MACM 401/MATH 701/MATH 819 Assignment 4, Spring 2009.

Michael Monagan

This assignment is to be handed in by Tuesday March 10th 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: Resultants (15 marks)

(a) Calculate the resultant of $A = 3x^2 + 3$ and $B = (x-2)(x+5)$ by hand.

(b) Let A, B be non-constant polynomials in $\mathbb{Z}[x]$ and $c \in \mathbb{Z}$. Let $\text{res}(A, B)$ denote the resulant of A and B. From the definition, determine $f(c)$ so that

$$\text{res}(cA, B) = \quad f(c)\ \text{res}(A, B).$$

(c) 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 iff $p|R$ 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 3.

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

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

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 (15 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 (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 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);
```

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

```
> d := linalg[det](A);
```

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

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

Question 5: (15 marks) (MACM 401 and MATH 701 students only)

For the Sparse Multivariate Polynomial data structure that you designed and implemented on assignment 2, implement a Maple procedure `SMPdiv(A,B)` that outputs the quotient Q if $B|A$ otherwise outputs FAIL. Test your routine on the examples in Question 6 below.

Question 6: (25 marks) (MATH 819 students only)

If you used a recursive form for the SMP polynomial data structure on your last assignment, use a distributed form this time. And if you used a distributed form on your last assignment use a recursive form this time. Implement the same 5 Maple procedures

- `Maple2SMP` - to convert from Maple's expanded form to SMP,
- `SMP2Maple` - to convert from SMP to Maple's expanded form,
- `SMPadd` - to add two polynomials,
- `SMPmul` - to multiply two SMP polynomials,
- `SMPdiv` - to divide two SMP polynomials.

Use Maple to do coefficient and exponent arithmetic. Test your routine on the following

```
> a := randpoly([x,y,z],degree=6,terms=15);
> b := randpoly([x,y,z],degree=6,terms=15);
> A := Maple2SMP(a);
> B := Maple2SMP(b);
> C := SMPadd(A,B);
> a+b - SMP2Maple(C));
> C := SMPmul(A,B);
> expand(a*b) - SMP2Maple(C); # should output 0
> SMPdiv(A,B); # should output FAIL
> Q := SMPdiv(C,A);
> expand(b-SMP2Maple(Q)); # should output 0
```