Name: ______________________________ Problem 1: ____________ /25

Problem 1(25 points) Let p be a prime. Consider the polynomial $f_p(x) = x^{p-1} - 1$. Every integer a_1 relatively prime to p satisfies $f_p(a_1) \equiv 0 \pmod{p}$ by Fermat's Little Theorem.

(a)(10 points) Show that $f_p'(a_1) \not\equiv 0 \pmod{p}$. In fact **find an integer-coefficient polynomial** $g(y)$ such that for every prime p and for every integer a_1 relatively prime to p,

$$uf_p'(a_1) \equiv 1 \pmod{p}$$

for $u = g(a_1)$.

(b)(15 points) For every integer a_1 relatively prime to p, show that there exists an integer a_2 such that both

(i) $a_2 \equiv a_1 \pmod{p}$, and

(ii) $f_p(a_2) \equiv 0 \pmod{p^2}$.

In fact **find an integer-coefficient polynomial** $h_p(y)$ (depending on p) such that for every integer a_1 relatively prime to p, $a_2 = h_p(a_1)$ satisfies (i) and (ii).

Bonus Problem. Only attempt after solving the rest of the exam.(5 points) Find an integer-coefficient polynomial $k_p(y)$ (depending onn p) such that for every integer a_1 relatively prime to p, $a_3 = k_p(a_1)$ satisfies (i) and satisfies $f_p(a_3) \equiv 0 \pmod{p^3}$.

$\boxed{\text{(a)}}$ Since $a_1 \not\equiv 0 \pmod{p}$, by Fermat's Little Theorem $a_1^{p-1} \equiv 1 \pmod{p}$.
And the derivative $f_p'(x)$ equals $(p-1)x^{p-2}$. Thus $f_p'(a_1) = (p-1)a_1^{p-2} \equiv \underline{-a_1^{p-2}} \pmod{p}$.
Therefore, for $\boxed{g(y) = -y}$, i.e., for $\underline{u = -a_1}$, we have $uf_p'(a_1) \equiv (-a_1)(-a_1^{p-2})$
$= +a_1^{p-1} \equiv +1 \pmod{p}$.

$\boxed{\text{(b)}}$ By Hensel's Lemma there exists an integer a_2 satisfying (i) & (ii).
Moreover Hensel's Lemma gives a formula for a_2.
$a_2 = a_1 - uf_p(a_1) = a_1 - (-a_1)(a_1^{p-1} - 1) = a_1 + a_1(a_1^{p-1} - 1) = a_1 + a_1^p - a_1 = \underline{a_1^p}$.
So for $\boxed{h_p(y) = y^p}$, $a_2 = h_p(a_1) = a_1^p$ satisfies (i) and (ii).

<u>Bonus</u>. The claim, proved by induction on e, is that $a_e = a_1^{(p^{e-1})}$ satisfies
(i) $a_e \equiv a_1 \pmod{p}$, and (ii) $f_p(a_e) \equiv 0 \pmod{p^e}$. The argument above proves the claim for $e = 2$. So assume the result holds for a fixed integer e, in particular $-a_e \equiv -a_1 = u \pmod{p}$. Then Hensel's Lemma gives a formula for an integer a_{e+1} with (i) $a_{e+1} \equiv a_e \pmod{p^e}$, and (ii) $f_p(a_{e+1}) \equiv 0 \pmod{p^{e+1}}$, namely
$a_{e+1} = a_e - (-a_e)(a_e^{p-1} - 1) = a_e + a_e^p - a_e = a_e^p = (a_1^{(p^{e-1})})^p = a_1^{(p^{e-1})p} = a_1^{(p^e)}$. ✓ So the claim is proved by induction. In particular, $\boxed{k_p(y) = y^{(p^2)}}$, $a_3 = (a_1)^{p^2}$.

Name: ______________________________ Problem 2: ____________ /40

Problem 2(40 points) The number field $\mathbb{Q}(\sqrt[3]{2})$ has an ordered $\mathbb{Q}$-basis $\mathcal{B} = (1, \sqrt[3]{2}, (\sqrt[3]{2})^2)$. Let α be the (nonzero) element $1 + \sqrt[3]{2} + (\sqrt[3]{2})^2$ in this number field.

