

Algebra für Informatiker/innen
11. Übungsblatt für den 4. und 5. Juni 2009

1. Berechnen Sie jeweils den ggT mit Kofaktoren für folgende Zahlenpaare:
(a) (184, 74) (b) (125, -95) (c) (332, 21) (d) (80, 16)
2. Bestimmen Sie jeweils die Lösungsmenge folgender diophantischer Gleichungen über \mathbb{Z} :
(a) $522x - 666y = 261$
(b) $225x - 126y = 135$
3. Lösen bzw. berechnen Sie jeweils:
(a) $x + 7 = 3 \text{ in } \mathbb{Z}_{12}$ (b) $4 - x = 6 \text{ in } \mathbb{Z}_8$ (c) $8x = 4 \text{ in } \mathbb{Z}_{14}$
(d) $15x = 10 \text{ in } \mathbb{Z}_{21}$ (e) $3^{81} \text{ in } \mathbb{Z}_5$
4. Bestimmen Sie alle Lösungen von folgendem System simultaner Kongruenzen
(Hinweis: Verwandeln Sie die Gleichungen in die Form $x = a \text{ mod } n$.)
$$\begin{aligned} 9x &\equiv 6 \pmod{42} \\ x &\equiv 45 \pmod{63} \end{aligned}$$
5. Bestimmen Sie alle Lösungen von folgendem System simultaner Kongruenzen
(Hinweis: Beschreiben Sie die Lösungsmenge der ersten beiden Gleichungen durch eine Gleichung der Form $x = a \text{ mod } n$.)
$$\begin{aligned} x &\equiv 4 \pmod{12} \\ x &\equiv 10 \pmod{15} \\ x &\equiv 20 \pmod{35} \end{aligned}$$
6. Zeigen Sie: In jedem Ring R gilt $0r = 0 = r0$ für alle $r \in R$.
7. Welche Eigenschaften eines Rings mit Einselement erfüllt $2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$ mit der gewohnten Addition und Multiplikation modulo 2?
8. Für das RSA-Verfahren wählen wir $p = 5$, $q = 11$ und $e = 13$.
Ist 13 eine gültige Wahl für e ?
Chiffrieren Sie die Zahl 3. (Freiwillige Aufgabe: Probe durch Entschlüsseln).
Entschlüsseln Sie 8.