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)**

Solution Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$. The binomial theorem with the substitution $x = \xi'$ gives

$$\begin{aligned} f(\xi') &= a_d(\xi + kp^e)^d + a_{d-1}(\xi + kp^e)^{d-1} + \cdots + a_1(\xi + kp^e) + a_0 \\ &= f(\xi) + kp^e f'(\xi) + p^{2e} \times t \end{aligned}$$

for some integer t. The condition $f(\xi') \equiv 0 \pmod{p^{2e}}$ implies that $f(\xi) + kp^e f'(\xi) \equiv 0 \pmod{p^{2e}}$, that is, $f'(\xi)k \equiv -\left(\frac{f(\xi)}{p^e}\right) \pmod{p^e}$. Each solution of this linear congruence modulo p^e gives a lifted root ξ' of $f(x)$ modulo p^{2e}.

(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)**

Solution Here, $f(x) = 2x^3 + 4x^2 + 3$, so $f'(x) = 6x^2 + 8x$. For $p = 5$, $e = 2$ and $\xi = 14$, we have $f(\xi) = 2 \times 14^3 + 4 \times 14^2 + 3 = 6275$, that is, $f(\xi)/25 \equiv 251 \equiv 1 \pmod{25}$. Also, $f'(\xi) \equiv 6 \times 14^2 + 8 \times 14 \equiv 1288 \equiv 13 \pmod{25}$. Thus, we need to solve $13k \equiv -1 \pmod{25}$. Since $13^{-1} \equiv 2 \pmod{25}$, we have $k \equiv -2 \equiv 23 \pmod{25}$. It follows that the only solution of $2x^3 + 4x^2 + 3 \equiv 0 \pmod{625}$ is $14 + 23 \times 25 \equiv 589 \pmod{625}$.

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

Solution We have the following sequence of computations:

$$
\begin{aligned}
&\xi_0 = \sqrt{3}, \quad a_0 = \lfloor \xi_0 \rfloor = 1,\\
&\xi_1 = 1/(\xi_0 - a_0) = 1/(-1+\sqrt{3}) = (1+\sqrt{3})/2, \quad a_1 = \lfloor \xi_1 \rfloor = 1,\\
&\xi_2 = 1/(\xi_1 - a_1) = 2/(-1+\sqrt{3}) = 1+\sqrt{3}, \quad a_2 = \lfloor \xi_2 \rfloor = 2,\\
&\xi_3 = 1/(\xi_2 - a_2) = 1/(-1+\sqrt{3}) = (1+\sqrt{3})/2, \quad a_3 = \lfloor \xi_3 \rfloor = 1,\\
&\ldots
\end{aligned}
$$

It follows that $\sqrt{3} = \langle 1, 1, 2, 1, 2, 1, 2, \ldots \rangle = \langle 1, \overline{1, 2} \rangle$.

(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)**

Solution Let $\zeta_k = \langle \underbrace{1, 2, 1, 2, \ldots, 1, 2}_{1,2 \text{ repeated } k \text{ times}}, 1 \rangle$. It suffices to show that $\zeta_k = \dfrac{b_{k+1}}{a_{k+1} - b_{k+1}}$ for all $k \geqslant 0$. We proceed by induction on k. For $k = 0$, we have $a_1 = 2$ and $b_1 = 1$, whereas $\zeta_0 = \langle 1 \rangle = 1 = \dfrac{1}{2-1} = \dfrac{b_1}{a_1 - b_1}$. So assume that $k \geqslant 0$ and $\zeta_k = \dfrac{b_{k+1}}{a_{k+1} - b_{k+1}}$. But then $\zeta_{k+1} = \langle 1, 2, \zeta_k \rangle = 1 + \dfrac{1}{2 + \frac{1}{\zeta_k}} = 1 + \dfrac{1}{2 + \frac{a_{k+1} - b_{k+1}}{b_{k+1}}} = 1 + \dfrac{b_{k+1}}{a_{k+1} + b_{k+1}} = \dfrac{a_{k+1} + 2b_{k+1}}{a_{k+1} + b_{k+1}}$. On the other hand, $a_{k+2} + b_{k+2}\sqrt{3} = (2+\sqrt{3})(a_{k+1} + b_{k+1}\sqrt{3}) = (2a_{k+1} + 3b_{k+1}) + (a_{k+1} + 2b_{k+1})\sqrt{3}$, that is, $a_{k+2} = 2a_{k+1} + 3b_{k+1}$ and $b_{k+2} = a_{k+1} + 2b_{k+1}$. Consequently, $\dfrac{b_{k+2}}{a_{k+2} - b_{k+2}} = \dfrac{a_{k+1} + 2b_{k+1}}{a_{k+1} + b_{k+1}} = \zeta_{k+1}$. This completes the inductive proof.

(**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.)