

Zahlentheorie ist die Mathematik der ganzen Zahlen.

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

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

### Diophantische Gleichungen

Gegeben:  $a, b, c \in \mathbb{N}$ , gesucht  $x, y \in \mathbb{Z}$  mit:  $ax + by = c$

Wir schreiben Lösungen als Zahlenpaar  $(x|y)$ .

#### Beispiele:

$$x + 3y = 10 \quad (x|y) = (7|1), (4|2), (1|3)$$

$$3x + 7y = 1 \quad (x|y) = (-2|1), (5|-2)$$

$$5x + 5y = 1 \quad \text{keine Lösung, da linke Seite durch 5 teilbar, rechte nicht.}$$

### Teiler und Primzahlen

#### Definition:

1) Seien  $x \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ .  $k$  heißt Teiler von  $x$ , geschrieben  $k|x$ , falls es ein  $q \in \mathbb{Z}$  gibt, so dass gilt:  $x = q \cdot k$ .

2) Seien  $a, b \in \mathbb{N}$ . Dann ist der größte gemeinsame Teiler von  $a$  und  $b$  definiert durch:

$$\text{ggT}(a, b) = \max \{k \in \mathbb{N} \mid k|a \wedge k|b\}$$

#### Beispiele:

$$3|12, \text{ denn } 12 = 3 \cdot 4$$

$$2|-8, \text{ denn } -8 = 2 \cdot (-4)$$

$$a = 70, b = 98$$

$$\text{Teiler von } a = \{1, 2, 5, 7, 10, 14, 35, 70\}$$

$$\text{Teiler von } b = \{1, 2, 7, 14, 49, 98\}$$

$$\text{gemeinsame Teiler von } a \text{ und } b = \{1, 2, 7, 14\}$$

$$\text{ggT}(a, b) = 14$$

#### Definition:

Eine natürliche Zahl  $p > 1$  heißt Primzahl oder prim, wenn sie genau zwei Teiler hat: die 1 und sich selbst.

#### Beispiele:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

### Hauptsatz der elementaren Zahlentheorie

Jede natürliche Zahl  $n > 1$  lässt sich, bis auf die Reihenfolge der Faktoren, eindeutig als Produkt von Primzahlen darstellen.

Beispiele:

$$\left. \begin{array}{l} 70 = 2 \cdot 5 \cdot 7 \\ 98 = 2 \cdot 7 \cdot 7 \end{array} \right\} \quad \text{ggT}(70, 98) = 2 \cdot 7 = 14$$

$$\left. \begin{array}{l} 360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \\ 756 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 \end{array} \right\} \quad \text{ggT}(360, 756) = 2 \cdot 2 \cdot 3 \cdot 3 = 36$$

Der  $\text{ggT}(a, b)$  besteht aus allen gemeinsamen Primfaktoren von  $a$  und  $b$ .

Also: Jeder gemeinsame Teiler von  $a$  und  $b$  ist auch Teiler von  $\text{ggT}(a, b)$ .

Definition: Ein Ausdruck der Form  $ax + by$  mit  $a, b \in \mathbb{N}$  und  $x, y \in \mathbb{Z}$  nennen wir Vielfachsumme von  $a$  und  $b$ .

Satz

Ist  $k$  ein gemeinsamer Teiler von  $a$  und  $b$ , dann teilt  $k$  auch jede Vielfachsumme von  $a$  und  $b$ , also:

$$k|a \wedge k|b \Rightarrow k|(ax + by) \quad \text{für } a, b, k \in \mathbb{N}, x, y \in \mathbb{Z}$$

Beweis:

$$\left. \begin{array}{l} k|a \Rightarrow \exists k_1 \in \mathbb{Z}: a = q_1 \cdot k \\ k|b \Rightarrow \exists k_2 \in \mathbb{Z}: b = q_2 \cdot k \end{array} \right\} \Rightarrow ax + by = q_1 \cdot kx + q_2 \cdot ky = k(\underbrace{q_1 x + q_2 y}_{\in \mathbb{Z}}) \Rightarrow k | (ax + by) \quad \text{q.e.d.}$$

Satz

Besitzt die Gleichung  $ax + by = c$  eine Lösung  $(x, y)$ , so folgt:  $\text{ggT}(a, b) | c$

Beweis:

Gibt  $ax + by = c$ , dann ist  $c$  eine Vielfachsumme von  $a$  und  $b$ . Nach dem letzten Satz folgt also:  $\text{ggT}(a, b) | c$  q.e.d.

Satz (Teilen mit Rest)

Seien  $a, b \in \mathbb{N}$ . Dann gibt es eindeutig bestimmte Zahlen  $q, r \in \mathbb{N}_0$ , so dass gilt:  
 $a = q \cdot b + r$  mit  $0 \leq r < b$ .

Beispiele:

$$a = 13, b = 4 : \quad \frac{a}{b} = \underline{q} \cdot b + r$$

$$a = 223, b = 25 : \quad 223 = 8 \cdot 25 + 23$$

Satz

Seien  $a, b \in \mathbb{N}$  und  $a = q \cdot b + r$  (Teilen mit Rest).

