

Datenschutz und Datensicherheit / Systemsicherheit

4. Übung

1. Aufgabe:

Bestimmen Sie mit Hilfe des Euklidischen Algorithmus

- a) $\text{ggT}(3, 2)$,
- b) $\text{ggT}(132, 12)$,
- c) $\text{ggT}(523, 256)$.

2. Aufgabe:

Zeigen Sie $a \cdot b = \text{ggT}(a, b) \cdot \text{kgV}(a, b)$.

3. Aufgabe:

- a) Erweitern Sie den Euklidischen Algorithmus, so daß er (bei Eingabe $a, b \in \mathbb{Z}$) $\lambda_1, \lambda_2 \in \mathbb{Z}$ ausgibt, für die gilt

$$\lambda_1 \cdot a - \lambda_2 \cdot b = \text{ggT}(a, b).$$

- b) Zeigen Sie, daß es unendlich viele Paare (λ_1, λ_2) gibt, die die Bedingung aus a) erfüllen.
- c) Analysieren Sie die Laufzeit Ihres Verfahrens.
- d) Ermitteln Sie Linearkombinationen für die Paare aus Aufgabe 1.

4. Aufgabe:

Berechnen Sie die Inversen bezüglich der Multiplikation mod 131 für die Zahlen 38 und 39.