



PROBE-PRÜFUNG 1

1. Zeigen oder widerlegen Sie:

a) $(AFFE)_{16} = 10 \cdot 16^3 + 15 \cdot 16^2 + 15 \cdot 16^1 + 14 \cdot 16^0$.

b) $\text{ggT}(2^2 \cdot 3^5 \cdot 5, 2^2 \cdot 3^3 \cdot 7) = 2^2 \cdot 3^3$.

c) $10 \in \mathbb{Z}_{25}$ ist multiplikativ invertierbar.

d) 3 ist das multiplikativ Inverse zu 3 in \mathbb{Z}_5 .

e) $(\mathbb{Z}_{11} \setminus \{0\}, \cdot)$ ist eine Gruppe.

f) $4x \equiv 2 \pmod{25}$ ist eindeutig lösbar in \mathbb{Z}_{25} .

g) $10x + 7y = 6$ besitzt eine Lösung $x, y \in \mathbb{Z}$.

h) $f: \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}, f(x) = 8x \pmod{12}$ ist bijektiv.

2. Gegeben die Aussage $(P \oplus Q) \Leftrightarrow Q$.

a) Fertigen Sie eine Wahrheitstabelle an.

b) Bestimmen Sie die disjunktive Normalform (DNF).

c) Skizzieren Sie die dazugehörige Schaltung.

3. Zeigen Sie mittels vollständiger Induktion:

$$\sum_{k=0}^n 2^k = 2^{n+1} - 1.$$

4. Bestimmen Sie alle Lösungen $x \in \mathbb{Z}$ von $9x \equiv 3 \pmod{150}$.

5. Bestimmen Sie alle Lösungen $x \in \mathbb{Z}$ von

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 5 \pmod{11}$$

6. Bestimmen Sie alle Lösungen $x, y \in \mathbb{Z}$ mit $-10 \leq x, y \leq 10$ von $5x + 7y = 3$.

7. Knacken Sie RSA: Gegeben der öffentliche Schlüssel $(N, e) = (3233, 17)$ und die verschlüsselte Nachricht $G = 2790$. Was ist die ursprüngliche unverschlüsselte Nachricht T ?