CS60082 Computational Number Theory

Class Test 1

Maximum marks: 20 February 11, 2010 **Duration:** 1 hour

[*This test is open-notes. Answer all questions. Be brief and precise.*]

1 Let $a_1, a_2, \ldots, a_n$ be non-zero integers, and $d = \gcd(a_1, a_2, \ldots, a_n)$. Prove that there exist integers $u_1, u_2, \ldots, u_n$ with the property that $u_1a_1 + u_2a_2 + \cdots + u_na_n = d$. **(6)**

2 Prove that the multivariate linear congruence $a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}$ is solvable for $x_1, x_2, \ldots, x_n$ if and only if $\gcd(a_1, a_2, \ldots, a_n, m) \mid b$. **(6)**

3 Let p be a prime > 3. Prove that 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{12}$. **(8)**