Foundations of Computer Algebra. CS424b: Quiz 3+4. UWO, March 22, 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. Let R be a commutative ring with 1. We recall the algorithm for computing the inverse of a polynomial $f \in R[x]$ modulo a power of x.

Input: $f \in R[x]$ such that $f(0) = 1$ and $\ell \in \mathbb{N}$.

Output: $g \in R[x]$ such that $f\, g \equiv 1 \mod x^{\ell}$

g_0 := 1
r := $\lceil \log_2(\ell) \rceil$
for $i = 1 \cdots r$ **repeat**
  g_i := $(2g_{i-1} - f\, {g_{i-1}}^2) \mod x^{2^i}$
return g_r

Exercise 1. Let $f = x^4 + 1$ be in $\mathbb{Z}[x]$. Compute the inverse of f modulo x^5. Note that the example has been chosen such that computations can easily be made by hand.

Answer 1

(We just give elements of corrections.) Applying the algorithm recalled above, we compute

- $r = 3$,
- $g_0 = 1$,
- $g_1 = 1$,
- $g_2 = 1$,
- $g_3 = -x^4 + 1$, the desired answer.

Exercise 2. The algorithm recalled above computes the inverse of $f \in R[x]$ modulo x^ℓ. Using Newton iteration step

$$g_{i+1} = g_i - \frac{\phi(g_i)}{\phi'(g_i)} \tag{1}$$

derive an algorithm which, given $f \in R[x]$ and $\ell \in \mathbb{N}$, computes $g \in R[x]$ such that $fg^2 \equiv 1 \mod x^\ell$ holds. Then, prove that the algorithm is correct.

Answer 2

(We just give elements of corrections.) By analogy to what we did for the modular inversion algorithm, we consider

$$\Psi(g) = 1/g^2 - f, \tag{2}$$

which leads to the Newton iteration step:

$$g_{i+1} = \frac{3g_i - fg_i^3}{2} \tag{3}$$

For this to bring an algorithm, one needs to check that the following implication holds:

$$fg_i^2 \equiv 1 \mod x^{2^i} \implies fg_{i+1}^2 \equiv 1 \mod x^{2^{i+1}}. \tag{4}$$

The calculations involves the following algorithm:

$$x^3 - 6x^2 + 9x - 4 = (x-1)^2(x-4). \tag{5}$$