# *1.2. Teilbarkeit und Kongruenz*

Aus den Begriffen der *Teilbarkeit* bzw. *Teilers* ergeben sich die Begriffe *Rest* und *Restklassen*. Natürliche Zahlen, die sich nur durch sich selbst oder die 1 dividieren lassen, bilden die Menge der *Primzahlen*. Die Frage nach dem Wesen der Primzahlen beschäftigt Zahlentheoretiker seit zwei Jahrtausenden. Die *Primfaktorzerlegung* aller natürlicher Zahlen ergibt sich aus dem *Hauptsatz der Elementaren Zahlentheorie*. Solche zahlentheoretische Verfahren spielen in der modernen Kryptographie eine herausragende Rolle.

## *1.2.1. Teiler und Teilbarkeit*

### *1.2.1.1. Definition*

Seien $z, t \in \mathbb{Z}$ zwei ganze Zahlen mit $t =/= 0$. Die Zahl *t teilt die Zahl* z oder *z ist durch t teilbar*, notiert $t \mid z$ , wenn z ganzzahliges Vielfaches von t ist, d.h. wenn gilt

$$t / z \leftrightarrow \bigvee_{k \in \mathbb{Z}} (k * t = z)$$

### *Beispiel*

Die Zahl t = 3 teilt die Zahl z = 12, denn mit k = 4 gilt $4 \cdot 3 = 12$. Die ganze Zahl 12 ist also durch 3 teilbar. Gleichermaßen teilt t = 3 unter anderem die Zahlen 15, -12, 3 und auch die 0. ■

### *1.2.2.2. Definition*

Ist die Zahl $z \in \mathbb{Z}$ durch $t \in \mathbb{Z}$ teilbar und ist $t > 0$, so heißt t ein *Teiler von z*. Die Teiler 1 und $|z|$ heißen *triviale* Teiler von *z*. Die nichttrivialen Teiler von z heißen *echte Teiler* oder *Faktoren* von *z*.

## *1.2.2.3. Folgerung:*

Ist eine Zahl $z \in \mathbf{Z}$ durch t teilbar, dann ist sie auch durch -t teilbar, d.h. für alle $z \in \mathbf{Z}$ gilt:

$$t \mid z \rightarrow -t \mid z$$

***Beispiele***

- Die natürliche Zahl 15 hat die triviale Teiler t mit $\mid t \mid = 1$ oder $\mid t \mid = 15$. Das sind -15, -1, 1, 15 . Die nichttrivialen Teiler sind -5, -3, 3, 5 .
- Die natürliche Zahl 20 hat die Teiler -20, -10, -5, -4, -2, -1, 1, 2, 4, 5, 10, 20 und die echten Teiler (Faktoren) -10, -5, -4, -2, 2, 4, 5 und 10.
- Die Zahl 7 hat die beiden trivialen Teiler 1 und 7. ■

***Bemerkung***

Für die ganze Zahl 0 gelten besondere Gegebenheiten:

- Jede Zahl $z \in \mathbf{Z}$ ist durch 1 teilbar. Jedes $z \in \mathbf{Z}$, $z =/= 0$ ist durch sich selbst teilbar.
- Die Zahl 0 ist durch alle $z \in \mathbf{Z}$, $z =/= 0$ teilbar. Es gilt nicht $0 \mid 0$.
- Keine Zahl ist durch 0 teilbar, d.h. für alle $z \in \mathbf{Z}$ gilt:

  0 ist kein Teiler von $z$. ■

Wenn x ein Teiler von y und y seinerseits Teiler von z ist, dann ist x ein Teiler von z. Es gilt folgender

### *1.2.2.4. Satz*

Die Relation *teilt*, notiert | , ist *transitiv* in $\mathbb{Z}$, d.h. für alle x, y, z $\in \mathbb{Z}$ gilt

$$x \mid y \ \wedge \ y \mid z \ \rightarrow \ x \mid z.$$

***Beispiel***

(1) $5 \mid 15 \wedge 15 \mid 75 \rightarrow 5 \mid 75$

(2) $-25 \mid 25 \wedge 25 \mid 75 \rightarrow -25 \mid 75$ ■

## *1.2.3. Primzahlen*

### *1.2.3.1. Definition*

Eine Zahl $p \in \mathbb{N}$, $p > 1$ heißt *Primzahl*, wenn sie nur die trivialen Teiler 1 und p besitzt.

