Übungsblatt 3

Abgabe der schriftlichen Lösungen bis 19.05.2022, 24 Uhr

Aufgabe 14 Sei $p \geq 2$ prim. ***mündlich***

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

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

Aufgabe 15 ***mündlich***

(a) Bestimmen Sie alle Schlüssel der binären (d.h. $m = 2$) digrafischen (d.h. $\ell = 2$) Hill-Chiffre. Welche davon sind involutorisch?

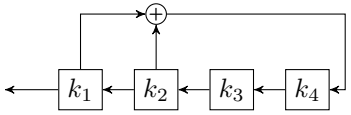
(b) Bestimmen Sie die Anzahl der involutorischen Schlüssel einer digrafischen Hill-Chiffre über einem Alphabet der Größe $m = p$, $p \geq 3$ prim.

Hinweis: Benutzen Sie Aufgabe 13 (a).

Aufgabe 16 ***mündlich***

Bestimmen Sie die Anzahl aller involutorischen Schlüssel der Blocktranspositionschiffre mit Blocklänge ℓ und maximaler Schlüsselzahl $\ell!$. Wieviele davon sind echt involutorisch?

Aufgabe 17 ***mündlich***



Ein lineares Schieberegister (LSR) der Länge ℓ ist eine Anordnung von ℓ Speicherzellen $k_1, \ldots, k_\ell$, in denen jeweils ein Bit gespeichert ist. Seien $c_0, \ldots, c_{\ell-1} \in \{0,1\}$ Konstanten mit $c_0 = 1$. Ein Rechenschritt eines LSR besteht darin, zunächst das Bit $b = \bigoplus_{j=0}^{\ell-1} c_j k_{j+1}$ zu berechnen. Dann wird k_1 ausgegeben und der Inhalt der Speicherzellen um eine Position nach links verschoben, wobei k_ℓ den Wert b erhält. Die auf diese Art entstehende Bitfolge z_i mit $z_i = k_i$, $1 \leq i \leq \ell$, und

$$z_{i+\ell} = \sum_{j=0}^{\ell-1} c_j z_{i+j} \bmod 2, \; i \geq 1$$

besteht (abgesehen von einem Anfangsstück) aus einem sich ständig wiederholenden Muster, dessen (minimale) Länge als Periode des LSR mit dem Schlüssel $k = (k_1, \ldots, k_\ell, c_0, \ldots, c_{\ell-1})$ bezeichnet wird. Zwei Schlüssel k und k' heißen *äquivalent*, wenn Sie den gleichen Schlüsselstrom erzeugen.

(a) Konstruieren Sie ein LSR der Länge $\ell = 5$ mit Periode 31 und zeigen Sie, dass die Periode niemals größer als $2^\ell - 1$ sein kann.

(b) Wie kann der Schlüssel einer auf einem LSR basierenden Stromchiffre bei Kenntnis von 2ℓ aufeinanderfolgenden Klartext/Kryptotext-Bitpaaren (bis auf Äquivalenz eindeutig) bestimmt werden?

Aufgabe 18 ***10 Punkte***

Bestimmen Sie für jede Blocklänge $\ell \geq 2$ die Schlüsselzahl der Hill-Chiffre über einem Alphabet der Größe $m = p \geq 2$ prim.

Hinweis: Benutzen Sie, dass eine quadratische Matrix über einem Körper genau dann invertierbar ist, wenn die Zeilenvektoren der Matrix linear unabhängig sind.