 + \frac{1}{2}}\right) \\ 2 &= \boxed{2} \cdot 1 + 0 & \text{(bei Rest 0 bricht es ab)} \end{aligned}$$

**Bemerkung 7.7.** *Dieser Algorithmus lässt sich auf jede positive rationale Zahl anwenden und bricht immer ab. (wg. des Euklidischen Algorithmus's)*

**Bedeutung:** Die Kettenbruchdarstellung approximiert den gegebenen Bruch (hier im Beispiel  $\frac{31}{14}$ ) schrittweise immer besser:

Approximation	Kettenbruch	Differenz/Ungenauigkeit
0-te von $\frac{31}{14}$	2	$\left \frac{31}{14} - 2\right  = \frac{3}{14} \approx 0,214$
1-te von $\frac{31}{14}$	$2 + \frac{1}{4}$	$\left \frac{31}{14} - \left(2 + \frac{1}{4}\right)\right  = \frac{1}{28} \approx 0,0357$
2-te von $\frac{31}{14}$	$2 + \frac{1}{4 + \frac{1}{1}}$	$\left \frac{31}{14} - \left(2 + \frac{1}{4 + \frac{1}{1}}\right)\right  = \frac{1}{70} \approx 0,0143$
3-te von $\frac{31}{14}$	$2 + \frac{1}{4 + \frac{1}{1 + \frac{1}{2}}}$	$\left \frac{31}{14} - \left(2 + \frac{1}{4 + \frac{1}{1 + \frac{1}{2}}}\right)\right  = 0$



**Anwendung: Kalender**

1 tropisches Jahr:  $365^{\text{d}} 5^{\text{h}} 48^{\text{min}} 45,8^{\text{s}}$

Der "Teil-Tag" soll durch einen Bruch approximiert werden:

$$\begin{aligned}
 5^{\text{h}} 48^{\text{min}} 45,8^{\text{s}} &= \frac{1}{24} \left( 5 + \frac{48}{60} + \frac{45,8}{60^2} \right) & (\text{"Tage"}) \\
 &= \frac{1}{24} \left( 5 + \frac{48}{60} + \frac{45 + \frac{4}{5}}{60^2} \right) \\
 &= \frac{5^2 \cdot 60^2 + 48 \cdot 60 \cdot 5 + 45 \cdot 5 + 4}{24 \cdot 60^2 \cdot 5} = \frac{104629}{432000}
 \end{aligned}$$

Kettenbruchentwicklung via Euklidischem Algorithmus:

Nr.	Division mit Rest	Approximation
0-te	$104629 = 0 \cdot 432000 + 104629$	0
1-te	$432000 = 4 \cdot 104629 + 13484$	$0 + \frac{1}{4}$
2-te	$104629 = 7 \cdot 13484 + 10241$	$0 + \frac{1}{4 + \frac{1}{7}}$
3-te	$13484 = 1 \cdot 10241 + 3243$	$0 + \frac{1}{4 + \frac{1}{7 + \frac{1}{1}}}$
4-te	$10241 = 3 \cdot 3243 + 512$	$\vdots$
5-te	$3243 = 6 \cdot 512 + 171$	$\vdots$
6-te	$512 = 2 \cdot 171 + 170$	$\vdots$
7-te	$171 = 1 \cdot 170 + 1$	$  \frac{1}{4 + \frac{1}{7 + \frac{1}{1 + \frac{1}{3 + \frac{1}{6 + \frac{1}{2 + \frac{1}{1 + \frac{1}{170}}}}}}}}  $

Es folgt:

$$\frac{104629}{432000} = \frac{1}{4 + \frac{1}{7 + \frac{1}{1 + \frac{1}{3 + \frac{1}{6 + \frac{1}{2 + \frac{1}{1 + \frac{1}{170}}}}}}}$$

Interpretation:



1-te Approx.:  $\frac{104629}{432000} \approx \frac{1}{4}$  Julianischer Kalender mit einem Schalttag alle 4 Jahre

2-te Approx.:  $\frac{104629}{432000} \approx \frac{1}{4 + \frac{1}{7}} = \frac{7}{29}$

$\vdots$   $\vdots$

5-te Approx  $\frac{104629}{432000} \approx \frac{1}{4 + \frac{1}{7 + \frac{1}{1 + \frac{1}{3 + \frac{1}{6}}}}} = \frac{194}{801} \approx 0,2422 \Rightarrow$  gregorianischer Kalender

In 400 Jahren summiert sich dieser Bruchteil eines Tages auf:

$$\frac{194}{801} \cdot 400 \approx 96,8789 \approx 97 \text{ Tage}$$

Sinnvollerweise muss es also in 400 Jahren mit je 365 Tagen zusätzlich 97 Schalttage geben um bestmöglich 400 tropische Jahre auszumachen. Das wird im Gregorianischen Kalender realisiert: jedes vierte Jahr einen Schalttag machen 100 Schalttage in 400 Jahren, aber die Jahrhundertregel (nur die Jahrhunderte  $\equiv 0 \pmod{4}$  sind Schaltjahre) bewirkt, daß unter den vier Jahrhundert-Jahren innerhalb 400 Jahren nur ein Jahrhundert-Jahr Schaltjahr ist, drei Schaltjahre/Tage fallen also weg, also gibt es im Gregorianischen Kalender innerhalb 400 Jahren nur 97 Schaltjahre/Tage.

## 8. TEILBARKEITSREGELN

WDH. Für  $a, b, c, d \in \mathbb{Z}$  und  $t \in \mathbb{N}$  gilt:

$$\text{Addition von Kongruenzen: } \left. \begin{array}{l} a \equiv b \pmod{t} \\ c \equiv d \pmod{t} \end{array} \right\} \Rightarrow a + c \equiv b + d \pmod{t}$$

$$\text{Multiplikation von Kongruenzen} \quad a \equiv b \pmod{t} \Rightarrow c \cdot a \equiv c \cdot b \pmod{t}$$

$$\text{Potenzieren von Kongruenzen} \quad a \equiv b \pmod{t} \Rightarrow a^n \equiv b^n \pmod{t} \quad \forall n \in \mathbb{N}$$



$$a \equiv b \pmod{t} \Leftrightarrow \begin{cases} a = q_1 \cdot t + r \\ b = q_2 \cdot t + r \end{cases}$$

das heißt, sind  $a$  und  $b$  kongruent modulo  $t$ , so haben sie bei Division durch  $t$  denselben Rest  $r$ . Für Teilbarkeitsuntersuchungen bezüglich einer Zahl  $t$  gilt damit:

$a \equiv b \pmod{t} \Leftrightarrow a$  und  $b$  haben dieselben Teilbarkeitseigenschaften bzgl.  $t$   
Anders formuliert:

*Wenn  $a \equiv b \pmod{t}$ , so gilt:  $a$  ist genau dann durch  $t$  teilbar, wenn auch  $b$  durch  $t$  teilbar ist.*

### 8.1. Endstellenregeln.

Beispiel:

$$65\,432 = 6 \cdot 10^4 + 5 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10 + 2 \equiv 2 \pmod{10}$$

allgemein:

$$z_n z_{n-1} \dots z_1 z_0 = z_n \cdot 10^n + z_{n-1} \cdot 10^{n-1} \dots z_1 \cdot 10 + z_0 \cdot 10^0 = \sum_{i=0}^n z_i \cdot 10^i$$

für Ziffern  $0 \leq z_i \leq 9$ ,  $i = 0, \dots, n$ ,  $z_n \neq 0$ . Also

$$z_n z_{n-1} \dots z_1 z_0 \equiv z_0 \pmod{10}$$

Mehr noch, weil  $10 \equiv 0 \pmod{t}$  für alle Teiler  $t$  von 10:

**Satz 8.1 (Endstellenregel 1ter Ordnung).**

$z_n z_{n-1} \dots z_1 z_0 \equiv z_0 \pmod{t}$  für alle Teiler  $t$  von 10.

#### Folgerung

Eine natürliche Zahl  $z$  (Basis 10) ist genau dann durch 2 (bzw. 5, bzw. 10) teilbar, wenn ihre Endziffer  $z_0$  durch 2 (bzw. 5, bzw. 10) teilbar ist.



**Beweis:**

Es gilt

$$\begin{aligned}
10 &\equiv 0 \pmod{t} \Leftrightarrow t \mid (10 - 0) = 10 \\
&\Leftrightarrow t \in \{1, 2, 5, 10\} = T_{10} \\
&\Rightarrow 10^i \equiv 0 \pmod{t} \quad \text{für } t \in T_{10} \quad \text{und } i \geq 1 \\
&\Rightarrow z_i \cdot 10^i \equiv 0 \pmod{t} \quad \text{für } t \in T_{10} \quad \text{und } i \geq 1 \\
&\Rightarrow \sum_{i=1}^n z_i \cdot 10^i \equiv 0 \pmod{t} \quad \text{für } t \in T_{10} \quad \text{und } i \geq 1 \\
&\Rightarrow z_n z_{n-1} \cdots z_1 z_0 = \sum_{i=0}^n z_i \cdot 10^i = \sum_{i=1}^n z_i \cdot 10^i + z_0 \equiv z_0 \pmod{t}
\end{aligned}$$

□

Geht das auch in anderen Stellenwertsystemen?Sei  $b > 1$  eine Basis eines Stellenwertsystems.

$$\Rightarrow b \equiv 0 \pmod{t} \quad \forall \quad t \in T_b$$

Eine Zahl im  $b$ -System:

$$\begin{aligned}
z_{(b)} &= \sum_{i=0}^n z_i b^i = z_n z_{n-1} \cdots z_1 z_0 \quad \text{mit } 0 \leq z_i < b \\
&\Rightarrow z_{(b)} = \sum_{i=1}^n z_i b^i + z_0 \equiv z_0 \pmod{t} \quad \text{für } t \in T_b
\end{aligned}$$

**Korollar 8.2.** Eine natürliche Zahl  $z_{(b)}$  (dargestellt mittels der Basis  $b > 1$ ) ist genau dann durch einen Teiler  $t$  von  $b$  teilbar, wenn ihre Endziffer  $z_0$  durch  $t$  teilbar ist.

**Beispiel:**  $b = 8$ Untersuche ob 4 die Zahl  $152_{(8)}$  teilt!

$$152_{(8)} = 1 \cdot 8^2 + 5 \cdot 8^1 + 2 \equiv 2 \pmod{4} \quad \text{da } 4 \nmid 8$$

aber  $4 \nmid 2$  !!

Neue Frage: Welche Zahlen sind durch 4 teilbar?

Dazu

$$z_0 \in V_4 \cup \{0\}, \quad z_0 < 8 \quad \Rightarrow \quad z_0 \in \{0, 4\}$$



Also alle Zahlen mit den Endziffern 0 oder 4 sind durch 4 teilbar.

$$\text{z.B.: } 4 \mid 150_{\textcircled{8}} \quad \text{und} \quad 4 \mid 154_{\textcircled{6}}$$

Translation ins Dezimalsystem:

$$150_{\textcircled{8}} = 8^2 + 5 \cdot 8 + 0 = 104 = 4 \cdot 26 \quad \checkmark$$

**Beispiel:**  $b = 6, t = 3$

Endziffern  $z_0 < 6$  mit  $3 \mid z_0 \Rightarrow z_0 \in \{0, 3\}$

$$\Rightarrow \quad 3 \mid 570_{\textcircled{6}}, \quad 3 \mid 573_{\textcircled{6}}$$

aber

$$3 \nmid 571_{\textcircled{6}}, \quad 3 \nmid 572_{\textcircled{6}}, \quad 3 \nmid 574_{\textcircled{6}}, \quad 3 \nmid 575_{\textcircled{6}}$$

### Endstellenregeln 2ter Ordnung

Es geht um die Teilbarkeit von Teilern von  $100 = 10^2$  bzw.  $t \in T_{b^2}$  im  $b$ -System.

