Übungen zur Vorlesung Kryptographie

Blatt 2

Aufgabe 5: (Einheitengruppen)
(a) Was sind die Elemente von Z_5^*? Was sind jeweils ihre inversen Elemente? Was ist der Wert von $\varphi(5)$?

(b) Was sind die Elemente von Z_{24}^*? Was sind jeweils ihre inversen Elemente? Was ist der Wert von $\varphi(24)$?

(c) Was sind die Elemente von Z_p^*, wenn p eine Primzahl ist?

Aufgabe 6: (Inverse berechnen)
(a) Berechnen Sie das inverse Element von 250 in Z_{501}^* und das inverse Element von 89 in Z_{144}^* mittels des erweiterten euklidischen Algorithmus.

(b) Bestimmen Sie alle $n \in \mathbb{N}$, so dass die jeweilige Einheitengruppe Z_n^* genau vier Elemente hat. Begründen Sie, warum das wirklich alle sind!

Aufgabe 7: (Gruppen, Ringe, Körper)
(a) Welche der folgenden Objekte sind Gruppen, welche nicht? Falls nein, warum nicht? Falls ja, was ist jeweils das neutrale Element, und was das inverse Element zu einem Element x?

$$(\mathbb{C},+),\ (\mathbb{R}^+,\cdot),\ (\mathbb{R}^{2\times 2},+),\ (\{-1,0,1\},\cdot),\ (\{-1,1\},\cdot),(\{\left(\begin{smallmatrix}\pm1 & 0\\ 0 & \pm1\end{smallmatrix}\right),\left(\begin{smallmatrix}0 & \pm1\\ \pm1 & 0\end{smallmatrix}\right)\},+),\ (\{\left(\begin{smallmatrix}\pm1 & 0\\ 0 & \pm1\end{smallmatrix}\right),\left(\begin{smallmatrix}0 & \pm1\\ \pm1 & 0\end{smallmatrix}\right)\},\cdot)$$

Dabei ist $\mathbb{R}^+$ die Menge der positiven reellen Zahlen, $\mathbb{R}^{2\times 2}$ die Menge aller reellen 2-mal-2-Matrizen, und $\{\left(\begin{smallmatrix}\pm1 & 0\\ 0 & \pm1\end{smallmatrix}\right),\left(\begin{smallmatrix}0 & \pm1\\ \pm1 & 0\end{smallmatrix}\right)\}$ steht für die Menge der acht Matrizen

$$\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right),\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right),\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right),\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right),\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right),\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right),\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right),\left(\begin{smallmatrix}0 & -1\\ -1 & 0\end{smallmatrix}\right).$$

(b) Welche der folgenden Objekte sind Ringe, welche nicht? Und welche sind Körper, welche nicht? Falls nein, warum nicht? Falls "Körper": was ist jeweils das neutrale Element bezüglich der Multiplikation, und das inverse Element zu einem Element $x \neq 0$ bezüglich der Multiplikation?

$$(Z_6,+,\cdot),(Z_5,+,\cdot),(\{0,1\},\mathrm{XOR},\mathrm{AND}),(\{\left(\begin{smallmatrix}\pm1 & 0\\ 0 & \pm1\end{smallmatrix}\right),\left(\begin{smallmatrix}0 & \pm1\\ \pm1 & 0\end{smallmatrix}\right)\},+,\cdot),(\mathbb{R}^{2\times 2},+,\cdot)$$

Aufgabe 8: (Amazon und der chinesische Restsatz)
Ein hochqualifizierter, teamfähiger, motivierter und preiswerter Lagerarbeiter der Firma Amazon packt m Alexas in 16er-Kartons. Dabei bleiben 7 Alexas übrig. Daher packt er alles wieder aus und packt die m Alexas nun in 25er-Kartons. Dabei bleiben 8 Alexas übrig. Daher packt er erneut alles wieder aus und packt die m Alexas nun in 49er-Kartons. Diesmal bleiben 9 Alexas übrig. Es sind insgesamt weniger als 10 000 Alexas. Was ist der Wert von m?

Lösen Sie die Aufgabe mit dem chinesischen Restsatz und beschreiben Sie den Rechenweg.

Abgabe: Mittwoch 17.4.2019 bis 14 Uhr in Postfach 2183 in V3, oder per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben! (Di oder Do)

Philipp Braukmann pbraukmann@techfak.uni-bielefeld.de
Oliver Tautz otautz@techfak.uni-bielefeld.de