MACM 401/MATH 701/MATH 819/CMPT 881 Assignment 2, Spring 2011.

Michael Monagan

This assignment is to be handed in by Thursday February 10th at the beginning of class.
Late Penalty: -20% for up to 24 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: Univariate and Multivariate Polynomials (15 marks)

Reference sections 2.5 and 2.6

(a) Program the *extended* Euclidean algorithm for $\mathbb{Q}[x]$ in Maple. Use the Maple command `quo(a,b,x)` to compute the quotient of a divided b. Remember, you need to explicitly expand products in Maple using the `expand` command. Your program should take as input two non-zero polynomials $a, b \in \mathbb{Q}[x]$. It should return (s, t, g) where g is the *monic* gcd of a and b and $sa + tb = g$ holds. Execute your program on the following inputs.

```
a := randpoly(x,dense,degree=5);
b := randpoly(x,dense,degree=4);
```

Check that your output agrees with the output from Maple's `g := gcdex(a,b,x,'s','t');` command.

(b) Consider

$$a(x) = x^3 - 1, b(x) = x^2 + 1, c(x) = x^2.$$

Apply the algorithm in the proof of theorem 2.6 to solve the polynomial diophantine equation $\sigma a + \tau b = c$ for $\sigma, \tau \in \mathbb{Q}[x]$ satisfying $\deg \sigma < \deg b - \deg g$ where g is the monic gcd of a and b. Use Maple's gcdex command to solve $sa + tb = g$ for $s, t \in \mathbb{Q}[x]$ or your algorithm from part (a) above.

(c) Consider the following polynomial in $\mathbb{Z}[x, y]$.

$$2xy^3 + 3x^3 + 5x^2y^2 + 7xy + 8yx^2 + 9y^5$$

Write the polynomial with terms sorted in descending pure lexicographical order with $x > y$ and, secondly, graded lexicographical order with $x > y$.

Question 2: The Primitive Euclidean Algorithm (15 marks)

Reference section 2.7

(a) Calculate the content and primitive part of the following polynomial $a \in \mathbf{Z}[x, y]$, first as a polynomial in $\mathbb{Z}[y][x]$ and then as a polynomial in $\mathbb{Z}[x][y]$, i.e., first with x the main variable then with y the main variable. Use the Maple command `gcd` to calculate the GCD of the coefficients. The `coeff` and `collect` commands may also be useful.

```
> a := expand( (x^4-3*x^3*y-x^2-y)*(8*x-4*y+12)*(2*y^2-2) );
```

(b) Calculate the pseudo-remainder p and the pseudo-quotient q of the polynomials $a(x)$ divided by $b(x)$ where $a, b \in \mathbf{Z}[y][x]$. Do this by dividing ma by b using the division algorithm. You may use Maple to assist you with the polynomial arithmetic.

```
> a := 2*x^3-(y+1)*x^2-x+y;
> b := (y+2)*x^2-2*x+y;
```

(c) Given the following polynomials $a, b \in \mathbf{Z}[x, y]$, calculate the $\mathrm{GCD}(a, b)$ using the primitive PRS algorithm with x the main variable.

```
> a := expand( (x^4-3*x^3*y-x^2-y)*(2*x-y+3)*(8*y^2-8) );
> b := expand( (x^3*y^2+x^3+x^2+3*x+y)*(2*x-y+3)*(12*y^3-12) );
```

You may use the Maple command `prem`, `gcd` and `divide` for the intermediate calculations. You should obtain

$$\mathrm{GCD}(a, b) \;=\; \pm 8\,xy \mp 4\,y^2 \mp 8\,x \pm 16\,y \mp 12.$$

Question 3: Data structures for multivariate polynomials (20 marks)

Design and implement SMP, a Sparse Multivariate Polynomial data structure for $\mathbb{Z}[x_1, \ldots, x_n]$. Use an ordered, expanded form, either recursive or distributed. Use any data structure of your choice to represent the polynomials, e.g. an array, linked list, or hash table. Implement 4 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

Use Maple to do coefficient and exponent arithmetic. Test your code on

```
> 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));
```

Question 4: Polynomial division (10 marks) MATH 819 and CMPT 881 students only.

Program also `SMPdiv` - to divide two polynomials A by B and output $FAIL$ if B does not divide A and output the quotient A/B if B does divides A.

Test your program on

```
> SMPdiv(A,B);
> SMPdiv(B,A);
> SMPdiv(C,A);
> SMPdiv(C,B);
```

Question 5: Chinese Remaindering (10 marks)

(a) By hand, find $0 \leq u < 5 \times 7 \times 9$ such that

$$u \equiv 3 \bmod 5, \quad u \equiv 1 \bmod 7, \quad \text{and} \quad u \equiv 3 \bmod 9$$

using the "mixed radix representation" for $\mathbb{Z}$ AND also the "Lagrange representation". You should get $u = 183$.

(b) Consider the following recursive algorithm for finding the integer u in the Chinese remainder theorem. For n moduli $m_1, m_2, ..., m_n$, to find $0 \leq u < \Pi_{i=1}^{n} m_i$, first find $0 \leq \bar{u} < \Pi_{i=1}^{n-1} m_i$, satisfying $\bar{u} \equiv u_i \bmod m_i$ for $i = 1, 2, \ldots, n-1$, *recursively*. Using this result and $u \equiv u_n \bmod m_n$ now find u. Apply the method by hand to the problem in part (a). Now write a Maple procedure which implements the method. Test your procedure on the problem in part (a). Note, you can compute the inverse of $a \in \mathbb{Z}_m$ in Maple using `1/a mod m`.