(a)(10 points) With respect to the given ordered basis $\mathcal{B}$, find the matrix representative of the $\mathbb{Q}$-linear operator

$$L_\alpha : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}), \quad L_\alpha(\beta) = \alpha \cdot \beta.$$

(b)(10 points) Find a degree 3, monic polynomial $c(x)$ with rational coefficients such that $c(\alpha) = 0$.

(c)(5 points) Explain why your polynomial $c(x)$ is irreducible as a polynomial with rational coefficients.

(d)(5 points) Determine whether or not α is an algebraic integer.

(e)(10 points) Find a rational-coefficient, degree 2 polynomial $g(y)$ such that $1/\alpha$ equals $g(\alpha)$. Is α a unit, i.e., is $1/\alpha$ an algebraic integer?

Bonus Problem. Only attempt after solving the rest of the exam.(10 points) Let t be an integer with $|t| > 1$ and such that t is not divisible by p^3 for every prime p, i.e., t is *cube free.* List all such integers t for which $\alpha = 1 + \sqrt[3]{t} + (\sqrt[3]{t})^2$ is an algebraic integer whose inverse $1/\alpha$ is also an algebraic integer.

(a) For a $\mathbb{Q}$-vector space V with ordered basis $\mathcal{B} = (\mathbb{b}_1, \dots, \mathbb{b}_n)$, the coordinate vector of an element $\vec{v} \in V$ w.r.t. $\mathcal{B}$ is the unique column vector $[\vec{v}]_{\mathcal{B}} = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \in \mathbb{Q}^n$ s.t. $\vec{v} = c_1\mathbb{b}_1 + \dots + c_n\mathbb{b}_n$.
For a $\mathbb{Q}$-linear operator $T: V \to V$, the matrix representative of T w.r.t. $\mathcal{B}$ is $A = [T]_{\mathcal{B}} := \left[[T(\mathbb{b}_1)]_{\mathcal{B}} \cdots [T(\mathbb{b}_n)]_{\mathcal{B}} \right]$, an $n \times n$ matrix with rational entries.

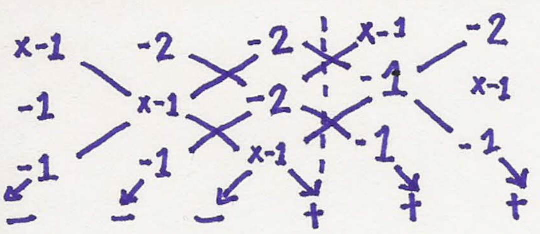
$L_\alpha(\mathbb{b}_1) = L_\alpha(1) = (1 + \sqrt[3]{2} + (\sqrt[3]{2})^2) \cdot 1 = 1 \cdot 1 + 1 \cdot \sqrt[3]{2} + 1 \cdot (\sqrt[3]{2})^2 = 1 \cdot \mathbb{b}_1 + 1 \cdot \mathbb{b}_2 + 1 \cdot \mathbb{b}_3$, $[L_\alpha(\mathbb{b}_1)]_{\mathcal{B}} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$.

$L_\alpha(\mathbb{b}_2) = L_\alpha(\sqrt[3]{2}) = (1 + \sqrt[3]{2} + (\sqrt[3]{2})^2)\sqrt[3]{2} = 1 \cdot \sqrt[3]{2} + 1(\sqrt[3]{2})^2 + 2 \cdot 1 = 2\mathbb{b}_1 + 1\mathbb{b}_2 + 1\mathbb{b}_3$, $[L_\alpha(\mathbb{b}_2)]_{\mathcal{B}} = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$.

$L_\alpha(\mathbb{b}_3) = L_\alpha(\sqrt[3]{2}^2) = (1 + \sqrt[3]{2} + (\sqrt[3]{2})^2)(\sqrt[3]{2})^2 = 1 \cdot (\sqrt[3]{2})^2 + 2 \cdot 1 + 2 \cdot \sqrt[3]{2} = 2\mathbb{b}_1 + 2\mathbb{b}_2 + 1\mathbb{b}_3$, $[L_\alpha(\mathbb{b}_3)]_{\mathcal{B}} = \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}$.

So $\boxed{A = \begin{bmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix}}$.

