EE 605: Error Correcting Codes (Autumn 2015)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Problem Set 4 | Date: October 13, 2015

1. [5 points] Let F_q be a finite field. Evaluate the sum and product of the non-zero elements of F_q.

2. [5 points] Construct a finite field F_8 with 8 elements. You have to write down the addition and multiplication tables for this field.

3. [5 points] Determine all the primitive elements of F_7 and F_{17}.

4. [5 points] Determine all the prime polynomials of degree 5 in $F_2[x]$.

5. [5 points] Let α and β be elements in a field F. If α has order m, β has order n and $\gcd(m,n) = 1$, prove that $\alpha\beta$ has order mn.

6. [5 points] Let F_q be a finite field with q elements.
   (a) For any $\beta \in F_q^*$, consider the sequence $\beta, \beta^2, \beta^3, \beta^4, \ldots$. Show that the first element to repeat in this sequence is β, i.e. there exists a positive integer n such that $\beta^i \neq \beta^j$ for $1 \leq i < j \leq n-1$ and $\beta^n = \beta$.
   (b) Using the above result, show that all the elements in F_q are roots of the polynomial $x^q - x$.

7. [5 points] Let $\mathbb{F}_3$ be the finite field with three elements. Let $\mathbb{F}_3[x]$ be the set of polynomials with coefficients in $\mathbb{F}_3$.
   (a) Find the prime polynomials of degree 1 and degree 2 in $\mathbb{F}_3[x]$.
   (b) Let $g(x)$ be a degree 2 prime polynomial found in the previous part. Let $R_{\mathbb{F}_3,2}$ be the set of remainders when polynomials in $\mathbb{F}_3[x]$ are divided by $g(x)$. $R_{\mathbb{F}_3,2}$ is a field under addition and multiplication modulo $g(x)$. Find the multiplicative inverses of all the non-zero elements in $R_{\mathbb{F}_3,2}$.

8. [5 points] Find all the minimal polynomials of the field of 9 elements.

9. [5 points] Let F_q be a field with p^m elements where p is a prime and m is a positive integer. Prove that the minimal polynomial of a primitive element in F_q has degree m.

10. [5 points] Let F_q be a field with p^m elements where p is a prime and m is a positive integer. A degree m irreducible polynomial in $\mathbb{F}_p[x]$ is said to be primitive if the smallest value of N for which it divides $x^N - 1$ is $p^m - 1$. Show that the minimal polynomial of a primitive element in F_q is a primitive polynomial.