Übungsblatt 2

Abgabe für die mündlichen Aufgaben bis 04. 05. 2020 und für die schriftliche Aufgabe bis 11. 05. 2020

Aufgabe 10 ***mündlich***

Sei $p \geq 2$ prim. Bestimmen Sie alle Lösungen der Kongruenz $x^2 \equiv_p 1$.

Aufgabe 11 ***mündlich***

(a) Bestimmen Sie alle involutorischen und alle echt involutorischen Schlüssel der affinen Chiffre für $m = 2, 3, 5, 13, 15, 26$.

(b) Wie viele involutorische Schlüssel besitzt die affine Chiffre für *quadratfreies* m (d.h. m ist durch keine Quadratzahl p^2, p prim, teilbar)? Wie viele davon sind echt involutorisch?

Hinweis: Betrachten Sie zuerst den Fall $m = p$ prim. Benutzen Sie für quadratfreies $m = p_1 \cdots p_l$, $l > 1$, dann den Chinesischen Restsatz, um aus jeder Kollektion $(k_1, \cdots, k_l)$ von l involutorischen Schlüsseln $k_i = (b_i, c_i)$ für p_i einen involutorischen Schlüssel $k = (b, c)$ für m zu gewinnen.

Aufgabe 12 ***mündlich***

Sei A eine Matrix in $\mathbb{Z}_m^{l \times l}$.

(a) Wie wirken sich elementare Zeilenoperationen (Addition einer Zeile auf eine andere, Vertauschung zweier Zeilen, Multiplikation einer Zeile mit einer Zahl $r \in \mathbb{Z}_m$) auf die Determinante $\det(A)$ aus? Begründen Sie.

(b) Zeigen Sie, dass sich A durch elementare Zeilenumformungen in eine obere *Dreiecksmatrix* $D = (d_{ij})$ (d.h. $d_{ij} = 0$ für $1 \leq j < i \leq l$) umformen lässt (Gauß-Verfahren). Was ist dabei zu beachten, wenn m nicht prim ist? Warum lässt sich $\det(A)$ auf diese Weise effizient berechnen?

(c) Erweitern Sie das Verfahren in (b) so, dass es neben $\det(A)$ im Fall $\mathrm{ggT}(\det(A), m) = 1$ auch A^{-1} effizient berechnet (Gauß-Jordan-Verfahren). Wenden Sie das Verfahren auf die Schlüsselmatrix $k \in \mathbb{Z}_{26}^{4 \times 4}$ aus der Vorlesung sowie auf die Matrix

$$A = \begin{pmatrix} 13 & 2 & 2 \\ 2 & 13 & 2 \\ 13 & 2 & 13 \end{pmatrix}$$

in $\mathbb{Z}_{26}^{3 \times 3}$ an.

Aufgabe 13 ***mündlich***

Ver- und entschlüsseln Sie den Text `DREIEINS` mittels

(a) einer Vigenère-, Beaufort- und Autokey-Chiffre (mit Klar- und mit Kryptotextschlüsselstrom) mit dem Schlüssel $k =$ `TIM`,

(b) einer Hill-Chiffre mit der (4×4)-Schlüsselmatrix k aus der Vorlesung.

Aufgabe 14 Sei $A = (a_{ij}) \in \mathbb{Z}_m^{l \times l}$ eine $(l \times l)$-Matrix über $\mathbb{Z}_m$. ***10 Punkte***

(a) Zeigen Sie die Gleichung $\mathrm{adj}\, A \cdot A = \det(A) \cdot E$. Hierbei ist $\mathrm{adj}\, A = (\mathrm{cof}\, A)^T$ die zu A *adjungierte* Matrix, $\mathrm{cof}\, A = (\tilde{a}_{i,j})$ die *Kofaktormatrix* von A mit Einträgen $\tilde{a}_{i,j} = (-1)^{i+j} \det(A_{ij})$, E die Einheitsmatrix und A_{ij} die durch Streichen der i-ten Zeile und j-ten Spalte aus A hervorgehende Matrix.

Hinweis: Benutzen Sie den laplaceschen Entwicklungssatz.

(b) Folgern Sie, dass die Abbildung $f : \mathbb{Z}_m^l \to \mathbb{Z}_m^l$ mit $f(x) = xA$ genau dann injektiv ist, wenn $\mathrm{ggT}(\det(A), m) = 1$ ist.