Dazu:

$$100 = 10^2 \equiv 0 \pmod{t} \quad \forall t \in T_{10^2} \quad \text{bzw.} \quad b^2 \equiv 0 \pmod{t} \quad \forall t \in T_{b^2}$$

**Satz 8.3** (Basis 10).

$$z_n z_{n-1} \cdots z_1 z_0 = \sum_{i=0}^n z_i 10^i \equiv z_1 \cdot 10 + z_0 = z_1 z_0 \pmod{t} \quad \forall t \in T_{10^2}$$

*Damit gilt: Eine Zahl  $z \in \mathbb{N}$  ist genau dann durch einen Teiler  $t$  von 100 teilbar, wenn ihre aus den letzten beiden Ziffern gebildete zweistellige Zahl (im Dezimalsystem!!) durch  $t$  teilbar ist:*

$$t \mid z_n z_{n-1} \cdots z_1 z_0 \quad \Leftrightarrow \quad t \mid z_1 z_0$$

Insbesondere folgen daraus die bekannten Teilbarkeitsregeln für  $4 = 2^2$  und  $25 = 5^2$ !

Satz 8.3 hat auch wieder ein Analogon für die beliebige Basis  $b$ !



**Beweis:**

$$\begin{aligned}
z_n z_{n-1} \cdots z_1 z_0 &= \cdots + (\cdots) \underset{t}{10^4} + (z_3 10 + z_2) \underset{t}{10^2} + (z_1 10 + z_0) \\
&\equiv z_1 10 + z_0 = z_1 z_0 \pmod{t}
\end{aligned}$$

□

Umformulierung und Verschärfung für  $t = 2^2 = 4$ :

Eine natürliche Zahl  $z = \sum_{i=0}^n z_i 10^i$  ist genau dann durch 4 teilbar, wenn  $2z_1 + z_0$  durch 4 teilbar ist.

**Beweis:**nach Satz 8.3 und weil  $10 = 2 \cdot 4 + 2 \equiv 2 \pmod{4}$  gilt:

$$\begin{aligned}
4 \mid z &\Leftrightarrow 4 \mid z_1 \cdot 10 + z_0 && (\text{da: } z_1 \cdot 10 + z_0 \equiv z_1 \cdot 2 + z_0) \\
&\Leftrightarrow z_1 \cdot 10 + z_0 \equiv z_1 \cdot 2 + z_0 \equiv 0 \pmod{4}
\end{aligned}$$

□

**Endstellenregeln 3ter Ordnung**Aus  $1000 = 10^3 \equiv 0 \pmod{t}$  für alle  $t \in T_{10^3}$  folgt analog:

$$t \mid z = \sum_{i=0}^n z_i 10^i = z_n z_{n-1} \cdots z_1 z_0 \Leftrightarrow t \mid z_2 z_1 z_0 = z_2 \cdot 100 + z_1 \cdot 10 + z_0 \quad \forall t \in T_{10^3}$$

Analoges kann man auch wieder im Stellenwertsystem zur Basis  $b > 1$  formulieren!**8.2. Quersummenregeln.****Streichholzspiel:**

Schritt 1 Gebe Deinem Mitspieler eine Streichholzschachtel mit mindestens 10 Hölzern.

Schritt 2 Lasse den Mitspieler die Hölzer zählen (er soll die Anzahl geheimhalten!) **die Anzahl ist eine Zahl  $n$  zwischen 10 und 38. Dann gilt  $n = z_1 \cdot 10 + z_0$  mit  $z_1 \in \{1, 2, 3\}$  und  $z_0 \in \{0, 1, \dots, 9\}$** Schritt 3 Fordere den Mitspieler auf: Bilde die Quersumme  $Q(n)$  (nicht verraten)  **$Q(n) = z_1 + z_0$** Schritt 4 Fordere den Mitspieler auf: Entferne  $Q(n)$  Hölzer aus der Schachtel

Schritt 5 Behauptung: Du kannst nun (ohne abzuzählen) abschätzen, wieviele Hölzer noch in der Schachtel sind!

Die Anzahl ist  $n - Q(n) = (z_1 \cdot 10 + z_0) - (z_1 + z_0) = z_1 \cdot 10 - z_1 = z_1 \cdot 9$ ,

Da  $z_1 \in \{1, 2, 3\}$ , können es nur 9, 18 oder 27 Hölzer sein.

Teilbarkeit durch 3 und 9:

**Satz 8.4.** Eine natürliche Zahl  $z = \sum_{i=0}^n z_i \cdot 10^i$  ist genau dann durch einen Teiler  $t$  von 9 teilbar, wenn ihre Quersumme  $\sum_{i=0}^n z_i$  durch  $t$  teilbar ist.

**Beweis**  $t \in T_9 = \{1, 3, 9\}$ , also  $t = 3$  oder 9, da 1 uninteressant.

$$\begin{aligned} 10 &= 9 + 1 \equiv 1 \pmod{t} \\ \Rightarrow 10^i &\equiv 1 \pmod{t} && \text{für } i \in \mathbb{N}_0 \\ \Rightarrow z_i \cdot 10^i &\equiv z_i \pmod{t} && \text{für } i \in \mathbb{N}_0 \\ \Rightarrow z = \sum_{i=0}^n z_i 10^i &\equiv \sum_{i=0}^n z_i \pmod{t} && \square \end{aligned}$$

Läßt sich die Idee des Beweises verallgemeinern?

Ja, benutze:

$$10^2 = 99 + 1 \equiv 1 \pmod{t} \quad \text{für } t \in T_{99}$$

und schreibe:

$$\begin{aligned} z &= \sum_{i=0}^n z_i 10^i = \dots + (z_{2j+1} \cdot 10 + z_{2j}) \cdot 10^{2j} + \dots + (z_3 \cdot 10 + z_2) \cdot 10^2 + (z_1 \cdot 10 + z_0) \\ &\equiv \dots + (z_{2j+1} \cdot 10 + z_{2j}) + \dots + (z_3 \cdot 10 + z_2) + (z_1 \cdot 10 + z_0) \pmod{t} \\ &\quad \text{für } t \in T_{99} \\ &= \underbrace{\dots (z_{2j+1} z_{2j}) + \dots + (z_3 z_2) + (z_1 z_0)}_{\text{Quersumme 2ter Ordnung}} \end{aligned}$$

**Korollar 8.5.** Eine natürliche Zahl ist genau dann durch einen Teiler  $t$  von 99 teilbar, wenn ihre Quersumme 2-ter Ordnung durch  $t$  teilbar ist.

Da  $T_{99} = \{1, 3, 9, 11\}$  erhalten wir damit insbesondere eine Teilbarkeitsregel für 11!!

**Beispiel:** Sei  $t \in \{1, 3, 9, 11\}$





$$\begin{aligned}
738514 &\equiv 73 + 85 + 14 \pmod{t} \\
&= 172 \\
&\equiv 1 + 72 \pmod{t} \\
&= 73
\end{aligned}$$

Aber  $t \nmid 73 \Rightarrow t \nmid 738514$

### Weitere Verallgemeinerungen:

$1000 = 10^3 = 999 + 1 \Rightarrow$  Teilbarkeitsregeln für Teiler von 999 mittels Quersumme 3-ter Ordnung.

Da  $999 = 3^3 \cdot 37$  liefert das z.B. Teilbarkeitsregel für 37.

$\vdots$

### Alternierende Quersummenregeln:

$$z = \sum_{i=0}^n z_i 10^i \Rightarrow \text{alternierende Quersumme} \quad Q'(z) := \sum_{i=0}^n (-1)^i z_i$$

**Beispiel:**  $Q'(3712) = -3 + 7 - 1 + 2 = 5$

#### Satz 8.6.

$$11 \text{ teilt } z \Leftrightarrow 11 \text{ teilt } Q'(z)$$

#### Beweis

$$10 = 11 - 1 \equiv -1 \pmod{11}$$

$\vdots \quad \vdots$

$$z = \sum_{i=0}^n z_i 10^i \equiv \sum_{i=0}^n z_i (-1)^i = Q'(z) \pmod{11} \quad \square$$

#### Beispiel:

$$\begin{aligned}
13846173 &\stackrel{11}{\equiv} Q'(13846173) = -1 + 3 - 8 + 4 - 6 + 1 - 7 + 3 = -11 \equiv 0 \pmod{11} \\
&\Rightarrow 11 \mid 13846173
\end{aligned}$$

### Verallgemeinerungen

Idee:  $100 = 10^2 = 101 - 1 \equiv -1 \pmod{101}$

Da 101 PZ, liefert das nur Teilbarkeitsregeln für 101.



Aber  $1001 = 7 \cdot 11 \cdot 13$  liefert Teilbarkeitsregeln für 7 und 13 und eine weitere für 11:

$$10^3 = 1001 - 1 \equiv -1 \pmod{t} \quad (\text{für } t \in T_{1001})$$

$$\vdots$$

$$\begin{aligned} z &= \cdots + (z_5 10^2 + z_4 10 + z_3) \cdot (10^3)^1 + (z_2 10^2 + z_1 10 + z_0) \cdot (10^3)^0 \\ &\equiv \cdots + (z_5 10^2 + z_4 10 + z_3) \cdot (-1)^1 + (z_2 10^2 + z_1 10 + z_0) \cdot (-1)^0 \pmod{t} \\ &= \underbrace{\cdots - (z_5 10^2 + z_4 10 + z_3) + (z_2 10^2 + z_1 10 + z_0)}_{\text{alternierende Quersumme 3-ter Ordnung}} \end{aligned}$$

**Korollar 8.7.** Für  $t \in T_{1001}$  gilt:

$$t \text{ teilt } z \iff t \text{ teilt die alternierende Quersumme 3-ter Ordnung von } z$$

**Beispiel:**  $t = 7$

$$\begin{aligned} \underbrace{681} - \underbrace{359} + \underbrace{126} &\equiv +681 - 359 + 126 \pmod{7} \\ &= 448 \\ &= 64 \cdot 7 \equiv 0 \pmod{7} \\ &\Rightarrow 7 \mid 681\,359\,126 \end{aligned}$$

**Bemerkung:** Auch hier gibt es Verallgemeinerungen auf andere Stellenwertsysteme.

↑ 19.1.17 1/2

### 8.3. Weitere Teilbarkeitsregeln für Primzahlen.

Teilbarkeit durch 7:

**Beispiel:** Frage: ist 65 625 durch 7 teilbar?

$$\begin{array}{r} \phantom{0} 6 \phantom{0} 5 \phantom{0} 6 \phantom{0} 2 \phantom{0} \cancel{5} \\ - \phantom{0} \phantom{0} \phantom{0} \phantom{0} 1 \phantom{0} 0 \\ \hline \phantom{0} 6 \phantom{0} 5 \phantom{0} 5 \phantom{0} \cancel{2} \\ - \phantom{0} \phantom{0} \phantom{0} 4 \\ \hline \phantom{0} 6 \phantom{0} 5 \phantom{0} \cancel{1} \\ - \phantom{0} \phantom{0} 2 \\ \hline \phantom{0} 6 \phantom{0} 3 \\ = 9 \phantom{0} \cdot 7 \end{array} \quad \begin{array}{l} 10 = 2 \cdot \cancel{5} \\ 4 = 2 \cdot \cancel{2} \\ 2 = 2 \cdot \cancel{1} \end{array}$$

Also auch  $7 \mid 65\,625$

**Beschreibung:**

- (1) Streiche letzte Ziffer  $\Rightarrow$  Stellen verschieben sich nach rechts!



- (2) Subtrahiere (von der neuen Zahl) das Doppelte der gestrichenen Ziffer.  
 (3) Wenn nötig beginne mit Algorithmus von neuem.

