Übungen zur Vorlesung Kryptographie

Blatt 2

Bitte alle Aufgaben von Hand lösen (ohne `sagemath`, `python` *usw). Computerlösungen zählen diesmal ausnahmsweise nicht. Rechnungen wie* $234 + (-56)$ *oder* $7 \cdot 47$ *oder* $41778 \bmod 400$ *dürfen Sie mit dem Rechner oder sagemath oder Taschenrechner oder Handy-App oder... ausführen und müssen das nicht extra hinschreiben. Ansonsten wollen wir aber den Rechenweg sehen.*

Aufgabe 5: (Einheitengruppen)
(a) Was sind die Elemente von Z_7^*? Was sind jeweils ihre inversen Elemente?

(b) Was sind die Elemente von Z_{12}^*? Was sind jeweils ihre inversen Elemente?

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

Aufgabe 6: (Inverse berechnen)
(a) Berechnen Sie das inverse Element von 180 in Z_{541}^* 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 zwei Elemente hat. Begründen Sie, warum das wirklich alle sind.

(c) Bestimmen Sie alle $N \in \mathbb{N}$, so dass $\varphi(N)$ ungerade ist. Begründen Sie Ihre Antwort.

Aufgabe 7: (Amazon und der chinesische Restsatz)
(a) Ein hochqualifizierter, teamfähiger, motivierter und sehr preiswerter Lagerarbeiter der Firma Amazon packt m Alexas in 16er-Kartons. Dabei bleiben 2 Alexas übrig. Daher packt er alles wieder aus und packt die m Alexas nun in 25er-Kartons. Dabei bleiben 3 Alexas übrig. Daher packt er erneut alles wieder aus und packt die m Alexas nun in 49er-Kartons. Diesmal bleiben 4 Alexas übrig. Es sind insgesamt weniger als 10 000 Alexas. Was ist der Wert von m? Und welche Größe k müssten die Kartons haben, damit all diese Alexas in ℓ Kartons der Größe k passen?

(b) Lösen Sie das Gleichungssytem

$$x \equiv 3 \bmod 4 \quad \wedge \quad x \equiv 1 \bmod 7 \quad \wedge \quad x \equiv 5 \bmod 9.$$

Aufgabe 8: (Ringe und Körper)
Welche der folgenden fünf 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?

$(Z_3, +, \cdot)$, $(Z_9, +, \cdot)$, $(\{0,1\}, \mathrm{OR}, \mathrm{AND})$, $(\mathbb{R}^{2\times 2}, \cdot, +)$, $P_3 = (\{a_3x^3 + a_2x^2 + a_1x + a_0 \mid a_i \in \mathbb{R}\}, +, \cdot)$.

P_3 ist also die Menge aller Polynome vom Grad 3 oder kleiner.

Abgabe bis Mittwoch 29.4.2026 bis 12:00 Uhr per Email an die Tutorin.
Bitte auf jeder Abgabe das Tutorium angeben!

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de