Dann gilt:  $\text{ggT}(a, b) = \text{ggT}(b, r)$

Beweis:

Wir zeigen zunächst:  $\text{ggT}(a,b) \leq \text{ggT}(b,r)$  (I)

dann:  $\text{ggT}(b,r) \leq \text{ggT}(a,b)$

Aus (I) und (II) folgt dann die Behauptung

(I):

$$\left. \begin{array}{l} \text{ggT}(a,b) | a \\ \text{ggT}(a,b) | b \\ \text{ggT}(a,b) | r \end{array} \right\} \xrightarrow{\text{Satz über Vielfachsumme}} \text{ggT}(a,b) | a - q \cdot b = r$$

$$\left. \begin{array}{l} \text{ggT}(a,b) | r \end{array} \right\} \xrightarrow{\text{Definition von ggT}} \text{ggT}(a,b) \leq \text{ggT}(b,r)$$

(II):

$$\left. \begin{array}{l} \text{ggT}(b,r) | b \\ \text{ggT}(b,r) | r \\ \text{ggT}(b,r) | a \end{array} \right\} \Rightarrow \text{ggT}(b,r) | q \cdot b + r = a$$

$$\text{ggT}(b,r) | a \Rightarrow \text{ggT}(b,r) \leq \text{ggT}(a,b) \quad \text{q.e.d.}$$

Der Euklidische Algorithmus zur Bestimmung des ggT

$$a = 126, b = 98$$

$$\text{ggT}(126, 98) = 14$$

$$\begin{array}{r} 126 & 98 \\ 98 & 28 \\ 28 & 14 \\ 14 & 0 \end{array} \xrightarrow{\text{ggT}} \begin{array}{l} = \text{Rest von } 126 : 98 \\ = \text{Rest von } 98 : 28 \\ = \text{Rest von } 28 : 14 \\ \hline \text{ggT} \quad \text{fertig} \end{array}$$

$$a = 28, b = 52$$

$$\text{ggT}(28, 52) = 4$$

$$\begin{array}{r} 28 & 52 \\ 52 & 28 \\ 28 & 24 \\ 24 & 4 \\ 4 & 0 \end{array}$$

Satz

Zu beliebig gewählten natürlichen Zahlen  $a, b$  gibt es ganze Zahlen  $x, y$ , so dass gilt:  
 $ax + by = \text{ggT}(a,b)$

Beweis:

Beschreibung eines Verfahrens, wie  $x$  und  $y$  gefunden werden (an einem Beispiel).

Erweiterter Euklidischer Algorithmus

$$a = 110, b = 32$$

$$\begin{array}{l} 110 = 3 \cdot 32 + 14 \\ 32 = 2 \cdot 14 + 4 \\ 14 = 3 \cdot 4 + 2 \\ 4 = 2 \cdot 2 + 0 \end{array}$$

↑      ↑      ↑      ↑

$$\begin{array}{l} 2 = -32 \cdot 3 + 7 \cdot (110 - 3 \cdot 32) = 7 \cdot 110 - 24 \cdot 32 \\ 2 = 14 - 3 \cdot (32 - 2 \cdot 14) = -3 \cdot 32 + 7 \cdot 14 \\ 2 = 14 - 3 \cdot 4 \\ 2 = 2 \cdot 2 + 0 \end{array}$$

GGT fertig

Ergebnis:  $110 \cdot 7 + 32 \cdot (-24) = 2$   
 $a \cdot x + b \cdot y = \text{GGT}(a, b)$

Tabellenschreibweise:

$$\begin{array}{ccccccc} a & b & q & r & x & y \\ 110 & 32 & 3 & 14 & 7 & -24 & = (-3 - (7 \cdot 3)) \\ 32 & 14 & 2 & 4 & -3 & 7 & = (1 - (-3 \cdot 2)) \\ 14 & 4 & 3 & 2 & 1 & -3 & = (0 - (1 \cdot 3)) \\ 4 & 2 & 2 & 0 & 0 & 1 & \end{array}$$

GGT fertig Start für ↑

Weiteres Beispiel:

$$a = 99, b = 78$$

$$\begin{array}{ccccccc} a & b & q & r & x & y \\ 99 & 78 & 1 & 21 & -11 & 14 \\ 78 & 21 & 3 & 15 & 3 & -11 \\ 21 & 15 & 1 & 6 & -2 & 3 \\ 15 & 6 & 2 & 3 & 1 & -2 \\ 6 & 3 & 2 & 0 & 0 & 1 \end{array}$$

Ergebnis:  $99 \cdot (-11) + 78 \cdot 14 = 3$

Satz

Seien  $a, b, c \in \mathbb{N}, x, y \in \mathbb{Z}$ . Dann gilt:

$$ax + by = c \text{ hat Lösung} \iff \text{ggT}(a, b) | c$$

Beweis:

$\Rightarrow$ : früher Satz

$\Leftarrow$ : Der Erweiterte Euklidische Algorithmus liefert  $x_0, y_0 \in \mathbb{Z}$  mit  $ax_0 + by_0 = \text{ggT}(a, b)$ .

$$\text{ggT}(a, b) | c \Rightarrow \exists k \in \mathbb{Z}: \text{ggT}(a, b) \cdot k = c \Rightarrow ax_0 \cdot k + by_0 \cdot k = \text{ggT}(a, b) \cdot k = c$$

$\Rightarrow (kx_0, ky_0)$  ist Lösung. q.e.d.

