Foundations of Computer Algebra. CS424b: Quiz 2. UWO, April 11, 2007.

Student ID number:
Student Last Name:

Guidelines. Every printed document is allowed but computers and calculators are not. The duration of the quiz is 50 minutes. This quiz consists of two exercises located on pages 2 and 4: 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 $a = x^8 + 1$, $b = x^4 + x + 1$, $f = x^4 + x^3 + 1$ be in $\mathbb{Q}[x]$.

1. Compute the inverse of f modulo x^5.
2. Deduce the quotient and the remainder in the Euclidean division of a w.r.t. b.

Note that the example has been chosen such that computations can easily be carried out by hand.

Answer 1

Answer 2

Exercise 2. The goal of this exercise is to understand how the *fast division with remainder* is slow when the underlying polynomial multiplication is not fast.

Let n be a non-negative integer. Let $g \in R[x]$ be a polynomial of degree less than n and let $f \in R[x]$ be a polynomial of degree less than $2n$. For this exercise, we rely on classical "quadratic" polynomial multiplication. Hence, **we ignore** all the tricks (Karatsuba, FFT) learnt in class.

1. Using classical arithmetic what is the number of operations in R for computing $g^2 \mod x^{2n}$.
2. Using classical arithmetic what is the number of operations in R for computing $fg^2 \mod x^{2n}$.
3. Deduce a (sharp) upper bound for the algorithm recalled on the first page.
4. Deduce a (sharp) upper bound for the *(not so) fast division with remainder* when applied to a pair of polynomials in $R[x]$ with respective degrees m and n, assuming that $m - n + 1$ is a power of 2.
5. Compare with classical division.

Answer 3

Answer 4

Answer 5

Answer 6