Error-Correcting Codes: Assignment #5

Alfred Menezes (cryptography101.ca)

NOTE: You can attempt a question after watching all video lectures up to and including the one listed in the question title.

1. **Minimal polynomials** (V6a)
   Let $\alpha \in GF(q^m)^*$, and let $m_\alpha(y)$ denote the minimal polynomial of α over $GF(q)$. Prove that $m_\alpha(y)$ divides $y^{q^m-1} - 1$ in $GF(q)[y]$.

2. **Extension fields** (V6b)
   Let $GF(4)$ be defined by $GF(4) = \mathbb{Z}_2[x]/(x^2 + x + 1)$.

   (a) Show that $\alpha = x$ is a generator of $GF(4)^*$.

   (b) Show that $u(z) = z^2 + \alpha z + 1$ is irreducible over $GF(4)$.

   (c) By (b), $GF(4^2)$ can be defined by $GF(4^2) = GF(4)[z]/(z^2 + \alpha z + 1)$. Show that $\beta = \alpha z$ is a generator of $GF(4^2)^*$.

   (d) Find the minimial polynomial of $\gamma = \alpha z + \alpha$ over $GF(4)$.

3. **Factoring** $y^n - 1$ (V6d)
   Consider $GF(3^3)$ defined by $GF(3^3) = \mathbb{Z}_3[x]/(x^3 + x^2 - 1)$.

   (a) Show that $\beta = x^2$ has order 13 in $GF(3^3)$.

   (b) Factor $y^{13} - 1$ into a product of monic irreducible polynomials over GF(3).

4. **Cyclic subspaces** (V6d)
   How many cyclic subspaces of $V_{735}(GF(7^2))$ are there?

5. **Existence of linear codes** (V6f)
   Does there exist a $(29, 15)$-code over $\mathbb{Z}_7$ of distance at least 6?