**Foundations of Computer Algebra. CS424b: Quiz 5+6. UWO, April 5, 2006.**

| **Student ID number**: |
| --- |
| **Student Last Name**: |

**Guidelines.** Every printed document is allowed but computers and calculators are not. The duration of the quiz is 40 minutes. This double quiz consists of two exercises located on pages 2 and 4: **Each of these exercises has the value of one quiz.** All answers should be written in the *answer boxes*. No justifications for the answers are needed, unless explicitly required. You are expected to do this quiz on your own without assistance from anyone else in the class. If possible, please avoid pencils and use pens with dark ink. Thank you.

**Notations.** The set of non-negative integer numbers, integer numbers and rational numbers are denoted respectively $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, as usual. For an integer $n \in \mathbb{Z}$ the set of the multiples of $n$ (all of them: positive, null or negative) is denoted by $n\mathbb{Z}$. For an integer $n \in \mathbb{Z}$ the residue class ring of the binary relation $(a, b) \longmapsto a \equiv b \mod n$ is denoted by $\mathbb{Z}/n\mathbb{Z}$, as usual. For a ring $\mathbb{A}$, we denote by $\mathbb{A}[x]$ the ring of univariate polynomials in $x$ with coefficients in $\mathbb{A}$.

**Formulas for Linear Symbolic Newton Iteration.** Let $R$ be an Euclidean domain with a regular Euclidean size $\delta$. Let $p \in R$ be a prime element. Let $\phi \in R[y]$ and let $a, a_0 \in R$ such that

1. $\phi(a) = 0$,
2. $a \equiv a_0 \mod p$,
3. $\phi'(a_0) \neq 0 \mod p$.

If $a$ is unknown, but $\phi$ and $a_0$ are known then we can compute a $p$-adic expansion of $a$ as follows. Let $(a_0, a_1, \ldots, a_d)$ be a $p$-adic expansion of $a$ w.r.t. $p$. Let $k < d + 1$ be a positive integer. Recall that the element

$$a^{(k)} = a_0 + a_1 p + \cdots a_{k-1} p^{k-1} \tag{1}$$

is a $p$-adic approximation of $a$ at order $k$. Let us denote by $\Phi_p$ the canonical homomorphism from $R$ to $R/\langle p \rangle$. The following formula computes $a_k$ from $a^{(k)}$:

$$\Phi_p(\frac{\phi(a^{(k)})}{p^k}) = -\Phi_p(\phi'(a_0))\Phi_p(a_k) \tag{2}$$

**Exercise 1.** In $\mathbb{Q}[x]$ we consider the polynomial $b = x^4 + 6x^3 + 11x^2 + 6x + 1$. We assume that $b$ is the square of a polynomial $a$ in $\mathbb{Q}[x]$. **Using symbolic Newton Iteration**, compute such a polynomial $a$.

**Answer 1**

**Answer 2**

**Exercise 2.** **Using Symbolic Newton Iteration**, show that $529$ is the square of a positive integer $a$ and compute $a$. **Hint:** $529 \equiv 1 \mod 11$ and $528 = 11 \times 48$.

**Answer 3**

**Answer 4**

**Answer 5**