ECE 563: FALL 2024
HOMEWORK 4
ISSUED: 18TH OF NOVEMBER. DUE 29TH OF NOVEMBER.

Note: The HW is due in class, before the lecture starts.

- **Problem 1.** Prove Fermat's little theorem (please read the statement online and if needed, consult external sources for a proof).
- **Problem 2.** State and prove the Möbius inversion formula (I stated the theorem in class).
- **Problem 3.** Primitive polynomials can be used for pseudo-random bit generation. Explain how (please feel free to read about it online and report on what you read).
- **Problem 4.** Construct the field $\mathbb{F}_{2^4}$ using a primitive polynomial and provide the multiplication and addition tables.
- **Problem 5.** Let $P(x)$ be irreducible over $\mathbb{F}_p[x]$ and of degree d. Show that for any $n \geqslant 0$, $P(x)|x^{p^n} - x$ is equivalent to $d|n$. This was proven in the lecture and was part of the lecture notes by Dr. Forney.
- **Problem 6.** Let $P(x) \in \mathbb{F}_2[x]$ be of degree $d = 7$. Then, $P(x)$ being irreducible is equivalent to $P(x)$ being primitive. Hint: difficult, you want to read about Mersenne primes.