Problem 1

Hensel Lifting and Factoring (20 points)

1. Given

\[ a(x) = x^42x^3233x^2214x + 85 \]

and image polynomials

\[ u_0(x) = x^23x2 \quad \text{and} \quad w_0(x) = x^2 + x + 3, \]

satisfying \( a \equiv u_0w_0 \mod 7 \), lift the image polynomials using Hensel lifting to find (if there exist) \( u(x) \) and \( w(x) \) in \( \mathbb{Z}[x] \) such that \( a = uw \).

2. Given

\[ b(x) = 48x^422x^3 + 47x^2 + 144 \]

and an image polynomials

\[ u_0(x) = x^2 + 4x + 2 \quad \text{and} \quad w_0(x) = x^2 + 4x + 5 \]

satisfying \( b \equiv 6u_0w_0 \mod 7 \), lift the image polynomials using Hensel lifting to find (if there exist) \( u(x) \) and \( w(x) \) in \( \mathbb{Z}[x] \) such that \( b = uw \).

Acknowledgment: this problem was given to us by Michael Monagan
Problem 2

Vectors of small norm in lattice (20 points)

Let $g_1, \ldots, g_n \in \mathbb{R}^n$ be linearly independent and $L = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_n$ be the lattice they generate. Prove that for any vector $x \in \mathbb{R}^n$ there is a vector $g \in L$ such that

$$||x - g||_2^2 \leq \frac{1}{4} \cdot (||g_1||_2^2 + \cdots + ||g_n||_2^2)$$

**Hint:** Prove it by induction on $n$. For the induction step, find $\lambda \in \mathbb{Z}$ such that the vector $x - \lambda g_n$ has minimal distance to hyperplane spanned by $g_1, \ldots, g_{n-1}$.

Problem 3

Reducing dimension of a low-dimensional lattice (20 points)

Let $m < n$ be integers. If $b_1, \ldots, b_m \in \mathbb{R}^n$ are linearly independent vectors, then we will show that we can construct vectors $c_1, \ldots, c_m \in \mathbb{R}^{n-1}$ such that the lattices corresponding to $\mathbb{Z}b_1 + \cdots + \mathbb{Z}b_m$ and to $\mathbb{Z}c_1 + \cdots + \mathbb{Z}c_m$ are essentially equivalent (up to a multiplicative constant).

1. Show that there exists a vector $h_1 \in \mathbb{R}^n$ such that $\langle h_1, b_i \rangle = 0$, for all $i \in [m]$.

2. Use the Gram-Schmidt procedure to construct an orthogonal basis $(h_1, \ldots, h_n)$ of $\mathbb{R}^n$ with each $h_i \in \mathbb{R}^n$ and $||h_i||_2 = ||h_j||_2$.

3. Let $H$ be the $n \times n$ matrix given by

$$H = \begin{pmatrix} h_1^T \\ h_2^T \\ \vdots \\ h_n^T \end{pmatrix}.$$ 

Let

$$\begin{pmatrix} c_1 & c_2 & \cdots & c_n \end{pmatrix} = H \cdot \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix},$$

where the matrix of $c_i$’s and $b_j$’s are column matrices.

If $\alpha = ||h_i||_2$ from the previous part, show that for each $k \in [m]$:

$$||c_k||_2 = \alpha \cdot ||b_k||_2$$
4. Show that $H^T \cdot H = \alpha^2 \cdot I$. Show that the lattices $\alpha^2 (\mathbb{Z}b_1 + \cdots + \mathbb{Z}b_m)$ and $\alpha^2 (\mathbb{Z}c_1 + \cdots + \mathbb{Z}c_m)$ are equivalent, that is:

$$u \in \alpha^2 (\mathbb{Z}c_1 + \cdots + \mathbb{Z}c_m) \iff \frac{1}{\alpha^2} \cdot H^T u \in \alpha^2 (\mathbb{Z}b_1 + \cdots + \mathbb{Z}b_m)$$

Thus, a vector $u$ is a shortest vector in $\alpha^2 (\mathbb{Z}c_1 + \cdots + \mathbb{Z}c_m)$ iff $\frac{1}{\alpha^2} \cdot H^T u$ is a shortest vector in $\alpha^2 (\mathbb{Z}b_1 + \cdots + \mathbb{Z}b_m)$.

But notice that each $c_i$ has its last coordinate equal to 0, so the $c_i$'s are naturally integer vectors in $\mathbb{R}^{n-1}$.

**Problem 4**

**Issues with the division algorithm - CLO 2.3.5 (20 points)**

Let $f(x, y, z) = x^3 - x^2 y - x^2 z + x$, $f_1(x, y, z) = x^2 y - z$, and $f_2(x, y, z) = xy - 1$.

1. Compute using the graded lexicographic order:

   \[ r_1 = \text{remainder of } f \text{ on division by } (f_1, f_2) \]
   \[ r_2 = \text{remainder of } f \text{ on division by } (f_2, f_1) \]

   Your results should be different. Where in the division algorithm did the difference occur?

2. If $r = r_1 - r_2$ in the ideal $(f_1, f_2)$? If so, find an explicit expression $r = Af_1 + Bf_2$. If not, say why not.

3. Compute the remainder of $r$ on division by $(f_1, f_2)$. Why could you have predicted your answer before doing the division?

4. Find another polynomial $g \in (f_1, f_2)$ such that the remainder of division by $g$ by $(f_1, f_2)$ is non-zero.

   **Hint:** $(xy + 1) \cdot f_2 = x^2 y^2 - 1$ whereas $y \cdot f_1 = x^2 y^2 - yz$.

5. Does the division algorithm give us a solution to the ideal membership problem for $(f_1, f_2)$? Explain.
PROBLEM 5

Different monomial orders - CLO 2.4.10 (20 points)

The following orders are called weight orders. Let \( u = (u_1, \ldots, u_n) \in \mathbb{R}^n \) such that \( u_1, \ldots, u_n \) are positive real numbers which are linearly independent over \( \mathbb{Q} \). We say that \( u \) is an independent weight vector. Then, for \( \alpha, \beta \in \mathbb{N}^n \), define:

\[
\alpha >_u \beta \iff u \cdot \alpha > u \cdot \beta
\]

This is the weight order determined by \( u \).

1. Use the corollary of Dickson’s lemma from class to prove that \( >_u \) is a monomial order.

2. Show that \( u = (1, \sqrt{2}) \) is an independent weight vector, so that \( >_u \) is a weight order on \( \mathbb{N}^2 \)

PROBLEM 6

Monomial Ideals (20 points)

Let \( I_1 = (x^{\alpha_1}, \ldots, x^{\alpha_s}) \) and \( I_2 = (x^{\beta_1}, \ldots, x^{\beta_t}) \) be monomial ideals of \( \mathbb{C}[x_1, \ldots, x_n] \), where each \( \alpha_i, \beta_j \in \mathbb{N}^n \).

1. Show that \( I_1 \cap I_2 \) is generated by the elements \( LCM(x^{\alpha_i}, x^{\beta_j}) \).

2. When is \( I_1I_2 = I_1 \cap I_2 \)? Provide proof of your statement.