***Bemerkung***

Anderenfalls heißt eine Zahl $z \in \mathbb{Z}$ *zusammengesetzt*. Die 1 ist weder Primzahl noch zusammengesetzt. Die ersten Primzahlen sind 2, 3, 5, 7, 11, 13, 17, 19, ... [1] ■

### *1.2.3.2. Hauptsatz der Zahlentheorie.*

Ein grundlegender Satz der Zahlentheorie ist folgender *Hauptsatz*. Er sagt aus, daß eine natürliche Zahl eine Darstellung als Produkt von *Primfaktoren* besitzt. Dieser Satz ist allerdings ein Existenzsatz. Für das Auffinden der Primfaktoren insbesondere großer Zahlen steht bisher kein effizienter Algorithmus zur Verfügung.

---

[1] Zu beachten sind die Primzahlzwillinge (2,3), (3,5), (5,7), (11,13), (17,19). Weitere Primzahlzwillinge sind z.B. (29,31) und (87,89).

## *1.2.3.2.1. Satz (Hauptsatz der Elemtaren Zahlentheorie)*

Für jede natürliche Zahl n Zahl $n \in \mathbf{N}$, $z > 1$ existieren Primzahlen $p_j$ und natürliche Zahlen $r_j \in N_0$ ( $1 \leq j \leq k$), so daß sich n als Produkt

$$n = p_1^{r1}\, p_2^{r2} \ldots p_k^{rk}$$

$$= \prod_{j=1}^{n} p_i^{rj}$$

von Primzahlpotenzen darstellen läßt.

## *1.2.3.2.2. Beweis:*

Der Beweis von (1.2.3.2.1) ergibt sich durch Vollständige Induktion über $n \in \mathbf{N}$. Der Induktionsanfang ist $n = 1$. Für $n = 1$ ist die Behauptung erfüllt. Es gilt $1 = 2^0$. Die Induktionsannahme sei: alle $x \leq n$, $x \in \mathbf{N}$ besitzen Primfaktorzerlegungen nach (1.2.3.2.1) Der Induktionsschluß von n auf (n+1) erfolgt durch folgende Fallunterscheidung:

1. Fall: $n+1$ sei eine Primzahl.

Dann gilt $p_1 = n+1$ und $r_1 = 1$. Also gilt: $n+1 = p_1^{r1} = (n + 1)^1$

2. Fall: $n+1$ sei keine Primzahl.

Dann gibt es Faktoren x, $m \leq n$ ($x, m \in \mathbf{N}$) mit $n+1 = x * m$. Dann besitzen x und m nach (1.2.3.2.1) je eine Primfaktorzerlegung. Somit besitzt aber auch das Produkt $x * m$ eine Primfaktorzerlegung und damit auch (n+1).

***Bemerkung***

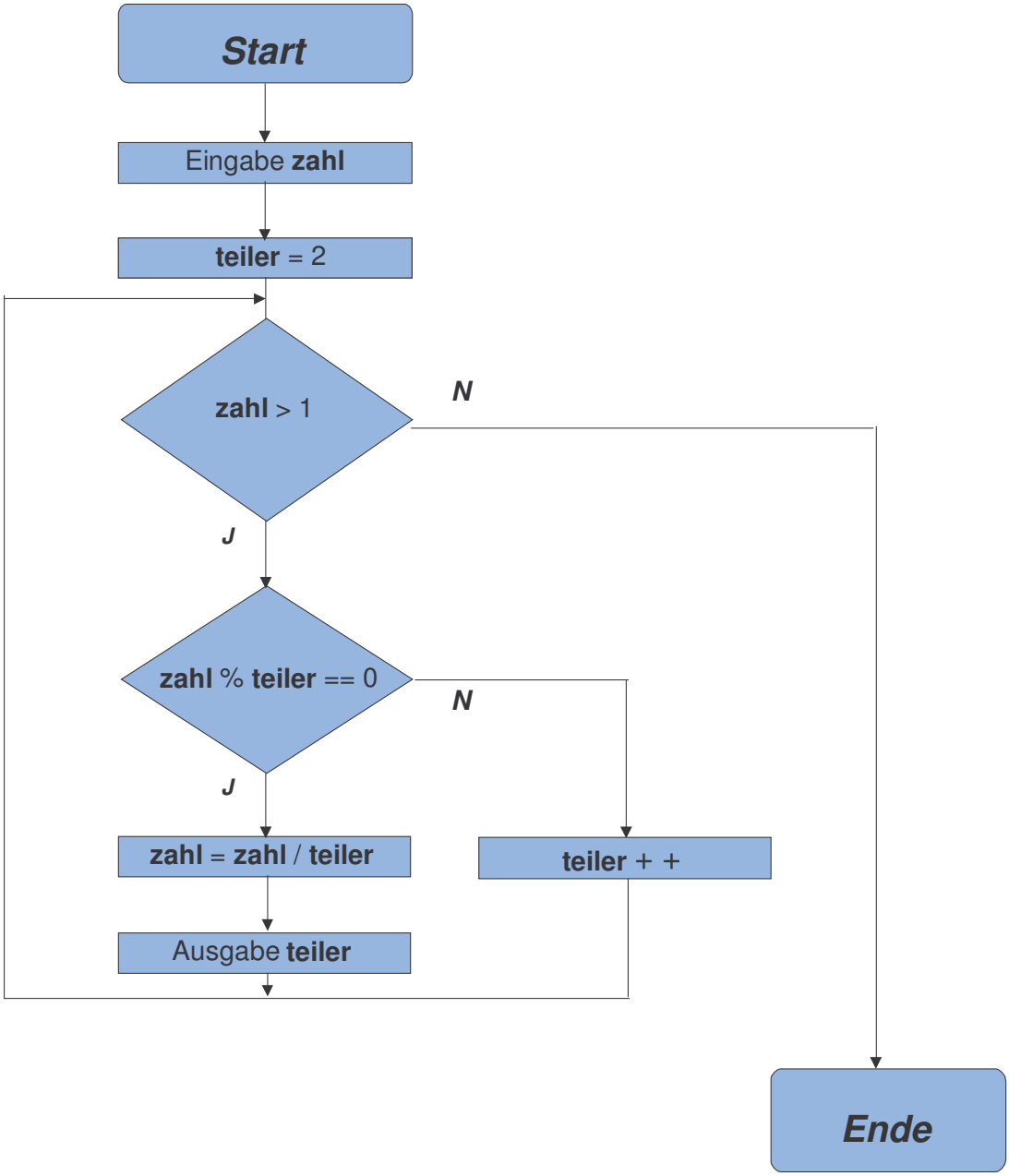
Darüber hinaus läßt sich zeigen: für $n>1$ sind die (verschiedenen) Basen $p_1,\ldots, p_k$

