Homework 3

Algorithms for Elementary Algebraic Geometry

Math 191, Fall Quarter 2007

Due Friday, October 26, 2007.

1. In words, sketch an algorithm which solves the *ideal membership problem* in $k[x]$, that is, a procedure which, given polynomials f and $f_1, \ldots, f_s$ in $k[x]$, decides whether $f \in \langle f_1, \ldots, f_s \rangle$. Use this method, with help from a computer algebra system, to decide whether in $\mathbb{Q}[x]$ we have
$$x^2 - 4 \in \langle x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2 \rangle.$$
2. Use a computer algebra package to compute
$$\mathrm{GCD}(x^3 - 1, x^6 - 1), \quad \mathrm{GCD}(x^{19} - 1, x^7 - 1), \quad \mathrm{GCD}(x^{99} - 1, x^{27} - 1).$$
Can you conjecture a formula for $\mathrm{GCD}(x^m - 1, x^n - 1)$ for general m and n? (You do not need to prove your conjecture.)
3. Let $f \in \mathbb{C}[x]$ be nonzero.
   (a) Show that f factors completely. That is, we can write
   $$f = c(x - a_1)^{r_1} \cdots (x - a_m)^{r_m}$$
   for some nonzero $c \in \mathbb{C}$, pairwise distinct $a_1, \ldots, a_m \in \mathbb{C}$ and positive integers $r_1, \ldots, r_m$.
   (b) Show that $V(f) = \{a_1, \ldots, a_m\}$.
   (c) Let $f_{\mathrm{red}} := (x - a_1) \cdots (x - a_m)$ (the **square-free part of** f). Show that $I(V(f)) = \langle f_{\mathrm{red}} \rangle$.
   (d) The formal derivative of a polynomial
   $$p = p_0 + p_1 x + \cdots + p_d x^d \in \mathbb{C}[x]$$
   is defined to be the polynomial
   $$p' = p_1 + 2p_2 x + \cdots + d p_d x^{d-1}.$$
   Prove that
   $$\mathrm{GCD}(f, f') = (x - a_1)^{r_1 - 1} \cdots (x - a_m)^{r_m - 1}.$$
   (Exercises 13 and 14 in Section I.5 of the book provide more hints.)
   (e) Show that $f_{\mathrm{red}} = \frac{f}{\mathrm{GCD}(f, f')}$. This means that we can compute f_{red} without factoring f—purely symbolically!
   (f) What is
   $$I(V(x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1))?$$
   (You may want to use a computer algebra package.)