Satz

(i) Ist  $(x_0, y_0)$  Lösung von  $ax + by = c$ , dann sind alle Zahlenpaare  $(x, y) = (x_0 + kb, y_0 - ka)$  mit  $k \in \mathbb{Z}$  Lösungen.

(ii) Gilt  $\text{ggT}(a, b) = 1$ , dann sind dadurch alle Lösungen gegeben.

Beweis:

$$(i): ax + by = a(x_0 + kb) + b(y_0 - ka) = ax_0 + akb + by_0 - bka = ax_0 + by_0 = c.$$

(ii): Sei  $(x, y)$  irgendeine Lösung und  $\text{ggT}(a, b) = 1$ .

$$0 = c - c = (ax + by) - (ax_0 + by_0) = a(x - x_0) + b(y - y_0)$$

$$\Rightarrow a(x - x_0) = -b(y - y_0). \quad (1)$$

Da  $\text{ggT}(a, b) = 1$ , sind alle Primfaktoren von  $a$  in  $(y - y_0)$  enthalten.

$$\Rightarrow a \mid (y - y_0) \Rightarrow \exists k \in \mathbb{Z}: a \cdot k = y - y_0 \Rightarrow y = y_0 + ak \quad (2) \quad \left\{ \begin{array}{l} \text{das ist die gewünschte} \\ \text{Darstellung für } y \end{array} \right.$$

$$(2) \text{ einsetzen in (1): } a(x - x_0) = -b(y_0 + ak - y_0) = -bak \quad | :a$$

$$x - x_0 = -bk$$

$$x = x_0 - bk \quad \left\{ \begin{array}{l} \text{Das ist gewünschte} \\ \text{Darstellung für } x \end{array} \right.$$

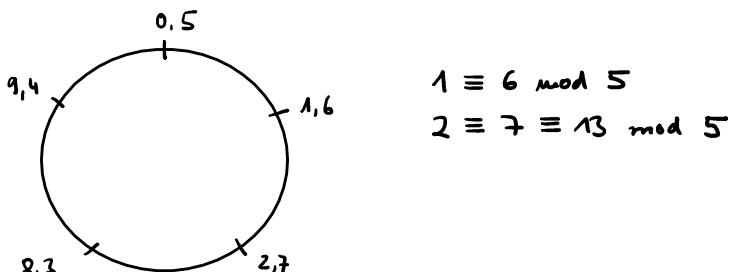
q.e.d.

Kongruenz

Definition:

Seien  $a, b \in \mathbb{Z}$ ,  $m \in \mathbb{N}$ . Dann heißt  $a$  kongruent zu  $b$  modulo  $m$ , geschrieben  $a \equiv b \pmod{m}$ , falls  $a - b$  durch  $m$  teilbar ist.

Beispiel:  $m = 5$

Satz

Folgende Aussagen sind äquivalent:

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

$$(2) \exists k \in \mathbb{Z}: a = b + k \cdot m$$

(3) Beim Teilen durch  $m$  lassen  $a$  und  $b$  denselben Rest.

Beweis:

$$(1) \Rightarrow (2): a \equiv b \pmod{m} \Rightarrow m \mid (a - b) \Rightarrow \exists k \in \mathbb{Z}: m \cdot k = a - b$$

$$a = b + m \cdot k$$

(2)  $\Rightarrow$  (3): Sei  $r$  der Rest beim Teilen von  $a$  durch  $m$ .

$$\Rightarrow \exists q \in \mathbb{Z}: a = q \cdot m + r \quad \left\{ \begin{array}{l} \text{mit } 0 \leq r < m. \\ a = b + m \cdot k \end{array} \right\} \Rightarrow b = q \cdot m - k \cdot m + r = (q - k) \cdot m + r$$

Wegen der Eindeutigkeit des Teiles mit Rest folgt: Teilen von  $b$  durch  $m$  ergibt Rest  $r$

$$(3) \Rightarrow (1): a = km + r \quad \left\{ \begin{array}{l} (a - b) = (\underbrace{k - k'}_{\in \mathbb{Z}})m \Rightarrow m \mid (a - b) \Rightarrow a \equiv b \pmod{m} \\ b = k'm + r \end{array} \right.$$

q.e.d.

Doppelte Verwendung von 'mod'

'mod' wird auch als modulo-Operator verwendet.

$r = a \bmod b$  bedeutet:  $r$  ist der Rest bei der Division von  $a$  durch  $b$ .