(b) One degree 3, monic polynomial $c(x)$ with rational coefficients such that $c(\alpha) = 0$ is the characteristic polynomial of A, $c_A(x) = \det(x \cdot Id_{3\times3} - A) = \begin{vmatrix} x-1 & -2 & -2 \\ -1 & x-1 & -2 \\ -1 & -1 & x-1 \end{vmatrix}$,



$= +\left[(x-1)^3 + (-2)^2(-1) + (-2)(-1)^2\right] - \left[(-2)(-1)(x-1) + (-2)(-1)(x-1) + (-2)(-1)(x-1)\right]$

$= (x-1)^3 - 4 - 2 - 6(x-1)$

$\boxed{c_A(x) = x^3 - 3x^2 - 3x - 1}$.

(c) There are two methods to prove irreducibility of $c_A(X) = X^3 - 3X^2 - 3X - 1$.

First method. (1) A quadratic or cubic polynomial is reducible if and only if it has a root.
(2) An integer coefficient polynomial $a_0 X^d - a_1 X^{d-1} + \dots + (-1)^{d-1} a_{d-1} X + (-1)^d a_d$, $a_d \neq 0$, only has roots (if any) which are of the form $\pm v/u$ for an integer v dividing $|a_d|$ and a nonzero integer u dividing $|a_0|$.
In our case, the only possible roots are $\frac{\pm 1}{1}$. But $c_A(-1) = -2 \neq 0$, and $c_A(1) = -6 \neq 0$.
Thus $c_A(X)$ has no rational roots, hence $c_A(X)$ is irreducible.

Second method. For the minimal polynomial $m_\alpha(X)$, there is an integer $e \geqslant 1$ such that $c_A(X) = (m_\alpha(X))^e$. If e equals 1, then $c_A(X)$ equals $m_\alpha(X)$, hence is irreduc.
Since $3 = \deg(c_A(X)) = e \cdot \deg(m_\alpha(X))$, either $e = 1$ or $e = 3$ and then $\deg(m_\alpha(X)) = 1$.
Since $m_\alpha(\alpha) = 0$, $\deg(m_\alpha(X)) = 1$ if and only if $m_\alpha(X) = X - \alpha$, i.e., $\alpha \in \mathbb{Q}$.
However $\alpha \notin \mathbb{Q}$, since $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = [\alpha]_{\mathcal{B}}$ is not of the form $\begin{bmatrix} t \\ 0 \\ 0 \end{bmatrix}$. So again $c_A(X)$ is irreducible.

(d) Since $c_A(X) = m_\alpha(X) = X^3 - 3X^2 - 3X - 1$ has integer coefficients, $\boxed{\alpha \text{ is an algebraic integer.}}$

(e) The equation $\alpha^3 - 3\alpha^2 - 3\alpha - 1 = 0$ gives $\alpha^3 - 3\alpha^2 - 3\alpha = 1$ or $\alpha(\alpha^2 - 3\alpha - 3) = 1$.
So for $\boxed{g(Y) = Y^2 - 3Y - 3}$, $\frac{1}{\alpha}$ equals $g(\alpha) = \alpha^2 - 3\alpha - 3$. Since sums, differences and products of algebraic integers are again algebraic integers, and since α is an alg. integer, also $\alpha^2 - 3\alpha - 3$ is an algebraic integer. $\boxed{\text{Therefore } \alpha \text{ is a unit.}}$

Bonus. Since t is not a cube, $X^3 - t$ has no rational roots and so is irreducible: $m_{\sqrt[3]{t}}(X) = X^3 - t$. Thus a basis for $\mathbb{Q}(\sqrt[3]{t})$ is $\mathcal{B} = (1, \sqrt[3]{t}, (\sqrt[3]{t})^2)$. With respect to this basis, $A = [L_{1 + \sqrt[3]{t} + (\sqrt[3]{t})^2}]_{\mathcal{B}}$ equals $\begin{bmatrix} 1 & t & t \\ 1 & 1 & t \\ 1 & 1 & 1 \end{bmatrix}$. So the characteristic polynomial is
$c_A(X) = (X-1)^3 - t^2 - t - 3t(X-1) = X^3 - 3X^2 - 3(t-1)X - (t-1)^2$. Thus $1 + \sqrt[3]{t} + (\sqrt[3]{t})^2$ is an algebraic integer. Moreover $N_{\mathbb{Q}(\sqrt[3]{t})}(1 + \sqrt[3]{t} + (\sqrt[3]{t})^2) = \det(A)$ equals $(t-1)^2$. An algebraic integer is a unit if and only if the norm equals ± 1. Hence $1 + \sqrt[3]{t} + (\sqrt[3]{t})^2$ is a unit if and only if $(t-1)^2$ equals ± 1. So the only possibility is $\boxed{t = 2}$.

