MACM 401/MATH 801/CMPT 981
Assignment 2, Spring 2021.

Michael Monagan

Due Monday February 8th at 11pm. For problems involving Maple calculations and Maple programming, you should export your work to a .pdf file. Late Penalty: −20% for up to 24 hours late. Zero after that.

Question 1 (15 marks): The Extended Euclidean Algorithm

Given $a, b \in E$, a Euclidean domain, the extended Euclidean algorithm solves $sa + tb = g$ for $s, t \in E$ and $g = \gcd(a, b)$. More generally, for $k = 0, 1, ..., n, n{+}1$ it computes $(r_k, s_k, t_k) \in E^3$ where $r_0 = a, r_1 = b, r_{n+1} = 0$ and $s_k a + t_k b = r_k$ for $0 \le k \le n + 1$.

(a) For integers $a = 99$, $b = 28$ execute the extended Euclidean algorithm by hand. Use the tabular method presented in class that shows the values for r_k, s_k, t_k, q_k. Identify $b^{-1} \mod a$.

(b) Program the *extended* Euclidean algorithm for $\mathbb{Q}[x]$ in Maple. The input is two non-zero polynomials $a, b \in \mathbb{Q}[x]$. The output is three polynomials (s, t, g) where g is the *monic* gcd of a and b and $sa + tb = g$ holds.

Please print out the values of (r_k, s_k, t_k) that are computed after each division step so that we can observe the exponential growth in the size of the rational coefficients of the r_k, s_k, t_k polynomials.

Use the Maple commands `quo(a,b,x)` and/or `rem(a,b,x)` to compute the quotient and remainder of a divided b in $\mathbb{Q}[x]$. Remember, in Maple, you must explicitly expand products of polynomials using the `expand(...)` command.

Execute your Maple code on the following inputs.

```
> a := expand((x+1)*(2*x^4-3*x^3+5*x^2+3*x-1));
> b := expand((x+1)*(7*x^4+5*x^3-12*x^2-x+4));
```

Check that your output satisfies $sa + tb = g$ and check that your result agrees with Maple's `g := gcdex(a,b,x,'s','t');` command.

(c) Consider $a(x) = x^3 - 1$, $b(x) = x^2 + 1$, and $c(x) = x^2$. Apply the algorithm in the proof of Theorem 2.6 (as presented in class) 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 `g := gcdex(a,b,x,'s','t');` command to solve $sa + tb = g$ for $s, t \in \mathbb{Q}[x]$.

Question 2 (10 marks): Multivariate Polynomials

(a) Consider the polynomials

$$A = 3 + 5x^2y^2 + 7xy - 2x^2 + 4y^3 \quad \text{and} \quad B = 7xyz + 9x^2 + 3x^2z - 5y^3$$

For each polynomial, write it in graded lexicographical order with $x > y > z$.
Write down $\mathrm{lc}(A), \mathrm{lm}(A), \mathrm{lt}(A), \mathrm{lc}(AB), \mathrm{lm}(AB)$ and $\mathrm{lt}(AB)$.
Repeat this using pure lexicographical order monomial ordering with $x > y > z$.
See the MultiPolyDefinitions handout for lecture 6.

(b) Consider the polynomials

$$A = 6\,y^2x^3 + 2\,x^2y^2 + 5\,yx^2 + 3\,xy^2 + yx + y^2 + x + y \quad \text{and} \quad B = 2\,yx^2 + x + y.$$

You are to divide the polynomials A by B over $\mathbb{Z}$. Write $A \in \mathbb{Z}[y][x]$ and test if $B|A$ by doing the division in $\mathbb{Z}[y][x]$ by hand. If $B|A$ determine the quotient Q of $A \div B$. Note, the quotient must be a polynomial in $\mathbb{Z}[y][x]$. Show your working.

Repeat the calculation using

$$A = 6\,y^2x^3 + 2\,x^2y^2 + 6\,yx^2 + 3\,xy^2 + yx + y^2 + x + y$$

Check your answers using Maple's `divide` command.

Question 3 (15 marks): The Primitive Euclidean Algorithm

Reference section 2.7

(a) Calculate the content and primitive part of the following polynomial $a \in \mathbb{Z}[x, y]$, 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` command will be useful.

