Übungen zur Kryptologie

Blatt 6 SoS 2024 — H. Kiechle

Präsenzaufgaben

17. Es sei $m \in \mathbb{N}$. Zeigen Sie unter Verwendung von der Darstellung des ggT aus der Vorlesung, dass ein Element $\overline{a} \in \mathbb{Z}_m$ genau dann invertierbar ist, wenn gilt $\mathrm{ggT}(a, m) = 1$.

Hausaufgaben

18. Es sei $m = 52961$ und $a \in \{1055, 10555\}$.

(a) Bestimmen Sie mit dem erweiterten euklidischen Algorithmus jeweils Zahlen $x, y \in \mathbb{Z}$ mit $ax + my = \mathrm{ggT}(a, m)$.

(b) Bestimmen Sie — soweit möglich — $a' \in \mathbb{Z}$ mit $aa' \equiv 1 \mod m$.

19. Wir rechnen $\mod 15$.

(a) Bestimmen Sie die Quadrate $\mod 15$. Unterscheiden Sie die Elemente aus $\mathbb{Z}_{15}^{\times}$ (invertierbare) und andere.

(b) Wie viele und welche Lösungen haben die Kongruenzen

$x^2 \equiv 4 \mod 15$ und $x^2 \equiv 9 \mod 15$?

(c) Lösen Sie die quadratische Gleichung $x^2 + \overline{7}x + \overline{12} = \overline{0}$ in $\mathbb{Z}_{15}$.

Hinweis: Quadratische Ergänzung!