Computer Science & Engineering Department

IIT Kharagpur

Computational Number Theory: CS60094

Tutorial VI

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1. Let $p(x) = 3x^2 + x + 4$ and $q(x) = 4x^2 + 4x + 6$ be two polynomials in $\mathbb{Z}_7[x]$. What is the $gcd(p(x), q(x))$. If $d = gcd(p(x), q(x))$, then express $d = up + vq$, where $u, v \in \mathbb{Z}_7[x]$.

2. What are the *irreducible* polynomials of degree-4 over $\mathbb{F}_2$?

3. What are the elements of $\mathbb{F}2[x]/(x^4 + x + 1)$ and show the product of $[x^3 + x] \times [x^3 + x^2 + 1]$.

4. Let G be a commutative group and H_1, H_2 are subgroups of G such that $H_1 \cap H_2 = \{1_G\}$. Prove that $H_1H_2 = \{h_1h_2 : h_1 \in H_1, h_2 \in H_2\}$ and $H_1 \times H_2 = \{(h_1, h_2) : h_1 \in H_1, h_2 \in H_2\}$ are group isomorphic.

5. Let G be a commutative group and $a, b \in G$. The orders of a and b are finite (n_a and n_b respectively) and relatively prime.
   Prove that order of ab is n_an_b.