MACM 401/MATH 701/MATH 819
Assignment 5, Spring 2015.

Michael Monagan

This assignment is to be handed in by Monday March 30th by 12 noon. Late Penalty: -20% for up to 48 hours late. Zero after that. For problems involving Maple calculations and Maple programming, you should submit a printout of a Maple worksheet of your Maple session.

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) As an application, compute the square-roots of the integers $a = 3, 5, 7$ in the integers modulo p, if they exist, for $p = 10^{20} + 129 = 10000000000000000129$ by factoring the polynomial $x^2 - a \bmod p$ using the Cantor-Zassenhaus algorithm. Show your working. You will have to use `Powmod` here.

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 Newton 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: Cost of the linear p-adic Newton iteration (15 marks)

Let $a \in \mathbb{Z}$ and $u = \sqrt{a}$. Suppose $u \in \mathbb{Z}$. The linear P-adic Newton iteration for computing u from $u \bmod p$ that we gave in class is based on the following linear p-adic update formula:

$$u_k = -\frac{\phi_p(f(u^{(k)})/p^k)}{f'(u_0)} \bmod p.$$

where $f(u) = a - u^2$. A direct coding of this update formula for the $\sqrt{}$ problem in $\mathbb{Z}$ led to the code below where I've modified the algorithm to stop if the error $e < 0$ instead of using a lifting bound B.

```
ZSQRT := proc(a,u0,p) local U,pk,k,e,uk,i;
    u := mods(u0,p);
    i := modp(1/(2*u0),p);
    pk := p;
    for k do
        e := a - u^2;
        if e = 0 then return(u); fi;
        if e < 0 then return(FAIL) fi;
        uk :=  mods( iquo(e,pk)*i, p );
        u := u + uk*pk;
        pk := p*pk;
    od;
end:
```

The running time of the algorithm is dominated by the squaring of `u` in `a := a - u^2` and the long division of `u` by `pk` in `iquo(e,pk)`. Assume the input a is of length n base p digits. At the beginning of iteration k, $u = u^{(k)} = u_0 + u_1 p + ... + u_{k-1}p^{k-1}$ is an integer of length at most k base p digits. Thus squaring `u` costs $\mathrm{O}(k^2)$ (assuming classical integer arithmetic). In the division of `e` by `pk` $= p^k$, `e` will be an integer of length n base p digits. Assuming classical integer long division is used, this division costs $O((n-k+1)k)$. Since the loop will run $k = 1, 2, ..., n/2$ for the $\sqrt{}$ problem the total cost of the algorithm is dominated by $\sum_{k=1}^{n/2}(k^2 + (n-k+1)k) \in O(n^3)$.

Redesign the algorithm so that the overall time complexity is $O(n^2)$ assuming classical integer arithmetic. Prove that your algorithm is $O(n^2)$. Now implement your algorithm in Maple and verify that it works correctly and that the running time is $\mathrm{O}(n^2)$. Use the prime $p = 9973$.

Hint 1: $e = a - u^2 = a - u^{(k)^2} = a - (u^{(k-1)} + u_{k-1}p^{k-1})^2 = (a - u^{(k-1)^2}) - 2u^{k-1}u_{k-1}p^{k-1} - u_{k-1}^2 p^{2k-2}$. Notice that $a - u^{(k-1)^2}$ is the error that was computed in the previous iteration.
Hint 2: We showed that the algorithm for computing the p-adic representation of an integer is $\mathrm{O}(n^2)$. Notice that it does not divide by p^k, rather, it divides by p each time round the loop.

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.

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

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

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