PROBLEM 1

Resultants and Polynomial GCD

1. Calculate the resultant of $A = 3x^2 + 3$ and $B = (x-2)(x+5)$ by hand.
2. Let A, B, C be non-constant polynomials in $R[x]$. Show that
$$\mathrm{Res}_x(A, BC) = \mathrm{Res}_x(A, B) \cdot \mathrm{Res}_x(A, C).$$
3. Let A, B be two non-zero polynomials in $\mathbb{Z}[x]$. Let $A = G\overline{A}$ and $B = G\overline{B}$ where $G = \gcd(A, B)$. We say that a prime p is **unlucky** when $p \mid \mathrm{Res}_x(\overline{A}, \overline{B}) \in \mathbb{Z}$. Let
$$\overline{A} = 58x^4 - 415x^3 - 111x + 213$$
and
$$\overline{B} = 69x^3 - 112x^2 + 413x + 113.$$
Write a Macaulay2 program to compute the resultant $\mathrm{Res}_x(\overline{A}, \overline{B})$ and identify all unlucky primes. For each unlucky prime p, compute the gcd of the polynomials $\overline{A}$ and $\overline{B}$ modulo p to verify that the primes are unlucky.

PROBLEM 2

Chinese remaindering and interpolation

Let
$$a = (9y - 7)x + (5y^2 + 12)$$
and
$$b = (13y + 23)x^2 + (21y - 11)x + (11y - 13)$$
be polynomials in $\mathbb{Z}[y][x]$.

In this question you will compute the product $a \times b$ by developing a modular algorithm. First reduce modulo primes $p_1, \ldots, p_\ell$, where you need to determine an $\ell \in \mathbb{N}$. Then, evaluate at points $y = \beta_1, \ldots, \beta_k$ and $x = \alpha_1, \ldots, \alpha_m$, where k and m in $\mathbb{N}$ also need to be determined, so that you end up multiplying in $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_\ell}$. Then use Chinese remaindering and polynomial interpolation to reconstruct the product in $\mathbb{Z}[y][x]$.

You can either do this by hand or by writing Macaulay2 code. If you write code, make sure to show all your steps.

PROBLEM 3

Univariate polynomial factoring over finite fields

1. Factor the following polynomials over $\mathbb{Z}_{11}$ using both the Cantor-Zassenhaus algorithm and the Berlekamp algorithm

$$a_1 = x^4 + 8x^2 + 6x + 8$$

$$a_2 = x^6 + 3x^5 - x^4 + 2x^3 - 3x + 3$$

$$a_3 = x^8 + x^7 + x^6 + 2x^4 + 5x^3 + 2x^2 + 8.$$

You can either do this by hand or by writing Macaulay2 code. If you write code, make sure to show all your steps.

PROBLEM 4

Newton Iteration and Extended Euclidean Algorithm (EEA)

Let $p = 101$, $\mathbb{F} = \mathbb{Z}_{101}$, $f = 30x^7 + 31x^6 + 32x^5 + 33x^4 + 34x^3 + 35x^2 + 36x + 37 \in \mathbb{F}[x]$ and $g = 17x^3 + 18x^2 + 19x + 20 \in \mathbb{F}[x]$.

1. Compute $\mathrm{rev}_3(g)^{-1} \bmod x^8$ using Newton iteration. Show the result after each iteration.
2. Use part (1) and the algorithm given in class to find $q, r \in \mathbb{F}[x]$ with $f = q \cdot g + r$ and $\deg r < 3$.
3. Use the EEA to find $f^{-1} \bmod g$ (that is, find $h \in \mathbb{F}[x]$ with $f \cdot h \equiv 1 \bmod g$).
4. Now use Newton iteration to find $f^{-1} \bmod g^4$. Show each step of the Newton iteration.

Your answer to this question should be in the form of a Macaulay2 session showing the input and output.

Problem 5

Linear Variant of Newton Iteration

Let $\ell \in \mathbb{N}$ and $f = f_0 + f_1 x + \cdots + f_{\ell-1} x^{\ell-1} \in \mathbb{F}[x]$ with $f_0 \neq 0$ be given.

We consider the linear variant of Newton iteration to compute the inverse $g = g_0 + g_1 x + \cdots + g_{\ell-1} x^{\ell-1} \in \mathbb{F}[x]$ of f modulo x^ℓ.

In this linear variant, we start with the guess $g^{(0)} = f_0^{-1}$ and given $g^{(k)} = g_0 + g_1 \cdot x + \cdots + g_k x^k$ such that $f \cdot g^{(k)} \equiv 1 \bmod x^{k+1}$ we want to find $g^{(k+1)}$ of degree $k+1$ such that:

1. $g^{(k+1)} \equiv g^{(k)} \bmod x^{k+1}$
2. $f \cdot g^{(k+1)} \equiv 1 \bmod x^{k+2}$

For $i = 0, 1, \ldots, \ell-2$, derive an explicit formula for the coefficient g_{i+1} in terms of the coefficients $g_0, g_1, \ldots, g_i$ and the coefficients of the input polynomial f.

Analyze this algorithm, and determine the number of operations in $\mathbb{F}$ to compute g using the method.

Problem 6

Understanding Abnormalities via the Resultant

Let $R = \mathbb{Q}[y]$ and suppose $f, g \in R[x]$ both have $\deg_x = 10$ and $\deg_y = 6$, and suppose $h := \gcd(f, g)$ has $\deg_x h = 4$ and $\deg_y h = 2$.

Derive an upper bound (as good as possible) on the number of distinct integers ℓ such that $\gcd(f(x,\ell), g(x,\ell)) \in \mathbb{Q}[x]$ has degree not equal to 4.