FTK3, WS 2023/24
7. Übungsblatt für den 19.1.2024

1. Sei p das irreduzible Polynom $x^6 + x + 1 \in \mathbb{Z}_2[x]$. Wir rechnen nun mit Restklassen modulo p. Berechne
   (a) $[x^5 + x + 1]_p + [x^3 + x^2]_p$
   (b) $[x^5 + x + 1]_p - [x^3 + x^2]_p$
   (c) $[x^5 + x + 1]_p \cdot [x^3 + x^2]_p$

2. Sei p wieder das irreduzible Polynom $x^6 + x + 1 \in \mathbb{Z}_2[x]$. Berechne

$$\frac{[x^5 + x + 1]_p}{[x^3 + x^2]_p}$$

3. Berechne in $\mathbb{Z}_7(\alpha) = \mathbb{Z}_7[x]/(x^3 + x^2 + 1)$
   (a) $(5\alpha^2 + 2\alpha)^4$

4. Betrachte den endlichen Körper $\mathbb{Z}_3(\alpha) = \mathbb{Z}_3[x]/(x^2 + 1)$.
   (a) Zähle alle Elemente des Körpers auf. Wie viele sind es?
   (b) Gib alle Produkte von Elementen in diesem Körper in Form einer Multiplikationstafel an (vgl. Beispiel 5.4 im Skriptum).

5. Konstruiere einen endlichen Körper $\mathbb{Z}_p[x]/f$ mit 16 Elementen.
   (a) Nenne die Primzahl p und das Polynom f.
   (b) Zähle alle Elemente des endlichen Körpers auf.
   (c) Gib alle Produkte von Elementen in diesem Körper in Form einer Multiplikationstafel an (vgl. Beispiel 5.4 im Skriptum).

6. Berechne mit dem Modul `galois` die multiplikative Ordnung aller Elemente des endlichen Körpers aus Beispiel 5.

7. Berechne in $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2[x]/(x^8+x^4+x^3+x+1)$ den Kehrwert von $\alpha^7+\alpha^3$.

8. Interpretiere das Ergebnis aus Beispiel 7 als 8-dimensionalen Vektor über dem Körper $\mathbb{Z}_2$ und berechne die affine Transformation auf Seite 83 des Skriptums. Vergleiche dein Ergebnis mit dem Ergebnis in der S-Box von AES (Abbildung 5.2 im Skriptum).