Warum, was passiert hier??

Benutzt werden folgende Aussagen:

$$20 + 1 = 21 \equiv 0 \pmod{7} \quad (8)$$

$$z \cdot 10 \equiv 0 \pmod{7} \Leftrightarrow z \equiv 0 \pmod{7} \quad (9)$$

(9) in Worten:  $z \cdot 10$  ist genau dann durch 7 teilbar, wenn  $z$  durch 7 teilbar ist.

$$65\,625 = 6 \cdot 10^4 + 5 \cdot 10^3 + 6 \cdot 10^2 + 2 \cdot 10 + 5 \quad (\text{Schritt 1})$$

$$= 6 \cdot 10^4 + 5 \cdot 10^3 + \underbrace{6 \cdot 10^2 - 2 \cdot 5 \cdot 10}_{=5 \cdot 10^2} + 2 \cdot 10 + \underbrace{(2 \cdot 5 \cdot 10 + 5)}_{(20+1) \cdot 5 = 21 \cdot 5 \equiv 0 \pmod{7}}$$

$$\equiv 6 \cdot 10^4 + 5 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10 \pmod{7}$$

$$= \underbrace{(6 \cdot 10^3 + 5 \cdot 10^2 + 5 \cdot 10^1 + 2)}_{=:z_1=6\,552} \cdot 10 = z_1 \cdot 10 = 6\,552 \cdot 10$$

mit (9): 65 625 ist genau dann durch 7 teilbar, wenn es auch für  $z_1 = 6\,552$  gilt

$$z_1 = 6\,552 = 6 \cdot 10^3 + 5 \cdot 10^2 + \underbrace{5 \cdot 10 - 2 \cdot 2 \cdot 10}_{1 \cdot 10} + \underbrace{(2 \cdot 2 \cdot 10 + 2)}_{21 \cdot 2 \equiv 0 \pmod{7}} \quad (\text{Schritt 2})$$

$$\equiv 6 \cdot 10^3 + 5 \cdot 10^2 + 1 \cdot 10 \pmod{7}$$

$$= \underbrace{(6 \cdot 10^2 + 5 \cdot 10^1 + 1)}_{=:z_2=651} \cdot 10 = z_2 \cdot 10$$

$$\text{mit (9)} \quad z_1 \equiv z_2 \cdot 10 \equiv 0 \pmod{7} \Leftrightarrow z_2 \equiv 0 \pmod{7}$$

$$z_2 = 6 \cdot 10^2 + 5 \cdot 10 - \underbrace{2 \cdot 10}_{=21 \equiv 0 \pmod{7}} + \underbrace{(2 \cdot 10 + 1)}_{=21 \equiv 0 \pmod{7}} \quad (\text{Schritt 3})$$

$$\equiv 6 \cdot 10^2 + 3 \cdot 10 \pmod{7}$$

$$= \underbrace{(6 \cdot 10 + 3)}_{=:z_3} \cdot 10 = 63 \cdot 10 = 9 \cdot 7 \cdot 10 \equiv 0 \pmod{7} \quad (\text{oder:})$$

$$z_3 = \underbrace{6 \cdot 10 - 3 \cdot 2 \cdot 10}_{=0} + \underbrace{3 \cdot 2 \cdot 10 + 3}_{=3 \cdot 21 \equiv 0 \pmod{7}}$$

$$\equiv 0 \pmod{7}$$

Teilbarkeit durch 11



**Beispiele:** Untersuche ob 11 ein Teiler von 4785 bzw. 4766 ist:

$$\begin{array}{r}
 4 \quad 7 \quad 8 \quad \cancel{5} \\
 - \quad 5 \\
 \hline
 4 \quad 7 \quad \cancel{3} \\
 - \quad 3 \\
 \hline
 4 \quad \cancel{4} \\
 - \quad 4 \\
 \hline
 0
 \end{array}
 \quad \Rightarrow \quad \begin{array}{l} \text{ja!} \\ 11 \mid 4785 \end{array}
 \quad \left| \quad
 \begin{array}{r}
 4 \quad 7 \quad 6 \quad \cancel{6} \\
 - \quad 6 \\
 \hline
 4 \quad 7 \quad \cancel{0} \\
 - \quad 0 \\
 \hline
 4 \quad 7
 \end{array}
 \right.
 \begin{array}{l}
 \text{Aus } 11 \nmid 47 \Rightarrow \\
 \text{nein! } 11 \nmid 4766
 \end{array}$$

Warum, was passiert hier?? Benutze wie oben:

$$z \cdot 10 \equiv 0 \pmod{11} \quad \Leftrightarrow \quad z \equiv 0 \pmod{11} \quad (10)$$

$$4785 \equiv (4785 - 5 \cdot 11) \pmod{11}$$

$$= 4730 = 473 \cdot 10$$

$$473 \equiv 473 - 3 \cdot 11 \pmod{11} \quad (\text{wegen (10) genügt es } 473 \text{ zu untersuchen})$$

$$= 44 = 4 \cdot 11 \equiv 0 \pmod{11}$$

Weitere Verallgemeinerungen möglich!! (vgl. [P], p. 181)

## 9. VOLLKOMMENE ZAHLEN

## 9.1. Beispiele und Definition.

**Beispiel**Zahl **6**:  $T_6 = \{1, 2, 3, 6\}$ Summe der Teiler  $\sum_{i \in T_6} i = 1 + 2 + 3 + 6 = 12 = 2 \cdot \mathbf{6}$ **Bemerkung:** Bei den Pythagoreern mit ihrer Zahlenmystik stand die Zahl 6 für das Universum, weil sie Summe sowie auch Produkt ihrer echten Teiler ist:

$$1 + 2 + 3 = 6 = 1 \cdot 2 \cdot 3$$

Die Zahl 6 ist also gewissermaßen 'super-'vollkommen. □

Weitere Beispiele:

**28**:  $\sum_{i \in T_{28}} i = 1 + 2 + 4 + 7 + 14 + 28 = 4 \cdot 14 = 2 \cdot \mathbf{28}$ 

Aber das gilt nicht immer:

$$3: \sum_{i \in T_3} i = 1 + 3 = 4 < 2 \cdot 3$$

$$4: \sum_{i \in T_4} i = 1 + 2 + 4 = 7 < 2 \cdot 4$$

$$5: \sum_{i \in T_5} i = 1 + 5 = 6 < 2 \cdot 5$$

$$7: \sum_{i \in T_7} i = 1 + 7 = 8 < 2 \cdot 7$$

$$8: \sum_{i \in T_8} i = 1 + 2 + 4 + 8 = 15 < 2 \cdot 8$$

⋮

$$12: \sum_{i \in T_{12}} i = 1 + 2 + 3 + 4 + 6 + 12 = 28 > 2 \cdot 12$$

Eine Zahl  $n \in \mathbb{N}$  heißt *vollkommen*, wenn die Summe ihrer positiven Teiler gleich  $2 \cdot n$  ist, d.h.

$$\sum_{i \in T_n} i = 2 \cdot n$$

 $n$  heißt *defizient*, wenn  $\sum_{i \in T_n} i < 2 \cdot n$  $n$  heißt *abundant*, wenn  $\sum_{i \in T_n} i > 2 \cdot n$ 

**Satz 9.1** (Satz von Euklid (ca 300 v.Chr.)). Ist  $2^p - 1$  eine Primzahl, dann ist  $2^{p-1}(2^p - 1)$  eine vollkommene Zahl.

**Beweis:**Sei  $n = 2^{p-1}(2^p - 1)$  mit  $2^p - 1$  PZ.

$$\begin{aligned}
& \left. \begin{aligned} T_{2^p-1} &= \{1, 2^p - 1\} \text{ weil PZ} \\ T_{2^{p-1}} &= \{1, 2^1, 2^2, \dots, 2^{p-1}\} \end{aligned} \right\} \Rightarrow 2^{p-1} \text{ und } 2^p - 1 \text{ sind teilerfremd} \\
& \Rightarrow T_n = T_{2^{p-1}(2^p-1)} = \{1, 2, 2^2, \dots, 2^{p-1}, \\
& \quad 1(2^p - 1), 2(2^p - 1), 2^2(2^p - 1), \dots, 2^{p-1}(2^p - 1)\} \\
& \Rightarrow \sum_{i \in T_n} i = \cancel{(1 + 2 + 2^2 + \dots + 2^{p-1})} + (1 + 2 + 2^2 + \dots + 2^{p-1})(2^p - 1) \\
& \quad = (1 + 2 + 2^2 + \dots + 2^{p-1})2^p \quad (\text{geometrische Reihe } \sum_{k=0}^{p-1} 2^i) \\
& \quad = \sum_{k=0}^{p-1} 2^i \cdot 2^p \quad (\sum_{k=0}^{s-1} q^i = \frac{q^s - 1}{q - 1}) \\
& \quad = \frac{2^p - 1}{2 - 1} \cdot 2^p = (2^p - 1) \cdot 2^p \\
& \quad = 2 \cdot 2^{p-1}(2^p - 1) = 2 \cdot n
\end{aligned}$$

□

**Satz 9.2** (Notwendige Bedingung für  $2^p - 1 = \text{Primzahl}$ ). *Ist  $2^p - 1$  eine Primzahl, so auch  $p$ .*

**Beweis:**

Beweis durch Widerspruch: z.z.: *Ist  $p$  zusammengesetzte Zahl, so auch  $2^p - 1$ .*

Schreibe die zusammengesetzte Zahl  $p$  als nichttriviales Produkt:  $p = a \cdot b$  mit  $1 < a, b < p$ .

Wir wollen folgendes benutzen:

$$\sum_{k=1}^{s-1} q^k = \frac{q^s - 1}{q - 1} \quad \Leftrightarrow \quad (q - 1) \sum_{k=0}^{s-1} q^k = q^s - 1$$

Mit  $q = 2^a$  und  $s = b$ :

$$\underbrace{(2^a - 1) \cdot \left( \sum_{k=0}^{b-1} (2^a)^k \right)}_{\text{zusammengesetzt!}} = (2^a)^b - 1 = 2^{a \cdot b} - 1 = 2^p - 1$$

Die linke Seite ist eine zusammengesetzte Zahl, also auch die rechte Seite der Gleichung!

M.a.W.:  $p$  zusammengesetzt  $\Rightarrow 2^p - 1$  zusammengesetzt! □

Umkehrung von Euklid:



**Satz 9.3** (Euler, 18 Jd.). *Ist  $n$  eine gerade vollkommene Zahl, so gilt*

$$n = 2^{p-1}(2^p - 1) \quad \text{und} \quad 2^p - 1 \quad \text{ist Primzahl.}$$

**Beweis:**

$n$  gerade  $\Rightarrow n = 2^{p-1} \cdot u$ , mit  $u \in \mathbb{N}$  ungerade, also  $ggT(u, 2) = 1$ , und  $p > 1$ .

Wäre  $u = 1 \Rightarrow$

$$\begin{aligned} n &= 2^{p-1} \\ \Rightarrow T_n &= T_{2^{p-1}} = \{1, 2, 2^2, 2^3, \dots, 2^{p-1}\} \\ \Rightarrow \sum_{t \in T_n} t &= \sum_{i=0}^{p-1} 2^i = \frac{2^p - 1}{2 - 1} = \underbrace{2^p - 1}_{\text{ungerade}} \quad \nexists \end{aligned}$$

Widerspruch zu  $n$  gerade!!!  $\Rightarrow u \neq 1$ .

Jeder Teiler  $t$  von  $n = 2^{p-1}u$  ist von der Form  $t = 2^i \cdot d$  mit  $d \mid u$  und  $i \leq p-1$ .

