MAT 311 Number Theory
Final Exam, Chem 128, 11:15 AM – 1:45 PM
Friday, May 20th, 2011

Jason Starr
Spring 2011

MAT 311 Solutions to Final Exam Practice

Remark. If you are comfortable with all of the following problems, you will be very well prepared for the midterm. Some of the problems below are more difficult than a problem that would be asked on the midterm. But all of the problems will help you practice the skills and results from this part of the course.

Exam Policies. You must show up on time for all exams. Within the first 30 minutes of each exam, no students will be allowed to leave the exam room. No students arriving after the first 30 minutes will be allowed to take the exam. Students finishing within the last 10 minutes of the exam may be asked to remain until the exam is over and then follow special instructions for turning in their exams (for instance, students are often asked to turn in exams row-by-row).

If you have a university-approved reason for taking an exam at a time different than the scheduled exam (because of a religious observance, a student-athlete event, etc.), please contact your instructor as soon as possible. Similarly, if you have a documented medical emergency which prevents you from showing up for an exam, again contact your instructor as soon as possible.

For excused absences from a midterm, the usual policy is to drop the missed exam and compute the exam total using the other exams. In exceptional circumstances, a make-up exam may be scheduled for the missed exam. For an excused absence from the final exam, the correct letter grade can only be assigned after the student has completed a make-up final exam.

All exams are closed notes and closed book. Once the exam has begun, having notes or books on the desk or in view will be considered cheating and will be referred to the Academic Judiciary.

For all exams, you must bring your Stony Brook ID. The IDs may be checked against picture sheets.

It is not permitted to use cell phones, calculators, laptops, MP3 players, Blackberries or other such electronic devices at any time during exams. If you use a hearing aid or other such device, you should make your instructor aware of this before the exam begins. You must turn off your cell phone, etc., prior to the beginning of the exam. If you need to leave the exam room for any reason before the end of the exam, it is still not permitted to use such devices. Once the exam has begun, use of such devices or having such devices in view will be considered cheating and will be referred to the Academic Judiciary. Similarly, once the exam has begun any communication with a person other than the instructor or proctor will be considered cheating and will be referred to the Academic Judiciary.

Practice Problems.

MAT 311 Number Theory — Jason Starr
Final Exam, Chem 128, 11:15 AM – 1:45 PM — Spring 2011
Friday, May 20th, 2011

(1) In each of the following cases, for the given pair $(m,n) \neq (0,0)$ of integers, find the greatest common divisor $c > 0$. Find the integers m/c and n/c. Find integers u and v such that c equals $um + vn$. Given integers (x,y), know a necessary and sufficient condition in terms of c such that there exists an integer z with $z \equiv x \pmod{m}$ and $z \equiv y \pmod{n}$. Assuming the condition is true, find a formula for one particular such integer z, and know how to describe the general such integers in terms of a particular integer.

(a) $(m,n) = (114, 91)$.
(b) $(m,n) = (51, 85)$.
(c) $(m,n) = (-56, 92)$.
(d) $(m,n) = (72, 54)$.
(e) $(m,n) = (b^3, (b+1)^3)$, where b is an arbitrary integer.

(2) For each of the following sequences $(n_1, \dots, n_r)$ of pairwise relatively prime integers, find a formula for a particular integer z such that

$$z \equiv x_1 \pmod{n_1}, \dots, \ z \equiv x_r \pmod{n_r},$$

for a variable sequence of residues $(x_1, \dots, x_r)$. Finally, for the given sequence of residues $(a_1, \dots, a_r)$, find the integer z as above with smallest absolute value.

(a) $(n_1, n_2, n_3) = (1, 2, 3)$, $(a_1, a_2, a_3) = (0, 1, 2)$.
(b) $(n_1, n_2, n_3) = (4, 9, 25)$, $(a_1, a_2, a_3) = (1, 1, 1)$.
(c) $(n_1, n_2, n_3, n_4) = (16, 27, 25, 7)$, $(a_1, a_2, a_3, a_4) = (-1, 1, -1, 1)$.
(d) $(b, b+1, b(b+1)+1)$, $(a_1, a_2, a_3) = (1, 0, 0)$, where b is an arbitrary integer.

(3) Prove that there are infinitely many primes congruent to 5 modulo 6.

(4) For the following list $a_1, \dots, a_r$ of integers and for the following list $n_1, \dots, n_s$ of positive integers, determine precisely which integers a_i are invertible modulo n_j. In each such case, find an integer $b_{i,j}$ such that $b_{i,j} a_i \equiv 1 \pmod{n_i}$.

$$(n_1, n_2, n_3, n_4, n_5)) = (8, 27, 25, 49, 51), \quad (a_1, a_2, a_3, a_4) = (1, 2, 3, 4).$$

(5) In each of the following cases, determine $\phi(n)$.

$$n = 2, \ n = 7, \ n = 16, \ n = 14, \ n = 105, \ n = 75.$$

(6) In each of the following cases, say whether or not the given integer n is a sum of two squares. When it is a sum of two squares, find integers a and b such that $a^2 + b^2$ equals n.

$$n = 0, \ n = 1, \ n = 4, \ n = 19, \ n = 29, \ n = 49, \ n = 61.$$

(7) In each of the following cases, find all solutions of the polynomial congruence $f(x) \equiv 0$ modulo the two given relatively prime integers a and b. Then find all solutions modulo the integer ab.

(a) $f(x) = 7$, $(a, b) = (2, 7)$.
(b) $f(x) = 3x - 1$, $(a, b) = (2, 5)$.
(c) $f(x) = x^2$, $(a, b) = (8, 9)$.
(d) $f(x) = x^6 - 1$, $(a, b) = (7, 13)$.
(e) $f(x) = x^6 + 1$, $(a, b) = (7, 13)$.

(8) In each of the following cases, for the given polynomial $f(x)$, given prime p, and given integer a_1, say whether or not the given integer a_1 is a solution of $f(x) \equiv 0 \pmod{p}$. Further, say whether or not a is a critical point of $f(x)$ modulo p. If not, give formulas for solutions a_2, resp. a_3, of $f(x) \equiv 0 \pmod{p^2}$, resp. of $f(x) \equiv 0 \pmod{p^3}$, which are congruent to a_1 modulo p.

(a) $f(x) = 7$, $p = 2$, $a_1 = 3$.
(b) $f(x) = 3x - 1$, $p = 5$, $a_1 = 2$.
(c) $f(x) = x^2$, $p = 3$, $a_1 = 1$.
(d) $f(x) = x^6 - 1$, $p = 7$, $a_1 = 3$.
(e) $f(x) = x^6 + 1$, $p = 13$, $a_1 = 2$.

