Course: CS 1050D – Sample Test Questions (Spring'06)

Instructor : Prasad Tetali, office: Skiles 234, email: tetali@math.gatech.edu

Please explain all your answers.

REVIEW SESSION : Monday (March 6th) 6:10pm – 7:10pm in SKILES 270

1. Show that the gcd of $8a + 3$ and $5a + 2$ is equal to 1 for all positive integers a.

2. Prove or disprove: if $g = gcd(m, n)$, then $gcd(m/g, n/g) = 1$.

3. Define a bijection.

4. Given integers a, b, and n, when is there an integer solution to $ax \equiv b \pmod{n}$?

5. What do we mean by the inverse of an integer b mod n?

6. Define the Euler ϕ function.

7. (a) Compute the Euler ϕ-function of the following integers: 15, 19, 27.

(b) For which integers m, n, is it the case that $\phi(mn) = \phi(m)\phi(n)$?

8. Suppose that $e = 3$ and $n = 23 \times 47$ in Alice's RSA cryptosystem.
Find Alice's decrypting exponent d.

9. Find the smallest nonnegative integer x that satisfies the system of congruences:

$x \equiv 6 \pmod{8}$
$x \equiv 17 \pmod{25}$

10. What is the computational significance of the Chinese Remainder Theorem?

11. Is every function from the set of natural numbers to $\{0, 1\}$ computable in a given programming language?

12. Is $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = 5x - 2|x|$ a bijection? ($\mathbf{R}$ represents the set of reals.)