$3 \equiv 7 \bmod 2$  -  $3$  kongruent  $7$  mod  $2$  ist wahr

$3 = 7 \bmod 2$  -  $3$  ist  $7$  modulo  $2$  ist falsch

Es gilt:  $a \bmod m = b \bmod m \Leftrightarrow a \equiv b \bmod m$

Rechenregeln für KongruenzenSatz

Die Relation "kongruent modulo  $m$ " ist eine Äquivalenzrelation auf  $\mathbb{Z}$ .

(1)  $a \equiv a \bmod m$  (Reflexivität)

(2)  $a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$  (Symmetrie)

(3)  $a \equiv b \bmod m$  und  $b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$  (Transitivität)

Satz

Wenn  $a \equiv b \pmod{m}$  und  $c \equiv d \pmod{m}$ , dann gilt:

$$(4) -a \equiv -b \pmod{m}$$

$$(5) a+c \equiv b+d \pmod{m}$$

$$(6) ac \equiv bd \pmod{m}$$

$$(7) a^2 \equiv b^2 \pmod{m}, a^3 \equiv b^3 \pmod{m}, \dots$$

Beweis (nur (6)):

$$\begin{aligned} a \equiv b \pmod{m} &\Rightarrow \exists k \in \mathbb{Z}: a = b + km \\ c \equiv d \pmod{m} &\Rightarrow \exists k' \in \mathbb{Z}: c = d + k'm \end{aligned} \quad \left. \begin{aligned} a \cdot c &= (b+km)(d+k'm) = bd + bk'm + kmd + kk'm^2 \\ &= bd + \underbrace{(bk' + kd + kk'm)}_{\in \mathbb{Z}} \cdot m \Rightarrow ac \equiv bd \pmod{m} \end{aligned} \right. \quad \text{q.e.d.}$$

Beispiele:

$$m=7: 73+155 \equiv 3+1 \equiv 4 \pmod{7}$$

$$73 \cdot 155 \equiv 3 \cdot 1 \equiv 3 \pmod{7}$$

$$73^{155} \equiv 3^{155} \equiv 5 \pmod{7}$$

NR:

$$3^1 \equiv 3 \pmod{7}$$

$$3^2 \equiv 2$$

$$3^4 \equiv 4 \equiv 3^{16} \equiv 3^{64}$$

$$3^3 \equiv 2 \equiv 3^{32} \equiv 3^{128}$$

$$3^{155} \equiv 3^{128+16+8+2+1} = \underbrace{2 \cdot 4 \cdot 2 \cdot 2 \cdot 3}_{32} \equiv -3 \cdot 3 \equiv -9 \equiv 5$$

Beispiel (Wochentag bestimmen)

Der 1.11.2021 ist ein Montag. Welcher Wochentag ist der 24.12.2025?

$$29 + 24 + 365 + 365 + 366 + 365 \equiv 1+3+1+1+2+1 \equiv 9 \equiv 2 \pmod{7}$$

↑ Vom 1.11. ausgabend ↑ Schaltjahr 2024  
Sind es noch 29 wahre Tage  
bis Ende November

⇒ 24.12.2025 ist ein Mittwoch

Satz (Teilbarkeitsregeln)

Sei  $n \in \mathbb{N}$ . Dann gilt:

$n|2 \Leftrightarrow$  die letzte Ziffer ist gerade

$n|3 \Leftrightarrow$  die Quersumme ist durch 3 teilbar

$n|4 \Leftrightarrow$  die Zahl aus den letzten beiden Ziffern ist durch 4 teilbar

$n|5 \Leftrightarrow$  die letzte Ziffer ist 5 oder 0

$n|6 \Leftrightarrow n|2$  und  $n|3$

$n|7 \Leftrightarrow$  die Zahl, die entsteht, wenn man das Doppelte der letzten Ziffer von der ursprünglichen Zahl abzieht, ist durch 7 teilbar.

$n|8 \Leftrightarrow$  die Zahl aus den letzten drei Ziffern ist durch 8 teilbar

$n|9 \Leftrightarrow$  die Quersumme ist durch 9 teilbar

$n|10 \Leftrightarrow$  die letzte Ziffer ist eine 0

$n|11 \Leftrightarrow$  die alternierende Quersumme ist durch 11 teilbar.

$n|12 \Leftrightarrow n|3$  und  $n|4$

Beweis (nicht alle):

$n$  bestehe aus den Ziffern  $a_n a_{n-1} \dots a_1 a_0$ . Dann ist  $n = a_0 + a_1 \cdot 10^1 + \dots + a_n \cdot 10^n$

$$n \mid 3: n \equiv \underbrace{a_0 + a_2 + \dots + a_n}_{\text{Quersumme von } n} \pmod{3}$$

$$n \mid 9: n \equiv a_0 + a_1 + \dots + a_n \pmod{9}$$

$$n \mid 11: n \equiv a_0 + \underbrace{10 a_1}_{-} + \underbrace{10 \cdot 10 a_2}_{-} + \underbrace{10 \cdot 10 \cdot 10 a_3}_{-} + \dots$$

$$\equiv a_0 - a_1 + a_2 - a_3 + \dots \quad (= \text{alternierende Quersumme}) \pmod{11}$$

$n \mid 7$ : Es sei  $m$  die Zahl ohne die letzte Ziffer, also  $n = 10 \cdot m + a_0$ .

$$\Rightarrow 2n = 20 \cdot m + 2a_0 = 21m - m + 2a_0 \equiv -m + 2a_0 \pmod{7}$$

Also:  $7 \mid n \Leftrightarrow 7 \mid 2n \Leftrightarrow 7 \mid (-m + 2a_0) \Leftrightarrow 7 \mid (m - 2a_0)$  q.e.d.

