Computer Science & Engineering Department

IIT Kharagpur

Computational Number Theory: CS60094

Tutorial IV

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1. If $\mathbb{Z}_n^*$ is *cyclic* then there are $\phi(\phi(n))$ generators of it i.e. if n has a *primitive root*, then there are $\phi(\phi(n))$ *primitive roots*.

2. Prove that a finite *integral domain* is a *field*.

3. A subring J of a ring R is called an *ideal* of R if for all $a \in J$ and $r \in R$, both ar and ra are in J. If R is commutative, then one of the conditions is sufficient.

   (a) If R is commutative and $a \in R$, prove that $J = \{ra : r \in R\}$ is an ideal.

   (b) If R is a commutative ring and $a \in R$, then $< a >= \{ra + na : r \in R,\ n \in \mathbb{Z}\}$ is the smallest ideal containing a.

   (c) If R is a commutative ring with identity and $a \in R$, then $< a >= \{ra : r \in R,\ n \in \mathbb{Z}\}$ is the smallest ideal containing a.

4. If R is a commutative ring and $a \in R$, then the ideal $< a >$ is called a *principlal ideal* generated by a. If J is an ideal we define a binary relation on R modulo J: $a, b \in R$ are related if $a - b \in J$. We write $a \equiv b (\bmod J)$.

   (a) Prove that "$\equiv (\bmod J)$" is an equivalence relation.

   (b) What is the *equivalence class* $[a]$?

   (c) Define addition '+' and multiplication '$\times$' on the quotient set R/J so that it forms a ring.