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 resultant of \( A \) and \( B \). From the definition, determine \( f(c) \) so that 
\[ \text{res}(cA, B) = f(c) \text{ res}(A, B). \]

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

Consider the following pair of polynomials from assignment 3.
\[ A = 58x^4 - 415x^3 - 111x + 213, \text{ and } \]
\[ B = 69x^3 - 112x^2 + 413x + 113. \]
They are relatively prime, i.e., \( G = 1 \), \( \overline{A} = A \) and \( \overline{B} = B \). 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 
\[ u(x) = 28x^2 + 24x + 58 \]
with \( p = 3 \) using, first the positive representation for \( \mathbb{Z}_3 \), then the symmetric representation.

(b) Determine the cube-root, if it exists, of the following polynomials
\[ a(x) = x^6 - 531x^5 + 94137x^4 - 5598333x^3 + 4706850x^2 - 1327500x + 125000, \]
\[ b(x) = x^6 - 406x^5 + 94262x^4 - 5598208x^3 + 4706975x^2 - 1327375x + 125125 \]
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 \( u_0 = \sqrt[3]{a} \mod 5 \) use any method. Use Maple to do the calculations.
Question 3: Hensel lifting (15 marks)
Reference: Section 6.4 and 6.5.

(a) Given
\[ a(x) = x^4 - 2x^3 - 23x^2 - 214x + 85 \]
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
\[ u_0(x) = x^2 + 4x + 2 \quad \text{and} \quad w_0(x) = x^2 + 4x + 5 \]
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 \( d \).

\begin{align*}
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} \\
\end{align*}

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

(a) Let \( A \) by an \( n \) by \( n \) matrix of polynomials in \( \mathbb{Z}[x] \) and let \( d = \det(A) \in \mathbb{Z}[x] \). 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

\begin{verbatim}
> B := A mod p;
\end{verbatim}
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 $n \times n$ 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 $n \times n$ 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
```