Beispiele:

$$n = 65585520$$

$$n \mid 11: \text{Alternierende Quersumme} = 0 - 2 + 5 - 5 + 8 - 5 + 5 - 6 = 0 \Rightarrow n \mid 11$$

$$n \mid 7: 65585520 \equiv$$

$$6558552 \equiv$$

$$655851 \equiv$$

$$65583 \equiv$$

$$6552 \equiv$$

$$651 \equiv$$

$$63 \equiv 0 \Rightarrow n \mid 7$$

### Restklassen

Betrachte alle Zahlen, die beim Teilen durch eine Zahl  $m \in \mathbb{N}$  denselben Rest lassen.

Diese Zahlen werden zu einer Menge zusammengefasst, der Restklasse.

### Definition

Die Restklasse  $\bar{a}$  von  $a$  modulo  $m$  ist definiert durch:

$$\bar{a} := \{ b \in \mathbb{Z} : b \equiv a \pmod{m} \} \quad (\text{andere Schreibweise: } [a] \text{ statt } \bar{a})$$

### Beispiel:

Die Restklassen modulo 5:

$$\bar{0} = \{ \dots, -10, -5, 0, 5, 10, \dots \} = \overline{5} = \overline{10} \dots$$

$$\bar{1} = \{ \dots, -9, -4, 1, 6, 11, \dots \} = \overline{6} = \overline{11} \dots$$

$$\bar{2} = \{ \dots, -8, -3, 2, 7, 12, \dots \} = \overline{7} = \overline{12} \dots$$

$$\bar{3} = \{ \dots, -7, -2, 3, 8, 13, \dots \} = \overline{8} = \overline{13} \dots$$

$$\bar{4} = \{ \dots, -6, -1, 4, 9, 14, \dots \} = \overline{9} = \overline{14} \dots$$

### Definition

Die Menge aller Restklassen heißt Restklassenring modulo  $m$ , geschrieben  $\mathbb{Z}_m$

$$\text{Beispiel: } \mathbb{Z}_5 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$$

Rechnen im RestklassenringDefinition:

Seien  $a, b \in \mathbb{Z}$   
 $\bar{a} + \bar{b} := \overline{a+b}$   
 $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$

Beispiel in  $\mathbb{Z}_5$ 

$$\begin{array}{rcl} \bar{2} + \bar{2} & = & \bar{4} \\ \frac{\bar{1}}{7} + \frac{\bar{1}}{12} & = & \bar{1}\bar{9} \end{array} \quad \text{Es ist egal, welche Darstellung von } \bar{a} \text{ und } \bar{b} \text{ für die Berechnung verwendet wird. Die Addition auf Restklassen ist "wohldefiniert".}$$

Die Verknüpfungstabelle für Addition und Multiplikation in  $\mathbb{Z}_5$ :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Subtraktion in  $\mathbb{Z}_5$ :  $\bar{a} - \bar{b} := \bar{a} + \overline{(-b)}$ . Dann gilt  $\bar{a} - \bar{a} = \bar{a} + \overline{(-a)} = \overline{a-a} = \overline{0}$

Hilfsfrage für negative Restklassen: wieviel fehlt vom Absolutbetrag zum nächsten Vielfachen von  $m$ ?

Division in  $\mathbb{Z}_5$ :  $\frac{\bar{1}}{\bar{2}} = \bar{x} \Leftrightarrow \bar{1} = \bar{2} \cdot \bar{x} \stackrel{\text{Tabelle}}{\Rightarrow} \bar{x} = \bar{3}$

$$\frac{\bar{2}}{\bar{3}} = \bar{x} \Leftrightarrow \bar{2} = \bar{3} \cdot \bar{x} \Rightarrow \bar{x} = \bar{4}$$

Aber betrachte  $\mathbb{Z}_4$ :

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\frac{\bar{1}}{\bar{2}} = \bar{x} \Leftrightarrow \bar{1} = \bar{2} \cdot \bar{x}$ , es gibt kein  $\bar{x}$

$\frac{\bar{2}}{\bar{3}} = \bar{x} \Leftrightarrow \bar{2} = \bar{3} \cdot \bar{x} \Rightarrow \bar{x} = \bar{1} \text{ oder } \bar{x} = \bar{3}$   
 $\Rightarrow \bar{x}$  ist nicht eindeutig