Name: ______________________ Problem 3: __________ /25

Problem 3(25 points) Consider the following matrices and column vectors,

$$A = \begin{bmatrix} 1 & 0 & -1 & 0 & 1 \\ 2 & 4 & -2 & 0 & 2 \\ 0 & 0 & 0 & -1 & 0 \\ 1 & 4 & -1 & 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}, \quad B = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}.$$

(a)(15 points) Find necessary and sufficient conditions on the integers b_1, b_2, b_3, and b_4 such that there exist integers x_1, x_2, x_3, x_4, and x_5 solving the linear system $AX = B$. Express your conditions as linear equations and linear congruences in the variables b_1, b_2, b_3, b_4 (and only in these variables).

(b)(10 points) When (b_1, b_2, b_3, b_4) equals $(1, -2, 3, -3)$, find the general solution $X \in \mathbb{Z}^4$ of the linear system $AX = B$.

(a) Given a 4×4 invertible matrix $\mathcal{U}$ and a 5×5 invertible matrix V such that $\mathcal{U}AV$ is a block diagonal matrix $\tilde{A} = \left[\begin{array}{c:c} \begin{matrix} \tilde{a}_{11} & \cdots & O \\ O & \cdots & \tilde{a}_{rr} \end{matrix} & O_{s-r} \\ \hdashline O_{4-r,r} & O_{4-r,s-r} \end{array}\right]$, then after the transformations $\tilde{B} = \mathcal{U}B$, $X = V\tilde{X}$, the new system is $\tilde{A}\tilde{X} = \tilde{B}$, i.e. $\begin{bmatrix} \tilde{a}_{11}\tilde{x}_1 \\ \vdots \\ \tilde{a}_{rr}\tilde{x}_r \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} \tilde{b}_1 \\ \vdots \\ \tilde{b}_r \\ \tilde{b}_{r+1} \\ \vdots \\ \tilde{b}_4 \end{bmatrix}$, i.e., $\underline{\tilde{b}_i \equiv 0 \pmod{\tilde{a}_i}}$ for $i = 1, \dots, r$ and $\underline{\tilde{b}_i = 0}$ for $i = r+1, \dots, 4$.

So to determine consistency, we should find the matrices $\mathcal{U}$, V and $\tilde{A}$ as above such that the augmented matrix $\left[\begin{array}{c|c} A & Id_{4\times4} \\ \hline Id_{5\times5} & \end{array}\right]$ is elementary equivalent to $\left[\begin{array}{c|c} \tilde{A} & \mathcal{U} \\ \hline V & \end{array}\right]$:

__Row operations:__

$$\left[\begin{array}{ccccc|cccc} 1 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 2 & 4 & -2 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 4 & -1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \end{array}\right] \begin{matrix} \\ -2R_1 \\ (-1) \\ -R_1 \\ \\ \\ \\ \\ \\ \end{matrix} \to \left[\begin{array}{ccccc|cccc} 1 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 4 & 0 & 0 & 0 & -1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \end{array}\right] \begin{matrix} \\ \\ \\ -R_2 \\ \\ \\ \\ \\ \\ \end{matrix} \to$$

__Column Operations:__

$$\left[\begin{array}{ccccc|cccc} 1 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 4 & 0 & 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \end{array}\right] \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}$$

$$+C_1 \quad -C_1$$

$$\to \left[\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 4 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & -1 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \end{array}\right]$$

$$\to \left[\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 4 & 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 & -1 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \end{array}\right].$$

