

Hinweis:

► Denken Sie an den OMB+ Kurs (<https://www.ombplus.de>) - dort absolvieren Sie bitte die Lektion II (Gleichungen in einer Unbekannten) und die Lektion IV (Lineare Gleichungssysteme). In Ihrer Übungsstunde der 5. Vorlesungswoche werden Sie einen Test über die Inhalte dieser Lektionen schreiben. Mit Hilfe dieses Testes können Sie Zusatzpunkte erwerben - diese Punkte werden Ihnen als Hausaufgabenpunkte angerechnet, aber nicht auf die zu erreichende Gesamthausaufgabenpunktzahl dazugezählt.

Aufgabe 3.1

4 Punkte

Berechnen Sie mit Hilfe des erweiterten euklidischen Algorithmus die folgenden größten gemeinsamen Teiler (geben Sie jeden Rechenschritt in Tabellenform wie im Skript vorgeführt an).

- a) $\text{ggT}(112, 38)$
- b) $\text{ggT}(89, 55)$
- c) Finden Sie dabei ganze Zahlen u, v und x, y so dass gilt

$$\begin{aligned}\text{ggT}(112, 38) &= u \cdot 112 + v \cdot 38 \\ \text{ggT}(89, 55) &= x \cdot 89 + y \cdot 55.\end{aligned}$$

Aufgabe 3.2

4 Punkte

- a) Beweisen Sie Lemma 3.4.4 aus der Vorlesung. Es seien $a, b, n \in \mathbb{N}$ dann gilt

$$\text{ggT}(a \cdot b, n) \mid \text{ggT}(a, n) \cdot \text{ggT}(b, n).$$

- b) Wann gilt

$$\text{ggT}(a \cdot b, n) = \text{ggT}(a, n) \cdot \text{ggT}(b, n).$$

Aufgabe 3.3

4 Punkte

- a) Finden Sie ein $n \in \mathbb{N}$, das die folgende Modul-Gleichungen korrekt ergänzt:

$$4 \equiv 18 \pmod{n}$$

Ist die Lösung eindeutig? - wenn nicht, nennen Sie alle Lösungen für $n \in \mathbb{N}$.

- b) Finden Sie ein $z \in \mathbb{Z}$, das die folgende Modul-Gleichungen korrekt ergänzt:

$$3 \equiv z \pmod{9}$$

Ist die Lösung eindeutig? - wenn nicht, nennen Sie alle Lösungen für $z \in \mathbb{Z}$.

- c) Finden sie zwei unterschiedliche Zahlen $z_1, z_2 \in \mathbb{Z}$ mit $|z_1| < 9$ und $|z_2| < 9$, so dass

$$(4102)^{10} \equiv z \pmod{9}.$$

- d) Ist das folgende System von Modul-Gleichungen lösbar?

$$\begin{aligned}x &\equiv 3 \pmod{5} \\ x &\equiv 7 \pmod{10}.\end{aligned}$$

Aufgabe 4.4**4 Punkte**

a) Seien $a, b, c \in \mathbb{Z}$. Beweisen Sie

$$c|a \text{ und } c|a+b \implies c|b.$$

b) Für welchen Input $a, b \in \mathbb{N}$ terminiert der euklidische Algorithmus zur Berechnung des $\text{ggT}(a, b)$ nach nur einem Schritt?