MACM 401/MATH 701/MATH 819/CMPT 881
Assignment 5 Spring 2011.

Michael Monagan

This assignment is to be handed in by Monday March 28th at the start of class.
For problems involving Maple calculations and Maple programming, you should submit a printout of a Maple worksheet of your Maple session.
Late Penalty: -20% for up to 24 hours late. Zero after that.

Question 1: Factorization in $\mathbb{Z}_p[x]$ (30 marks)

(a) Factor the following polynomials over $\mathbb{Z}_{11}$ using the Cantor-Zassenhaus algorithm.

$$a_1 = x^4 + 8\,x^2 + 6\,x + 8,$$

$$a_2 = x^6 + 3\,x^5 - x^4 + 2\,x^3 - 3\,x + 3,$$

$$a_3 = x^8 + x^7 + x^6 + 2\,x^4 + 5\,x^3 + 2\,x^2 + 8.$$

Use Maple to do all polynomial arithmetic, that is, you can use the `Gcd(...) mod p` and `Powmod(...) mod p` commands etc., but not `Factor(...) mod p`.

(b) Compute the square-roots of the integers $a = 3, 5, 7$ in the integers modulo p, if they exist, for $p = 10^{20} + 129 = 100000000000000000129$ by factoring the polynomial $x^2 - a \bmod p$ using the Cantor-Zassenhaus algorithm. Show your working.

Question 2: A linear x-adic Newton iteration (15 marks).

Let p be an odd prime and let $a(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}_p[x]$ with $a_0 \neq 0$ and $a_n \neq 0$. Suppose $\sqrt{a_0} = \pm u_0 \bmod p$. The goal of this question is to design an x-adic Newton iteration algorithm that given u_0, determines if $u = \sqrt{a(x)} \in \mathbb{Z}_p[x]$ and if so computes u. Let

$$u = u_0 + u_1 x + ... + u_{k-1} x^{k-1} + ... + u_{n-1} x^{n-1}.$$

Derive the update formula for u_k given $u^{(k)}$. Show your working.

Now implement your algorithm in Maple and test it on the two polynomials $a_1(x)$ and $a_2(x)$ below using $p = 101$ and $u_0 = +5$. Please print out the sequence of values of $u_0, u_1, u_2, ...$ that your program computes. Note, one of the polynomials has a $\sqrt{}$ in $\mathbb{Z}_p[x]$, the other does not.

$$a_1 = 81\,x^6 + 16\,x^5 + 24\,x^4 + 89\,x^3 + 72\,x^2 + 41\,x + 25$$

$$a_2 = 81\,x^6 + 46\,x^5 + 34\,x^4 + 19\,x^3 + 72\,x^2 + 41\,x + 25$$

Question 3: Polynomial Resultants (15 marks)

Consider the following pairs of polynomials

$$f_1 = 2x^3 + 2x - x^2 - 1,\ g_1 = x^2 - 2$$

$$f_2 = (x^2 + 1 - x)z + (x^4 + 2\,x^2 - x),\ g_2 = z^2 + 1 \ \text{ and}$$

$$f_3 = 2yx^3 - x^2y^2 + (2y + 1)x - 3,\ g_3 = 2x^2 - (3 - y^2)x + (2y^2 - 5).$$

Compute the resultants $\mathrm{res}_x(f_1, g_1)$, $\mathrm{res}_z(f_2, g_2)$ and $\mathrm{res}_x(f_3, g_3)$ (please note which variable is being eliminated!) using the Maple command `resultant` (so that you know what the answers are). In class we showed how to modify the natural Euclidean algorithm to compute the resultant. Program this in Maple. Execute it on the above inputs. Now modify the primitive Euclidean algorithm to compute the resultant using pseudo-division. Program your algorithm in Maple. Execute it on the above inputs.

Question 4: Rational Function Integration (20 marks)

Reference: sections 11.3, & 11.4 and 11.5.

(a) Calculate the Trager-Rothstein resultant for the rational function integral below by hand by constructing Sylvester's matrix for the resultant and computing the determinant by hand. Complete the integral.

$$\int \frac{2x + 1}{x^2 - 2}\mathrm{dx}.$$

(b) Integrate the three rational functions below as follows. First compute the rational function part of integral using either Hermite's method or Horrowitz's method (or both if you wish). Then compute the logarithmic part (if any) using the Trager-Rothstein resultant. Use Maple to help with arithmetic e.g. you may use `gcd`, `gcdex`, `solve`, `resultant` etc.

$$f_1 = \frac{3\,x^5 - 2\,x^4 - x^3 + 2\,x^2 - 2\,x + 2}{x^6 - x^5 + x^4 - x^3}$$

$$f_2 = \frac{4\,x^7 - 16\,x^6 + 28\,x^5 - 351\,x^3 + 588\,x^2 - 738}{2\,x^7 - 8\,x^6 + 14\,x^5 - 40\,x^4 + 82\,x^3 - 76\,x^2 + 120\,x - 144}$$

$$f_3 = \frac{6\,x^5 - 4\,x^4 - 32\,x^3 + 12\,x^2 + 34\,x - 24}{x^6 - 8\,x^4 + 17\,x^2 - 8}$$