

EE 605: Error Correcting Codes
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2011

Quiz 2 : **10 points**

Duration: 60 minutes

Every nontrivial step in a proof should be accompanied by justification.

1. Let m be a positive integer. If m is not a prime, prove that the set $\{1, 2, 3, \dots, m-1\}$ is not a group under modulo- m multiplication. [2 points]
2. Prove that a group G cannot have a subgroup H with $|H| = n-1$, where $n = |G| > 2$. [2 points]
3. Prove that a nonzero finite field element β satisfies $\beta^m = 1$ for some positive integer m if and only if m is divisible by the order of β . [3 points]
4. Construct a finite field F_8 with 8 elements. You have to write down the addition and multiplication tables for this field. [3 points]