EE 605: Error Correcting Codes
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 2 : 25 points October 20, 2015

1. (5 points) State and prove Lagrange's theorem.
2. (5 points) Prove that the a cyclic group of order n has $\phi(n)$ generators where $\phi(n)$ is the Euler totient function. For argument n, this function gives the number of positive integers less than or equal to n that are relatively prime to n.
3. (5 points) Using any of the results proved in class, show that the following fields are isomorphic. You have to explicitly specify the bijection and prove that it satisfies the required properties.
   - $F = \left\{ a_0 + a_1 y + a_2 y^2 \middle| a_i \in \mathbb{F}_2 \right\}$ under $+$ and $*$ modulo $y^3 + y + 1$
   - $G = \left\{ a_0 + a_1 y + a_2 y^2 \middle| a_i \in \mathbb{F}_2 \right\}$ under $+$ and $*$ modulo $y^3 + y^2 + 1$
4. (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.
5. (5 points) Find all the minimal polynomials of the field of 27 elements.