Existenz von Brüchen in  $\mathbb{Z}_m$ :

$$\begin{aligned} \frac{\bar{a}}{\bar{b}} = \bar{x} &\Leftrightarrow \bar{a} = \bar{b} \cdot \bar{x} = \overline{bx} \Leftrightarrow a \equiv bx \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z}: km = bx - a \\ &\Leftrightarrow \exists k \in \mathbb{Z}: bx - km = a \quad \left. \begin{array}{l} \text{diophantische Gleichung} \\ x \in \mathbb{Z} \text{ gesucht} \\ k \in \mathbb{Z} \text{ unbekannt} \end{array} \right\} \quad a, b, m \in \mathbb{N} \text{ gegeben} \end{aligned}$$

Falls  $m$  Primzahl gilt:  $\text{ggT}(m, b) = 1$ . Dann hat diese Gleichung für jedes  $a$  eine Lösung  $x_0$  und alle anderen Lösungen sind gegeben durch  $x_0 + l \cdot m$  ( $l \in \mathbb{Z}$ ). Dies sind die

Elemente von  $\overline{X_0}$ .

Satz vom Dirichlet

Sei  $p$  Primzahl,  $a \in \mathbb{Z}$ ,  $b \in \{1, \dots, p-1\}$ , dann besitzt die Gleichung  $\bar{b} \cdot \bar{x} = \bar{a}$  in  $\mathbb{Z}_p$  genau eine Lösung  $\bar{x}$ , d.h.  $\frac{\bar{a}}{\bar{b}} := x$  ist definiert.

Merkregel: Wenn wir  $\frac{\bar{1}}{\bar{a}}$  in  $\mathbb{Z}_m$  suchen, dann lösen wir  $ax + my = 1$ . Dann gilt:  $\frac{1}{a} = \bar{x}$

Der kleine Satz von Fermat:

Sei  $p$  Primzahl,  $a \in \mathbb{N}$  kein Vielfaches von  $p$ . Dann gilt:  
 $\bar{a}^{p-1} = \bar{1}$  in  $\mathbb{Z}_p$  bzw.  $a^{p-1} \equiv 1 \pmod{p}$

Beispiel in  $\mathbb{Z}_5$ 

$$\begin{aligned} 1^4 &\equiv 1 \pmod{5} & 2^4 &= (4)^2 = (-1)^2 = 1 \pmod{5} \\ 3^4 &= (9)^2 = (-1)^2 = 1 \pmod{5}, & 4^4 &= (-1)^4 = 1 \pmod{5} \end{aligned}$$

Beweis (kleiner Satz von Fermat):

$$A = \{\bar{0a}, \bar{1a}, \bar{2a}, \dots, \bar{(p-1)a}\} \subseteq \mathbb{Z}_p$$

Wir zeigen zunächst  $A = \mathbb{Z}_p$ , indem wir zeigen, dass alle Elemente in  $A$  verschieden sind.

Annahme:  $\bar{j}a = \bar{k}a$  für ein  $j > k$ .  $\Rightarrow \bar{0} = \bar{j}a - \bar{k}a = \bar{j}a - \bar{k}a = \bar{(j-k)}a$

$\Rightarrow \bar{(j-k)} \cdot \bar{a} = \bar{0}$  mit  $j-k \neq 0 \Rightarrow \bar{\frac{0}{(j-k)}} = \bar{a} \Rightarrow \bar{0} = \bar{a} \Rightarrow a$  ist Vielfaches von  $p$ .  $\checkmark$

Also  $A = \mathbb{Z}_p$ . Wir entfernen  $\bar{0a}$  aus  $A$  und  $\bar{0}$  aus  $\mathbb{Z}_p$ . Das Produkt der restlichen Elemente muss gleich sein.  $\bar{a} \cdot \bar{2a} \cdot \bar{3a} \cdots \bar{(p-1)a} = \bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \bar{(p-1)} \Rightarrow \bar{a}^{p-1} = \bar{1}$  q.e.d.

Definition:

Ein Element  $\bar{g} \in \mathbb{Z}_m$  heißt Primivwurzel, falls durch  $\bar{g}^k$  alle Elemente von  $\mathbb{Z}_m$  außer  $\bar{0}$  dargestellt werden können

Beispiel

$$\begin{array}{ll} 2^0 \equiv 1 \pmod{7} & 3^0 \equiv 1 \pmod{7} \\ 2^1 \equiv 2 & 3^1 \equiv 3 \\ 2^2 \equiv 4 & 3^2 \equiv 2 \\ 2^3 \equiv 1 & 3^3 \equiv 6 \\ 2^4 \equiv 2 & 3^4 \equiv 4 \\ 2^5 \equiv 4 & 3^5 \equiv 5 \\ 2^6 \equiv 1 & 3^6 \equiv 1 \end{array}$$

2 ist keine Primivwurzel, 3 ist Primivwurzel in  $\mathbb{Z}_7$ .

Tritt bei  $\bar{g}^k$  vor  $\bar{g}^{p-1}$  die Restklasse  $\bar{1}$  auf, so wiederholen sich die Restklassen, es kann keine Primivwurzel vorliegen.

Zahlentheorie ist die Mathematik der ganzen Zahlen.

