MACM 401/MATH 701/MATH 819 Assignment 4, Spring 2007.

Michael Monagan

This assignment is to be handed in by Tuesday March 13th before 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 each day late.

Question 1: Resultants (10 marks)

(a) Let A, B be non-zero polynomials in $\mathbb{Z}[x]$. Let $\deg A = m$ and $\deg B = n$ and let c be an integer. Let $\text{res}(A, B)$ denote the resulant of A and B. Complete the identities.

$$\text{res}(A, B) = \;\; ?? \;\; \text{res}(B, A) \;\; \text{and}$$

$$\text{res}(cA, B) = \;\; ?? \;\; \text{res}(A, B).$$

(b) Let A, B be two non-zero polynomials in $\mathbb{Z}[x]$. Let $A = G\bar{A}$ and $B = G\bar{B}$ where $G = \gcd(A, B)$. Recall that a prime p in the modular gcd algorithm is unlucky if $p|R$ where $R = \text{res}(\bar{A}, \bar{B}) = 0$ is the resultant of $\bar{A}$ and $\bar{B}$, an integer.

Consider the following pair of polynomials (from assignment 4)

$$A \;=\; 58\,x^4 - 415\,x^3 - 111\,x + 213, \quad \text{and}$$

$$B \;=\; 69\,x^3 - 112\,x^2 + 413\,x + 113.$$

They are relatively prime, i.e., $G = 1$, $\bar{A} = A$ and $\bar{B} = B$. Using Maple compute the resultant R and identify all unlucky primes. For each unlucky prime p compute the gcd of the polynomials A and B modulo p to verify that the primes are indeed unlucky.

Question 2: P-adic Lifting (20 marks)

Reference: Section 6.3.

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

Using Maple, determine the p-adic representation for the polynomial

$$u(x) = 28\,x^2 + 24\,x + 58$$

with $p = 3$ using, first the positive representation for $\mathbf{Z}_3$, then the symmetric representation.

(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. Factor the polynomials so you know what the answers are. Express 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 the calculations.

Question 3: Hensel lifting (20 marks)

Reference: Section 6.4 and 6.5.

(a) Given

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

and image polynomials

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

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

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

and an image polynomials

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

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

Question 4: Determinants (20 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 := linalg[randmatrix](3,3,entries=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 := linalg[det](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 costs $O(n^3)$ arithmetic operations in $\mathbb{Z}_p$, may be used.

You will need to 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

```
> p := 7: phip := proc(f) f mod p end:
> B := map( phip, A );
```

To evaluate the polynomials in B at $x = alpha$ (mod p) in Maple use

```
> alpha := 1: phix := proc(f) Eval(f,x=alpha) mod p end:
> C := map( phix, B );
```

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. Also helpful is $\ln n! < n \ln n$. State your assumptions.