(9) For each of the following integers n, say whether or not the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. If so, find one generator, say how many generators there are, and give a formula for finding all generators in terms of the particular generator.

$$n = 13,\ n = 14,\ n = 8,\ n = 27,\ n = 257.$$

(10) For each of the following integers n, list all units modulo n which are quadratic residues. Then list all units modulo n which are quadratic nonresidues.

$$n = 5,\ n = 7,\ n = 8,\ n = 9,\ n = 10,\ n = 257.$$

(11) Compute each of the following Legendre symbols directly, without using quadratic reciprocity.

$$\left(\frac{2}{3}\right),\ \left(\frac{3}{7}\right),\ \left(\frac{-1}{11}\right),\ \left(\frac{2}{11}\right),\ \left(\frac{6}{19}\right),\ \left(\frac{-9}{23}\right)$$

(12) Compute each of the following Legendre symbols by any method, including quadratic reciprocity.

$$\left(\frac{2}{11}\right),\ \left(\frac{7}{53}\right),\ \left(\frac{14}{53}\right),\ \left(\frac{30}{53}\right),\ \left(\frac{53}{257}\right),\ \left(\frac{-2}{257}\right)$$

(13) In each of the following cases, for the given integer a, find a necessary and sufficient condition for a variable odd prime p (not dividing a) that a is a quadratic residue modulo p in terms of a congruence involving p modulo a fixed integer n (not varying with p).

$$a = 7,\ a = 13,\ a = 91,\ a = 44,\ a = 27.$$

(14) In each of the following cases, determine whether or not the system is consistent. If it is consistent, find the general solution.

(i)
$$7x + 15y = 9$$

(ii)
$$84x - 39y = 41$$

(iii)
$$84x - 39y = 42$$

(iv)
$$84x - 39y = b, \quad b \text{ arbitrary}$$

(v)
$$15x + 21y + 35z = 14$$

(15) For each of the following matrices A, find invertible, square matrices with integer entries U and V such that UAV is defined and is in block diagonal form.

$$\text{(i) } A = \begin{bmatrix} 2 & 0 \\ 3 & -1 \end{bmatrix}, \quad \text{(ii) } A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -5 & 0 \\ 3 & 0 & -1 \end{bmatrix}, \quad \text{(iii) } A = \begin{bmatrix} 5 & 10 \\ 9 & 3 \\ 4 & -7 \end{bmatrix},$$

$$\text{(iv) } A = \begin{bmatrix} 1 & 1 & -3 & 2 \\ 5 & 5 & -3 & 10 \\ 2 & 2 & 0 & 4 \end{bmatrix}, \quad \text{(v) } A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \\ 1 & 3 & 6 \end{bmatrix},$$

(16) For each of the matrices A from **Problem 15**, find necessary and sufficient conditions on a column vector B so that there exists a column vector X with integer entries solving the linear system $AX = B$. Assuming the system is consistent, find the general integer solution of the system.

(17) In each of the following cases, for the given integer d, find necessary and sufficient conditions on a prime p such that it is properly represented by an integral, binary quadratic form with discriminant equal to d.

$$d = 1, \ d = 2, \ d = -4, \ d = -3, d = -60.$$

(18) In each of the following cases, find an "admissible" linear change of coordinates that transforms the given binary quadratic form to reduced form.

$$\text{(i) } 6x^2 - 5xy + 3y^2, \quad \text{(ii) } 3x^2 - 3xy - 3y^2, \quad \text{(iii) } 17x^2 - 18xy + 4x^2.$$

(19) For each of the following integers d, find all the positive definite, reduced, integral, binary quadratic forms which have discriminant d. In particular, compute the class number $H(d)$.

$$d = -3,\ d = -4,\ d = -8,\ d = -11.$$

(20) For each of the cases from **Problem 19**, find a necessary and sufficient condition on an odd prime p not dividing d such that p is properly represented by a positive definite, reduced, integral, binary quadratic form with discriminant d. Can you determine which form represents which prime p in terms of the residue class of p modulo $4d$?

(21) Does there exist a Pythagorean triple (x, y, z) such that xy is a square integer?

(22) In each of the following cases, find an invertible linear change of coordinates (with rational coefficients) that transforms the given ternary quadratic form to diagonal form. Then use Legendre's theorem to determine whether or not this quadratic form has a solution.

$$f(x, y, z) = (x^2 + yz) + 3(y^2 + xz) + 4(z^2 + xy),$$

$$g(x, y, z) = x^2 - y^2 + 2xz + z^2,$$

$$h(x, y, z) = x^2 + y^2 + z^2 - 2xy - 2xz - 2yz.$$

(23) In each of the following cases, for the given polynomials $(f(x), g(x)) \neq (0, 0)$ with integer coefficients, find the monic greatest common divisor polynomial $c(x)$ as polynomials with rational coefficients. Find the polynomials $f(x)/c(x)$ and $g(x)/c(x)$. Find polynomials $u(x)$ and $v(x)$ with rational coefficients such that $c(x)$ equals $u(x)f(x) + v(x)g(x)$. Finally, find a polynomial with integer coefficients $F_1(x)$, resp. $G_1(x)$, which is a scalar multiple of $f(x)/c(x)$, resp. $g(x)/c(x)$, and such that $F(x)/F_1(x)$ has integer coefficients, resp. $G(x)/G_1(x)$ has integer coefficients.

(a) $f(x) = x + 2$, $g(x) = 2x + 1$.
(b) $f(x) = x^3 + x^2 + x + 1$, $g(x) = x + 1$.
(c) $f(x) = x^3 + x^2 + x + 1$, $g(x) = x^5 + x^4 + x^3 + x^2 + x + 1$.
(d) $f(x) = (x^3 + x)^3$, $g(x) = f'(x) = 3(x^3 + x)^2(3x^2 + 1)$.

(24) For each of the following nonzero algebraic numbers α, find the minimal polynomial $m_\alpha(x)$ of α. Then describe $1/\alpha$ as $f(\alpha)$ for some polynomial $f(x)$ with rational coefficients. Finally, find the minimal polynomial for $1/\alpha$, and find the minimal polynomial for $\alpha - (1/\alpha)$.

(a) $\alpha = 1$.
(b) $\alpha = \sqrt{7}$.
(c) $\alpha = \sqrt[3]{7}$.
(d) $\alpha = \sqrt[3]{7} + 2\sqrt[3]{49}$.
(e) $\alpha = \sqrt{2} + \sqrt{3}$.

(25) For each of the following pairs of algebraic numbers (α, β), find the minimal polynomial of $\alpha + \beta$ and find the minimal polynomial of $\alpha \cdot \beta$.

(a) $(\alpha, \beta) = (1, 2)$.
(b) $(\alpha, \beta) = (\sqrt[3]{7}, \sqrt[3]{7})$.
(c) $(\alpha, \beta) = (\sqrt[3]{7}, \sqrt{3})$.
(d) $(\alpha, \beta) = (\sqrt{2} + \sqrt{3}, \sqrt{3} + \sqrt{6})$.

(26) For each of the following nonzero algebraic numbers α, determine whether or not α is an algebraic integer. When it is an algebraic integer, determine all positive integers n which can be written in the form $\alpha \cdot \beta$ for some choice of algebraic integer β. Finally, for the least positive integer n_1 which can be written in this form, find an algebraic integer β such that $\alpha \cdot \beta$ equals n_1. In particular, say whether or not α is a unit, and if so, find a formula for the multiplicative inverse.

(a) $\alpha = (-1 + \sqrt{2})/2$.
(b) $\alpha = (-1 + \sqrt{3})/2$.
(c) $\alpha = \sqrt{2} + \sqrt{3}$.
(d) $\alpha = \sqrt[3]{81}/3$.

(27) For each of the following squarefree integers m, find the general form of an algebraic integer in $\mathbb{Q}(\sqrt{m})$. When m is negative, describe the group of units in the ring of integers.

$$m = 2,\ m = -1,\ m = -3,\ m = -5.$$

Solution to Problems.

