Problem 1. (*AES mix columns*) The step **MixColumns** of the AES scheme is given by \( r = Tc \) with input \( c = (c_0, c_1, c_2, c_3)' \in \mathbb{F}_{2^8}^4 \), output \( r = (r_0, r_1, r_2, r_3)' \in \mathbb{F}_{2^8}^4 \), and the circulant matrix 

\[
T = \begin{pmatrix}
    x & (x+1) & 1 & 1 \\
    1 & x & (x+1) & 1 \\
    (x+1) & 1 & 1 & x \\
\end{pmatrix} \in \mathbb{F}_{2^8}^{4 \times 4},
\]

for the polynomial field \( \mathbb{F}_{2^8} = \mathbb{F}_2[X]/(x^8 + x^4 + x^3 + x + 1)\mathbb{F}_2[X] \).

Show \((c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \mod (u^4+1) = r_3u^3 + r_2u^2 + r_1u + r_0.\)

Problem 2. (*block ciphers are permutations*) A block cipher is a cryptosystem where both plaintext and ciphertext space are the set \( \mathcal{A}^n \) of words of length \( n \) over an alphabet \( \mathcal{A} \).

a) Show that the encryption functions of block ciphers are permutations.

b) How many different block ciphers exist if \( \mathcal{A} = \{0, 1\} \) and the block length is \( n = 6 \)?

Problem 3. (*determine \( \varphi \)*) Let \( \varphi : \mathbb{N} \to \mathbb{N} \) be the Euler \( \varphi \)-function, i.e., \( \varphi(n) = |\mathbb{Z}_n^*| \).

a) Determine \( \varphi(p) \) for a prime \( p \).

b) Determine \( \varphi(p^k) \) for a prime \( p \) and \( k \in \mathbb{N} \).

c) Determine \( \varphi(p \cdot q) \) for two different primes \( p \neq q \).

d) Determine \( \varphi(4913) \) and \( \varphi(899) \).