Übungsblatt 2

Aufgabe 7 ***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 8 ***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.

Aufgabe 9 ***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 10 ***mündlich***

Bestimmen Sie für $m = 6, 8$ und 26 die Anzahl der invertierbaren (2×2)-Matrizen über $\mathbb{Z}_m$.

Hinweis: Benutzen Sie Aufgabe 12 und den Chinesischen Restsatz.

Aufgabe 11 ***mündlich***

(a) Zeigen Sie, dass für jede selbstinverse Matrix A über $\mathbb{Z}_{26}$ gilt: $\det(A) \equiv_{26} \pm 1$.

(b) Bestimmen Sie die Anzahl der selbstinversen (2×2)-Matrizen über $\mathbb{Z}_{26}$.

Aufgabe 12 Sei p prim. ***10 Punkte***

(a) Zeigen Sie, dass genau $(p^2 - 1)(p^2 - p)$ invertierbare (2×2)-Matrizen über $\mathbb{Z}_p$ existieren.

(b) Bestimmen Sie die Anzahl aller invertierbaren $(k \times k)$-Matrizen über $\mathbb{Z}_p$.

Hinweis: Benutzen Sie, dass eine $(k \times k)$-Matrix über $\mathbb{Z}_p$, p prim, genau dann invertierbar ist, wenn die Zeilen der Matrix linear unabhängige Vektoren (über $\mathbb{Z}_p$) sind.