So $\mathcal{U}_{4\times4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ -2 & 1 & 0 & 0 \\ 1 & -1 & 0 & 1 \end{bmatrix}$, $V_{5\times5} = \begin{bmatrix} 1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$, and $\tilde{A} = \left[\begin{array}{ccc:cc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 0 \end{array}\right]$

i.e. $\begin{bmatrix} \tilde{b}_1 \\ \tilde{b}_2 \\ \tilde{b}_3 \\ \tilde{b}_4 \end{bmatrix} = \begin{bmatrix} b_1 \\ -b_3 \\ -2b_1 + b_2 \\ b_1 - b_2 + b_4 \end{bmatrix}$, i.e. $\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} \tilde{x}_1 + \tilde{x}_4 - \tilde{x}_5 \\ \tilde{x}_3 \\ \tilde{x}_4 \\ \tilde{x}_2 \\ \tilde{x}_5 \end{bmatrix}$

(over 2)

so that the new system is $\begin{cases} \tilde{x}_1 = \tilde{b}_1 \\ \tilde{x}_2 = \tilde{b}_2 \\ 4\tilde{x}_3 = \tilde{b}_3 \\ 0 = \tilde{b}_4 \end{cases}$. Thus the system is consistent if and only if $\underline{\tilde{b}_3 \equiv 0 \pmod 4}$ and $\underline{\tilde{b}_4 = 0}$.

In terms of the original variables, the system is consistent if and only if both $\boxed{-2b_1 + b_2 \equiv 0 \pmod 4}$ and $\boxed{b_1 - b_2 + b_4 = 0}$.

When this holds, the general solution of the new system is $\begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \\ \tilde{x}_3 \\ \tilde{x}_4 \\ \tilde{x}_5 \end{bmatrix} = \begin{bmatrix} b_1 \\ -b_3 \\ \frac{1}{4}(-2b_1+b_2) \\ t_1 \\ t_2 \end{bmatrix}$, for arbitrary integers t_1, t_2.

In terms of the original variables, this is $\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} b_1 + t_1 - t_2 \\ \frac{1}{4}(-2b_1+b_2) \\ t_1 \\ -b_3 \\ t_2 \end{bmatrix}$.

(b) For $\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = \begin{bmatrix} 1 \\ -2 \\ 3 \\ -3 \end{bmatrix}$, $-2b_1+b_2 = -2-2 = -4 \equiv 0 \pmod 4$ ✓, so the system is consistent.

$b_1 - b_2 + b_4 = 1-(-2)-3 = 0$ ✓

So the general solution is $\boxed{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 1+t_1-t_2 \\ -1 \\ t_1 \\ -3 \\ t_2 \end{bmatrix}}$ for t_1, t_2 arbitrary integers.

Name: ______________________________ Problem 4: ____________ /25

Problem 4(25 points) Consider the following integer, binary quadratic form

$$f(x,y) = 5x^2 + 14xy + 11y^2.$$

Find a 2×2, integer-valued matrix with determinant $+1$,

$$V = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

such that after the linear change of variables,

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \tilde{x} \\ \tilde{y} \end{bmatrix} = \begin{bmatrix} \alpha\tilde{x} + \beta\tilde{y} \\ \gamma\tilde{x} + \delta\tilde{y} \end{bmatrix},$$

the new binary quadratic form

$$g(\tilde{x},\tilde{y}) = f(x,y) = a\tilde{x}^2 + b\tilde{x}\tilde{y} + c\tilde{y}^2$$

is in reduced form, i.e., $|a| \le |c|$ and either $-|a| < b \le |a|$ if $|a| < |c|$ or $0 \le b \le |a|$ if $|a|$ equals $|c|$. Also give the binary quadratic form $g(\tilde{x},\tilde{y})$.

We begin with the binary form $f_1(x_1,y_1) = a_1x_1^2 + b_1x_1y_1 + c_1y_1^2$ $= 5x_1^2 + 14x_1y_1 + 11y_1^2$ and proceed to perform admissible linear variable changes until the transformed binary form is reduced.

Step 1. Although $|a_1| \le |c_1|$ holds, $|b_1|$ is greater than $|a_1|$. So write $b_1 = (2a_1)q + r$, $-|a_1| < r \le |a_1|$, i.e., $14 = (10)\cdot \underset{q}{1} + \underset{r}{4}$. Make the coordinate change $(x_1,y_1) = (x_2 - qy_2, y_2) = \underline{(x_2 - y_2, y_2)}$.