und die ihnen zugeordneten Exponenten $r_1, \ldots, r_k \geq 1$ der Primfaktorzerlegung bis auf die Anordnung der Faktoren eindeutig. ■

### *1.2.3.3. Ermittlung der Primfaktoren*

*(in Vorbereitung)*

Der Algorithmus zum Auffinden der Primfaktoren[2] lässt sich durch folgendes Flußdiagramm darstellen:




[2] `Laufzeitverhalten (in Vorbereitung)`

## *1.2.4. Kongruenz modulo* n

Die Division ist im Bereich der ganzen Zahlen nicht abgeschlossen. Die Division ergibt unter Umständen einen *Rest*. In vielen Fällen ist aber gerade dieser Rest bzw. die *Restklasse*, die bei der Division durch einen bestimmten Teiler entsteht, interessant. Restklassen spielen in der theoretischen Zahlentheorie aber auch in Anwendungen wie z.B. der Kryptologie, eine besondere Rolle.

### *1.2.4.1. Definition*

Sei $z \in \mathbf{Z}, n \in \mathbf{N}$. Die *modulo*-Operation *mod* ist wie folgt definiert:

$$z \bmod n = r \leftrightarrow z \equiv r \pmod{n} \wedge 0 \leq r < n,$$

### *Bemerkung*

Die Definition (1.2.4.1) bedeutet, daß z *mod* n den Repräsentanten der Restklasse liefert, zu der z gehört. Dabei ist zwischen der Operation mod n und der Relation $\equiv \pmod{n}$ zu unterscheiden. Wenn $z \bmod n = r$ ist, so gilt immer $z \equiv r \pmod{n}$, die Umkehrung gilt jedoch nicht, wie folgendes Beispiel zeigt. Es gilt zwar

$$8 \equiv 6 \pmod 2, \text{ da } 8 \bmod 2 \equiv 0 \wedge 6 \bmod 2 \equiv 0$$

(d.h. die ganzen Zahlen 6 und 8 liegen bei Division durch 2 in der gleichen Restklasse, nämlich in $[0]_{/2}$ ), aber aus

$$8 \equiv 6 \pmod 2,$$

folgt nicht

***8 mod 2 = 6.***

Tatsächlich ist $8 \bmod 2 \equiv 0$. ■

Die Division mit Rest erzeugt auf $\mathbb{Z}$ Klassen von Zahlen, die auf den gleichen Rest führen. Diesen Sachverhalt beschreibt der Begriff *Kongruenz*. Die Klassen, die die Zahlen enthalten, die bei der Division durch $a \in \mathbb{Z}$ jeweils den gleichen ganzzahligen Rest haben, werden als Restklassen bezeichnet. Dazu zunächst folgende

