Problems Finite Fields, July 27, 2023

Problem 1. *Show that*

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$

Problem 2. *Let $N_n(q)$ be the number of irreducible monic polynomials over $\mathbb{F}_q$ of degree n. Show that*

$$N_n(q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Deduce that for $n \geq 2$ we have

$$\frac{q^n}{2n} \leq N_n(q) \leq \frac{q^n}{n}.$$

Problem 3. *The field $\mathbb{F}_{64}$ is an extension of degree 6 of the prime field $\mathbb{F}_2$.*

(i) List the subfields of $\mathbb{F}_{64}$.

(ii) Decompose $X^{64} - X$ into irreducible polynomials over $\mathbb{F}_2$. Check the correspondence between the minimal subsets of $\mathbb{Z}/63\mathbb{Z}$ which are stable under the multiplication by 2 and the irreducible factors of $X^{63} - 1$ over $\mathbb{F}_2$.

(iii) Which are the degrees of the elements $\alpha \in \mathbb{F}_{64}$ with $\mathrm{Tr}_{\mathbb{F}_{64}/\mathbb{F}_2}(\alpha) = 0$?