Solution to (1) In general, we can compute c, u and v by repeated application of the division algorithm (this is sometimes called the "Euclidean algorithm"). The simultaneous congruences

$$z \equiv x \pmod{m}, \quad z \equiv y \pmod{n}$$

has a solution if and only if $x \equiv y \pmod{c}$. Indeed, in this case $z = x + cw$ is a solution for every integer w such that $w \equiv 0 \pmod{(m/c)}$ and $w \equiv (y - x)/c \pmod{(n/c)}$. Since n/c and m/c are relatively prime, we can solve this last system of congruences by the Chinese Remainder Theorem, namely $w = um(y - x)/c^2 + qmn/c^2$ for arbitrary integers q.

(a) By repeated application of the division algorithm, $\boxed{c = 1,\ u = 4,\ v = -5}$, i.e., $4 \cdot 114 + (-5) \cdot 91 = 1$. This gives $m/c = 114$, $n/c = 91$. The system of congruences always has a solution, namely $\boxed{z = (-5) \cdot 91 \cdot x + 4 \cdot 114 \cdot y + q \cdot 114 \cdot 91}$ for an arbitrary integer q.

(b) By repeated application of the division algorithm, $\boxed{c = 17,\ u = 2,\ v = -1}$, i.e., $2 \cdot 51 + (-1) \cdot 85 = 17$. This gives $m/c = 3$, $n/c = 5$. The system of congruences has a solution if and only if $x \equiv y \pmod{17}$. In that case the general solution is $\boxed{z = -5x + 6y + q \cdot 3 \cdot 5 \cdot 17}$ for an arbitrary integer q.

(c) By repeated application of the division algorithm, $\boxed{c = 4,\ u = -5,\ v = -3}$, i.e., $(-5) \cdot (-56) + (-3) \cdot 92 = 4$. This gives $m/c = -14$, $n/c = 23$. The system of congruences has a solution if and only if $x \equiv y \pmod{4}$. In that case the general solution is $\boxed{z = -69x + 70y + q \cdot (-14) \cdot 23 \cdot 4}$ for an arbitrary integer q.

(d) By repeated application of the division algorithm, $\boxed{c = 18,\ u = 1,\ v = -1}$, i.e., $1\cdot 72 + (-1)\cdot 54 = 18$. This gives $m/c = -4$, $n/c = 3$. The system of congruences has a solution if and only if $x \equiv y \pmod{18}$. In that case the general solution is $\boxed{z = -3x + 4y + q \cdot 4 \cdot 3 \cdot 18}$ for an arbitrary integer q.

(e) Begin with the equation $1 = (-1)\cdot b + (+1)\cdot(b+1)$. Raising both sides to the fifth power, using the binomial theorem to expand, and gathering factors divisible by b^3 and factors divisible by $(b+1)^3$ gives

$$1 = 1^5 = (-1)^5 b^5 + 5\cdot(-1)^4 b^4 (b+1) + 10\cdot(-1)^3 b^3 (b+1)^2 + 10\cdot(-1)^2 b^2 (b+1)^3 + 5\cdot(-1) b (b+1)^4 + (b+1)^5 =$$

$$(-6(b+1)^2 - 3(b+1) - 1)b^3 + (6b^2 - 3b + 1)(b+1)^3.$$

Thus $\boxed{c = 1,\ u = -6(b+1)^2 - 3(b+1) - 1,\ v = 6b^2 - 3b + 1}$. Thus the congruence always holds. And the general solution is

$$z = \boxed{(6b^2 - 3b + 1)(b+1)^3 x + (-6(b+1)^2 - 3(b+1) - 1)b^3 y + q b^3 (b+1)^3}$$

for an arbitrary integer q.

Solution to (2) Denote $n_1 \cdot \dots \cdot n_r$ by $n_{1,\dots,r}$. Let $u_{r,1}, \dots, u_{r,r}$ be integers such that

$$1 = u_{r,1}\frac{n_{1,\dots,r}}{n_1} + \dots + u_{r,k}\frac{n_{1,\dots,r}}{n_k} + \dots + u_{r,r}\frac{n_{1,\dots,r}}{n_r}.$$

Then for every sequence of integers $(x_1, \dots, x_r)$, for the following integer z,

$$z = u_{r,1}\frac{n_{1,\dots,r}}{n_1}x_1 + \dots + u_{r,k}\frac{n_{1,\dots,r}}{n_k}x_k + \dots + u_{r,r}\frac{n_{1,\dots,r}}{n_r}x_r,$$

for every $k = 1, \dots, r$, $z \equiv x_k \pmod{n_k}$. And the general solution of this system of congruences is $z + qn_{1,\dots,r}$ for an arbitrary integer q. Moreover, given an integer n_{r+1} which is relatively prime to every integer $n_1, \dots, n_r$, then n_{r+1} is relatively prime to the product $n_{1,\dots,r}$. Thus there exist integers v_{r+1} and $u_{r+1,r+1}$ such that

$$1 = v_{r+1}n_{1,\dots,r} + u_{r+1,r+1}n_{1,\dots,r}.$$

Then defining $u_{r+1,k} := v_{r+1}u_{r,k}$ for $k = 1, \dots, r$, we have

$$1 = u_{r+1,1}\frac{n_{1,\dots,r,r+1}}{n_1} + \dots + u_{r+1,k}\frac{n_{1,\dots,r,r+1}}{n_k} + \dots + u_{r+1,r}\frac{n_{1,\dots,r,r+1}}{n_r} + u_{r+1,r+1}\frac{n_{1,\dots,r,r+1}}{n_{r+1}}.$$

Thus the integers $u_{r,k}$ can be computed recursively in r using the Euclidean algorithm.

(a) One solution is $(u_{3,1}, u_{3,2}, u_{3,3}) = (0, 1, -1)$, i.e., $1 = 0(2\cdot 3) + 1(1\cdot 3) + (-1)(1\cdot 2)$. Thus the general solution of the system of congruences is

$$z = \boxed{0x_1 + 3x_2 - 2x_3 + 6q}$$

for an arbitrary integer q. For $(a_1, a_2, a_3) = (0, 1, 2)$, the smallest solution is $\boxed{z = -1}$.

(b) One solution is $(u_{3,1}, u_{3,2}, u_{3,3}) = (1, 1, -9)$, i.e., $1 = 1(9 \cdot 25) + 1(4 \cdot 25) + (-9)(4 \cdot 9)$. Thus the general solution of the system of congruences is

$$z = \boxed{225x_1 + 100x_2 - 324x_3 + 900q}$$

for an arbitrary integer q. For $(a_1, a_2, a_3) = (1, 1, 1)$, the smallest solution is $\boxed{z = 1}$.

(c) One solution is $(u_{4,1}, u_{4,2}, u_{4,3}, u_{4,4}) = (3, 10, -1, 1)$ i.e., $1 = 3(27 \cdot 25 \cdot 7) + 10(16 \cdot 25 \cdot 7) + (-1)(16 \cdot 27 \cdot 7) + (-1)(16 \cdot 27 \cdot 25)$. Thus the general solution of the system of congruences is

$$z = \boxed{(-14175)x_1 + 28000x_2 + (-3024)x_3 - (10800)x_4 + 75600q}$$

for an arbitrary integer q. For $(a_1, a_2, a_3, a_4) = (-1, 1, -1, 1)$, the smallest solution is $\boxed{z = 34399}$.