The new form is $f_2(x_2,y_2) = a_2x_2^2 + b_2x_2y_2 + c_2y_2^2 = 5(x_2-y_2)^2 + 14(x_2-y_2)y_2 + 11y_2^2 = \underline{5x_2^2 + 4x_2y_2 + 2y_2^2}$.

Step 2. Since $|a_2| \le |c_2|$ does not hold, make the coord. change $(x_2,y_2) = \underline{(-y_3, x_3)}$.

The new form is $f_3(x_3,y_3) = a_3x_3^2 + b_3x_3y_3 + c_3y_3^2 = \underline{2x_3^2 - 4x_3y_3 + 5y_3^2}$.

Step 3. Although $|a_3| \le |c_3|$ holds, $|b_3|$ is greater than $|a_3|$. So write $b_3 = (2a_3)q + r$, $-|a_3| < r \le$ [illegible] i.e., $-4 = (4)\underset{q}{(-1)} + \underset{r}{0}$. Make the coordinate change $(x_3,y_3) = (x_4 - qy_4, y_4) = \underline{(x_4 + y_4, y_4)}$.

The new form is $f_4(x_4,y_4) = 2(x_4+y_4)^2 - 4(x_4+y_4)y_4 + 5y_4^2 = \underline{2x_4^2 + 3y_4^2}$. This is reduced.

So set $(\tilde{x},\tilde{y}) = (x_4,y_4)$, i.e. $(x,y) = (x_1,y_1) = (x_2 - y_2, y_2) = (-x_3 - y_3, x_3) = (-\tilde{x} - 2\tilde{y}, \tilde{x} + \tilde{y})$.

So for the linear change $\boxed{\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -1 & -2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \tilde{x} \\ \tilde{y} \end{bmatrix}}$, the new binary quadratic form $\boxed{\tilde{f}(\tilde{x},\tilde{y}) = 2\tilde{x}^2 + 3\tilde{y}^2}$ is reduced.

Name: ______________________ Problem 5: ____________ /30

Problem 5(30 points) Consider the integer, binary quadratic forms

$$f(x,y) = ax^2 + bxy + cy^2$$

which are positive definite and which have discriminant $b^2 - 4ac$ equal to -24.

(a)(10 points) Find all such forms $f(x,y)$ which are reduced. In particular, give the number of such forms.

(b)(20 points) For all odd primes p different from 3, find a necessary and sufficient condition that p is properly represented by a quadratic form f as above (with discriminant equal to -24). Write your condition in terms of p being congruent to a list of residues modulo a fixed integer (using the Chinese Remainder Theorem if necessary to combine congruences modulo relatively prime integers).

$\boxed{\text{(a)}}$ First of all, since $b^2 \equiv -24 \pmod{4ac}$, we have b is even and also $b \equiv 0 \pmod 4$ if a is even. Since $f(x,y)$ is positive definite, a and c are positive. Since $f(x,y)$ is reduced, $b^2 \leq a^2$ and $4ac \geq 4a^2$ so that $24 = -b^2 + 4ac \geq 4a^2 - b^2 \geq 3a^2$. So $a^2 \leq \frac{24}{3} = 8$. Thus $a=1$ or $a=2$.

$\underline{a=1}$. Then $|b| \leq a = 1$ and b is even $\Rightarrow b=0$. So $24 = -b^2 + 4ac = -0^2 + 4(1)c$, so that $c=6$. So when $a=1$, $f_1(x,y) = \underline{x^2+6y^2}$.

$\underline{a=2}$. Then $|b| \leq a = 2$ and $b \equiv 0 \pmod 4$ (since a is even). So again $b=0$. So $24 = -b^2 + 4ac = -0^2 + 4(2)c$, so that $c=3$. So when $a=2$, $f_2(x,y) = \underline{2x^2+3y^2}$.

Therefore there are $\boxed{\text{two}}$ distinct reduced, positive definite forms of discriminant -24, $\boxed{f_1(x,y) = x^2+6y^2}$ and $\boxed{f_2(x,y) = 2x^2+3y^2}$.

