CS60082/CS60094 Computational Number Theory, Spring 2010–11

Class Test 1

Maximum marks: 20 | Date: February 16, 2011 (6:00–7:00pm) | Duration: 1 hour

---

Roll no: ____________________ **Name:** ____

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

1. In the Hensel lifting procedure discussed in the class, we lifted solutions of polynomial congruences of the form $f(x) \equiv 0 \pmod{p^e}$ to the solutions of $f(x) \equiv 0 \pmod{p^{e+1}}$. In this exercise, we investigate lifting the solutions of $f(x) \equiv 0 \pmod{p^e}$ to solutions of $f(x) \equiv 0 \pmod{p^{2e}}$, that is, the exponent in the modulus doubles every time (instead of getting incremented by only 1).

(a) Let $f(x) \in \mathbb{Z}[x]$, $e \in \mathbb{N}$, and ξ a solution of $f(x) \equiv 0 \pmod{p^e}$. Write $\xi' = \xi + kp^e$. Show how we can compute all values of k for which ξ' satisfies $f(\xi') \equiv 0 \pmod{p^{2e}}$. **(5)**

(b) It is given that the only solution of $2x^3 + 4x^2 + 3 \equiv 0 \pmod{25}$ is $14 \pmod{25}$. Using the lifting procedure of Part (a), compute all the solutions of $2x^3 + 4x^2 + 3 \equiv 0 \pmod{625}$. **(5)**

2. (a) Compute the infinite simple continued fraction expansion of $\sqrt{3}$. **(5)**

(b) For all $k \geqslant 1$, write $a_k + b_k\sqrt{3} = (2+\sqrt{3})^k$ with a_k, b_k integers. Prove that for all $n \geqslant 0$, the $(2n+1)$-th convergent of $\sqrt{3}$ is $r_{2n+1} = a_{n+1}/b_{n+1}$. **(5)**

(**Remark:** a_k, b_k for $k \geqslant 1$ constitute all the non-zero solutions of the Pell equation $a^2 - 3b^2 = 1$. Proving this requires some exposure to algebraic number theory.)