(d) One solution is $(u_{3,1}, u_{3,2}, u_{3,3}) = (1, -b-2, b^2+b)$, i.e., $1 = 1 \cdot (b+1) \cdot (b(b+1)+1) + (-b-2) \cdot b \cdot (b(b+1)+1) + (b^2+b) \cdot b \cdot (b+1)$. Thus the general solution of the system of congruences is

$$z = \boxed{(b+1)(b(b+1)+1)x_1 + (-b-2)b(b(b+1)+1)x_2 + (b^2+b)b(b+1)x_3 + b(b+1)(b(b+1)+1)q}$$

for an arbitrary integer q. For $(a_1, a_2, a_3) = (1, 0, 0)$, the smallest solution is $\boxed{z = (b+1)(b(b+1)+1)}$.

Solution to (3) Every prime p different from 2 and 3 is congruent to either 1 or -1 modulo 6. In particular, always $p^2 \equiv 1 \pmod{6}$. Let $p_1, \dots, p_r$ be any sequence of primes different from 2 and 3. Consider the integer $n = p_1^2 p_2^2 \cdot \dots \cdot p_r^2 - 2$. This is congruent to $1 \cdot 1 \cdot \dots \cdot 1 - 2 = -1$ modulo 6. Hence it is also congruent to -1 modulo 2 and modulo 3. In particular, it is divisible by neither 2 nor 3. Thus every prime divisor of n is different from 2 and 3.

The claim, to be proved by contradiction, is that at least one prime divisor q of n is congruent to -1 modulo 6. Otherwise n is a product of prime integers, each of which is congruent to 1 modulo 6. And thus also n is congruent to 1 modulo 6, which contradicts that $n \equiv -1 \pmod{6}$. Therefore there exists a prime divisor q which is congruent to -1 modulo 6. If q equals any of $p_1, \dots, p_r$, then q also divides $m = p_1^2 \cdot p_2^2 \cdot \dots \cdot p_r^2$. Thus q divides the difference $m - n = 2$. But this contradicts that q is different from 2. Therefore q is a prime different from each of $p_1, \dots, p_r$ such that $q \equiv -1 \pmod{6}$. Thus there exist infinitely many primes which are congruent to -1 modulo 6.

Solution to (4) In the following table, assuming there exists an integer $b_{i,j}$ such that $b_{i,j}a_i \equiv 1 \pmod{n_j}$, one such integer $b_{i,j}$ is given in the (i, j) position.

	8	27	25	49	51
1	1	1	1	1	1
2		-13	-12	-24	-25
3	3		-8	-16	
4		7	-6	-12	13

Solution to (5) The main properties of the Euler phi function are that $\phi(mn) = \phi(m)\phi(n)$ if m and n are relatively prime, and $\phi(p^r) = p^{r-1}(p-1)$ for every prime integer p and every integer $r > 0$. Also $\phi(1) = 1$. Together these rules determine $\phi(n)$ for every positive integer n.

$$\boxed{\phi(2) = 1,\ \phi(7) = 6,\ \phi(16) = 8,\ \phi(14) = 6, \phi(105) = 24,\ \phi(75) = 40}.$$

Solution to (6) An integer n is a sum of two squares if and only if the squarefree part m of n is divisible by no odd prime congruent to 3 modulo 4. In the following, for each integer which is a sum of two squares, one such representation is given.

$$\boxed{0 = 0^2 + 0^2,\ 1 = 0^2 + 1^2,\ 4 = 0^2 + 2^2,\ 29 = 2^2 + 5^2,\ 49 = 0^2 + 7^2\ 61 = 5^2 + 6^2}.$$

Solution to (7) In each of the following cases, (u, v) are integers such that $1 = ua + vb$. Let (x, y) be given integers. The integers z such that $z \equiv x \pmod{a}$ and $z \equiv y \pmod{b}$ are precisely the integers $z = vbx + uay + qab$ for arbitrary integers q. And by the Chinese Remainder Theorem, $f(z) \equiv 0 \pmod{ab}$ if and only if $f(x) \equiv 0 \pmod{a}$ and $f(y) \equiv 0 \pmod{b}$. Therefore the set of integers z such that $f(z) \equiv 0 \pmod{ab}$ are precisely the integers z as above for pairs (x, y) of integers solving f modulo a, resp. modulo b.

(a) One pair (u, v) is $(-3, 1)$, i.e., $1 = (-3) \cdot 2 + 1 \cdot 7$. There are $\boxed{\text{no solutions}}$ of $7 \equiv 0 \pmod{2}$. And the solutions of $7 \equiv 0 \pmod{7}$ are $\boxed{\text{all integers}}$. Since there are no solutions modulo 2, also there are $\boxed{\text{no solutions}}$ modulo $2 \cdot 7$.

(b) One pair (u, v) is $(-2, 1)$, i.e., $1 = (-2) \cdot 2 + 1 \cdot 5$. The solutions of $3x - 1 \equiv 0 \pmod{2}$ are the integers $x = \boxed{1 + 2q}$ where q is an arbitrary integer. The solutions of $3y - 1 \equiv 0 \pmod{5}$ are the integers $y = \boxed{2 + 5q}$ where q is an arbitrary integer. Therefore the solutions of $3z - 1 \equiv 0 \pmod{2 \cdot 5}$ are the integers $z = 1 \cdot 5 \cdot 1 + (-2) \cdot 2 \cdot 2 + 2 \cdot 5 \cdot q = \boxed{-3 + 10q}$ where q is an arbitrary integer.

(c) One pair (u, v) is $(-1, 1)$, i.e., $1 = (-1) \cdot 8 + 1 \cdot 9$. The solutions of $x^2 \equiv 0 \pmod{8}$ are the integers $x = \boxed{0 + 8q}$ and $x = \boxed{4 + 8q}$ where q is an arbitrary integer, i.e., $x = \boxed{4m + 8q}$ where $m = 0, 1$ and where q is an arbitrary integer. The solutions of $y^2 \equiv 0 \pmod{9}$ are the integers $y = \boxed{0 + 9q}$, $y = \boxed{3 + 9q}$ and $y = \boxed{-3 + 9q}$ where q is an arbitrary integer, i.e., $y = \boxed{3n + 9q}$ where $n = -1, 0, 1$ and where q is an arbitrary integer. Therefore the solutions of $z^2 \equiv 0 \pmod{8 \cdot 9}$ are the integers

$$z = 1 \cdot 9 \cdot 4m + (-1) \cdot 8 \cdot 3n + 8 \cdot 9 \cdot q = 12(3m - 2n) + 72q.$$

Letting m and n vary, this just gives $z = \boxed{12k}$ for arbitrary integers k.

(d) One pair is $(u, v) = (2, -1)$, i.e., $1 = 2 \cdot 7 + (-1) \cdot 13$. By Fermat's Little Theorem, the solutions of $x^6 - 1 \equiv 0 \pmod{7}$ are precisely all integers x with $\boxed{x \not\equiv 0 \pmod{7}}$, i.e., $x = \pm 3 + 7q, \pm 2 + 7q, \pm 1 + 7q$. And by computation, the solutions of $y^6 - 1 \equiv 0 \pmod{7}$ are the integers $y = \boxed{3^n + 13q}$ with

$n = 0, \dots, 5$, i.e., $y = \pm 4 + 13q, \pm 3 + 13q, \pm 1 + 13q$. Therefore the solutions of $z^6 - 1 \equiv 0 \pmod{7 \cdot 13}$ are the integers

$$z = (-1) \cdot 13x + 2 \cdot 7 \cdot y + 7 \cdot 13 \cdot q = -13x + 14y + 91q.$$

Thus the solutions are

$$z = \boxed{\pm 1, \pm 3, \pm 4, \pm 9, \pm 10, \pm 12, \pm 16, \pm 17, \pm 22, \pm 23, \pm 25, \pm 27, \pm 29, \pm 30, \pm 36, \pm 40, \pm 43, \pm 53 + 91q}$$

where q is an arbitrary integer.

