

G. Zusatzbeispiele

Übung Z1. Löse die Gleichungen:

(a) $4x + 3 \equiv 1 \pmod{7}$

(b) $4x + 5 \equiv 2 \pmod{9}$

(2P.)

Übung Z2. Löse das Gleichungssystem:

$$x + 5y = 9$$

$$3x + 2y = 4$$

in \mathbb{Z}_{11} . Gibt es auch eine Lösung in \mathbb{Z}_{13} ?

(3P.)

Übung Z3. Löse die Gleichung:

$$4x^2 + 5x + 3 = 0 \pmod{69}.$$

Hinweis: Zerlege $69 = 3 \cdot 23$ und löse zuerst die Gleichung in \mathbb{Z}_3 und \mathbb{Z}_{23} . Bestimme dann mit dem Chinesischen Restsatz die Lösungen in \mathbb{Z}_{69} .

(4P.)

Übung Z4. Die Zahlenfolge

$$(1966, 2119, 952)$$

wurde mit dem RSA-Algorithmus mit öffentlichem Schlüssel

$$(m = 2701, r = 1111)$$

verschlüsselt.

Finde den privaten Schlüssel s und entschlüssele die Nachricht (Die Buchstaben sind mit der Konvention von Beispiel **(B.5.7)** codiert).

Hinweis: Für einen Teil der Berechnungen ist wahrscheinlich ein Computer erforderlich.

(4P.)

Übung Z5. Formalisiere die folgenden Aussagen mittels Aussagenlogik:

- Von A , B und C gilt genau eines.
- Von A , B und C gelten genau zwei.
- Von A , B und C gilt mindestens eins.

Übung Z6. Für die Erstellung es neuen Mensa Speiseplans gelten die folgenden Bedingungen:

- (i) Zu jeder Mahlzeit muß es Brot geben, wenn kein Dessert gereicht wird.
- (ii) Wird Brot und Dessert serviert, darf es dazu keine Suppe geben.
- (iii) Wenn aber Suppe gereicht wird, oder kein Dessert gereicht wird, darf es auch kein Brot geben.

Formalisiere diese Bedingungen mittels Aussagenlogik, und finde eine möglichst einfache äquivalente Formel.