16.11.23

$3 \mid 9 = 3 \cdot 3$

$22 = 2 \cdot 11$ $\quad 33 = 3 \cdot 11$ $\quad 44 = 2 \cdot 2 \cdot 11$

Teilbarkeitsregeln: a) $3 \mid 12$ und $12 \mid 24 \Rightarrow 3 \mid 24$

$2 \mid 4$ und $4 \mid 20 \Rightarrow 2 \mid 20$

$4 = 2 \cdot 2$ $\quad 20 = 2 \cdot 2 \cdot 5$ $\quad 120 = 2 \cdot 2 \cdot 5$

b) $3 \mid 12$ und $5 \mid 10 \Rightarrow 3 \cdot 5 \mid 120$

$12 = 3 \cdot 2 \cdot 2$ $\quad 10 = 5 \cdot 2$ $\quad 15 = 3 \cdot 5$ $\quad 120 = 3 \cdot 2 \cdot 2 \cdot 5 \cdot 2$

c) $3 \mid 9$ und $3 \mid 6 \Rightarrow 3 \mid 4 \cdot 9 - 1 \cdot 6 = 3 \cdot (4 \cdot 3 - 1 \cdot 2)$

$9 = 3 \cdot 3$ $\quad 6 = 3 \cdot 2$

d) $3 \mid -3$ und $-3 \mid 3 \Rightarrow 3 = -(-3)$

$3 = (-3) \cdot (-1)$

Modulo-Rechnen:

- $a = -6$, $b = 12$: $\overline{-6} = -6 \bmod 12 = (\underbrace{-12}_{(-1) \cdot 12} + 6) \bmod 12 = 6$
- $a = -11$, $b = 5$ in $\mathbb{Z}/5\mathbb{Z}$: $\overline{-11} = \underbrace{(-3) \cdot 5}_{5 \mid -15} + 4 \bmod 5 = 4 \bmod 5$
- $a = 25$, $b = 7$: $25 \bmod 7 = (3 \cdot 7 + 4) \bmod 7 = 4 \bmod 7$
- $a = -2$, $b = 7$: $-2 \bmod 7 = (\underbrace{-7}_{(-1) \cdot 7} + 5) \bmod 7 = 5 \bmod 7$

$\{0, \dots, 6\}$.

$\mathbb{Z}/3\mathbb{Z}$: Multiplikative Inverse von $\overline{2} \odot \overline{a} = \overline{1}$

$\overline{2} \odot \overline{2} = \overline{2 \cdot 2} = \overline{4} = \overline{1}$

Äquivalenzklasse beim Teilen durch 3 $\overline{2} = \{2, 5, 8, \dots, -1, -4, \dots\}$

Euklidische Algorithmus:

z.B. $a = 42,\ b = 28$ $\Leftarrow$ $42 = 1 \cdot 28 + 14 \Rightarrow r = 14$

$ggT(42, 28) = ggT(28, 14) = 14$

Aufgabe: $ggT(351, 213) = ?$

$a \quad b$

$351 = 1 \cdot 213 + 138$ $\Rightarrow ggT(351, 213) = ggT(213, 138)$

$213 = 1 \cdot 138 + 75$ $\Rightarrow ggT(213, 138) = ggT(138, 75)$

$138 = 1 \cdot 75 + 63$ $\Rightarrow ggT(138, 75) = ggT(75, 63)$

$75 = 1 \cdot 63 + 12$ $\Rightarrow ggT(75, 63) = ggT(63, 12)$

$63 = 5 \cdot 12 + 3$ $\Rightarrow ggT(63, 12) = ggT(12, 3)$

$12 = 4 \cdot 3 + 0$ ✓ $\qquad ggT(12, 3) = 3$

ggT ↑ bis hier das erste Mal eine 0 steht

$351 = 1 \cdot 213 + 138$
$a \quad b \quad r_1$

$213 = 1 \cdot 138 + 75$
$b \quad r_1 \quad r_2$

$138 = 1 \cdot 75 + 63$
$r_1 \quad r_2 \quad r_3$

$75 = 1 \cdot 63 + 12$
$r_2 \quad r_3 \quad r_4$

$63 = 5 \cdot 12 + 3$
$r_3 \quad 5 \cdot r_4 \quad ggT$

$r_1 = 1 \cdot a - 1 \cdot b$

$r_2 = b - 1 \cdot r_1$

$= b - 1 \cdot (a - b) = b - a + b$
$= 2b - a$

$r_3 = r_1 - 1 \cdot r_2$

$= (a - b) - (2b - a)$
$= a - b - 2b + a = 2a - 3b$

$r_4 = r_2 - r_3 = (2b - a) - (2a - 3b)$
$= 2b - a - 2a + 3b = 5b - 3a$

$3 = ggT(351, 213) = r_3 - 5 \cdot r_4$
$= 2a - 3b - 5 \cdot (5b - 3a) = 2a - 3b - 25b + 15a$

