5. Übungsblatt
Diskrete Strukturen (Winter 2018/19)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Dr. Stefan Lucks, Nathalie Dittrich
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`

Abgabe: Bis zum 08. Januar 2019 vor Beginn der Übung oder per E-Mail an `eik.list(at)uni-weimar.de`. Lösungen sind bevorzugt in LaTeX zu verfassen. Ein Template finden Sie auf der Übungsseite der Veranstaltung.

Aufgabe 1 – Generatoren (2 Punkte)
Ermitteln Sie alle Generatoren (erzeugenden Elemente) von $(\mathbb{Z}_{13}^*, \cdot)$.

Aufgabe 2 – Isomorphismus (4 Punkte)
Wiederholen Sie Definition 55 aus Kapitel 4 der Vorlesung (Gruppenisomorphie). Zeigen oder widerlegen Sie dann, dass die folgenden Gruppoide isomorph sind.

a) $(\mathbb{Z}_7^*, \cdot)$ und $(\mathbb{Z}_6, +)$

b) $(\mathbb{Z}_6, +)$ und $(\mathbb{Z}_6, -)$

Hinweis (für Tasks 1 und 2): Beachten Sie dass für einen Generator $g \in \mathbb{Z}_p^*$ bekanntlich gilt: $g^{a+b} \bmod p = (g^a \cdot g^b) \bmod p$.

Aufgabe 3 – Diffie-Hellman-Schlüsselaustausch (3 Punkte)
Alice und Bob haben sich mit Hilfe des Diffie-Hellman-Schlüsselaustausches auf einen geheimen Schlüssel K geeinigt. Eve hat im Laufe des Austausches folgende Parameter von der unsicheren Leitung abgehört: $p = 61$, $g = 2$, $A = 52$, $B = 53$. Ermitteln Sie den geheimen Schlüssel K nur mit Hilfe dieser Informationen.

Aufgabe 4 – Secret Sharing (4 Punkte)
Um ein Geheimnis $S = p(0)$ eines Polynoms p nicht einer einzelnen Person anzuvertrauen, wurden 3 Paare $(x_i, p(x_i))$ an 3 Personen weitergereicht. Finden Sie an Hand der Wertepaare

$$\begin{aligned}(a_1, b_1) &= (1, 1)\\ (a_2, b_2) &= (5, 84)\\ (a_3, b_3) &= (11, 124),\end{aligned}$$

mit $a_i, b_i \in \mathbb{Z}_{127}$ das Geheimnis $S = p(0)$ mit Hilfe der Interpolationsformel von Lagrange heraus.

Aufgabe 5 – CRC (3 Punkte)
Berechnen Sie für den Bitstrom `1011 1011 1011` die CRC-5-USB-Prüfsumme inklusive Probe. Das zugehörige CRC-USB-Polynom lautet $p(\mathtt{x}) = \mathtt{x}^5 + \mathtt{x}^2 + \mathtt{1}$.

Aufgabe 6 – Irreduzible Polynome (4 Punkte)
Betrachten Sie den Körper $\mathbb{Z}_2[X]_{p(\mathtt{x})}$.

a) Zeigen oder widerlegen Sie: $p(\mathtt{x}) = \mathtt{x}^4 + \mathtt{x} + \mathtt{1}$ ist irreduzibel über $\mathbb{Z}_2$.

b) Stellen Sie für alle Elemente aus $\mathbb{Z}_2[X]_{p(\mathtt{x})}$ mit $p(\mathtt{x}) = \mathtt{x}^3 + \mathtt{x} + \mathtt{1}$ die Additions- und Multiplikationstabelle auf.

Fröhliche Weihnachten und einen guten Start ins Neue Jahr!