

10. Elemente der Zahlentheorie

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

Satz: Division mit Rest

$\forall a, b \in \mathbb{Z}$ mit $b \neq 0 \exists! q, r \in \mathbb{Z}$ mit $0 \leq r < |b|$ und $a = qb + r$

Definition:

$a, b \in \mathbb{Z} : b|a \Leftrightarrow \exists q \in \mathbb{Z}$ mit $a = qb$
 $a \neq 0, b \neq 0 : ggT(a, b) := \max \underbrace{\{c \in \mathbb{Z} : c|a \text{ und } c|b\}}_{\text{endl. Menge}}$

Bemerkungen, Rechenregeln

- $b|a, a \neq 0 \Rightarrow |b| \leq |a|, |a| = |q||b|$
- $b|a$ ist eine refl. und trans. Relation in \mathbb{Z} ;
 - $a|a$
 - $(c|b \wedge b|a) \Rightarrow c|a : b = pc, a = qb \Leftrightarrow a = \underbrace{qp}_{\in \mathbb{Z}} c$
- $(b|a_1 \wedge b|a_2) \Rightarrow b|c_1a_1 + c_2a_2 \forall c_1, c_2 \in \mathbb{Z}$
 $a_1 = q_1b, a_2 = q_2b \Rightarrow c_1a_1 + c_2a_2 = b \underbrace{(c_1q_1 + c_2q_2)}_{\in \mathbb{Z}}$
- $(b_1|a_1 \wedge b_2|a_2) \Rightarrow b_1b_2|a_1a_2 : a_1 = q_1b_1, a_2 = q_2b_2 \Rightarrow a_1a_2 = \underbrace{q_1q_2}_{\in \mathbb{Z}} b_1b_2$

Satz

$$ggT(a, b) = ggT(b, a \pmod{b})$$

Euklidischer Algorithmus zur Berechnung von $ggT(a, b)$:

$a = q_0b + c_0, 0 \leq c_0 < |b|$
 $r_0 = 0 : b = ggT(a, b)$
 $c_0 > 0 : b = q_1r_0 + c_1, 0 \leq r_1 < r_0, ggT(a, b) = ggT(b, r_0)$
 $r_1 = 0 : ggT(a, b) = ggT(b, r_0) = r_0$
 $r_1 > 0 : r_0 = q_2r_1 + r_2, 0 \leq r_2 < r_1, ggT(a, b) = ggT(b, r_0) = ggT(r_0, r_1)$
 $r_2 = 0 : ggT(a, b) = r_1$
 $r_2 > 0 : \text{usw.} \dots$

allgemein

$r_{n-2}q_n r_{n-1} + r_n, 0 \leq r_n < r_{n-1}$
 $ggT(a, b) = ggT(r_{n-2}, r_{n-1})$
 $r_n = 0 : ggT(a, b) = r_{n-1}$
 $r_n > 0 : \text{weiter} \dots$

Folgerung

$$\exists \alpha, \beta \in \mathbb{Z} : ggT(a, b) = \alpha a + \beta b$$

Satz: Primzahlzerlegung

$$\forall n = 2, 3, 4, \dots \exists m = 1, 2, 2, \dots \exists (p_1, \dots, p_m) \in \mathbb{P}^m : n = p_1 \cdot p_2 \cdot \dots \cdot p_m$$

Satz

Die Menge der Primzahlen ist unendlich.

Beweis:

Gegenteil: $\mathbb{P} = \{p_1, \dots, p_m\}$

$$a := p_1 p_2 \dots p_n + 1 = p_n p_{j_1} p_{j_2} \dots p_{j_k} \in \mathbb{P}$$

$$p_{j_1} | a \Rightarrow p_{j_1} | (p_1 p_2 \dots p_n + 1) \Rightarrow p_{j_1} | (p_1 p_2 \dots p_n + 1 - p_1 p_2 \dots p_n) \Rightarrow p_{j_1} | 1 \Rightarrow$$

Widerspruch

$$p_{j_1} | p_1 p_2 \dots p_n$$