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

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

### Diophantische Gleichungen

Gegeben:  $a, b, c \in \mathbb{N}$ , gesucht  $x, y \in \mathbb{Z}$  mit:  $ax + by = c$

Wir schreiben Lösungen als Zahlenpaar  $(x/y)$ .

Beispiele:

$$x + 3y = 10 \quad (x/y) = (7/1), (4/2), (1/3)$$

$$3x + 7y = 1 \quad (x/y) = (-2/1), (5/-2)$$

$$5x + 5y = 1 \quad \text{keine Lösung, da linke Seite durch 5 teilbar, rechte nicht.}$$

### Teiler und Primzahlen

Definition:

1) Seien  $x \in \mathbb{Z}, n \in \mathbb{N}$ .  $k$  heißt Teiler von  $x$ , geschrieben  $k|x$ , falls es ein  $q \in \mathbb{Z}$  gibt, so dass gilt:  $x = q \cdot k$ .

2) Seien  $a, b \in \mathbb{N}$ . Dann ist der größte gemeinsame Teiler von  $a$  und  $b$  definiert durch:

$$\text{ggT}(a, b) = \max \{k \in \mathbb{N} \mid k|a \wedge k|b\}$$

Beispiele:

$$3|12, \text{ denn } 12 = 3 \cdot 4$$

$$2|-8, \text{ denn } -8 = 2 \cdot (-4)$$

$$a = 70, b = 98$$

$$\text{Teiler von } a = \{1, 2, 5, 7, 10, 14, 35, 70\}$$

$$\text{Teiler von } b = \{1, 2, 7, 14, 49, 98\}$$

$$\text{gemeinsame Teiler von } a \text{ und } b = \{1, 2, 7, 14\}$$

$$\text{ggT}(a, b) = 14$$

Definition:

Eine natürliche Zahl  $p > 1$  heißt Primzahl oder prim, wenn sie genau zwei Teiler hat: die 1 und sich selbst.

Beispiele:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

### Hauptsatz der elementaren Zahlentheorie

Jede natürliche Zahl  $n > 1$  lässt sich, bis auf die Reihenfolge der Faktoren, eindeutig als Produkt von Primzahlen darstellen.



















Zahlentheorie ist die Mathematik der ganzen Zahlen.

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

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

### Diophantische Gleichungen

Gegeben:  $a, b, c \in \mathbb{N}$ , gesucht  $x, y \in \mathbb{Z}$  mit:  $ax + by = c$

Wir schreiben Lösungen als Zahlenpaar  $(x/y)$ .

### Beispiele:

$$x + 3y = 10 \quad (x/y) = (7/1), (4/2), (1/3)$$

$$3x + 7y = 1 \quad (x/y) = (-2/1), (5/-2)$$

$$5x + 5y = 1 \quad \text{Keine Lösung, da linke Seite durch 5 teilbar, rechte nicht.}$$

### Teiler und Primzahlen

#### Definition:

1) Seien  $x \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ .  $k$  heißt Teiler von  $x$ , geschrieben  $k|x$ , falls es ein  $q \in \mathbb{Z}$  gibt, so dass gilt:  $x = q \cdot k$ .

2) Seien  $a, b \in \mathbb{N}$ . Dann ist der größte gemeinsame Teiler von  $a$  und  $b$  definiert durch:

$$\text{ggT}(a, b) = \max \{k \in \mathbb{N} \mid k|a \wedge k|b\}$$

### Beispiele:

$$3|12, \text{ denn } 12 = 3 \cdot 4$$

$$2|-8, \text{ denn } -8 = 2 \cdot (-4)$$

$$a = 70, b = 98$$

$$\text{Teiler von } a = \{1, 2, 5, 7, 10, 14, 35, 70\}$$

$$\text{Teiler von } b = \{1, 2, 7, 14, 49, 98\}$$

$$\text{gemeinsame Teiler von } a \text{ und } b = \{1, 2, 7, 14\}$$

$$\text{ggT}(a, b) = 14$$

#### Definition:

Eine natürliche Zahl  $p > 1$  heißt Primzahl oder prim, wenn sie genau zwei Teiler hat: die 1 und sich selbst.

### Beispiele:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

### Hauptsatz der elementaren Zahlentheorie

Jede natürliche Zahl  $n > 1$  lässt sich, bis auf die Reihenfolge der Faktoren, eindeutig als Produkt von Primzahlen darstellen.

### Beispiele:

$$\left. \begin{array}{l} 70 = 2 \cdot 5 \cdot 7 \\ 98 = 2 \cdot 7 \cdot 7 \end{array} \right\} \text{ ggT}(70, 98) = 2 \cdot 7 = 14$$

$$\left. \begin{array}{l} 360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \\ 756 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 \end{array} \right\} \quad \text{ggT}(360, 756) = 2 \cdot 2 \cdot 3 \cdot 3 = 36$$

Der  $\text{ggT}(a, b)$  besteht aus allen gemeinsamen Primfaktoren von  $a$  und  $b$ .

