

Aufgabe 1 (größter gemeinsamer Teiler, Lemma von Bézout) [4 Punkte]

Der größte gemeinsame Teiler, $\text{ggT}(a, b)$, zweier ganzer Zahlen $a, b \in \mathbb{Z}$ kann mit dem Euklidischen Algorithmus berechnet werden. Der erweiterte Euklidische Algorithmus¹ liefert darüberhinaus Zahlen $s, t \in \mathbb{Z}$, für die $sa + tb = \text{ggT}(a, b)$ gilt. Diese Identität ist auch unter dem Namen Lemma von Bézout bekannt.

Für mehr als zwei ganze Zahlen kann der ggT rekursiv definiert werden über

$$\text{ggT}(a_1, \dots, a_n) = \text{ggT}(\text{ggT}(a_1, a_2, \dots, a_{n-1}), a_n) .$$

Geben Sie an, wie für ein Tupel $(a_1, \dots, a_n) \in \mathbb{Z}^n$ unter Verwendung des Lemmas von Bézout eine Lösung $(s_1, \dots, s_n) \in \mathbb{Z}^n$ für $s_1 a_1 + \dots + s_n a_n = \text{ggT}(a_1, \dots, a_n)$ berechnet werden kann und zeigen Sie, wie damit eine ganzzahlige Lösung der Gleichung $48s_1 + 30s_2 + 9s_3 = 3$ bestimmt werden kann.

Aufgabe 2 (Lösungen einer linearen diophantischen Gleichung) [8 Punkte]

Eine lineare diophantische Gleichung ist eine Gleichung der Form $a_1 x_1 + \dots + a_n x_n = b$ mit Koeffizienten $a_i, b \in \mathbb{Z}$, wobei man nur an Lösungen $(x_1, \dots, x_n) \in \mathbb{Z}^n$ interessiert ist.

a) Zeigen Sie: Die lineare diophantische Gleichung $a_1 x_1 + \dots + a_n x_n = b$ besitzt genau dann eine Lösung, wenn $\text{ggT}(a_1, \dots, a_n)$ ein Teiler von b ist.

b) Geben Sie ein Verfahren an, mit dem *alle* Lösungen einer linearen diophantischen Gleichung bestimmt werden können.

Aufgabe 3 (Gaußsche Zahlen) [8 Punkte]

Die gaußschen Zahlen sind eine Verallgemeinerung der ganzen Zahlen auf die komplexe Zahlenebene, d.h. eine gaußsche Zahl g hat die Form $g = a + bi$, wobei $a, b \in \mathbb{Z}$. Die gaußschen Zahlen bilden einen euklidischen Ring G unter den üblichen Rechenregeln für komplexe Zahlen, wobei die Bewertungsfunktion $g : G \setminus \{0\} \rightarrow \mathbb{N}$ als $g(a + bi) = a^2 + b^2$ definiert ist.

Die Division mit Rest für zwei gaußsche Zahlen z_1, z_2 sei wie folgt definiert: In $z_1 = qz_2 + r$ ist $q \in G$ der Quotient und $r \in G$ der Rest der Division von z_1 durch z_2 . Die Zahl $q = m + ni$ ist dabei die (nicht zwingend eindeutig definierte) Zahl, die dem Bruch $\xi = \frac{z_1}{z_2} \in \mathbb{C}$ am nächsten kommt, d.h., für die $|m - \text{Re}(\xi)| \leq \frac{1}{2}$ und $|n - \text{Im}(\xi)| \leq \frac{1}{2}$ gilt.

a) Bestimmen Sie die Einheiten des Rings G , d.h. die Elemente, die ein multiplikatives Inverses besitzen.

b) Zeigen Sie, dass für die oben definierte Division mit Rest die zwei Bedingungen für einen euklidischen Ring eingehalten sind, d.h. (1) $r = 0$ oder $g(r) < g(z_2)$ für $z_2 \neq 0$ und (2) $g(x \cdot y) \geq g(x)$ für alle $x, y \in G \setminus \{0\}$.

c) Bestimmen Sie den größten gemeinsamen Teiler von $z_1 = 5 + i$ und $z_2 = 4$ in G .

¹https://de.wikipedia.org/wiki/Erweiterter_euklidischer_Algorithmus