(e) The pair (u, v) is as in the previous part. There are no solutions to $x^6 + 1 \equiv 0 \pmod 7$. The solutions of $y^6 + 1 \equiv 0 \pmod{13}$ are the integers $y = 2 \cdot 3^n + 13q$ with $n = 0, \dots, 5$, i.e., $y = \boxed{\pm 2, \pm 5, \pm 6 + 13q}$ for q an arbitrary integer. Since there are no solutions modulo 7, there are no solutions modulo $7 \cdot 13$.

Solution to (8) Let p be a prime integer, let $e \geq 1$ be an integer, and let a_e be an integer such that $f(a_e) \equiv 0 \pmod{p^e}$, i.e., a_e is a solution of $f(x)$ modulo p^e. Further assume that there exists an integer u such that $uf'(a_e) \equiv 1 \pmod p$, i.e., u is a multiplicative inverse of $f'(a_e)$ modulo p. Such an integer u exists if and only if $f'(a_e) \not\equiv 0 \pmod p$, i.e., a_e is not a critical point of $f(x)$ modulo p. Then by Hensel's lemma there exists an integer a_{e+1} such that $a_{e+1} \equiv a_e \pmod{p^e}$ and $f(a_{e+1}) \equiv 0 \pmod{p^{e+1}}$, i.e., a_{e+1} is a solution modulo p^{e+1} which agrees with the given solution a_e modulo p^e. Moreover there is a formula for a_{e+1} by the "p-adic version of Newton's method",

$$a_{e+1} = a_e - uf(a_e) + p^{e+1}q,$$

where q is an arbitrary integer.

(a) There is no solution, in particular a_1 is not a solution.

(b) Since $f(a_1) = 5$, which is congruent to 0 modulo p, a_1 is a solution modulo p. Moreover $f'(a_1) = 3$ is nonzero modulo p, so a_1 is a not a critical point modulo p. For the integer $u = 2$, $uf'(a_1) \equiv 1 \pmod p$. Thus Hensel's lemma gives a formula for a_2,

$$a_2 = a_1 - uf(a_1) = 2 - 2 \cdot 5 = \boxed{-8} + p^2q$$

for q an arbitrary integer. And $f(a_2)$ equals $-25 + 3p^2q$. So applying Hensel's lemma once more gives a formula for a_3,

$$a_3 = a_2 - uf(a_2) = -8 + p^2q - 2(-25 + 3p^2q) = \boxed{42} + p^3q$$

for q an arbitrary integer.

(c) Since $f(a_1) = 1$ is not congruent to 0 modulo p, a_1 is not a solution modulo p.

(d) Since $f(a_1) = 728$, which is congruent to 0 modulo p, a_1 is a solution modulo p. Moreover $f'(a_1) = 6a_1^5 \equiv (-1)(-2) = 2 \pmod p$, so a_1 is a not a critical point modulo p. For the integer $u = -3$, $uf'(a_1) \equiv 1 \pmod p$. Thus Hensel's lemma gives a formula for a_2,

$$a_2 = a_1 - uf(a_1) + p^2q = 3 + 3 \cdot 728 + p^2q = \boxed{-18} + p^2\tilde{q}$$

for $\tilde{q}$ an arbitrary integer. And $f(a_2)$ equals $p^2(694127) + 2p^2\tilde{q} + p^3\tilde{q}_1$, where $\tilde{q}_1$ is divisible by q^2. Notice that 694127 happens to be divisible by p, $694127 = p \cdot 99161$. So applying Hensel's lemma once more gives the formula,

$$a_3 = a_2 - uf(a_2) = -18 + p^2\tilde{q} + 3p^3 99161 - p^2\tilde{q} + p^3\tilde{q}_2 = \boxed{-18} + p^3\tilde{q}_2$$

for $\tilde{q}_2$ an arbitrary integer.

(e) Since $f(a_1) = 65 = 5p$, a_1 is a solution modulo p. Moreover we have

$$f'(a_1) = 6a_1^5 = 6 \cdot 32 = p^2 + 2p - 3 \equiv -3 \pmod{p},$$

so a_1 is a not a critical point modulo p. While we are at it, also we have

$$f''(a_1)/2 = 6 \cdot 5 \cdot a_1^4/2 = 3 \cdot 5 \cdot 16 = p^2 + 5p + 6 \equiv 6 \pmod{p}.$$

For the integer $u = 4$, $uf'(a_1) \equiv 1 \pmod{p}$. Thus Hensel's lemma gives a formula for a_2,

$$a_2 = a_1 - uf(a_1) + p^2 q = 2 - 4 \cdot 5p + p^2 q = 2 + 6p + p^2\tilde{q} = \boxed{80} + p^2\tilde{q}$$

for $\tilde{q}$ an arbitrary integer. And by the Taylor expansion we have

$$f(a_2) \equiv f(a_1) - uf'(a_1)f(a_1) + u^2 f''(a_1)/2(f(a_1))^2 + f'(a_1)p^2\tilde{q} \pmod{p^3}.$$

This gives

$$f(a_2) \equiv 5p - 4(p^2 + 2p - 3)5p + 16 \cdot (p^2 + 5p + 6) \cdot 25p^2 + (p^2 + 2p - 3)\tilde{q}p^2$$
$$\equiv 5p - 40p^2 + 60p + 16 \cdot 6 \cdot 25p^2 - 3\tilde{q}p^2 \equiv 5p^2 - 1p^2 - 5p^2 - 3\tilde{q}p^2 \equiv -1p^2 - 3\tilde{q}p^2 \pmod{p^3}.$$

So applying Hensel's lemma once more gives the formula,

$$a_3 = a_2 - uf(a_2) \equiv 2 + 6p + p^2\tilde{q} + 4p^2 + 12\tilde{q}p^2 \equiv 2 + 6p + 4p^2 \pmod{p^3}.$$

So $a_3 = 2 + 6p + 4p^2 + p^3\tilde{q}_2 = \boxed{756} + p^3\tilde{q}_2$, where $\tilde{q}_2$ is an arbitrary integer.

Solution to (9) For an integer n, the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 1$, p^r, $2p^r$, 2 or 4, where p is an odd prime. The size of the multiplicative group is $\phi(n)$, which for these particular integers is given by

$$\phi(1) = 1,\ \phi(p^r) = (p-1)p^{r-1},\ \phi(2p^r) = (p-1)p^{r-1},\ \phi(2) = 1,\ \phi(4) = 2.$$

If g is one primitive root, then every primitive root is of the form g^e where e is a nonnegative integer relatively prime to $\phi(n)$. Moreover g^d equals g^e if and only if $d \equiv e \pmod{\phi(n)}$. So the set of primitive roots is in one-to-one correspondence with the units in $\mathbb{Z}/\phi(n)\mathbb{Z}$, i.e., with the multiplicative group $(\mathbb{Z}/\phi(n)\mathbb{Z})^\times$, which has size $\phi(\phi(n))$. For the integers n as above, this equals

$\phi(\phi(1)) = 1$, $\phi(\phi(p)) = \phi(\phi(2p)) = \phi(p-1)$, $\phi(\phi(p^r)) = \phi(\phi(2p^r)) = (p-1)p^{r-2}\phi(p-1)$ for $r \geq 2$, $\phi(\phi(2)) = 1$, To get all primitive roots precisely once, we can restrict to those integer exponents e relatively prime to $\phi(n)$ contained in a residue system modulo $\phi(n)$, say $0 \leq e < \phi(n)$.

