Übungsblatt 2

Abgabe der schriftlichen Lösungen bis 12.05.2022, 24 Uhr

Aufgabe 10 ***mündlich***

Bestimmen Sie die Anzahl $inv(m)$ der involutorischen Schlüssel sowie die Anzahl $e(m)$ der echt involutorischen Schlüssel der affinen Chiffre für *quadratfreies* m (d.h. m ist durch keine Quadratzahl p^2, p prim, teilbar).

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

Aufgabe 11 Sei A eine Matrix in $\mathbb{Z}_m^{n\times n}$ und sei $r \in \mathbb{Z}_m^*$. ***mündlich***

(a) Wie wirken sich elementare Zeilenoperationen (Addition des Vielfachen einer Zeile auf eine andere Zeile, Multiplikation einer Zeile mit r, Vertauschen zweier Zeilen) auf den Wert der Determinanten von A aus? Begründen Sie.

(b) Welche Auswirkung haben elementare Spaltenoperationen auf $\det(A)$?

(c) Wie lässt sich die Determinante $\det(D)$ einer oberen *Dreiecksmatrix* $D = (d_{ij})$ (d.h. $d_{ij} = 0$ für $1 \le j < i \le n$) effizient berechnen?

(d) Zeigen Sie, dass sich A für jedes Tripel i, i', j mit $(a_{ij}, a_{i'j}) \neq (0,0)$ und $(a_{ik}, a_{i'k}) = (0,0)$ für $k = 1, \ldots, j-1$ durch elementare Operationen auf den beiden Zeilen a_i und $a_{i'}$ in eine Matrix $A' = (a'_{ij}) = elim(A, i, i', j)$ mit $\det(A') = \det(A)$ und $\{a'_{ij}, a'_{i'j}\} = \{\mathrm{ggT}(a_{ij}, a_{i'j}), 0\}$ umformen lässt.
(*Hinweis:* Führen Sie die Operationen des Euklidschen Algorithmus' bei der Berechnung von $\mathrm{ggT}(a_{ij}, a_{i'j})$ auf den Zeilen a_i und $a_{i'}$ aus.)

(e) Zeigen Sie, dass sich A mit elementaren Zeilenoperationen in eine obere Dreiecksmatrix D mit $\det(D) = \det(A)$ umformen lässt (Gauß-Elimination).
Hinweis: Benutzen Sie Teilaufgabe (d).

(f) Erweitern Sie das Verfahren in Teilaufgabe (e) 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 folgende Matrizen über dem Ring $\mathbb{Z}_{26}$ an:

$$A = \begin{pmatrix} 13 & 2 & 2 \\ 2 & 13 & 2 \\ 13 & 2 & 13 \end{pmatrix} \quad \text{und} \quad k = \begin{pmatrix} 11 & 13 & 8 & 21 \\ 24 & 17 & 3 & 25 \\ 18 & 12 & 23 & 17 \\ 6 & 15 & 2 & 15 \end{pmatrix}$$

Aufgabe 12 ***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 Aufgabe 11.

Aufgabe 13 Sei $A = (a_{ij}) \in \mathbb{Z}_m^{n\times n}$ eine $(n \times n)$-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 $\tilde{a}_{1,1} = 1$ für $n = 1$ und $\tilde{a}_{i,j} = (-1)^{i+j} \det(A_{ij})$ für $n \ge 2$, E die Einheitsmatrix und A_{ij} für $n \ge 2$ 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 $f : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ mit $f(x) = xA$ genau dann injektiv ist, wenn $\mathrm{ggT}(\det(A), m) = 1$ ist.

Hinweis: Verwenden Sie den Determinantenproduktsatz: Für zwei quadratische Matrizen A, B über einem kommutativen Ring mit Eins gilt $\det(AB) = \det(A)\det(B)$.

(c) Folgern Sie zudem, dass die Spalten von A genau dann linear abhängig sind (d.h. es gilt $cA = (0, \ldots, 0)$ für ein $c \in \mathbb{Z}_m^n \setminus \{(0, \ldots, 0)\}$), wenn $\mathrm{ggT}(\det(A), m) > 1$ ist.