MACM 401/MATH 819
Assignment 4, Spring 2015.

Michael Monagan

This assignment is to be handed in by Monday March 16th by 12:00 midday (before 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 48 hours late. Zero after that.

Question 1: *P*-adic Lifting (15 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 $\mathbb{Z}_5$.

By hand or using Maple, determine the p-adic representation for the polynomial $u(x) = 28\,x^2 + 24\,x + 58$ for $p = 3$ for both the positive and symmetric representation for for $\mathbb{Z}_3$.

(b) 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);
```

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

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

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

(a) 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) 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: Factorization in $\mathbb{Z}[x]$ (25 marks)

Factor the following polynomials in $\mathbb{Z}[x]$.

$$p_1 = x^{10} - 6\,x^4 + 3\,x^2 + 13$$

$$p_2 = 8\,x^7 + 12\,x^6 + 22\,x^5 + 25\,x^4 + 84\,x^3 + 110\,x^2 + 54\,x + 9$$

$$p_3 = 9\,x^7 + 6\,x^6 - 12\,x^5 + 14\,x^4 + 15\,x^3 + 2\,x^2 - 3\,x + 14$$

$$p_4 = x^{11} + 2\,x^{10} + 3\,x^9 - 10\,x^8 - x^7 - 2\,x^6 + 16\,x^4 + 26\,x^3 + 4\,x^2 + 51\,x - 170$$

For each polynomial, first compute its square free factorization. You may use the Maple command `gcd(...)` to do this. Now factor each non-linear square-free factor as follows. Use the Maple command `Factor(...) mod p` to factor the square-free factors over $\mathbb{Z}_p$ modulo the primes $p = 13, 17, 19, 23$. From this information, determine whether each polynomial is irreducible over $\mathbb{Z}$ or not. If not irreducible, try to discover what the irreducible factors are by considering combinations of the modular factors and Chinese remaindering (if necessary) and trial division over $\mathbb{Z}$.

Using Chinese remaindering here is not efficient in general. Why? Thus for the polynomial p_4, use Hensel lifting instead. That is, using a suitable prime of your choice from $13, 17, 19, 23$, Hensel lift each factor mod p, then determine the irreducible factorization of p_4 over $\mathbb{Z}$.