MAT 311 Spring 2011 Final Exam

Name: ______________________________ SB ID number: ____________________

Problem 1:	________	/25
Problem 2:	________	/40
Problem 3:	________	/25
Problem 4:	________	/25
Problem 5:	________	/30
Problem 6:	________	/30
Total:	________	/175

Instructions: *Please write your name at the top of every page of the exam.* This exam is closed book, closed notes, calculators are not allowed, and all cellphones and other electronic devices must be turned off for the duration of the exam. Electronic language translators may be approved by the proctor for ESL students, but the student must identify himself or herself to the proctor so that the translator may be approved prior to using the translator.

You will have approximately 150 minutes for this exam. The point value of each problem is written next to the problem – use your time wisely. **Please show all work, unless instructed otherwise.** Partial credit will be given only for work shown.

You may use either pencil or ink. If you have a question, need extra paper, need to use the restroom, etc., raise your hand.

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,

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

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 $f_p(a_3) \equiv 0 \pmod{p^3}$.

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.

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 $AX = B$.

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

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).

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 $(\tilde{x},\tilde{y},\tilde{z}) \neq (0,0,0)$.