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

(b) By hand, calculate the pseudo-remainder $\tilde{r}$ and the pseudo-quotient $\tilde{q}$ of the polynomials $a(x)$ divided by $b(x)$ below where $a, b \in \mathbb{Z}[y][x]$.

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

Now compute $\tilde{r}$ and $\tilde{q}$ using Maple's `prem` command to check your work.

(c) Given the following polynomials $a, b \in \mathbb{Z}[x, y]$, calculate the $\mathrm{GCD}(a, b)$ using the primitive Euclidean 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 commands `prem`, `gcd` and `divide` for intermediate calculations.

Question 4 (20 marks): Chinese Remaindering

Reference section 5.3.

(a) By hand, find $0 \le u < M$ where $M = 5 \times 7 \times 9$ 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 u.

(b) We will solve the Chinese remainder problem in $F[y]$.

> Theorem: Let F be a field and let $m_1, m_2, \ldots, m_n$ and $u_1, u_2, \ldots, u_n$ be polynomials in $F[y]$ with $\deg(m_i) > 0$ for $1 \le i \le n$. If $\gcd(m_i, m_j) = 1$ for $1 \le i < j \le n$ then there exists a unique polynomial u in $F[y]$ s.t.
> (i) $u \equiv u_i \pmod{m_i}$ for $1 \le i \le n$ and
> (ii) $u = 0$ or $\deg u < \sum_{i=1}^{n} \deg m_i$.

Prove the theorem by modifying the proof of the Chinese remainder theorem for $\mathbb{Z}$ to work for $F[y]$. Note, in the congruence relation $u \equiv u_i \pmod{m_i}$ means $m_i | (u - u_i)$ in $F[y]$.

(c) Consider the polynomials

$$A = x^4 + x^3 + x + 1 \quad \text{and} \quad B = x^3 + 1$$

in the ring $\mathbb{Z}_p[x]$ for $p = 2$. Use Maple to compute AB, $\gcd(A, B)$, the remainder of $A \div B$, and to solve $SA + TB = G$ in $\mathbb{Z}_p[x]$ for S, T, G where $G = \gcd(A, B)$.

See the handout PolynomialOperations.pdf from lecture 6 for the Maple commands.

Now solve the following Chinese remainder problem in $F[y]$ for $F = \mathbb{Z}_2$. Find $u \in \mathbb{Z}_2[y]$ such that

$$u \equiv y^2 \pmod{y^3 + y + 1} \text{ and } u \equiv y^2 + y + 1 \pmod{y^3 + y^2 + 1}.$$

Question 5 (10 marks): Matrix Polynomials and Determinants

The symmetric Toeplitz matrix T_n is an $n \times n$ symmetric matrix where

$$T_{i,j} = x_{|i-j|} \text{ for } 1 \le i \le n \text{ and } 1 \le j \le n.$$

For example, here is T_3 and its determinant in Maple.

```
> T3 := Matrix(3,3):
> for i to 3 do for j to 3 do T[i,j] := x[abs(i-j)]; od od:
> T3;
```

$$\begin{bmatrix} x_0 & x_1 & x_2 \\ x_1 & x_0 & x_1 \\ x_2 & x_1 & x_0 \end{bmatrix}$$

```
> with(LinearAlgebra):  # this loads the Linear Algebra package
> Determinant(T3);
```

$$x_0^3 - 2\,x_0 x_1^2 - x_0 x_2^2 + 2\,x_1^2 x_2$$

Write a Maple procedure `Toeplitz` such that `Toeplitz(n,x)` constructs an $n \times n$ symmetric Toeplitz matrix in $x_0, x_1, \ldots, x_{n-1}$.

In a for loop use your Maple procedure to compute T_2, T_3, T_4, T_5. For each Toeplitz matrix compute and factor it's determinant. Print out the matrix T_n, the number of terms of the determinant, and the factorization of the determinant.

The number of terms of $\det(T_n)$ grows rapidly. I was able to compute $\det(T_{15})$ on a server. It has 19,732,508 terms. Computing $\det(T_{20})$ seems hopeless; it is just way too big. Maybe it will never be computed. Use an evaluation homomorphism to prove that $\det(T_{20}) \neq 0$.