### *1.2.4.2 Definition*

Sei $n \in \mathbb{N}$. Eine ganze Zahl z heißt *kongruent modulo n auf* $\mathbb{Z}$ genau dann, wenn für alle $z, r \in \mathbb{Z}$ gilt:

$$z \equiv r \pmod{n} \leftrightarrow n \mid z - r$$

### *Beispiel*

- Zwei Zahlen, die bei der ganzzahligen Division durch 9 in derselben Restklasse liegen, heißen *kongruent modulo 9*. Es gilt zum Beispiel:

  $20 \equiv 2 \bmod 9$ , denn $9 \mid 20 - 2$

- Zwei Zahlen $z, r \in \mathbb{Z}$ sind folglich kongruent (modulo *n*), wenn ihre Differenz $z - r$ durch $n$ teilbar ist. Es gilt beispielsweise:

  $17 \equiv 2 \pmod 5$, denn $5 \mid 17 - 2$
  $2 \equiv 17 \pmod 5$, denn $5 \mid 2 - 17$
  $6 \equiv 0 \pmod 2$, denn $2 \mid 6 - 0$
  $-6 \equiv 8 \pmod 2$ denn $2 \mid 8 - (-6)$

  Dagegen gilt *nicht*:

  $17 \equiv -17 \pmod 5$, denn $17 - (-17) = 34$, und 34 ist nicht durch 5 teilbar. ■

### *1.2.4.3. Restklasse*

Eine *Restklasse modulo einer ganzen Zahl m* ist die Menge aller derjenigen ganzen Zahlen $z \in \mathbb{Z}$, die bei Division durch *m* denselben Rest r aufweisen. Restklassen werden wie folgt definiert:

### *1.2.4.3,1. Definition*

Es sei $m \in \mathbb{Z}$, $m \neq 0$ und $x \in \mathbb{Z}$ beliebig. Die Restklasse von *x* modulo *m*, geschrieben

$$x + m\mathbb{Z}$$

ist die Äquivalenzklasse von $x$ bezüglich der Kongruenz modulo $m$. Die kleinste nichtnegative Zahl in jeder Restklasse heißt *Repräsentant* der Restklasse. ■

### *Bemerkung*

Die Restklasse modulo $m$ ($m \in \mathbb{Z}$) besteht aus allen ganzen Zahlen $b$, die sich aus $x$ durch die Addition des k-fachen ($k \in \mathbb{Z}$) von m ergeben. Dies sagt folgender

### *1.2.4.3.2. Satz*

$$x + m\mathbb{Z} = \{ b \mid b = x + k*m ; x, k \in \mathbb{Z} \}$$
$$= \{ b \mid b \equiv x \pmod m \}$$

### *Beispiele*

- Die Relation $\equiv \pmod n$ ist eine *Äquivalenzrelation*. Die Relation $\equiv \pmod n$ teilt $\mathbb{Z}$ in $n$ Restklassen mit den Repräsentanten $0, 1, 2, \ldots, n-1$

ein. Die Menge der Repräsentanten $\{0, 1, 2, ..., n-1\}$ wird mit $\mathbb{Z}_{/n}$ bezeichnet.

- Die *Äquivalenzrelation* Relation $\equiv$ (mod 9) bewirkt eine Klasseneinteilung von $\mathbb{Z}$ in 9 Klassen äquivalenter Elemente. Eine solche Menge nennt man *Restklasse modulo 9*. Die Äquivalenzklassen der Relation $\equiv$ (mod *9*) enthalten jeweils genau diejenigen Zahlen, die bei Division durch *9* denselben Rest ergeben.

- Die Zahlen -28, -19, -10, 1, 10, 19, 28, 37… führen bei Division durch 9 auf den Rest 1. Sie gehören daher in die gleiche Äquivalenzklasse. Diese wird mit ihrem kleinsten nichtnegativen Repräsentanten, hier der 1, als

  $[1] = \{ 1, 10, 19, 28, 37... \}$

  bezeichnet. Insgesamt bewirkt die Relation $\equiv$ (mod *9*) folgende Zerlegung von $\mathbb{Z}$ in Äquivalenzklassen:[3]

  $[0] = \{0, 9, 18, 27, 36 ... \}$
  $[1] = \{1, 10, 19, 28, 37... \}$
  $[2] = \{2, 11, 20, 29, 38... \}$
  $[3] = \{3, 12, 21, 30, 39 ... \}$
  $[4] = \{4, 13, 22, 31, 40... \}$
  $[5] = \{5, 14, 23, 32, 41 ... \}$
  $[6] = \{6, 15, 24, 33, 42... \}$
  $[7] = \{7, 16, 25, 34, 43... \}$
  $[8] = \{8, 17, 26, 35, 44... \}$