Da  $n$  vollkommene Zahl, folgt (mit geometrischer Reihe)

$$\begin{aligned} 2 \cdot n &= 2^p \cdot u = \sum_{t \in T_n} t = \left( \sum_{d \in T_u} d \right) \cdot (1 + 2 + \dots + 2^{p-1}) \\ &= \left( \sum_{d \in T_u} d \right) \cdot (2^p - 1) \end{aligned} \tag{11}$$

Aber:

$$\sum_{d \in T_u} d = \underbrace{1 + \dots}_{=:s} + u = s + u > u \quad \text{für ein } s \geq 1$$

Aus Gleichung (11) wird dann:

$$\begin{aligned} 2^p \cdot u &= (u + s) \cdot (2^p - 1) \\ \Leftrightarrow \cancel{2^p \cdot u} &= \cancel{u \cdot 2^p} - u + s \cdot (2^p - 1) \quad | + u \\ \Leftrightarrow u &= (2^p - 1) \cdot s \\ \Rightarrow s \mid u \text{ und } s < u &\quad (\text{denn } 2^p - 1 > 2^1 - 1 = 1) \\ \text{wäre } s \neq 1 \Rightarrow u + s &= \sum_{d \in T_u} d = 1 + \dots + s + \dots + u > s + u \quad \nexists \\ \Rightarrow s = 1 \Rightarrow \sum_{d \in T_u} d &= u + 1 \Rightarrow u \text{ Primzahl} \\ \Rightarrow u &= (2^p - 1) \cdot s = 2^p - 1 \text{ Primzahl} \end{aligned}$$

□

**Zusammenfassung:**



**Satz 9.4** (Euler-Euklid). *Eine gerade Zahl  $n$  ist genau dann vollkommen, wenn sie von der folgenden Form ist:*

$$n = 2^{p-1}(2^p - 1) \quad \text{mit einer Primzahl } 2^p - 1$$

↑ 19.1.17 2/2



## 10. FIBONACCIZAHLEN, GOLDENER SCHNITT UND IRRATIONALITÄT

**Die Sache mit den Kaninchen:**

*Ein neu geborenes Kaninchenpaar wirft von Ende des zweiten Lebensmonats an jeden Monat ein Paar Junge*

**Satz 10.1** (Rekursionsformel der Fibonacci-Zahlen).

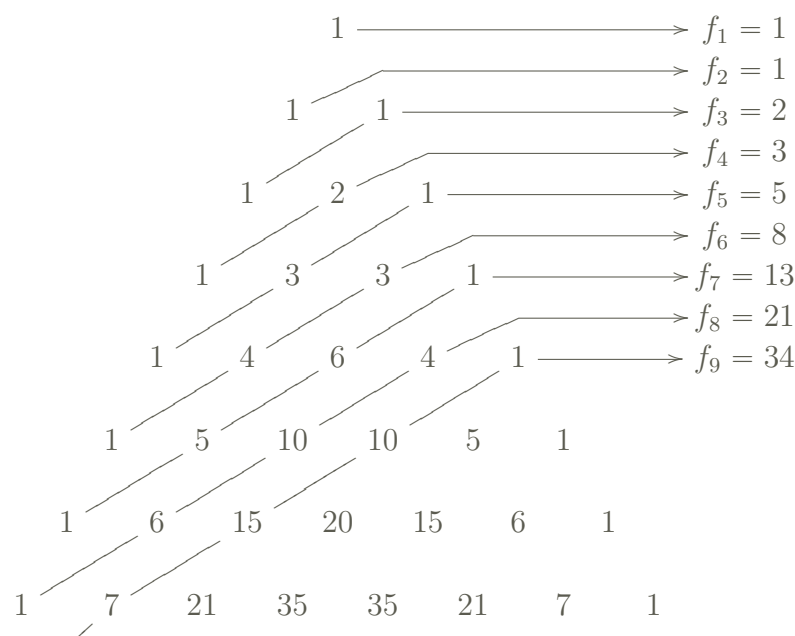
$$f_1 = 1$$

$$f_2 = 2$$

$$f_n = f_{n-2} + f_{n-1}$$

*Die Folge beginnt mit:*

$$[1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \dots]$$

**Fibonacci-Zahlen und  $\varphi$** 

$\varphi$  sei der unendliche Kettenbruch:

$$\varphi := 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}} = [1, 1, \dots] \stackrel{\text{Beh.}}{=} \frac{1}{2} + \frac{\sqrt{5}}{2} \approx 1,62 \dots$$

**Satz 10.2.**

$$q_n = \frac{f_{n+2}}{f_{n+1}}$$

**Beweis:**

Durch Induktion:

$$n = 0 : \quad \frac{f_2}{f_1} = \frac{1}{1} = 1 = q_0$$

$$n = 1 : \quad \frac{f_3}{f_2} = \frac{2}{1} = 2 = q_1$$

$$n - 1 \Rightarrow n : \text{Vor.} : q_{n-1} = \frac{f_{n+1}}{f_n}$$

$$q_n = 1 + \frac{1}{q_{n-1}} \stackrel{\text{Ind.Vor.}}{=} 1 + \frac{f_n}{f_{n+1}} = \frac{f_{n+1} + f_n}{f_{n+1}} \stackrel{\text{RF}}{=} \frac{f_{n+2}}{f_{n+1}}$$

□

**Satz 10.3.**

$$\varphi = \lim_{n \rightarrow \infty} q_n = \frac{1}{2} (1 + \sqrt{5}) = \text{Goldener Schnitt}$$

**Beweis:**Wegen der Kettenbruchdarstellung von  $\varphi$  gilt:

$$\begin{aligned} 1 + \frac{1}{\varphi} &= \varphi & | \cdot \varphi \\ \Rightarrow \varphi + 1 &= \varphi^2 \\ \Leftrightarrow \varphi^2 - \varphi - 1 &= 0 \end{aligned}$$

$$\begin{aligned} x_{1/2} &= \frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} & (\text{Lösung mit } pq\text{-Formel}) \\ &= \frac{1}{2} \pm \sqrt{\frac{5}{4}} = \frac{1}{2} (1 \pm \sqrt{5}) \end{aligned}$$

Da  $\varphi > 0$  folgt  $\varphi = x_1 = \frac{1}{2} (1 + \sqrt{5})$ .

□

**Korollar 10.4.** Der Goldene Schnitt  $\varphi$  ist die positive Lösung der quadratischen (algebraischen) Gleichung:

$$\varphi^2 = \varphi + 1$$

Insbesondere ist  $\varphi$  eine algebraische Zahl.**Satz 10.5.**

$$\varphi^n = f_{n-1} + f_n \varphi \quad \text{für } n \geq 2$$

**Beweis:**

Beweis durch vollständige Induktion:

$$n = 2 \quad \varphi^2 = 1 + \varphi = f_1 + f_2 \varphi.$$



Der Induktionsschritt  $n - 1 \rightarrow n$ :

$$\begin{aligned}
 \varphi^n &= \varphi^{n-1} \cdot \varphi \\
 &= (f_{n-2} + f_{n-1}\varphi)\varphi \quad (\text{nach Induktionsvoraussetzung}) \\
 &= f_{n-2}\varphi + f_{n-1}\varphi^2 = f_{n-2}\varphi + f_{n-1}(1 + \varphi) \\
 &= f_{n-1} + (f_{n-1} + f_{n-2})\varphi = f_{n-1} + f_n\varphi
 \end{aligned}$$

□

Ebenso gibt es eine Rekursionsformel für die negativen  $\varphi$ -Potenzen

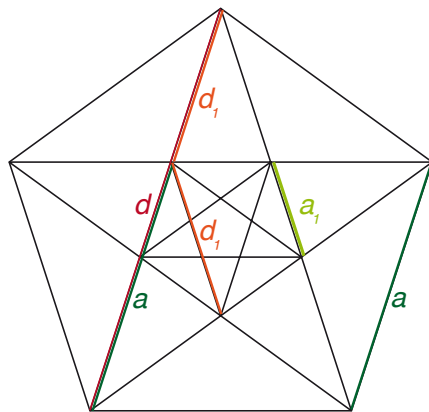
**Satz 10.6.**

$$\frac{1}{\varphi^n} = (-1)^n (f_{n+1} - f_n \varphi) \quad \text{für } n \geq 1.$$

### 10.1. Das regelmäßige 5-Eck - Goldener Schnitt.

*Es gibt kein gemeinsames Maß für die Diagonale und Seite des regelmäßigen Fünfecks.*

D.h. Die Diagonale und die Seite sind **inkommensurabel**!



$$\begin{aligned}
 d &= a + d_1 & a &= a_1 + d_1 \\
 d_1 &= a_1 + d_2 & a_1 &> a_2 + d_2 \\
 &\vdots & &\vdots
 \end{aligned}$$

$\Rightarrow$  Folge  $(d_n, a_n)_{n \in \mathbb{N}}$

**Annahme:**

$$d = n \cdot e \quad a = m \cdot e \quad \text{mit } n, m \in \mathbb{N}.$$

**Beweis:**

Hintereinander Einsetzen :



$$\begin{array}{ll}
d_1 = d - a = n_1 \cdot e & a_1 = a - d_1 = m_1 \cdot e \\
d_2 = d_1 - a_1 = n_2 \cdot e & a_2 = a_1 - d_2 = m_2 \cdot e \\
\vdots & \vdots
\end{array}$$

mit  $n_i, m_i \in \mathbb{N}$ .

**Aber:** Die Zahlen  $d_n$  und  $a_n$  werden bei jedem Schritt mehr als die Hälfte kleiner:

$$d_{n+1} < \frac{d_n}{2} \quad a_{n+1} < \frac{a_n}{2}.$$

$\Rightarrow$  Irgendwann gilt:

$$d_n < e \quad a_n < e \quad \text{für ein } n \in \mathbb{N}. \quad \nless$$

□

**Goldener Schnitt:** Was hat das mit dem Goldenen Schnitt zu tun?

Der Goldene Schnitt ist ein Streckenverhältnis:



Drei Längen:

$$\text{Lang } L = 1 + x, \quad \text{Mittel } M = x, \quad \text{Kurz } S = 1$$

Mit der folgendermaßen vorgeschriebenen Relation der Verhältnisse:

$$\frac{L}{M} = \frac{M}{S}$$

$$\frac{1+x}{x} = \frac{x}{1}$$

$$1+x = x^2$$

$$x^2 - x - 1 = 0$$

$$x_{1/2} = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

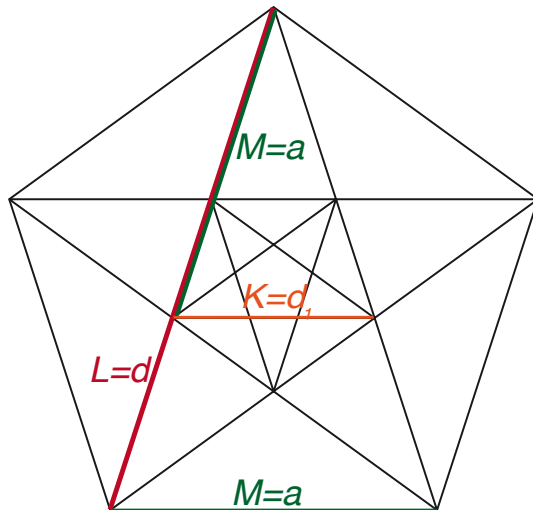
es muss + heißen, da negative Lösungen für Strecken keinen Sinn machen

$$\text{Lösung: } M = L - K = x = \frac{1 + \sqrt{5}}{2} =: \varphi \simeq 1,618 \dots$$



Für  $0 < M < L$  gilt:  $M$  teilt  $L$  im goldenen Schnitt, wenn:

$$L = \varphi \cdot M \quad \Leftrightarrow \quad \frac{L}{M} = \varphi \quad \left( \Leftrightarrow \quad M = \varphi \cdot \underbrace{(L - M)}_K \Leftrightarrow \frac{M}{L - M} = \varphi \right)$$



