Computational Number Theory (CS60094)

Spring Semester, 2023

Tutorial - 2

1. Represent $\mathbb{F}_{625} = \mathbb{F}_{5^4}$ by adjoining a root θ of $f(x) = x^4 + x + 4$ to $\mathbb{F}_5$, and let $\alpha = 2\theta^3 + 3\theta + 4$ and $\beta = \theta^2 + 2\theta + 4$. Compute $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$.

2. Define $\mathbb{F}_{27} = \mathbb{F}_{3^3} = \mathbb{F}_3(\theta)$, where θ is a root of $f(x)$, i.e., $\theta^3 + \theta^2 + 2 = 0$. Determine whether $\alpha = \theta + 1$ is a primitive element of $\mathbb{F}_{27}$.

3. Represent $\mathbb{F}_{2^n} = \mathbb{F}_2(\theta)$, let $\alpha \in \mathbb{F}_{2^n}$.

   - Prove that $\sqrt{\theta} = \theta^{2^{n-1}}$.
   - How can you express α as $A_0(\theta^2) + \theta \times A_1(\theta^2)$ (for polynomial A_0 and A_1)?

4. Consider $\mathbb{F}_{27} = \mathbb{F}_3(\theta)$ with θ as a root of $f(x) = x^3 + x^2 + 2$. Is $\alpha = \theta^2 \in \mathbb{F}_{27}$ a normal element of $\mathbb{F}_{27}$?

5. Let $\alpha \in \mathbb{F}^{\star}_{p^n}$ and $r = \frac{p^n-1}{p-1} = 1 + p + \cdots + p^{n-1}$. Prove that $\alpha^r \in \mathbb{F}_p$.