[3] Dabei gilt:

$\mathbb{Z}_{/9} = \{ [0], [1], [2], [3], [4], [5] [6], [7], [8]\}$ und
$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4] \cup [5] \cup [6] \cup [7] \cup [8]$

- Es sei $n = 2$. Die Relation $\equiv \pmod 2$ teilt $\mathbb{Z}$ in zwei Restklassen ein: die geraden und die ungeraden Zahlen. Die Restklasse von 0 modulo 2 ist die Menge der geraden Zahlen. Der Repräsentant der geraden Zahlen ist die 0. Die Restklasse von 1 modulo 2 ist die Menge der ungeraden Zahlen. Der Repräsentant der ungeraden Zahlen ist die 1. Somit ist also $\mathbb{Z}_{/2} = \{0, 1\}$.
- Die Restklasse von 0 modulo *m* ist die Menge der Vielfachen von *m*. Die Restklasse von 1 modulo 3 ist die Menge der Zahlen

  $\{ 1, 4, 7, 10, 13, \ ..., -2, -5, -8, -11, ...\}$ ■

### *1.2.4.3.3. Definition*

Eine Restklasse modulo *m* heißt *prime Restklasse*, wenn ihre Elemente teilerfremd zu *m* sind.[4]

### *1.2.4.3.4. Rechnen mit Restklassen: die Neunerprobe*

Der Neunerrest einer Zahl wird ermittelt, indem man ihre Ziffern addiert. Ist das Ergebnis größer als 9, so addiert man die Ziffern des Ergebnisses. Dieser Vorgang wird solange wiederholt, bis eine einstellige Zahl übrigbleibt. Zum Beispiel ist der Neunerrest von 2377:

$2 + 3 + 7 + 7 = 19$
$1 + 9 = 10$
$1 + 0 = 1$

[4] Die Menge aller Restklassen modulo *m* schreibt man $\mathbb{Z}/m\mathbb{Z}$. $\mathbb{Z}/m\mathbb{Z}$ hat die Struktur eines Rings (Restklassenring $m\mathbb{Z}$). Die Menge der primen Restklassen ist die *Gruppe der Einheiten* $\mathbb{Z}/m\mathbb{Z}$ im Restklassenring $m\mathbb{Z}$; sie ist die prime Restklassengruppe.

Anhand des Neunerrests läßt sich entscheiden, ob die Ausgangszahl ohne Rest durch 9 teilbar ist. Da der Neunerrest von 2377 nicht gleich 0 ist, ist 9 kein Teiler von 2377. Auf welchem zahlentheoretischen Sachverhalt beruht die Neunerprobe?

Addiert man etwa eine Zahl aus [2] und eine Zahl aus [3], ist das Ergebnis ein Element von [5].[5] Das gilt analog für alle anderen Zahlen. Daher läßt sich mit Restklassen rechnen. Nur muß man die Ergebnisse, die größer oder gleich 9 sind, durch ihren Rest bei der Division durch 9 ersetzen. Dies ergibt sich aus folgender Überlegung: Nach (1.2.4.3.1) läßt sich eine Zahl x aus der Restklasse [2] in folgender Form schreiben:

$$x = 2 + 9*m \ (m \in \mathbf{Z}).$$

Genauso schreibt man für eine Zahl y aus [3]:

$$y = 3 + 9*n \ (m \in \mathbf{Z}).$$

Die Summe ist dann

$$\begin{aligned} x + y &= (2 + 9*m) + (3 + 9*n) \\ &= 5 + 9 * (m + n) \end{aligned}$$

Die Summe 5 + das m*n-fache von 9 sind Element von [5]. Dies gilt für beliebige Elemente von [2] und [3], daher können wir schreiben

$$[2] + [3] = [2+3]$$

Bei der Neunerprobe wird also modulo 9 gerechnet. Es ist noch zuzeigen, daß die Ziffernsumme einer ganzen Zahl gleich ihrem Neunerrest ist. Es gilt

$$\begin{aligned} 10 &\equiv 1 \bmod 9 \\ 100 &\equiv 1 \bmod 9 \end{aligned}$$

[5] Analog gilt: Multipliziert man eine Zahl aus [2] mit einer Zahl aus [3], ist das Ergebnis ein Element von [6].

