

## Übungsblatt 13

### Aufgabe 45

Zeigen Sie, dass das System von linearen Kongruenzen

$$x \equiv a_i \pmod{m_i} \quad i = 1, \dots, n$$

genau dann lösbar ist, wenn  $\text{ggT}(m_i, m_j) \mid (a_i - a_j)$  für alle Paare  $(i, j)$  mit  $1 \leq i < j \leq n$ . Zeigen Sie: wenn eine Lösung existiert, dann ist sie eindeutig modulo  $\text{kgV}(m_1, m_2, \dots, m_n)$ .

*Hinweis:* Führen Sie einen Induktionsbeweis und verwenden Sie Aufgabe 44.

### Aufgabe 46

Sei  $a$  ein Element von  $\mathbb{Z}_m^*$  der Ordnung  $\text{ord}_m(a) = k$ . Zeigen Sie

$$\text{ord}_m(a^i) = \frac{k}{\text{ggT}(k, i)}.$$

### Aufgabe 47 (schriftlich, 10 Punkte)

- Verschlüsseln Sie den Klartext  $x = 444$  nach dem RSA-Verfahren, falls  $e = 613$  und  $n = 989$  ist.
- Entschlüsseln Sie den Kryptotext  $y = 444$ , d. h. bestimmen Sie den Klartext  $x$ , für den gilt  $E_{(613, 989)}(x) = 444$ .

### Aufgabe 48

Betrachten Sie folgendes Zufallsexperiment:

Ein probabilistischer Primzahltest  $T$  (mit einseitiger Fehlerwahrscheinlichkeit  $\varepsilon$  im Fall einer zusammengesetzten Eingabe) wird auf eine zufällig gewählte ungerade Binärzahl  $n \in [2^l, 2^{l+1} - 1]$  angewandt.

Bestimmen Sie näherungsweise die Wahrscheinlichkeiten der beiden Ereignisse “ $n$  ist prim” (Ereignis  $A$ ) und “ $T(n)$  gibt prim aus” (Ereignis  $B$ ). Wie groß sind die bedingten Wahrscheinlichkeiten  $\text{Prob}[A/B]$  und  $\text{Prob}[B/A]$  im Fall  $\varepsilon = 2^{-m}$ ,  $m = 1, 2, 5, 10, 20, 30, 50, 100$ ? Interpretieren Sie diese Zahlen.