For the integers $n = 13, 14 = 2 \cdot 7, 8 = 2^3, 27 = 3^3, 257$, the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic except for $n = 8$. Denote by g_n the smallest positive integer which is a primitive root modulo n. Then we have

$$g_{13} = 4,\ g_{14} = 3,\ g_{3^3} = 6,\ g_{257} = 3.$$

Except for the final one, these are easy to find by hand. For the final generator, use Problem 3.2.16, p. 141, from Problem Set 5. The number of primitive roots in each of these cases is

$$\phi(\phi(13)) = 4,\ \phi(\phi(14)) = 2,\ \phi(3^3) = 6,\ \phi(257) = 128.$$

For each integer n, the set of all primitive roots is g_n^e as e ranges over integers $0 \leq e < \phi(n)$ which are relatively prime to $\phi(n)$, hence,

$$g_{13}^1, g_{13}^5, g_{13}^7, g_{13}^{11};\ \ g_{14}^1, g_{14}^5;\ \ g_{3^3}^1, g_{3^3}^5, g_{3^3}^7, g_{3^3}^{11}, g_{3^3}^{13}, g_{3^3}^{17};\ \ g_{257}^e, 0 \leq e < 256, e \text{ is odd}\ .$$

Solution to (10) Let n be an integer such that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, i.e., there exists a primitive root g. Then units which are quadratic residues are precisely the units of the form g^e for $0 \leq e < \phi(n)$ with e even. And the units which are quadratic nonresidues are precisely the units of the form g^e for $0 \leq e < \phi(n)$ with e odd.

Solution to (11) For each of the integers $n = 3, 7, 11, 19, 23$, it is straightforward to compute by hand the set of units which are quadratic residues.

n	quad. res.
3	1.
7	$1, 2, -3$
11	$1, -2, 3, 4, 5.$
19	$1, -2, -3, 4,$ $5, 6, 7, -8, 9.$
23	$1, 2, 3, 4, -5, 6,$ $-7, 8, 9, -10, -11.$

From this table it is immediate to compute these Legendre symbols,

$$\left(\frac{2}{3}\right) = -1,\ \left(\frac{3}{7}\right) = -1,\ \left(\frac{-1}{11}\right) = -1,\ \left(\frac{2}{11}\right) = -1,\ \left(\frac{6}{19}\right) = +1,\ \left(\frac{-9}{23}\right) = -1.$$

The most basic identity for the Legendre symbol is

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$$

whenever $a \equiv a'$ (mod p). One can also use the identity

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

which in particular gives that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. And one can use the multiplicative properties

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right), \quad \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

Together these simplify several of the computations above.

Solution to (12) Quadratic reciprocity gives both

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

and

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)/2\cdot(q-1)/2}$$

for odd primes p and q. When combined with the multiplicative property of the Legendre symbol, this suffices to compute many Legendre symbols.

$$\left(\frac{2}{11}\right) = (-1)^{((12/2)\cdot(10/2))/2} = (-1)^{15} = \boxed{-1}.$$

$$\left(\frac{7}{53}\right)\left(\frac{53}{7}\right) = (-1)^{(6/2)\cdot(52/2)} = (-1)^{3\cdot 26} = +1.$$

$$\left(\frac{7}{53}\right) = +1\left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = \boxed{+1}.$$

$$\left(\frac{14}{53}\right) = \left(\frac{2}{53}\right)\cdot\left(\frac{7}{53}\right) = \left(\frac{2}{53}\right)\cdot(+1) = (-1)^{((54/2)\cdot(52/2))/2} = (-1)^{27\cdot 13} = \boxed{-1}.$$

$$\left(\frac{30}{53}\right) = \left(\frac{2}{53}\right)\left(\frac{3}{53}\right)\left(\frac{5}{53}\right) = (-1)\left(\frac{53}{3}\right)\left(\frac{53}{5}\right) = (-1)\left(\frac{-1}{3}\right)\left(\frac{-2}{5}\right) = (-1)(-1)(-1) = \boxed{-1}.$$

$$\left(\frac{53}{257}\right) = \left(\frac{257}{53}\right) = \left(\frac{-8}{53}\right) = \left(\frac{-1}{53}\right)\left(\frac{2}{53}\right) = (-1)^{26}(-1) = \boxed{-1}.$$

$$\left(\frac{-2}{257}\right) = \left(\frac{-1}{257}\right)\left(\frac{2}{257}\right) = (-1)^{128}(-1)^{(129\cdot 128)/2} = (+1)(+1) = \boxed{+1}.$$

Solution to (13) The goal in each of these cases is to determine when the Legendre symbol $\left(\frac{a}{p}\right)$ equals $+1$. Using the properties of the Legendre symbol and quadratic reciprocity, this can be reduced to a condition on the residue class of p modulo a fixed integer n depending only on a.

$$\left(\frac{7}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{7}\right).$$

Also $(-1)^{(p-1)/2}$ is congruent to p modulo 4, and $\left(\frac{b}{7}\right)$ equals $+1$ for $b \equiv 1, 2, -3 \pmod{7}$, resp. equals -1 for $b \equiv -1, -2, 3 \pmod{7}$. Using the Chinese remainder theorem, this gives

$$\left(\frac{7}{p}\right) = +1 \text{ if and only if } \boxed{p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}}.$$

$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = +1 \text{ if and only if } \boxed{p \equiv \pm 1, \pm 3, \pm 4 \pmod{13}}.$$

$$\left(\frac{91}{p}\right) = \left(\frac{7}{p}\right) \cdot \left(\frac{13}{p}\right).$$

This equals $+1$ if the two factors are either both $+1$ or both -1. Using the two previous cases, this happens if and only if $p \equiv i \pmod{28}$ and $p \equiv j \pmod{13}$ where i and j are among the following pairs of residue classes,

$$\boxed{i = \pm 1, \pm 3, \pm 9 \text{ and } j = \pm 1, \pm 3, \pm 4}$$

or else

$$\boxed{i = \pm 5, \pm 11, \pm 13 \text{ and } j = \pm 2, \pm 5, \pm 6}.$$

Using the Chinese Remainder Theorem, this is equivalent to saying that $p \equiv k \pmod{13 \cdot 28}$ where

$$k \equiv 13 \cdot 13i + (-6) \cdot 28 \cdot j \pmod{13 \cdot 28}.$$

$$\left(\frac{44}{p}\right) = \left(\frac{11}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{11}\right).$$

By the same type of argument as in the case of $a = 7$, this gives

$$\left(\frac{44}{p}\right) = +1 \text{ if and only if } \boxed{p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \pmod{44}}.$$

$$\left(\frac{27}{p}\right) = \left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

By the same type of argument as in the case of $a = 7$, this gives

$$\left(\frac{27}{p}\right) = +1 \text{ if and only if } \boxed{p \equiv \pm 1 \pmod{12}}.$$

Solution to (14) Let $(a, b) \neq (0, 0)$ be a pair of integers. Let g be the gcd and let (u, v) be integers such that $au + bv = g$. Then the system $ax + by = c$ is consistent if and only if g divides c, and then the general solution is

$$(x, y) = (u(c/g) + (b/g)q, v(c/g) - (a/g)q)$$

where q is an arbitrary integer.