$1000 \equiv 1 \bmod 9$ usw.,

also gilt z.B.:

$$\begin{aligned} 2377 &= 2*1000 + 3*100 + 7*10 + 7*1 \\ &\equiv 2 + 3 + 7 + 7 \bmod 9 \\ &\equiv 1 \bmod 9 \end{aligned}$$

Dann gilt $2377 \in [1]_{/9}$ . Also ist 2377 nicht ohne Rest durch 9 teilbar, wohl aber gilt:

$$\begin{aligned} 2376 &= 2*1000 + 3*100 + 7*10 + 6*1 \\ &\equiv 2 + 3 + 7 + 6 \bmod 9 \\ &\equiv 0 \bmod 9 \end{aligned}$$

Also ist 2376 ohne Rest durch 9 teilbar. ■

## *1.2.4.4. Größter gemeinsamer Teiler*

### *1.2.4.4,1. Definition*

Seien $x, y \in \mathbf{Z}$ und $x, y =/= 0$. Eine Zahl $t \in \mathbf{N}$ heißt ein *gemeinsamer Teiler von* x *und* y, wenn

$t \mid x$ und $t \mid y$

### *Bemerkung*

Die 1 ist stets gemeinsamer Teiler zweier beliebiger ganzer Zahlen.

### *1.2.4.4.2. Definition*

Seien $x, y \in \mathbf{Z}$. Eine Zahl $g = ggT(x, y) \in \mathbf{N}$ heißt *größter gemeinsamer Teiler von* x *und* y, wenn für alle $t \in \mathbf{N}$ gilt

$$t \mid x \ \wedge \ t \mid y \ \leftrightarrow \ t \mid g,$$

***Bemerkung***

- Alle gemeinsamen Teiler von x und y sind auch Teiler von g, und alle Teiler von g, also insbesondere g selbst, sind auch gemeinsame Teiler von x und y.
- Für alle $x \in \mathbf{Z}$ mit $x \neq 0$ gilt per definitionem:

  $$ggT(0, x) := |x|,$$

  d.h. der größte gemeinsame Teiler von 0 und x ist der Betrag von x.
- Der größte gemeinsame Teiler von 0 und 0 existiert nicht, es gilt per definitionem:

  $$ggT(0, 0) := 0$$

■

***1.2.4.4.3. Satz***

Seien $x, y \in \mathbf{N}$ zwei natürliche Zahlen. Dann heißt die ganze Zahl

$$ggT(x, y) = \max \{ k \in \mathbf{Z} : k \mid x \wedge k \mid y \}$$

der *größte gemeinsame Teiler von x und y*. Weiterhin heißt die ganze Zahl

$$kgV(x, y) = \min \{ k \in \mathbf{Z} : x \mid k \wedge y \mid k \}$$

das *kleinste gemeinsame Vielfache von x und y*.

***1.2.4.4.4. Berechnung von ggT und kgV***

Seien $x, y \in \mathbf{N}$ zwei natürliche Zahlen. Weiterhin sei

$$x = p_1^{r1} p_2^{r2} .... p_k^{rk}$$

$$y = p_1^{s1} p_2^{s2} .... p_k^{sk}$$

mit den Primfaktoren $p_1, p_2 ... p_k$ und den Exponenten $r_1, r_2 ... r_k, s_1, s_2 ... s_k \geqq 0$ gilt. Um den ggT $(x, y)$ zu ermitteln, bestimmen wir für jeden Primfaktor $p_j$ den niedrigeren der beiden Exponenten $r_j$ bzw. $s_j$ , d.h. $\min (r_j, s_j)$ . Es gilt dann

$$ggT (x, y) = p_1^{min(r1,s1)} p_2^{min(r2,s2)} .... p_k^{min(rk,sk)}$$

Um das $kgV (x, y)$ zu ermitteln, bestimmen wir für jeden Primfaktor $p_j$ den höheren der beiden Exponenten $r_j$ bzw. $s_j$ , d.h. $\max (r_j, s_j)$ . Es gilt dann

$$kgV (x, y) = p_1^{max(r1,s1)} p_2^{max(r2,s2)} .... p_k^{max(rk,sk)}$$

■

***Beispiel***

Seien $x = 99$ und $y = 84$. Für die Primfaktorzerlegungen gilt

$$99 = 2^0 * 3^2 * 5^0 * 7^0 * 11^1$$
$$84 = 2^2 * 3^1 * 5^0 * 7^1 * 11^0$$

Diese bestehen aus den Primfaktoren

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$$

und den Exponenten

$$r_1 = 0, r_2 = 2, r_3 = 0, r_4 = 0, r_5 = 1 \text{ bzw.}$$
$$s_1 = 2, s_2 = 1, s_3 = 0, s_4 = 1, s_5 = 0 .$$

