MACM 401/MATH 701/MATH 801
Assignment 4, Spring 2017.

Michael Monagan

This assignment is to be handed in by Monday March 13th by 4pm.
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 48 hours late. Zero after that.

Question 1: P-adic Lifting (20 marks)

Reference: Section 6.2 and 6.3.

(a) By hand, determine the p-adic representation of the integer $u = 116$ for $p = 5$, first using the positive representation, then using the symmetric representation for $\mathbb{Z}_5$.

(b) Theorem: Let $u, p \in \mathbb{Z}$ with $p > 2$. If $-\frac{p^n}{2} \le u < \frac{p^n}{2}$ there exist unique integers $u_0, u_1, \ldots, u_{n-1}$ such that $u = u_0 + u_1 p + \cdots + u_{n-1} p^{n-1}$ and $-\frac{p}{2} \le u_i < \frac{p}{2}$.

Prove uniqueness.

(c) Determine the cube-root, *if it exists*, of the following polynomials

$$a(x) = x^6 - 531x^5 + 94137x^4 - 5598333x^3 + 4706850x^2 - 1327500x + 125000,$$
$$b(x) = x^6 - 406\,x^5 + 94262\,x^4 - 5598208\,x^3 + 4706975\,x^2 - 1327375\,x + 125125$$

using reduction mod 5 and linear p-adic lifting. You will need to derivive the update formula by modifying the update formula for computing the $\sqrt{a(x)}$.

Factor the polynomials so you know what the answers are. Express your the answer in the p-adic representation. To calculate the initial solution $u_0 = \sqrt[3]{a} \bmod 5$ use any method. Use Maple to do all the calculations.

Question 2: Hensel lifting (15 marks)

Reference: Section 6.4 and 6.5.

(a) Given

$$a(x) = x^4 - 2\,x^3 - 233\,x^2 - 214\,x + 85$$

and image polynomials

$$u_0(x) = x^2 - 3\,x - 2 \quad \text{and} \quad w_0(x) = x^2 + x + 3,$$

satisfying $a \equiv u_0\,w_0 \pmod 7$, lift the image polynomials using Hensel lifting to find (if there exist) u and w in $\mathbb{Z}[x]$ such that $a = uw$.

(b) Given

$$b(x) = 48\,x^4 - 22\,x^3 + 47\,x^2 + 144$$

and an image polynomials

$$u_0(x) = x^2 + 4\,x + 2 \quad \text{and} \quad w_0 = x^2 + 4\,x + 5$$

satisfying $b \equiv 6\,u_0\,w_0 \pmod 7$, lift the image polynomials using Hensel lifting to find (if there exist) u and w in $\mathbb{Z}[x]$ such that $b = uw$.

Question 3: Determinants (25 marks)

Consider the following 3 by 3 matrix A of polynomials in $\mathbb{Z}[x]$ and its determinant d.

```
> P := () -> randpoly(x,degree=2,dense):
> A := Matrix(3,3,P);
```

$$A := \begin{bmatrix} -55 - 7\,x^2 + 22\,x & -56 - 94\,x^2 + 87\,x & 97 - 62\,x \\ -83 - 73\,x^2 - 4\,x & -82 - 10\,x^2 + 62\,x & 71 + 80\,x^2 - 44\,x \\ -10 - 17\,x^2 - 75\,x & 42 - 7\,x^2 - 40\,x & 75 - 50\,x^2 + 23\,x \end{bmatrix}$$

```
> d := LinearAlgebra[Determinant](A);
```

$$d := -224262 - 455486\,x^2 + 55203\,x - 539985\,x^4 + 937816\,x^3 + 463520\,x^6 - 75964\,x^5$$

(a) (15 marks) Let A by an n by n matrix of polynomials in $\mathbb{Z}[x]$ and let $d = \det(A)$. Develop a modular algorithm for computing $d = \det(A) \in \mathbb{Z}[x]$. Your algorithm will compute determinants of A modulo a sequence of primes and apply the CRT. For each prime p it will compute the determinant in $\mathbb{Z}_p[x]$ by evaluation and interpolation. In this way we reduce computation of a determinant of a matrix over $\mathbb{Z}[x]$ to many computations of determinants of matrices over $\mathbb{Z}_p$, a field, for which ordinary Gaussian elimination, which does $O(n^3)$ arithmetic operations in $\mathbb{Z}_p$, may be used.

You will need bounds for $\deg d$ and $||d||_\infty$. Use primes $p = [101, 103, 107, ...]$ and use Maple to do Chinese remaindering. Use $x = 1, 2, 3, ...$ for the evaluation points and use Maple for interpolation. Implement your algorithm in Maple and test it on the above example.

To reduce the coefficients of the polynomials in A modulo $p = 7$ in Maple use

```
> B := A mod p;
```

To evaluate the polynomials in B at $x = \alpha$ modulo p in Maple use

```
> C := eval(B,x=alpha) mod p;
```

To compute the determinant of a matrix C over $\mathbb{Z}_p$ in Maple use

```
> Det(C) mod p;
```

(b) (10 marks) Suppose A is an n by n matrix over $\mathbb{Z}[x]$ and $A_{i,j} = \sum_{k=0}^{d} a_{i,j,k} x^k$ and $|a_{i,j,k}| < B^m$. That is A is an n by n matrix of polynomials of degree at most d with coefficients at most m base B digits long. Assume the primes satisfy $B < p < 2B$ and that arithmetic in $\mathbb{Z}_p$ costs $O(1)$. Estimate the time complexity of your algorithm in big O notation as a function of n, m and d. Make reasonable simplifying assumptions such as $n < B$ and $d < B$ as necessary. State your assumptions. Also helpful is

$$\ln n! < n \ln n \quad \text{for} \quad n > 1.$$

Question 4: A linear x-adic Newton iteration (15 marks).

Let p be an odd prime and let $a(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}_p[x]$ 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.

(a) Let

$$u = u_0 + u_1 x + \ldots + u_{k-1} x^{k-1} + u_k x^k + \ldots$$

Derive the Newton update formula for u_k. Show your working.

(b) Now test your update formula 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 $u_0, u_1, u_2, \ldots$ as you compute them. Note, one of the polynomials has a $\sqrt{\ }$ in $\mathbb{Z}_p[x]$, the other does not. So you will need to work out when the algorithm should stop lifting.
Do all calculations in Maple.

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

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

(c) The update formula requires $u_0 \neq 0$. Explain briefly what you should you do if $a_0 = 0$ and you want to compute $\sqrt{a(x)} \in \mathbb{Z}_p[x]$ if it exists.