(i) We have $g = 1$ and $(u, v) = (-2, 1)$, i.e., $1 = -2 \cdot 7 + 1 \cdot 15$. Thus the system is $\boxed{\text{consistent}}$ and the general solution is

$$(x, y) = \boxed{(-3 + 15q, 2 - 7q)}$$

where q is an arbitrary integer.

(ii) We have $g = 3$ and $(u, v) = (-6, -13)$, i.e., $3 = (-6) \cdot 84 + (-13) \cdot (-39)$. Thus the system

$$84x - 39y = c$$

is consistent if and only if $c \equiv 0 \pmod{3}$, and then the general solution is

$$(x, y) = (-2c + 13q, -13(c/3) + 28q)$$

where q is an arbitrary integer. In particular, since $41 \not\equiv 0 \pmod{3}$, this system is $\boxed{\text{inconsistent}}$.

(iii) Since $42 \equiv 0 \pmod{3}$, this system is $\boxed{\text{consistent}}$. And the general solution is

$$(x, y) = (-84 + 13q, -182 + 28q) = \boxed{(7 + 13\tilde{q}, 14 + 28\tilde{q})}.$$

(iv) This was solved in (ii).

(v) The gcd of 15, 21 and 35 is 1, $1 = 1 \cdot 15 + 1 \cdot 21 + (-1) \cdot 35$. Thus the system $15x + 21y + 35z = t$ is always consistent, and the general solution is

$$(x, y, z) = (t - 21q - 14r, t - 20q - 15r, -t + 21q + 15r)$$

where q and r are arbitrary integers. In particular the system

$$15x + 21y + 35z = 14$$

is $\boxed{\text{consistent}}$ and the general solution is

$$(x, y, z) = \boxed{-21q - 14\tilde{r}, -1 - 20q - 15\tilde{r}, 1 + 21q + 15\tilde{r})}$$

where q and $\tilde{r}$ are arbitrary integers.

Solution to (15) Each of these are computed by the same elementary row and column operation algorithm as described on the review sheet for Midterm 2. So I will just give one answer for each problem (there are typically many choices for U and V).

(i)

$$U = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}, \ V = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \ UAV = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

(ii)

$$U = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 0 & -1 \\ 5 & -4 & 0 \end{bmatrix}, \ V = \begin{bmatrix} -2 & 0 & 5 \\ 1 & 0 & -2 \\ -6 & 1 & 15 \end{bmatrix}, \ UAV = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \end{bmatrix}.$$

(iii)

$$U = \begin{bmatrix} 1 & 0 & -1 \\ 4 & 0 & -5 \\ -1 & 1 & -1 \end{bmatrix}, \ V = \begin{bmatrix} 1 & -17 \\ 0 & 1 \end{bmatrix}, \ UAV = \begin{bmatrix} 1 & 0 \\ 0 & 75 \\ 0 & 0 \end{bmatrix}.$$

(iv)

$$U = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ -1 & 1 & -2 \end{bmatrix}, \ V = \begin{bmatrix} 1 & 3 & -1 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \ UAV = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

(v)

$$U = \begin{bmatrix} 3 & 0 & -2 \\ -1 & 0 & 1 \\ 1 & 1 & -2 \end{bmatrix}, \ V = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix}, \ UAV = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Solution to (16) Write $UAV = [a'_{i,j}]_{1\leq i\leq m, 1\leq j\leq n}$, where $a'_{i,j}$ equals 0 if $i \neq j$. Define $B' = UB = (b'_1, \dots, b'_m)^\dagger$ and $X = VX'$, where $X' = (x'_1, \dots, x'_n)^\dagger$. Then the original system $AX = B$ is equivalent to the new system $(UAV)X' = B'$. Since UAV is in block diagonal form, the system is consistent if and only if $a'_{i,i}$ divides b'_i for every $i = 1, \dots, m$. And in this case the general solution is $x'_j = b'_j/a_{j,j}$ for every $j = 1, \dots, m$ with $a_{j,j} \neq 0$, x'_j is free for every $j = 1, \dots, m$ with $a_{j,j} = b'_j = 0$, and x'_j is free for every $j = m+1, \dots, n$.

(i) The equation $B' = UB$ gives

$$\begin{bmatrix} b'_1 \\ b'_2 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} b_1 - b_2 \\ b_1 \end{bmatrix}.$$

The new system is

$$\left\{ \begin{array}{rcccr} x'_1 & = & b'_1 & = & b_1 - b_2 \\ 2x'_2 & = & b'_2 & = & b_1 \end{array} \right.$$

So the system is consistent if and only if

$$\boxed{b_1 \equiv 0 \pmod{2}}.$$

And in this case the general solution is $(x_1', x_2') = (b_1 - b_2, b_1/2)$. Changing back to the original coordinates gives the general solution $X = VX'$,

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} b_1 - b_2 \\ \frac{1}{2}b_1 \end{bmatrix} = \boxed{\begin{bmatrix} \frac{1}{2}b_1 \\ \frac{3}{2}b_1 - b_2 \end{bmatrix}}.$$

(ii) The equation $B' = UB$ gives

$$\begin{bmatrix} b_1' \\ b_2' \\ b_3' \end{bmatrix} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 0 & -1 \\ 5 & -4 & 0 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_1 - b_2 \\ -b_3 \\ 5b_1 - 4b_2 \end{bmatrix}.$$

The new system is

$$\left\{ \begin{array}{rcccc} x_1' & = & b_1' & = & b_1 - b_2 \\ x_2' & = & b_2' & = & -b_3 \\ 10x_3' & = & b_3' & = & 5b_1 - 4b_2 \end{array} \right.$$

So the system is consistent if and only if

$$\boxed{5b_1 - 4b_2 \equiv 0 \pmod{10}}.$$

And in this case the general solution is $(x_1', x_2') = (b_1 - b_2, -b_3, \frac{5}{10}b_1 - \frac{4}{10}b_2)$. Changing back to the original coordinates gives the general solution $X = VX'$,

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -2 & 0 & 5 \\ 1 & 0 & -2 \\ -6 & 1 & 15 \end{bmatrix} \begin{bmatrix} b_1 - b_2 \\ -b_3 \\ \frac{5}{10}b_1 - \frac{4}{10}b_2 \end{bmatrix} = \boxed{\begin{bmatrix} \frac{1}{2}b_1 \\ -\frac{1}{5}b_2 \\ \frac{3}{2}b_1 - b_3 \end{bmatrix}}.$$

(iii) The equation $B' = UB$ gives

$$\begin{bmatrix} b_1' \\ b_2' \\ b_3' \end{bmatrix} = \begin{bmatrix} 1 & 0 & -1 \\ 4 & 0 & -5 \\ -1 & 1 & -1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_1 - b_3 \\ 4b_1 - 5b_3 \\ -b_1 + b_2 - b_3 \end{bmatrix}.$$