Dann gilt

$$\min (r_1, s_1) = 0 , \min (r_2, s_2) = 1, \min (r_3, s_3) = 0 , \min (r_4, s_4) = 0 ,$$
$$\min (r_5, s_5) = 0$$

und

$$\max(r_1, s_1) = 2\ ,\ \max(r_2, s_2) = 2,\ \max(r_3, s_3) = 0\ ,\ \max(r_4, s_4) = 1\ ,$$
$$\max(r_5, s_5) = 1\ .$$

Somit ergeben sich größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches zu:

$$ggT(99, 84) = 2^0 * 3^1 * 5^0 * 7^0 * 11^0 = 3$$
$$kgV(99, 84) = 2^2 * 3^2 * 5^0 * 7^1 * 11^1 = 2772$$

■

### *1.2.4.4.5 Definition*

Zwei Zahlen $x, y \in \mathbb{Z}$ heißen *teilerfremd*, wenn gilt: $ggT(a, b) = 1$.

## *1.2.5. Euklidischer Algorithmus*

Der *euklidische Algorithmus* berechnet den größten gemeinsamen Teiler zweier natürlicher Zahlen. Er trägt den Namen des griechischen Mathematikers *EUKLID*.[6] Der größte gemeinsame Teiler zweier natürlicher Zahlen läßt sich leicht errechnen, wenn Primfaktorzerlegungen beider Zahlen bekannt sind. Sind diese Primfaktorzerlegungen der beiden Zahlen allerdings nicht bekannt, so ist der euklidische Algorithmus

[6] Das Verfahren wurde von *EUKLID* um ca. 300 v. Chr. in seinen *Elementen* (Buch VII, Proposition 1 und 2) beschrieben. Der von ihm als (übersetzt) *Wechselwegnahme* bezeichnete Algorithmus bezog sich auf ein geometrisches Problem, nämlich das gemeinsame „Maß" zweier Strecken zu finden. Der Algorithmus war bereits *EUDOXOS* von *KNIDOS* um ca. 375 v. Chr. und auch *ARISTOTELES* um ca. 330 v. Chr. bekannt. *HIPPASOS* von Metapont benutzte schon vor Euklid diese sogenannte *Wechselwegnahme*, um zu zeigen, daß bei bestimmten regelmäßigen n-Ecken keinen gemeinsamen Teiler gibt, z.B. im Quadrat und im regelmäßigen Fünfeck beim Verhältnis von Seiten und Diagonalen.

das effizienteste Verfahren zur Berechnung des größten gemeinsamen Teilers.[7] Der euklidische Algorithmus ist dabei nicht nur auf die natürlichen Zahlen anwendbar, sondern läßt sich für je zwei Elementen eines euklidischen Ring berechnet werden. [8]

### *1.2.5.1. Der klassische Euklidische Algorithmus*

Der *klassische Euklidische Algorithmus* läßt sich wie folgt formulieren: Der größte gemeinsame Teiler von x und y (x > y) ergibt sich dadurch, daß x sukzessive um y vermindert wird. Wird die Differenz kleiner als die kleinere Zahl y, so werden x und y getauscht und das Verfahren fortgesetzt. Ist das Ergebnis dieser Iteration gleich Null, ist der ggT von Zahlen x und y gefunden.

Ist die Differenz von *a* und *b* sehr groß, sind unter Umständen viele Subtraktionsschritte notwendig.

### *1.2.5.2. Der erweiterte Euklidische Algorithmus*

Im modernen Euklidischen Algorithmus ersetzt man die im klassischen Algorithmus nötige wiederholte Subtraktion eines bestimmten Wertes jeweils durch eine Division mit Rest. Der Euklidische Algorithmus bestimmt den größten gemeinsamen Teiler zweier natürlicher Zahlen x und y nunmehr durch eine Kette von Divisionen mit Rest.[9]

---

[7] Mit dem euklidischen Algorithmus kann man den ggT (x, y) mit im Vergleich zur Berechnung der Primfaktorzerlegung zweier Zahlen *x* und *y* geringem Aufwand berechnen. Der nachteiligste Fall für die Wahl von x und y sind zwei aufeinander folgende *Fibonacci*-Zahlen. Dann ergibt sich als Rest die nächstkleinere Fibonacci-Zahl. Die Anzahl der benötigten Divisionen beträgt dann höchstens O(*log(ab)*). *log(ab)* = log (a) + log (b) wächst selbst proportional zur Anzahl der Ziffern von x und y. Dies gilt auch für die für die Division von x und y erforderliche Zeit. Daher ergibt sich eine tatsächliche Laufzeit von $O(log(ab)^2)$.

[8] Dazu zählen beispielsweise Polynome über einem Körper.