Zusammenhang zum Fünfeck:

$$K = d_1 = d - a = L - M$$

Strahlensatz:  $\frac{L}{M} = \frac{M}{K}$

$$\frac{L}{M} = \frac{d}{a} = \frac{d_n}{a_n} = \varphi$$

**Warum ist  $\varphi = \frac{1+\sqrt{5}}{2}$  irrational????**

**Annahme:**  $\varphi = \frac{1+\sqrt{5}}{2}$  wäre rational!

$$\Rightarrow \quad \varphi = \frac{p}{q} \in \mathbb{Q}, \text{ also}$$

$$\Rightarrow \quad \frac{d}{a} = \varphi = \frac{p}{q}$$

$$\Rightarrow \quad \frac{d}{p} = \frac{a}{q}$$

Sei  $e := \frac{a}{p} = \frac{d}{q}$

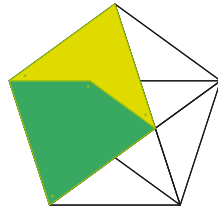


Dann gilt:

$$a = p \cdot e \quad \text{und} \quad d = q \cdot e \quad \Rightarrow \quad d, e \text{ sind kommensurabel} \quad \nexists$$

Also muss  $\varphi$  und damit auch  $\sqrt{5}$  irrational sein!  $\square$

## 10.2. Aperiodische Plasterungen.



Penrose (1973):

2 Fliesen:

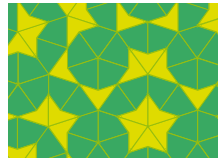
**Kite** und **Dart**

Seitenverhältnisse:

Goldener Schnitt  $\varphi$

Verlegevorschrift: Lege

Punkte aneinander



### Penrose Pflaster

- (1) Mit elementaren Argumenten lässt sich zeigen, daß diese Penrosepflaster immer aperiodisch sind
- (2) Es gibt  $\infty$ -viele verschiedene Penrose Pflaster, von einem kleinen Ausschnitt aus lässt sich aber nicht feststellen, welches man hat

## Nichtperiodische Parkette

**1966:** Robert Berger erfindet ein nichtperiodische Parkett mit 20 426 Grundbausteinen. Diese kann er darauf noch auf 104 Elemente reduzieren.

**1971:** Raphael Robinson: Nichtperiodisches Parkett mit 6 Grundbausteinen.

**1973:** Unabhängig von Robinson erfindet Roger Penrose ebenfalls ein nicht-periodische Parkett mit 6 Grundbausteinen, diesen kann er sogar auf 2 Bausteine *Kite* und *Dart* reduzieren.

**1982:** Dany Shechtman und Kollegen entdecken nicht-periodische Kristallformationen in einer Aluminium-Mangan-Legierung **Quasikristalle**.  
 $\Rightarrow$  **Nobelpreis 2011**

## 10.3. DIN-Norm für Papier.

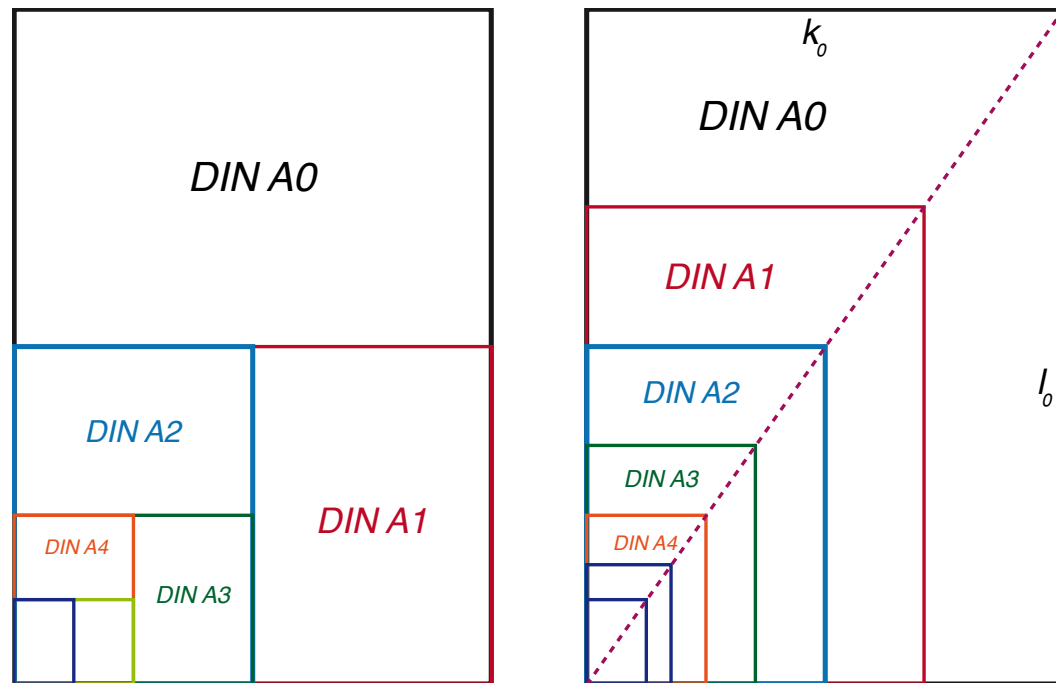
### Die DIN-Papier Norm



**Kravatte falten** $\Rightarrow$  Was sagt uns das? $\Rightarrow$  die lange Seite ist so lang wie die Diagonale des Quadrates über der kurzen Seite:

$$\Rightarrow \boxed{l = \sqrt{2} \cdot k}$$

Genauere Untersuchung der DIN-Norm:

Die Seiten  $l_n$  und  $k_n$  sind ein weiteres Beispiel inkommensurabler Zahlenpaare.

$i$	$l_i$	$k_i$	$F_i = F(Ai) = l_i \cdot k_i$
0	$l_0$	$k_0$	$(1 = 2^0 \quad (\text{m}^2) \text{ später})$
1	$l_1 = k_0$	$k_1 = \frac{l_0}{2}$	$\frac{1}{2}F_0 = 2^{-1}F_0$
	$\vdots$	$\vdots$	$\vdots$
$n+1$	$l_{n+1} = k_n$	$k_{n+1} = \frac{l_n}{2}$	$2^{-(n+1)}F_0$



Darüberhinaus: **Seitenverhältnisse konstant:**

$$\frac{l_n}{k_n} = \frac{l_{n+1}}{k_{n+1}} = \frac{k_n}{\binom{l_n}{2}} = \frac{2k_n}{l_n}$$

$$l_n^2 = 2k_n^2$$

$$\Rightarrow \boxed{l_n = \sqrt{2} \cdot k_n}$$

**Warum sind  $l_0$  und  $k_0$  inkommensurabel?**

Annahmen sie wären kommensurabel: Dann gibt es eine Einheitslänge  $e$  und natürliche Zahlen  $n_0, m_0 \in \mathbb{N}$  mit:

$$l_0 = m_0 \cdot e, \quad k_0 = n_0 \cdot e.$$

Aber

$$l_{2n} = k_{2n-1} = 2^{-1}l_{2n-2} = \cdots = 2^{-n}l_0 = \frac{l_0}{2^n}$$

$$k_{2n} = \frac{1}{2}l_{2n-1} = 2^{-1}k_{2n-2} = \cdots = 2^{-n}k_0 = \frac{k_0}{2^n}$$

mit ungeraden Indices geht das natürlich analog:

$$l_{2n+1} = k_{2n} = 2^{-1}l_{2n-1} = \cdots = 2^{-n}l_0 = 2^{-n}k_0 = \frac{k_0}{2^n}$$

$$k_{2n+1} = \frac{1}{2}l_{2n} = 2^{-1}k_{2n-1} = \cdots = 2^{-n}k_1 = 2^{-(n+1)}l_0 = \frac{l_0}{2^{n+1}}$$

**Kann man die Größen  $l_n$  und  $k_n$  auch explizit angeben?** Dazu müssen wir  $l_0$  und  $k_0$  kennen. Erst hier brauchen wir die Information/Definition:

$$F_0 := 1 \text{ m}^2.$$





Zusammen mit  $l_n = \sqrt{2} \cdot k_n$  folgt:

$$\begin{aligned}
 l_0 \cdot k_0 &= 1 \text{ m}^2 \\
 k_0 &= \frac{1}{l_0} = \frac{1}{\sqrt{2} \cdot k_0} \\
 k_0^2 &= \frac{1}{\sqrt{2}} = 2^{-\frac{1}{2}} \\
 k_0 &= 2^{-\frac{1}{4}} = \frac{1}{\sqrt[4]{2}} \\
 \Rightarrow \quad l_0 &= \frac{\sqrt{2}}{\sqrt[4]{2}} = 2^{\frac{1}{2} - \frac{1}{4}} = 2^{\frac{1}{4}} = \sqrt[4]{2}
 \end{aligned}$$

Ein bisschen Einsetzen und Rechnerei liefert:

$$\Rightarrow \quad l_n = \frac{\sqrt[4]{2}}{\sqrt[2]{2^n}} \text{ m} = 2^{\frac{1-2n}{4}} \text{ m} \quad k_n = \frac{1}{\sqrt[4]{2} \cdot \sqrt[2]{2^n}} \text{ m} = 2^{-\frac{2n+1}{4}} \text{ m}$$

**Probe:** DIN A4:

$$\begin{aligned}
 l_4 &= 2^{\frac{1-2 \cdot 4}{4}} \text{ m} = 2^{-\frac{7}{4}} \text{ m} = 0,2973 \text{ m} = 29,73 \text{ cm} \\
 \text{und} \quad k_4 &= 2^{-\frac{9}{4}} \text{ m} = 0,2102 \text{ m} = 21,02 \text{ cm}
 \end{aligned}$$

Die Irrationalität von  $\sqrt{2}$  lässt sich nun analog wie beim goldenen Schnitt zeigen!

## 11. EAN, ISBN, PZN UND IBAN

### 11.1. EAN im Supermarkt.

**EAN** = Europäische Artikelnummer

**Beispiele**

Bad Brückenauer Mineralwasser	4 001784 015309
Seitenbacher Müsli	4 008391 041721
Appel Heringsfilet	4 020500 966015

**Gemeinsamkeiten:**

- 13 Ziffern
- Anfangsziffer 4 oder bzw. 40

**Bedeutung der Ziffern**

z.B. Iglo Schlemmerfilet:

405	6100	04221	7
↑	↑	↑	↑

Ländernr.   Betriebsnummer   Artikelnummer   Prüfziffer

**Bemerkung:** Es gibt einige besondere Produkte mit nur 8 Ziffern!

400 – 440 sind für Deutschland reserviert (vgl. GS1-Länderpräfix).

**EAN** wurde in den 1970-er Jahren eingeführt und wird von der **GS1** verwaltet. **GS1** (**G**lobal **S**tandards **O**ne) ist eine weltweite, privatwirtschaftlich aufgestellte Organisation, die globale Standards zur Verbesserung von Wertschöpfungsketten gestaltet und umsetzt sowie weltweit für die Vergabe der Global Trade Item Number (GTIN) für Produkte sowie weiterer eindeutiger Idente zur Kennzeichnung von Anlagen, Behältern, Dokumenten und anderen Geschäftsobjekten zuständig ist.

In USA: 12-ziffriger **UPC**-Code.

Beide Codes sind kompatibel:

$$0 + \text{UPC} = \text{EAN}$$



Was ist die EAN-Prüfziffer?

