CS60082/CS60094 Computational Number Theory, Spring 2010–11

Mid-Semester Test

Maximum marks: 30 | Date: February 2011 | Duration: 2 hours

Roll no: __________________ **Name:** ____

[*Write your answers in the question paper itself. Be brief and precise. Answer all questions.*]

1. (a) Let $n = p^2 q$ with p, q distinct odd primes, $p \not| (q-1)$ and $q \not| (p-1)$. Prove that factoring n is polynomial-time equivalent to computing $\phi(n)$. **(3)**

(b) Let $n = p^2 q$ with p, q odd primes satisfying $q = 2p + 1$. Argue that one can factor n in polynomial time. **(3)**

2. Let a, b, c be non-zero integers, and $d = \gcd(a, b)$.

(a) Prove that the equation

$$ax + by = c \qquad (*)$$

is solvable in *integer values* of x, y if and only if $d \mid c$. **(3)**

(b) Suppose that $d \mid c$, and (s, t) is a solution of Eqn $(*)$. Prove that all the solutions of Eqn $(*)$ can be given as $(s + k(b/d), t - k(a/d))$ for all $k \in \mathbb{Z}$. Describe how one solution (s, t) can be efficiently computed. **(3)**

(c) Compute all the (integer) solutions of the equation $21x + 15y = 60$. **(3)**

3. Let p be an odd prime, $a \in \mathbb{Z}_p^*$, and $e \in \mathbb{N}$. Prove that the multiplicative order of $1 + ap$ modulo p^e is p^{e-1}.
(**Remark:** This result can be used to obtain primitive roots modulo p^e.) **(6)**

4. (a) Which of the polynomials $x^2 \pm 7$ is irreducible modulo 19? Justify. **(3)**

(b) Using the irreducible polynomial $f(x)$ of Part (a), represent the finite field $\mathbb{F}_{361} = \mathbb{F}_{19^2}$ as $\mathbb{F}_{19}(\theta)$, where $f(\theta) = 0$. Compute $(2\theta + 3)^{11}$ in this representation of $\mathbb{F}_{361}$ using the left-to-right square-and-multiply exponentiation algorithm. Show your calculations. **(6)**