$\boxed{\text{(b)}}$ For an odd prime different from 3, -24 is prime to p. Thus -24 is a square mod p, and hence p is represented by f_1 or f_2, if and only if $\left(\frac{-24}{p}\right) = +1$. Since $-24 = (-2)(-3)(2)^2$, $\left(\frac{-24}{p}\right)$ equals $\left(\frac{2}{p}\right)\left(\frac{-3}{p}\right)$. By quadratic reciprocity,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases}.$$

Also by quadratic reciprocity,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}\cdot 1} = \left(\frac{-1}{p}\right), \text{ so that}$$

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} +1, & p \equiv +1 \pmod 3 \\ -1, & p \equiv -1 \pmod 3 \end{cases}.$$

(over 2)

Name: ____________________

And the product $\left(\frac{2}{p}\right)\left(\frac{-3}{p}\right)$ equals $+1$ if either $\left(\left(\frac{2}{p}\right),\left(\frac{-3}{p}\right)\right) = (+1,+1)$ or $= (-1,-1)$, i.e. either ($p \equiv \pm 1 \pmod 8$ and $p \equiv +1 \pmod 3$) or ($p \equiv \pm 3 \pmod 8$ and $p \equiv -1 \pmod 3$).

Note that $1 = +3\cdot 3 + (-1)\cdot 8$ so that $z \equiv x \pmod 8$ and $z \equiv y \pmod 3$ if and only if $z \equiv 9x - 8y \pmod{24}$. Therefore $p \equiv \pm 1 \pmod 8$ and $p \equiv +1 \pmod 3$ if and only if $p \equiv 1$ or $7 \pmod{24}$. Also $p \equiv \pm 3 \pmod 8$ and $p \equiv -1 \pmod 3$ if and only if $p \equiv 5$ or $11 \pmod{24}$.

In conclusion, an odd prime p different from 3 is represented by a positive definite, integral, binary quadratic form of discriminant -24 if and only if either $\boxed{p \equiv 1 \text{ or } 7 \pmod{24}}$, in which case p is represented by x^2+6y^2;

or $\boxed{p \equiv 5 \text{ or } 11 \pmod{24}}$, in which case p is represented by $2x^2+3y^2$.

For completeness, also $2 = f_2(1,0)$ and $3 = f_2(0,1)$.

Name: ______________________________ **Problem 6**: ____________ /30

Problem 6(30 points) Consider the following integer, ternary quadratic form

$$f(x,y,z) = 3x^2 + 2y^2 + 6yz + 3z^2.$$

(a)(20 points) Find an invertible, 3×3 matrix with rational entries,

$$V = \begin{bmatrix} c_{1,1} & c_{1,2} & c_{1,3} \\ 0 & c_{2,2} & c_{2,3} \\ 0 & 0 & c_{3,3} \end{bmatrix}$$

with column vectors $\vec{w}_1$, $\vec{w}_2$, $\vec{w}_3$, such that after the linear change of variables,

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} c_{1,1} & c_{1,2} & c_{1,3} \\ 0 & c_{2,2} & c_{2,3} \\ 0 & 0 & c_{3,3} \end{bmatrix} \begin{bmatrix} \tilde{x} \\ \tilde{y} \\ \tilde{z} \end{bmatrix} = \tilde{x}\vec{w}_1 + \tilde{y}\vec{w}_2 + \tilde{z}\vec{w}_3,$$

the new binary quadratic form $g(\tilde{x},\tilde{y},\tilde{z})$ is in "Legendre diagonal form", i.e.,

$$g(\tilde{x},\tilde{y},\tilde{z}) = f(x,y,z) = q(a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2)$$

for a nonzero rational number q and for integers a, b, c such that abc is square free. Also give the binary quadratic form $g(\tilde{x},\tilde{y},\tilde{z})$.

Note. Even after finding a linear change of variables which makes the quadratic form diagonal, you may need to perform further (diagonal) linear changes of variables to insure that abc is square free.

(b)(10 points) Say whether or not $g(\tilde{x},\tilde{y},\tilde{z})$ has a nontrivial real solution. Finally use Legendre's theorem to determine whether or not $g(\tilde{x},\tilde{y},\tilde{z})$ has a nontrivial rational solution $(\tilde{x},\tilde{y},\tilde{z}) \neq (0,0,0)$.