Beim Schreiben einer Zahlenfolge passieren, wie beim Schreiben eines Textes, verschiedene Fehler:

- falsche Ziffer - falscher Buchstabe
- Zahlendreher
- eine Ziffer zuviel oder zuwenig
- Beschädigung des Codes

Bei Worten/Texten läßt sich der richtige Text meistens erraten,  
bei Zahlenfolgen aber nicht  $\Rightarrow$  **Problem!!**

Zur Fehlerentdeckung dient die Prüfziffer. Die **EAN** hat 13 Ziffern:  $z_1 z_2 z_3 \dots z_{12} z_{13}$ :

$$\underbrace{z_1 z_2 z_3}_{\text{Ländernr.}} \quad \underbrace{z_4 \dots z_7}_{\text{Betriebsnr.}} \quad \underbrace{z_8 \dots z_{12}}_{\text{Artikelnr.}}$$

Definiere dann die Prüfziffer  $0 \leq z_{13} < 10$  mit:

$$z_{13} \equiv -(z_1 + z_3 + z_5 + z_7 + z_9 + z_{11} + 3 \cdot (z_2 + z_4 + z_6 + z_8 + z_{10} + z_{12})) \pmod{10}$$

Für die Vollständige **EAN** gilt dann:

$$\begin{aligned} \text{Prüfsumme } S &:= z_1 + z_3 + z_5 + z_7 + z_9 + z_{11} + 3 \cdot (z_2 + z_4 + z_6 + z_8 + z_{10} + z_{12}) + z_{13} \\ &\equiv 0 \pmod{10} \end{aligned}$$

Überprüfung einer vollständigen EAN auf ihre Korrektheit:

Code wird akzeptiert, falls:  $S \equiv 0 \pmod{10}$

**Beispiele (1)**

$$\begin{array}{cccccccccccccc} 4 & 0 & 5 & 6 & 1 & 0 & 0 & 0 & 4 & 2 & 2 & 1 & 7 \\ \downarrow \times 1 & \downarrow \times 3 & \downarrow \times 1 & \downarrow \times 3 & \downarrow \times 1 & \downarrow \times 3 & \downarrow \times 1 & \downarrow \times 3 & \downarrow \times 1 & \downarrow \times 3 & \downarrow \times 1 & \downarrow \times 3 & \downarrow \times 1 \\ 4+ & 0+ & 5+ & 18+ & 1+ & 0+ & 0+ & 0+ & 4+ & 6+ & 2+ & +3 & +7 = 50 \\ \text{Prüfsumme : } & S = 50 \equiv 0 \pmod{10} & \checkmark \end{array}$$



(2)

$$\begin{array}{ccccccccccccccc}
 4 & 0 & 2 & 1 & & 3 & 7 & & 5 & 0 & 0 & 1 & & 7 & 4 & & 0 \\
 \downarrow & & & \downarrow \times 3 & & \downarrow \times 3 & & & \downarrow \times 3 & & \downarrow \times 3 & \downarrow & & & & & \\
 4+ & & 2+ & 3+ & & 3+ & 21+ & & 5+ & & 3+ & 7+ & 12+ & & 0 & = & 60
 \end{array}$$

$$S = 60 \equiv 0 \pmod{10} \Rightarrow \checkmark$$

$\Rightarrow$  Prüfgerät akzeptiert die Nummer!

Häufigkeit der verschiedenen Fehlertypen:

Z.B. beim Eintippen der Ziffer: 4711

Fehlertyp	Beispiel	Häufigkeit
(1) eine Ziffer falsch	4712	60%
(2) zuviel/zuwenig Ziffern	471 oder 47111	25%
(3) zwei oder mehr Ziffern falsch	4822	8%
(4) Zahlendreher	7411	5%
(5) Vertauschen von Blöcken	1147	1%

Hilft die Prüfziffer, diese Fehler zu entdecken?

**Satz 11.1.** Die Eingabe genau einer falschen Ziffer wird durch die Prüfziffer stets erkannt.

**Beweis:**

Wenn genau eine Ziffer falsch ist  $\Rightarrow$  drei Möglichkeiten:

- (1) Die falsche Ziffer ist unter den Zahlen mit ungeraden Indices:  $\{z_1, z_3, z_5, z_7, z_9, z_{11}\}$
- (2) Die falsche Ziffer ist unter den Zahlen mit geraden Indices:  $\{z_2, z_4, z_6, z_8, z_{10}, z_{12}\}$
- (3) Die Prüfziffer  $z_{13}$  ist falsch.

Fall (1): Sei  $\hat{z}_i$  mit  $1 \leq i \leq 11$  ungerade, die falsche Ziffer. Also  $\hat{z}_i \neq z_i$  und da beide Zahlen zwischen 0 und 9 liegen gilt:

$$\hat{z}_i \not\equiv z_i \pmod{10}$$

Damit wird eine falsche Prüfsumme  $\hat{S}$  berechnet:

$$\begin{aligned}
 \hat{S} &:= z_1 + \cdots + \hat{z}_i + \cdots + z_{11} + z_{13} + 3 \cdot (z_2 + z_4 + z_6 + z_8 + z_{10} + z_{12}) \\
 &= z_1 + \cdots + z_i + \cdots + z_{11} + z_{13} + 3 \cdot (z_2 + z_4 + z_6 + z_8 + z_{10} + z_{12}) + (\hat{z}_i - z_i) \\
 &\equiv 0 + (\hat{z}_i - z_i) \not\equiv 0 \pmod{10}
 \end{aligned}$$



⇒ Fehler wird entdeckt!

Fall (2): Sei  $\hat{z}_i$  mit  $2 \leq i \leq 12$  gerade, die falsche Ziffer. Also  $\hat{z}_i \neq z_i$  und da beide Zahlen zwischen 0 und 9 liegen gilt:

$$\hat{z}_i - z_i \not\equiv 0 \pmod{10} \Rightarrow 3(\hat{z}_i - z_i) \not\equiv 0 \pmod{10}$$

Damit wird eine falsche Prüfsumme  $\hat{S}$  berechnet:

$$\begin{aligned} \hat{S} &:= z_1 + \dots + z_{11} + z_{13} + 3 \cdot (z_2 + \dots + \hat{z}_i + \dots + z_{12}) \\ &\equiv 3(\hat{z}_i - z_i) \not\equiv 0 \pmod{10} \end{aligned}$$

⇒ Fehler wird entdeckt!

Fall (3): Prüfziffer falsch, klar wird erkannt! □

Werden auch Fehler mit zwei falschen Ziffern erkannt?

Diese Fehler werden nicht notwendigerweise erkannt:

**Beispiel:**

richtige **EAN**: 4 008391 041721

falsche **EAN**: 4 018291 041721

Prüfsummen:

$$\begin{aligned} \hat{S} - S &= 4 + \textcolor{red}{1} + \textcolor{red}{2} + 1 + 4 + 7 + 3(0 + 8 + 9 + 0 + 1 + 2) \\ &\quad - (4 + 0 + 3 + 1 + 4 + 7 + 3(0 + 8 + 9 + 0 + 1 + 2)) \\ &= \textcolor{red}{1} + \textcolor{red}{2} - 0 - 3 = 0 \end{aligned}$$

⇒ Fehler wird nicht entdeckt!

Drehfehler

**Satz 11.2.** Die einzigen Drehfehler benachbarter Ziffern  $z_i, z_{i+1}$ , die nicht entdeckt werden, sind diejenigen mit:

$$z_i \equiv z_{i+1} \pmod{5}$$

**Beweis:**

$$\text{EAN}_{\text{falsch}} : z_1 z_2 z_3 \dots \underbrace{z_{i+1} z_i}_{\text{Drehfehler}} \dots z_{12} z_{13}$$



Wenn  $i$  gerade  $\Rightarrow z_i$  steht an ungerader Position:

$$\begin{aligned}
 S_{\text{falsch}} &= z_1 + \cdots + \textcolor{red}{z_i} + \cdots + z_{13} + 3 \cdot (z_2 + \cdots + \textcolor{red}{z_{i+1}} + \cdots + z_{12}) \\
 &= \underbrace{z_1 + \cdots + z_{i+1} + \cdots + z_{13} + 3 \cdot (z_2 + \cdots + z_i + \cdots + z_{12})}_{S \text{ von korrekter EAN} \equiv 0 \pmod{10}} \\
 &\quad + \textcolor{red}{z_i} + 3\textcolor{red}{z_{i+1}} - z_{i+1} - 3z_i \\
 &= S + 2(z_{i+1} - z_i) \equiv 2(z_{i+1} - z_i) \pmod{10}
 \end{aligned}$$

Fehler wird genau dann nicht entdeckt, wenn:

$$\begin{aligned}
 S_{\text{falsch}} &\equiv 0 \pmod{10} \\
 \Leftrightarrow 2(z_{i+1} - z_i) &\equiv 0 \pmod{10} && (\text{durch 2 teilen}) \\
 \Leftrightarrow z_{i+1} - z_i &\equiv 0 \pmod{5} && (\text{weil } \frac{10}{\text{ggT}(2,10)} = \frac{10}{2} = 5)
 \end{aligned}$$

Wenn  $i$  ungerader Index ist, analoge Rechnung.  $\square$

Das lässt sich natürlich auf andere nicht benachbarte Drehfehler erweitern, dann aber viele Fallunterscheidungen. Aber, Drehfehler sind eigentlich immer benachbart!

## 11.2. ISBN.

Quelle: Sakurambo, English Wikipedia



Vor 2007 ISBN-10: 10 Ziffern

Nach 2007 ISBN-13: 13 Ziffern

**Beispiel:** Ende 2006 erschien: Franke, M., Didaktik der Geometrie in der Grundschule, mit den 2 ISBN Nummern:

ISBN-10: 3-8274-1511-X



ISBN-13: 978-3-8274-1511-0

ISBN-13 funktioniert analog EAN!

### Bedeutung der Ziffern bei ISBN-10:

Gruppennr.	Verlagsnr.	Titelnummer	Prüfziffer
↓	↓	↓	↓
3	- 8274	- 1511	- X

Gruppennummer 3: deutschsprachiger Raum (Deutschland, Österreich, Schweiz)  
(Die Gruppennummer kann auch mehrere Stellen haben, z.B. 82-Norwegen, 84-Spanien, 88-Italien, 956-Chile. . . Entsprechend hat die Verlagsnummer dann weniger Stellen.)

Prüfziffer: römisch  $X = 10$

Prüfsumme  $\Sigma$ :

$$\begin{aligned}\Sigma &:= 3 \cdot 10 + 8 \cdot 9 + 2 \cdot 8 + 7 \cdot 7 + 4 \cdot 6 + 1 \cdot 5 + 5 \cdot 4 + 1 \cdot 3 + 1 \cdot 2 + X \cdot 1 \\ &= 30 + 72 + 16 + 49 + 24 + 5 + 20 + 3 + 2 + 10 \\ &= 231 = 21 \cdot 11 \\ &\equiv 0 \pmod{11}\end{aligned}$$

Wenn  $\Sigma \equiv 0 \pmod{11}$  wird die **ISBN** akzeptiert!

### Allgemeine Beschreibung

**ISBN-10:**  $z_{10} - z_9 z_8 z_7 z_6 - z_5 z_4 z_3 z_2 - z_1$

Prüfziffer:  $z_1 := -(z_{10} \cdot 10 + z_9 \cdot 9 + \dots + z_2 \cdot 2) \pmod{11}$

ist also eine Ziffer  $0 \leq z_1 \leq 10$  und statt 10 schreibt man römisch  $X$

Prüfsumme:  $\Sigma := z_{10} \cdot 10 + z_9 \cdot 9 + \dots + z_2 \cdot 2 + z_1 \cdot 1$

Die **ISBN** wird akzeptiert, wenn die Prüfsumme kongruent 0 modulo 11 ist, denn dann:

$$\begin{aligned}\Sigma &\equiv 0 \pmod{11} \\ \Leftrightarrow 0 &\equiv z_{10} \cdot 10 + z_9 \cdot 9 + \dots + z_2 \cdot 2 + z_1 \cdot 1 \pmod{11} \\ \Leftrightarrow z_1 &\equiv -(z_{10} \cdot 10 + z_9 \cdot 9 + \dots + z_2 \cdot 2) \pmod{11} \quad (\text{wie es sein soll!})\end{aligned}$$



**Satz 11.3.**

- Das **ISBN** Prüfverfahren deckt alle Fehler auf, bei denen genau eine Ziffer falsch ist.
- Fehler mit genau 2 falschen Ziffern werden nicht immer entdeckt.
- Alle Drehfehler (benachbart oder nicht) werden entdeckt.
- Vertauschungen benachbarter 2-er Blöcke werden häufig entdeckt.

