Computer Science & Engineering Department
IIT Kharagpur
Computational Number Theory: CS60094
Tutorial II

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1. In a FFT based multiplication program $a = 7345 \equiv (73, 45)$ and $b = 5439 = (54, 39)$ (in base-100) produces (394252771755).
   (a) Interpret the result.
   (b) Show the computation steps.
   (c) When the input is $a = (71, 245)$ and $b = (51, 339)$, will the result *signal* be the same? Will the interpreted value of the product be the same?
2. Show that *well-ordering principle* on the set of positive integers implies the *principle of mathematical induction*.
3. Show that the *principle of mathematical induction* implies the *well-ordering principle* of positive integers.
4. Let $(R, +, 0, \times)$ be a ring. Prove the following facts:
   (a) $a \times 0 = 0$.
   (b) $a(-b) = -(ab)$ for all $a, b \in R$.
   (c) $(-a)(-b) = ab$.
   (d) $(-1)a = -a$.
5. Let $a, b, c \in \mathbb{Z}$, $gcd(a, b) = 1$ (relatively prime), and $a|bc$. Prove that $a|c$.
6. Consider the linear congruence $ax \equiv b(\text{mod } n)$, where $a, b, n \in \mathbb{Z}$ and $n > 1$. Let $d = gcd(a, n)$.
   (a) If the linear congruence has a solution, then it has a solution in $\mathbb{Z}_n$.
   (b) If x is a solution of the linear congruence, then every integer of the form $x + ni/d$, where $i \in \mathbb{Z}$, is also a solution; and every solution is of this form.

(c) If x is a solution of the linear congruence, then $x + ni/d$, where $i \in \{0, \cdots, d-1\}$ are incongruent solutions.

(d) Every solution of the linear congruence is congruent to a solution of the form $x + ni/d$, where $i \in \{0, \cdots, d-1\}$.

7. Let m, n be relatively prime integers and both of them divides a. Prove that $mn|a$.