$= 17 \cdot a - 28 \cdot b$

$\Rightarrow s = 17 \;,\; t = -28$

$\Rightarrow \underbrace{3}_{4} = \underline{17} \cdot 351 - \underline{28} \cdot 213$

$ggT(351, 213)$

Ziel: Was ist das multiplikative Inverse von $\overline{13}$ in $\mathbb{Z}/17\mathbb{Z}$ = Äquivalenzklassen / Restklassen beim Teilen durch 17.

$ggT(13, 17) = 1 \Rightarrow$ es gibt $s, t \in \mathbb{Z}$ s.d.

$s \cdot 17 + t \cdot 13 = 1$

in $\mathbb{Z}/17\mathbb{Z}$:

$$\overline{s \cdot 17 + t \cdot 13} = \overline{1}$$

$$\overline{t \cdot 13} = \overline{t} \odot \overline{13}$$

$\Rightarrow \overline{t} \odot \overline{13} = \overline{1}$ in $\mathbb{Z}/17\mathbb{Z}$

mult. Inverses von a ist ein b s.d. $a \cdot b = 1$

→ Berechne s, t mit dem erweiterten euklid. Alg.:

$17 = 1 \cdot 13 + 4$ (a, b, r_1)

$\Rightarrow r_1 = a - 1 \cdot b = a - b$

$13 = 3 \cdot 4 + 1$ (b, r_1, r_2)

$\Rightarrow 1 = ggT(13, 17) = b - 3 \cdot r_1$

$= b - 3 \cdot (a - b) = b - 3a + 3b$

$= 4b - 3a = 4 \cdot 13 - 3 \cdot 17$

$\Rightarrow \overline{t} = \overline{4}$

---

in $\mathbb{Z}/4\mathbb{Z}$: $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ $\overline{2}$ hat kein multiplikatives Inverses:

$\overline{0} \cdot \overline{2} = \overline{0}$, $\overline{1} \cdot \overline{2} = \overline{2}$, $\overline{2} \cdot \overline{2} = \overline{0}$, $\overline{3} \cdot \overline{2} = \overline{2}$

Satz von Euklid:

Beweis: mit Widerspruch:

Angenommen es gibt nur endlich viele Primzahlen, $n \in \mathbb{N}$ viele: $p_1, \dots, p_n$

Betrachte die natürliche Zahl $m = p_1 \cdot \dots \cdot p_n + 1$;

Da m größer ist als $p_1, \dots, p_n$, kann m keine Primzahl sein.

Wegen: $p_i \mid p_1 \cdot \dots \cdot p_n$, gilt: $p_i \nmid p_1 \cdot \dots \cdot p_n + 1 = m$

$\Rightarrow$ m ist eine natürliche Zahl, die nur durch 1 und sich selbst teilbar ist, also ist m eine Primzahl.

$\Rightarrow$ Widerspruch. $\square$

Verbesserung Primfaktorzerlegung: $n \neq 1$.

z.B. $45 = 5 \cdot 3 \cdot 3 = 3 \cdot 5 \cdot 3$

$\Rightarrow$ Teiler sind: $1, 3, 5, 3 \cdot 5 = 15, 3 \cdot 3 = 9, 3 \cdot 3 \cdot 5 = 45$.

Beispiel für Folgerung:

$a = 45$, $b = 16 = 2^4$

$3 \mid a \cdot b = \underline{5 \cdot 3 \cdot 3}; \underline{2 \cdot 2 \cdot 2 \cdot 2}$, $\Rightarrow 3 \mid 45$.

Dies ist falsch für nicht-Primzahlen!

z.B.: $6 \mid 3 \cdot 4$ aber es gilt nicht $6 \mid 3$ oder $6 \mid 4$!

$3 \cdot 2$