**11.3. Die Pharmazentralnummer PZN.**

Die Pharmazentralnummer **PZN** ist eine siebenstellige Ziffernfolge:

6 Ziffern + Prüfziffer:  $a_1 a_2 a_3 a_4 a_5 a_6 p$

Prüfsumme:  $S := 2 \cdot a_1 + 3 \cdot a_2 + 4 \cdot a_3 + 5 \cdot a_4 + 6 \cdot a_5 + 7 \cdot a_6$

Prüfziffer:  $p \equiv S \pmod{11}$

oder äquivalent: Die Prüfnummer ist der Rest beim Teilen der Prüfsumme mit Rest durch 11  $\Rightarrow$

$$S = b \cdot 11 + p \quad \text{mit } 0 \leq p \leq 10$$

**Beispiel: PZN - 3414966**

Auf Korrektheit überprüfen:

$$2 \cdot 3 + 3 \cdot 4 + 4 \cdot 1 + 5 \cdot 4 + 6 \cdot 9 + 7 \cdot 6 = 138 = 12 \cdot 11 + 6 \equiv 6 \pmod{11} \quad \checkmark$$

da  $p = 6$ !



#### 11.4. IBAN, Verfahren Modulo 97-10 (ISO 7064).

IBAN (=International **B**ank **A**ccount **N**umber) zusammen mit BIC (= Bank Identifier Code) bilden die international einheitlichen Daten zur Identifizierung eines Kontos, die im Rahmen von SEPA (Single Euro Payments Area) zum nationalen und internationalen Zahlungsverkehr benötigt werden. IBAN-Pflicht: 1. Februar 2016 (letzte Frist)

Format der BIC:  $\underbrace{\text{XXXX}}_{\text{Bankcode}} \underbrace{\text{XX}}_{\text{Ländercode}} \underbrace{\text{XX}}_{\text{Ortscode}} \underbrace{\text{XXX}}_{\text{Filiale}}$

Beispiel: VR Bank Nürnberg:

BIC: GENO DE F1 N02                      BLZ: 760 60 618

Format der IBAN: maximal 34 Alphanummerische Zeichen:

$\underbrace{\alpha_1 \alpha_2}_{\text{Land}} \underbrace{p_1 p_2}_{\text{Prüfzahl}} \underbrace{k_1 k_2 \cdots k_{30}}_{\text{Kontoidentifikation}}$

Für Deutschland gilt:

DE  $\underbrace{p_1 p_2}_{\text{Prüfzahl}} \underbrace{b_1 b_2 \cdots b_8}_{\text{Bankleitzahl}} \underbrace{k_1 k_2 \cdots k_{10}}_{\text{Kontonummer}}$

#### Berechnung einer IBAN bzw. der Prüfziffer(n)

Verfahren Modulo 97-10 (ISO 7064)

##### Beispiel:

BLZ: 760 60 618

Kontonummer: 218561 (ist eine zulässige fiktive Kn.)

Kontonummer hat 6 Stellen, mit Nullen zu 10 Stellen ergänzen  $\Rightarrow$

IBAN: DE  $p_1 p_2$  7606 0618 0000 2185 61

Zur Berechnung der Prüfziffern setzt man diese zunächst gleich 00

DE 00 7606 0618 0000 2185 61

Umstellen 7606 0618 0000 2185 61 DE 00

Ersetze Buchstaben durch Zahlen: A=10, B=11, C=12, D=13...

7606 0618 0000 2185 6113 1400



Teilen mit Rest modulo 97

$$7606\ 0618\ 0000\ 2185\ 6113\ 1400 \equiv 31 \pmod{97}$$

$$98 - 31 = 67 =: p_1 p_2$$

**Problem** Mein Taschenrechner macht Folgendes:

$$7606\ 0618\ 0000\ 2185\ 6113\ 1400 \boxed{\div R} \Rightarrow 7,8413 \cdot 10^{21}$$

Hilfsmethode (da  $\gcd(97, 10) = 1$ ):

$$\begin{aligned} 7606\ 0618\ 0000\ 2185\ 6113\ 1400 &= \overbrace{760606180}^{9 \text{ Ziffern}} 000\ 2185\ 6113\ 1400 \\ &\equiv_{80} \pmod{97} \\ &\equiv 80\ 000\ 2185\ 6113\ 1400 \pmod{97} \\ &= \overbrace{8000021}^{7 \text{ Ziffern}} 85\ 6113\ 1400 \\ &\equiv_{43} \pmod{97} \\ &\equiv 43\ 85\ 6113\ 1400 \pmod{97} \\ &= \overbrace{4385611}^{7 \text{ Ziffern}} 3\ 1400 \\ &\equiv_{47} \pmod{97} \\ &\equiv 47\ 3\ 1400 \pmod{97} \\ &= \overbrace{4731400}^{7 \text{ Ziffern}} \\ &\equiv_{31} \pmod{97} \\ &\equiv 31 \pmod{97} \end{aligned}$$

$$\text{Prüfzahl: } 98 - 31 = 67$$

$$\text{IBAN: } \text{DE } 67\ 7606\ 0618\ 0000\ 2185\ 61$$

- (1) Prüfziffern auf 00 setzen
- (2)  $\alpha_1 \alpha_2 p_1 p_2$  nach hinten umstellen
- (3) Buchstaben durch Zahlen ersetzen: A=10, B=11, C=12, D=13...
- (4) R = Rest modulo 97 berechnen
- (5) Prüfzahl  $p_1 p_2 = 98 - R$



**Prüfung einer IBAN auf Korrektheit**

IBAN: DE 67 7606 0618 0000 2185 61

Umstellen und Buchstaben ersetzen:

$$7606\ 0618\ 0000\ 2185\ 61 \underbrace{13\ 14\ 67}_{\text{DE}} \equiv 1 \pmod{97} \Rightarrow \text{korrekt}$$

Klar, denn

$$\begin{aligned} 7606\ 0618\ 0000\ 2185\ 6113\ 1400 &\equiv 31 \pmod{97} \\ \Rightarrow 7606\ 0618\ 0000\ 2185\ 6113\ 1467 &\equiv 31 + 67 = 98 \equiv 1 \pmod{97} \end{aligned}$$

## 12. KRYPTOGRAPHIE

## 12.1. Monoalphabetische Substitution.

Hierbei werden den Buchstaben des Alphabets  $\mathbb{A}$  (Klartextalphabet) eindeutig die Buchstaben eines Geheimentextalphabets  $\mathbb{G}$  zugeordnet (angeblich schon von Julius Cäsar angewandt). Der Code bzw. die Codierung oder Verschlüsselung ist die Abbildung:

$$\kappa : \mathbb{A} \longrightarrow \mathbb{G}$$

Der Schlüssel ist die Umkehrabbildung:

$$\kappa^{-1} : \mathbb{G} \longrightarrow \mathbb{A}$$

In diesem Abschnitt gilt:

$$\mathbb{G} = \mathbb{A}$$

**Methode 1: Zyklische Vertauschung**

$$\mathbb{A} = \{\alpha_1, \alpha_2, \dots, \alpha_d\} \quad \text{und} \quad \kappa_n(\alpha_i) = \alpha_{i+n}$$

wobei der Index modulo  $d$  zu verstehen ist, also eigentlich  $\alpha_i = \alpha_{\bar{i}}$

**Beispiel:**  $\mathbb{A}$  = unser Alphabet,  $n = 3$ :

Klartextalphabet    A B C D ... W X Y Z

Geheimentextalphabet D E F G ... Z A B C

Hat das Alphabet  $\mathbb{A}$  genau  $d$  (hier  $d = 26$ ) Elemente, so gibt es nur  $d - 1$  (bzw. 25) Verschlüsselungen dieser Art.

**Methode 2: Multiplikation statt Addition im Index:**

$$\mathbb{A} = \{\alpha_1, \alpha_2, \dots, \alpha_d\} \quad \text{und} \quad \kappa_m(\alpha_i) = \alpha_{i \cdot m}$$

**Beispiel:**  $m = 2$  und  $\mathbb{A} = \{A, B, \dots, Z\}$ , also  $d = 26$

Nr. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

$\mathbb{A}$  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

$\mathbb{G}$  B D F H J L N P R T V X Z B D F H J L N P R T V X Z

Problem: die Abbildung ist nicht injektiv!!

Verallgemeinerung:

Wenn  $\gcd(m, d) \neq 1$ , dann ist  $\kappa_m$  nicht injektiv und hat keine Umkehrabbildung, kommt also nicht in Frage.



Wenn  $ggT(m, d) = 1$ , dann ist  $\kappa_m$  injektiv, aber es gibt nicht allzu viele neue Verschlüsselungen, nämlich

$$\varphi(d) - 1 \quad (\text{bzw. } \varphi(26) - 1 = \varphi(13) \cdot \varphi(2) - 1 = 12 \cdot 1 - 1 = 11)$$

( $\varphi(d) - 1$ , weil  $\varphi(d)$  die Anzahl der Möglichkeiten für  $m$  mit  $ggT(m, d) = 1$ , aber  $m = 1$  bedeutet die Identität, fällt also heraus.)

Die Methode ist also auch ziemlich unsicher, weil die wenigen Möglichkeiten einfach und schnell durchgeprüft werden können.

### Methode 3: Multiplikation und Addition kombinieren:

$$\mathbb{G} = \mathbb{A} = \{\alpha_1, \alpha_2, \dots, \alpha_d\} \quad \text{und} \quad \kappa_{m,n}(\alpha_i) = \alpha_{i \cdot m + n}$$

Davon gibt es nach dem oben gesagten  $\varphi(d)$  Möglichkeiten für  $m$ , so daß  $ggT(m, d) = 1$ , sowie  $d$  Möglichkeiten für  $n$ , aber  $\kappa_{1,1} = \text{id}$  fällt heraus, also insgesamt gibt es

$$\varphi(d)d - 1 \quad \text{Möglichkeiten}$$

(bzw.  $\varphi(26) \cdot 26 - 1 = 12 \cdot 26 - 1 = 311$ ).

### Entschlüsselung von einem mit $\kappa_{m,n}$ codiertem Text

**Beispiel:**  $d = 26$  (also  $\mathbb{A} = \{A, B, \dots, Z\}$ ) und  $(m, n) = (3, 17)$ , also  $\kappa_{3,17}$ .

Behauptung:  $\kappa_{3,17}^{-1} = \kappa_{9,3}$ .

$$9 \cdot (3 \cdot i + 17) + 3 = 27 \cdot i + 9 \cdot 17 + 3 = \underset{\substack{\uparrow \\ 1 \bmod 26}}{27} \cdot i + \underset{\substack{\uparrow \\ 6 \cdot 26}}{156} \equiv i \pmod{26}$$

$$\kappa_{9,3} \circ \kappa_{3,17}(\alpha_i) = \alpha_{9 \cdot (3 \cdot i + 17) + 3} = \alpha_i \quad (\text{für alle } i)$$

□

Allgemein:

Angenommen es gibt  $m', n'$ , so daß für alle Indices  $i \in \{1, \dots, d\}$  gilt:

$$m' \cdot (i \cdot m + n) + n' \equiv i \pmod{d}$$

Dann gilt sicher

$$\kappa_{m',n'} \circ \kappa_{m,n} = \text{id}$$

**Satz 12.1.**  $\kappa_{m,n}$  ist genau dann invertierbar, wenn  $ggT(m, d) = 1$ . Dann gilt ferner

$$\kappa_{m,n}^{-1} = \kappa_{m',n'}$$

mit  $m', n' \in \mathbb{Z}$ , so daß  $\overline{m'} = \overline{m}^{-1}$  in  $\mathbb{Z}/d\mathbb{Z}$  und  $n' \equiv -m' \cdot n \pmod{d}$ .