[9] y < x ,y = r1

$$
\begin{aligned}
x &= q_1 \cdot r_1 + r_2 && \text{mit } 0 < r_2 < y \\
r_1 &= q_2 \cdot r_2 + r_3 && \text{mit } 0 < r_3 < r_2 \\
r_2 &= q_3 \cdot r_3 + r_4 && \text{mit } 0 < r_4 < r_3 \\
r_3 &= q_4 \cdot r_4 + r_5 && \text{mit } 0 < r_5 < r_4 \\
&\ldots \\
r_{n-3} &= q_{n-2} \cdot r_{n-2} + r_{n-1} && \text{mit } 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n && \text{mit } 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n \cdot r_n + 0
\end{aligned}
$$

Der Algorithmus läßt sich wie folgt definieren:

(1) Wähle x, y (y < x).

(2) Führe die Division x durch y mit Rest durch.

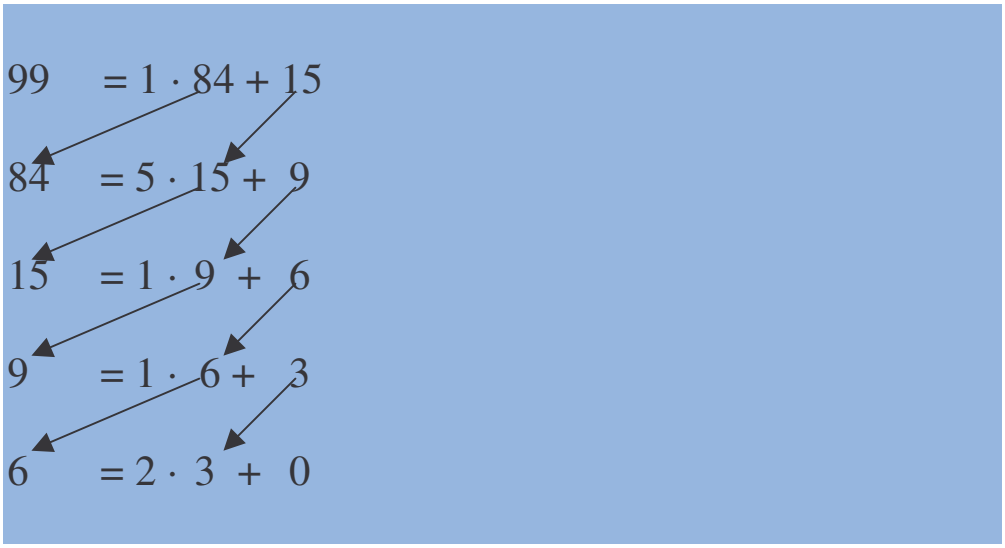
(3) Ist der Rest von x / y gleich Null, so gibt die zweite Zahl den ggT an.
→*Abbruch*

(4) Setze die zweite Zahl an die Stelle der ersten und den Rest an die Stelle der zweiten.
→(2).[10]

### *Beispiel*

Zu berechnen ist der größte gemeinsame Teiler von x = 99 und y = 84. Da y < x, gilt $r_1$ = 84. Der ggT (99, 84) wird dann in folgenden Schritten ermittelt:

[10] Kriterien für die Tauglichkeit des erweiterten Euklidischen Algorithmus sind:(*in Vorbereitung*)




Da nun $r_6 = 0$, bricht das Verfahren ab und es gilt ggT (99, 84) = 3.

### *1.2.5.3. Anwendungen des erweiterten Euklidischen Algorithmus*

Der erweiterte Euklidische Algorithmus berechnet neben dem größten gemeinsamen Teiler zweier natürlicher Zahlen x und y zusätzlich noch zwei ganze Zahlen *u* und *v*, die die folgende Gleichung erfüllen[11]

$$u * x + y * v = 1$$

Der Euklidischen Algorithmus gewinnt damit eine zentrale Bedeutung für die Berechnung inverser Elemente in ganzzahligen Restklassenringen. Die Berechnung inverser Elemente ermöglicht die Lösung der sogenannten *diophantischen* Gleichungen bzw. der Lösung ganzzahliger linearer Gleichungssysteme. Sie ist auch Grundlage für den *chinesischen Restsatz*. Der erweitere Euklidische Algorithmus führt auch zu einem konstruktiven Beweis des Lemmas von *BÉZOUT* und ist von Bedeutung für die Kryptographie.

[11] Ein besonderer Vorteil dieser Variante ist ihre Übertragbarkeit auf beliebige *euklidische Ringe* wie zum Beispiel *Polynomringe*, in denen der klassische Algorithmus versagt.