(a) With respect to the standard ordered basis for $\mathbb{Q}^3$, $\left(\vec{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \vec{v}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \vec{v}_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}\right)$.
For a vector $\vec{v} = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = x\vec{v}_1 + y\vec{v}_2 + z\vec{v}_3$, $f(\vec{v})$ equals $\vec{v} \cdot Q\vec{v}$ where Q is the symmetric 3×3 matrix $Q = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 2 & 3 \\ 0 & 3 & 3 \end{bmatrix}$. Our <u>first</u> goal is to find a new basis $(\vec{u}_1, \vec{u}_2, \vec{u}_3)$ such that $\vec{u}_i \cdot Q\vec{u}_j$ equals 0 for $i \neq j$. We find this basis by the Gram-Schmidt algorithm.

<u>Step 1</u>. $\vec{u}_1 := \vec{v}_1 = \underline{\underline{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}}}$, $Q\vec{u}_1 = \begin{bmatrix} 3 \\ 0 \\ 0 \end{bmatrix}$, $\vec{u}_1 \cdot Q\vec{u}_1 = \underline{3}$. <u>Step 2</u>. $\vec{v}_2 \cdot Q\vec{u}_1 = 0$. So $\vec{u}_2 = \vec{v}_2 - 0\vec{v}_1 = \vec{v}_2 = \underline{\underline{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}}}$,
$Q\vec{u}_2 = \begin{bmatrix} 0 \\ 2 \\ 3 \end{bmatrix}$, $\vec{u}_2 \cdot Q\vec{u}_2 = \underline{2}$

<u>Step 3</u>. $\vec{v}_3 \cdot Q\vec{u}_1 = 0$, $\vec{v}_3 \cdot Q\vec{u}_2 = 3$.
So $\vec{u}_3 = 2\vec{v}_3 - 3\vec{u}_2 = \underline{\underline{\begin{bmatrix} 0 \\ -3 \\ 2 \end{bmatrix}}}$.
$Q\vec{u}_3 = \begin{bmatrix} 0 \\ 0 \\ -3 \end{bmatrix}$, $\vec{u}_3 \cdot Q\vec{u}_3 = \underline{-6}$

Write $\vec{v} = \bar{x}\vec{u}_1 + \bar{y}\vec{u}_2 + \bar{z}\vec{u}_3$, i.e. $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{array}{c} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 2 \end{bmatrix} \\ \vec{u}_1 \ \ \vec{u}_2 \ \ \vec{u}_3 \end{array} \begin{bmatrix} \bar{x} \\ \bar{y} \\ \bar{z} \end{bmatrix}$.
Then $\bar{f}(\bar{x},\bar{y},\bar{z})$ equals $3\bar{x}^2 + 2\bar{y}^2 - 6\bar{z}^2$.
However, $3 \cdot 2 \cdot (-6)$ is <u>not</u> squarefree: 2 divides $\bar{y}, \bar{z}$ but not $\bar{x}$, & 3 divides $\bar{x}, \bar{z}$ but not $\bar{y}$.
So set $\bar{x} = 2\tilde{x}$, $\bar{y} = 3\tilde{y}$, $\bar{z} = \tilde{z}$.

(over 2)

Then $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 2 \end{bmatrix}\begin{bmatrix} 2\tilde{x} \\ 3\tilde{y} \\ \tilde{z} \end{bmatrix} = \boxed{\begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & -3 \\ 0 & 0 & 2 \end{bmatrix}\begin{bmatrix} \tilde{x} \\ \tilde{y} \\ \tilde{z} \end{bmatrix}}$. With respect to this coordinate change, we have

$\tilde{f}(\tilde{x},\tilde{y},\tilde{z}) = 3(2\tilde{x})^2 + 2(3\tilde{y})^2 + 6\tilde{z}^2 = \boxed{6\,(2\tilde{x}^2 + 3\tilde{y}^2 - \tilde{z}^2).}$

So $a=2$, $b=3$, $c=-1$ with $abc=-6$ is square free (and $q=6$).

(b) The form $6(2\tilde{x}^2 + 3\tilde{y}^2 - \tilde{z}^2)$ $\boxed{\text{does have a nontrivial real solution}}$, e.g., $(\tilde{x},\tilde{y},\tilde{z}) = (1, 0, \sqrt{2})$.

But since $-ac = 2$ is not a square mod $|b| = 3$, by Legendre's theorem the form $\boxed{\text{does not have a nontrivial rational solution.}}$