**Beweis:**

$\kappa_{m,n}$  ist genau dann invertierbar, wenn es  $m', n'$  gibt mit:

$$m' \cdot (i \cdot m + n) + n' \equiv i \pmod{d} \quad \forall i \quad (*)$$

Aber

$$m' \cdot (i \cdot m + n) + n' = m'm \cdot i + (m'n + n')$$

also (\*) gilt genau dann, wenn:

$$m'm \equiv 1 \pmod{d} \quad \text{und} \quad m'n + n' \equiv 0 \pmod{d}$$

Damit  $m'$  bzw.  $\overline{m}^{-1} \in \mathbb{Z}/d\mathbb{Z}$  existiert, muss  $ggT(m, d) = 1$  gelten!  $\square$

**Beispiel**  $d = 26$  und  $(m, n) = (3, 2)$ , also  $\kappa_{3,2}$ :

Da  $ggT(3, 26) = 1$  ist  $\kappa_{3,2}$  invertierbar. Aber:

$$\kappa_{3,2}(\alpha_{12}) = \alpha_{3 \cdot 12 + 2} = \alpha_{38} = \alpha_{12}$$

Also hat  $\kappa_{3,2}$  Fixpunkte und ist damit ungeeignet für eine Verschlüsselung!

Wann hat  $\kappa_{m,n}$  Fixpunkte?

Offenbar gilt:

$$\begin{aligned} \kappa_{m,n}(\alpha_i) = \alpha_i &\Leftrightarrow m \cdot i + n \equiv i \pmod{d} && \text{(für ein spezielles } i) \\ &\Leftrightarrow d \mid (mi + n - i) = (m-1)i + n && \text{(für dieses } i) \end{aligned}$$

Das läßt sich nur in Spezialfällen weiter untersuchen:

**Beispiel**  $d = 26$  und  $ggT(m, 26) = 1$

$$26 \mid (mi + n - i) = (m-1)i + n$$

Aus  $ggT(m, 26) = 1$  folgt, daß  $m$  ungerade ist, somit sind  $(m-1)$  und  $(m-1)i$  für alle  $i$  gerade. Wenn nun  $n$  ungerade wäre, dann wäre  $(m-1)i + n$  ungerade und damit kein Vielfaches der geraden Zahl 26.

**Folgerung:** Wenn  $d = 26$ ,  $ggT(m, 26) = 1$  und  $n$  ungerade ist, dann ist  $\kappa_{m,n}$  invertierbar und fixpunktfrei!

Je mehr Codes zur Verfügung stehen, desto schwieriger bzw. langsamer wird es, alle Möglichkeiten durchzuprobieren, um den richtigen Schlüssel zu finden. Mit den obigen Methoden gibt es aber nicht viele Codes, weniger als 311 im Fall  $d = 26$ .



Weitere Verallgemeinerung: man permutiert die Buchstaben des Alphabets nicht nur linear, wie oben beschrieben, sondern läßt alle denkbaren Permutationen der  $d$  Buchstaben zu. Dann erhöht sich die Anzahl der Möglichkeiten auf  $d!$  Codes!

Aber auch diese vielen Codes lassen sich relativ einfach (mit Rechneinsatz) entschlüsseln (d.h. den richtigen Schlüssel finden), wenn man zusätzliche Eigenschaften eines Textes, wie zum Beispiel Buchstabenhäufigkeiten (z.B. e, n, i, ...) und Häufigkeiten von Buchstaben-Kombinationen (z.B. qu, sch, st, ch ...) in Abhängigkeit von der Sprache natürlich, berücksichtigt. Denn diese Buchstaben- und Kombinationen findet man dann auch im Geheimtext und kann so auf gewisse Buchstaben zurückschließen.

## 12.2. Polyalphabetische Substitution.

Hierbei werden in Folge  $n$  verschiedene Codes  $\kappa_1, \dots, \kappa_n$  auf die Buchstaben des Klartextes angewandt:

Wenn z.B. wieder  $\mathbb{A} = \{A, B, \dots, Z\}$ , erfolgt die Verschlüsselung von einem Klartext folgendermaßen:

**Klartext:** dies ist ein code ... er kann sicher entschlüsselt werden ...

**Geheimtext:**  $\kappa_1(d) \kappa_2(i) \kappa_3(e) \kappa_4(s) \kappa_5(i) \kappa_6(s) \kappa_7(t) \kappa_8(e) \kappa_9(i) \kappa_{10}(n) \kappa_{11}(c) \kappa_{12}(o) \kappa_{13}(d) \kappa_{14}(e) \kappa_{15} \dots \kappa_{n-3}(e) \kappa_{n-2}(r) \kappa_{n-1}(k) \kappa_n(a) \kappa_1(n) \kappa_2(n) \kappa_3(s) \kappa_4(i) \kappa_5(c) \kappa_6(h) \kappa_7(e) \kappa_8(r) \kappa_9(e) \kappa_{10}(n) \kappa_{11}(t) \kappa_{12}(s) \kappa_{13}(c) \kappa_{14}(h) \kappa_{15}(l) \kappa_{16}(u) \kappa_{17}(e) \kappa_{18}(s) \kappa_{19}(s) \kappa_{20}(e) \kappa_{21}(l) \kappa_{22}(t) \dots$

Die Anzahl  $n$  der Codes  $\kappa_i$  heißt *Periodenlänge*. Die Anzahl der möglichen Codes bzw. Schlüssel ist damit  $(26!)^n$ .

Kennt man die Periodenlänge, so ist eine Entschlüsselung einfacher. Darauf bemüht man Methoden wie bei der monoalphabetischen Substitution.

## 13. RSA-VERSCHLÜSSELUNGSSYSTEM

Das RSA-Verschlüsselungssystem ist ein 1978 entwickeltes Verfahren. Benannt nach seinen Autoren **R.** Rivest, **A.** Shamir und **L.**Adleman.

**Vorgehensweise:**

Eine Sender A will dem Empfänger B eine verschlüsselte Nachricht übermitteln.

- (1) Der Empfänger B bestimmt zwei mindestens 100-ziffrige Primzahlen  $p$  und  $q$ .
- (2)  $n := p \cdot q$
- (3) Die Anzahl der zu  $n$  teilerfremden natürlichen Zahlen ist (vgl. Satz 5.30 in Abschnitt 5.4):

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$$

- (4) Sei  $1 < s < \varphi(n)$  eine zu  $\varphi(n)$  teilerfremde Zahl (also  $\text{ggT}(s, \varphi(n)) = 1$ ). Z.B. tuts eine Primzahl  $s > \max(p, q)$ , denn diese teilt weder  $(p-1)$  noch  $(q-1)$  !
- (5) Bestimme die natürliche Zahl  $1 < t < \varphi(n)$  mit:

$$s \cdot t \equiv 1 \pmod{\varphi(n)} \quad \Leftrightarrow \quad \bar{t} = \bar{s}^{-1}$$

Verwende dazu den Euklidischen Algorithmus wie in Kapitel 5.

- (6) Zur folgenden Ver- und Entschlüsselung werden nur die Zahlen  $s$ ,  $t$  und  $n$  benutzt. B veröffentlicht die Zahlen  $s$  und  $n$ .

Die Zahl  $t$  wird geheimgehalten!!

Die Zahlen  $p$ ,  $q$  und  $\varphi(n)$  werden nicht mehr gebraucht und sinnvollerweise vernichtet.

- (7) Der Sender A verwandelt den Klartext samt Satzzeichen in eine Ziffernfolge  $Z$ <sup>1</sup> und diese wiederum in gleichlange Ziffernblöcke

$$Z = Z_1, Z_2, \dots, Z_k$$

Die Länge dieser Ziffernblöcke sei  $\leq 100$ . Damit alle Ziffernblöcke gleich lang sind muss des letzte Block  $Z_k$  unter Umständen geeignet aufgefüllt werden.

<sup>1</sup> Üblich ist z.B. der ASCII-Code (**American Standard Code for Information Interchange**), eine 7 oder 8 Bit Zeichencodierung ( $2^7 = 128$  Zeichen können so kodiert werden, die deutschen Umlaute gibt es nicht, aber diverse Sonderzeichen, so gilt z.B.  $A = 1000001$ ,  $B = 1000010$  und  $C = 1000011$ ).





- (8) **Verschlüsselung:** A kennt die zur Verschlüsselung notwendigen Zahlen  $s$  und  $n$  von B (da öffentlich). Nun werden die  $Z_i$  durch  $C_i$  für  $i = 1, 2, \dots, k$  ersetzt, wobei:

$$C_i := Z_i^s \pmod n \quad \text{mit} \quad 1 < C_i < n$$

A übermittelt die Ziffernfolge  $C_1, C_2, \dots, C_k$  an B.

- (9) B kann mit Hilfe der Zahl  $t$  den Code entschlüsseln, also die Ziffernblöcke  $Z_i$  zurückgewinnen, denn:

$$C_i^t \equiv (Z_i^s)^t = Z_i^{s \cdot t} \stackrel{?}{\equiv} Z_i \pmod n$$

**Beweis von  $Z_i^{s \cdot t} \equiv Z_i \pmod n$**

Nach Voraussetzung haben  $p$  und  $q$  mindestens 100 Stellen, aber alle  $Z_i$  haben weniger als 100 Stellen. Somit gilt  $Z_i \notin \{p, q\}$ . Da  $p$  und  $q$  Primzahlen sind, gilt:

$$T_n = T_{p \cdot q} = \{1, p, q, p \cdot q\} \quad \Rightarrow \quad Z_i \notin T_n \quad \Rightarrow \quad \text{ggT}(Z_i, n) = 1$$

$\parallel$   
 $n$

Nach dem Eulerschen Satz (Abschnitt 5.4) gilt somit:

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

Andererseits gilt nach Wahl von  $s, t$  und  $n$ :

$$\begin{aligned} s \cdot t &\equiv 1 \pmod{\varphi(n)} \\ \Leftrightarrow s \cdot t &= 1 + b \cdot \varphi(n) && (\text{für ein } b \in \mathbb{N}) \\ \Rightarrow Z_i^{s \cdot t} &= Z_i^{1+b \cdot \varphi(n)} = Z_i \cdot \left( Z_i^{\varphi(n)} \right)^b \equiv Z_i \pmod n \\ &\quad \quad \quad \parallel \\ &\quad \quad \quad 1 \end{aligned}$$

□

**Fazit:** B muss einfach die Blöcke  $C_i$  mit  $t$  potenzieren um so die  $Z_i$  zurückzugewinnen.

Die *Sicherheit* des RSA-Verfahrens beruht auf dem immensen Zeitaufwand, große Zahlen in ihre Primfaktoren zu zerlegen. Denn zur Bestimmung des geheimen Decodierschlüssels  $t$  muß die Kongruenz  $s \cdot t \equiv 1 \pmod{\varphi(n)}$  gelöst werden. Weil aber  $p, q, \varphi(n) = (p-1) \cdot (q-1)$  und zudem  $t$  geheim gehalten wurde, ist die Zerlegung  $n = p \cdot q$  der bekannten Zahl  $n$  in ihre beiden Primfaktoren  $p$  und  $q$  nötig. Aber das ist auch für leistungsstarke Rechner sehr zeitaufwendig.