Übungsblatt 2

Abgabe der schriftlichen Lösungen am 9. 11. 2017 bis 13.10 Uhr

Aufgabe 8 ***mündlich***

Sei $(R, +, \cdot, 0, 1)$ ein Ring mit Eins. Zeigen Sie, dass die Multiplikation auf der Menge $R^* = \{a \in R \mid \exists b \in R : ab = 1 = ba\}$ aller **Einheiten** von R eine Gruppe $(R^*, \cdot, 1)$ bildet.

Aufgabe 9 ***mündlich***

Verschlüsseln Sie den Text `DREIEINS` mittels einer

(a) additiven Chiffre mit dem Schlüssel $k = 13$,

(b) affinen Chiffre mit dem Schlüssel $k = (17, 6)$,

(c) Vigenère-Chiffre mit dem Schlüssel $k =$ `TIM`,

(d) Hill-Chiffre mit der (4×4)-Schlüsselmatrix aus der Vorlesung. *(rechenintensiv)*

Aufgabe 10 ***mündlich***

(a) Sei $k = (b, c)$ ein Schlüssel der affinen Chiffre mit m Zeichen. Zeigen Sie, dass E_k genau dann involutorisch ist, wenn $b^2 \equiv_m 1$ und $c(b + 1) \equiv_m 0$ gilt.

(b) Bestimmen Sie alle involutorischen Schlüssel der affinen Chiffre mit $m = 35$ Zeichen.

(c) Wie viele involutorische Schlüssel besitzt die affine Chiffre mit m Zeichen, falls $m = pq$ das Produkt zweier Primzahlen p und q mit $2 < p < q$ ist?

Hinweis: Zeigen Sie, dass die Gleichung $x^2 \equiv_p d$ für jedes $d \in \mathbb{Z}_p^*$ entweder 0 oder 2 Lösungen in $\mathbb{Z}_p^*$ und für jedes $d \in \mathbb{Z}_m^*$ entweder 0 oder 4 Lösungen in $\mathbb{Z}_m^*$ hat.

Aufgabe 11 Betrachten Sie eine Matrix $A \in \mathbb{Z}_m^{l \times l}$. ***mündlich***

(a) Begründen Sie, warum sich das Addieren einer Zeile auf eine andere, der Tausch zweier Zeilen und die Multiplikation einer Zeile mit $r \in \mathbb{Z}_m$ auf die Determinante $\det(A)$ genauso so auswirken, wie entsprechende Operationen auf $\det(B)$ für Matrizen $B \in \mathbb{R}^{l \times l}$.

(b) Nutzen Sie a), um zu zeigen, dass sich das Gauß-Verfahren zur Berechnung der Determinante $\det(A)$ nutzen lässt. Wie muss man das Verfahren modifizieren, falls m nicht prim ist?

(c) Erweitern Sie die Methode aus b), sodass sie auch das Inverse A^{-1} effizient berechnet und wenden Sie sie (inkl. Determinante) auf $m = 26$ und folgende Matrix an:

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

Hinweis: Sie dürfen Aufgabe 12 nutzen.

(d) Begründen Sie kurz, warum $\det(AB) = \det(A)\det(B)$ auch für $A, B \in \mathbb{Z}_m^{l \times l}$ gilt.

Aufgabe 12 ***10 Punkte***

Sei $A = (a_{ij}) \in \mathbb{Z}_m^{l \times l}$ eine $(l \times l)$-Matrix, $l \geq 1$. Zeigen 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.

Hinweis: Betrachten Sie die zu A *adjungierte* Matrix $\widetilde{A} = (\widetilde{a}_{ij})$, wobei

$$\widetilde{a}_{ij} = (-1)^{i+j} \det(A_{ji})$$

ist, und leiten Sie die Gleichung

$$\widetilde{A} \cdot A = \det(A) \cdot E$$

her (E ist die Einheitsmatrix und A_{ij} ist die durch Streichen der i-ten Zeile und j-ten Spalte aus A hervorgehende Matrix.)