Also: Jeder gemeinsame Teiler von  $a$  und  $b$  ist auch Teiler von  $\text{ggT}(a, b)$ .

Definition: Eine Ausdruck der Form  $ax + by$  mit  $a, b \in \mathbb{N}$  und  $x, y \in \mathbb{Z}$  nennen wir Vielfachsumme von  $a$  und  $b$ .

### Satz

Ist  $k$  ein gemeinsamer Teiler von  $a$  und  $b$ , dann teilt  $k$  auch jede Vielfachsumme von  $a$  und  $b$ , also:

$$k|a \wedge k|b \Rightarrow k|l(ax + by) \quad \text{für } a, b, l \in \mathbb{N}, x, y \in \mathbb{Z}$$

Beweis:

$$\left. \begin{array}{l} k|a \Rightarrow \exists k_1 \in \mathbb{Z}: a = q_1 \cdot k \\ k|b \Rightarrow \exists k_2 \in \mathbb{Z}: b = q_2 \cdot k \end{array} \right\} \Rightarrow ax + by = q_1 kx + q_2 ky = k(\underbrace{q_1 x + q_2 y}_{\in \mathbb{Z}}) \Rightarrow k|(ax + by) \quad \text{q.e.d.}$$

### Satz

Besitzt die Gleichung  $ax + by = c$  eine Lösung  $(x, y)$ , so folgt:  $\text{ggT}(a, b) | c$

Beweis:

Gibt  $ax + by = c$ , dann ist  $c$  eine Vielfachsumme von  $a$  und  $b$ . Nach dem letzten Satz folgt also:  $\text{ggT}(a, b) | c$  q.e.d.

### Satz (Teilen mit Rest)

Seien  $a, b \in \mathbb{N}$ . Dann gibt es eindeutig bestimmte Zahlen  $q, r \in \mathbb{N}_0$ , so dass gilt:  
 $a = q \cdot b + r$  mit  $0 \leq r < b$ .

Beispiele:

$$a = 13, b = 4 : \quad \begin{array}{r} a \\ \hline q \cdot b + r \\ 13 \\ 4 \cdot 3 + 1 \end{array}$$

$$a = 223, b = 25 : \quad \begin{array}{r} a \\ \hline q \cdot b + r \\ 223 \\ 8 \cdot 25 + 23 \end{array}$$

### Satz

Seien  $a, b \in \mathbb{N}$  und  $a = q \cdot b + r$  (Teilen mit Rest).

Dann gilt:  $\text{ggT}(a, b) = \text{ggT}(b, r)$

Beweis:

Wir zeigen zunächst:  $\text{ggT}(a, b) \leq \text{ggT}(b, r)$  (I)

dann:  $\text{ggT}(b, r) \leq \text{ggT}(a, b)$  (II)

Aus (I) und (II) folgt dann die Behauptung

(I):

$$\left. \begin{array}{l} \text{ggT}(a, b) | a \\ \text{ggT}(a, b) | b \\ \text{ggT}(a, b) | r \end{array} \right\} \xrightarrow{\substack{\text{Satz über Vielfachsumme} \\ \swarrow \\ \uparrow \dots \downarrow}} \begin{array}{l} \text{ggT}(a, b) | a - q \cdot b = r \\ \text{ggT}(a, b) \leq \text{ggT}(b, r) \end{array}$$

$$\left. \begin{array}{l} \text{ggT}(a,b) | r \\ \text{ggT}(a,b) | b \end{array} \right\} \Rightarrow \text{ggT}(a,b) \leq \text{ggT}(b,r)$$

↑ Definition von ggT

(II):

$$\left. \begin{array}{l} \text{ggT}(b,r) | b \\ \text{ggT}(b,r) | r \end{array} \right\} \Rightarrow \text{ggT}(b,r) | q \cdot b + r = a$$

$$\text{ggT}(b,r) | a \quad \left. \right\} \Rightarrow \text{ggT}(b,r) \leq \text{ggT}(a,b) \quad \text{q.e.d.}$$

Der Euklidische Algorithmus zur Bestimmung des ggT

$$a = 126, \quad b = 98$$

$$\begin{array}{r} 126 & 98 \\ 98 & 28 \\ 28 & 14 \\ 14 & 0 \end{array} \quad \begin{array}{l} = \text{Rest von } 126 : 98 \\ = \text{Rest von } 98 : 28 \\ = \text{Rest von } 28 : 14 \end{array}$$

ggT  
fertig

$$\text{ggT}(126, 98) = 14$$

$$a = 28, \quad b = 52$$

$$\begin{array}{r} 28 & 52 \\ 52 & 28 \\ 28 & 24 \\ 24 & 4 \\ 4 & 0 \end{array}$$

$$\text{ggT}(28, 52) = 4$$

### Satz

Zu beliebig gewählten natürlichen Zahlen  $a, b$  gibt es ganze Zahlen  $x, y$ , so dass gilt:

$$ax + by = \text{ggT}(a,b)$$

Beweis:

Beschreibung eines Verfahrens, wie  $x$  und  $y$  gefunden werden (an einem Beispiel).