The new system is

$$\left\{ \begin{array}{rcccc} x_1' & = & b_1' & = & b_1 - b_3 \\ 75x_2' & = & b_2' & = & 4b_1 - 5b_3 \\ 0 & = & b_3' & = & -b_1 + b_2 - b_3 \end{array} \right.$$

So the system is consistent if and only if

$$\boxed{4b_1 - 5b_2 \equiv 0 \pmod{75} \text{ and } -b_1 + b_2 - b_3 = 0}.$$

And in this case the general solution is $(x'_1, x'_2) = (b_1 - b_3, \frac{1}{75}(4b_1 - 5b_3)$. Changing back to the original coordinates gives the general solution $X = VX'$,

$$\left[\begin{array}{c} x_1 \\ x_2 \end{array}\right] = \left[\begin{array}{rr} 1 & -17 \\ 0 & 1 \end{array}\right] \left[\begin{array}{c} b_1 - b_3 \\ \frac{1}{75}(4b_1 - 5b_3) \end{array}\right] = \boxed{\left[\begin{array}{c} \frac{7}{75}b_1 + \frac{10}{75}b_3 \\ \frac{4}{75}b_1 - \frac{5}{75}b_3 \end{array}\right]}.$$

(iv) The equation $B' = UB$ gives

$$\left[\begin{array}{c} b'_1 \\ b'_2 \\ b'_3 \end{array}\right] = \left[\begin{array}{rrr} 1 & 0 & 0 \\ -2 & 0 & 1 \\ -1 & 1 & -2 \end{array}\right] \left[\begin{array}{c} b_1 \\ b_2 \\ b_3 \end{array}\right] = \left[\begin{array}{c} b_1 \\ -2b_1 + b_3 \\ -b_1 + b_2 - 2b_3 \end{array}\right].$$

The new system is

$$\left\{\begin{array}{rcccc} x'_1 & = & b'_1 & = & b_1 \\ 6x'_2 & = & b'_2 & = & -2b_1 + b_3 \\ 0 & = & b'_3 & = & -b_1 + b_2 - 2b_3 \end{array}\right.$$

So the system is consistent if and only if

$$\boxed{-2b_1 + b_3 \equiv 0 \pmod{6} \text{ and } -b_1 + b_2 - 2b_3 = 0}.$$

And in this case the general solution is $(x'_1, x'_2, x'_3, x'_4) = (b_1, -\frac{2}{6}b_1 + \frac{1}{6}b_3, t_1, t_2)$ where t_1 and t_2 are arbitrary integers. Changing back to the original coordinates gives the general solution $X = VX'$,

$$\left[\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \end{array}\right] = \left[\begin{array}{rrrr} 1 & 3 & -1 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] \left[\begin{array}{c} b_1 \\ -\frac{2}{6}b_1 + \frac{1}{6}b_3 \\ t_1 \\ t_2 \end{array}\right] = \boxed{\left[\begin{array}{c} \frac{1}{2}b_3 - t_1 - 2t_2 \\ t_1 \\ -\frac{1}{3}b_1 + \frac{1}{6}b_3 \\ t_2 \end{array}\right]}$$

where t_1 and t_2 are arbitrary integers.

(v) The equation $B' = UB$ gives

$$\left[\begin{array}{c} b'_1 \\ b'_2 \\ b'_3 \end{array}\right] = \left[\begin{array}{rrr} 3 & 0 & -2 \\ -1 & 0 & 1 \\ 1 & 1 & -2 \end{array}\right] \left[\begin{array}{c} b_1 \\ b_2 \\ b_3 \end{array}\right] = \left[\begin{array}{c} 3b_1 - 2b_3 \\ -b_1 + b_3 \\ b_1 + b_2 - 2b_3 \end{array}\right].$$

The new system is

$$\left\{\begin{array}{rcccc} x'_1 & = & b'_1 & = & 3b_1 - 2b_3 \\ x'_2 & = & b'_2 & = & -b_1 + b_3 \\ 0 & = & b'_3 & = & b_1 + b_2 - 2b_3 \end{array}\right.$$

So the system is consistent if and only if

$$\boxed{b_1 + b_2 - 2b_3 = 0}.$$

And in this case the general solution is $(x_1', x_2', x_3') = (3b_1 - 2b_3, -b_1 + b_3, t)$ where t is an arbitrary integer. Changing back to the original coordinates gives the general solution $X = VX'$,

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3b_1 - 2b_3 \\ -b_1 + b_3 \\ t \end{bmatrix} = \boxed{\begin{bmatrix} 3b_1 - 2b_3 + 3t \\ -b_1 + b_3 - 3t \\ t \end{bmatrix}}$$

where t is an arbitrary integer.

Solution to (17) For an integer d and a prime p, there exists an integral, binary quadratic form with discriminant d representing p if and only if d is congruent to a square modulo $4p$. So 2 is represented if and only if d is congruent to a square modulo 8, i.e., $d \equiv 0, 1, 4 \pmod{8}$. And for every odd prime p, p is represented if and only if d is congruent to a square modulo 4, i.e., $d \equiv 0, 1 \pmod{4}$, and d is congruent to a square modulo p. If p divides d, this second condition is automatic. If d is relatively prime to p, then the second condition says precisely that $\left(\frac{d}{p}\right) = +1$. And using quadratic reciprocity this can be reduced to a condition on the residue class of p modulo a fixed integer e, just as in **Problem 13**. The following results follow by the same method as in the **Solution to Problem 13**.

(i) For $d = 1$, for every integer n, $d \equiv 1^2 \pmod{n}$. Therefore $\boxed{\text{every prime is represented}}$ by an integral, binary quadratic form with discriminant 1. To be explicit, the quadratic form $f(x, y) = xy$ has discriminant 1 and represents p: $f(p, 1) = p$.

(ii) For $d = 2$, d is not congruent to a square modulo 4. Thus there does not exist an integral, binary quadratic form with discriminant 2. Therefore $\boxed{\text{no prime is represented}}$ by an integral, binary quadratic form with discriminant 2.

(iii) For $d = -4$, $d \equiv 0^2 \pmod{4}$, so there does exist at least one integral, binary quadratic form with discriminant -4. In fact every such (positive definite) form is equivalent to the unique reduced form $f(x, y) = x^2 + y^2$. Since $d \equiv 2^2 \pmod{8}$, $\boxed{\text{2 is represented}}$ by $f(x, y)$; explicitly $f(1, 1) = 2$. For every odd prime p,

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Therefore an odd prime p is represented by $f(x, y)$ if and only if $\boxed{p \equiv 1 \pmod{4}}$.

(iv) For $d = -3$, $d \equiv 1^2 \pmod{4}$, so there does exist at least one integral, binary quadratic form with discriminant -3. In fact every such (positive definite) form is equivalent to the unique reduced form $f(x, y) = x^2 + xy + y^2$. And $d \not\equiv 0, 1, 4 \pmod{8}$. Thus $\boxed{\text{2 is not represented}}$ by $f(x, y)$. Since 3 divides d, $\boxed{\text{3 is represented}}$ by $f(x, y)$; explicitly $f(1, 1) = 3$. And for odd primes $p \neq 3$, by quadratic reciprocity

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right).$$

Therefore an odd prime $p \neq 3$ is represented by $f(x, y)$ if and only if $\boxed{p \equiv 1 \pmod{3}}$.

(v) For $d = -60$, $d \equiv 0^2 \pmod 4$, so there do exist integral, binary quadratic forms with discriminant -60. The (positive definite) reduced forms are

$$f_{1,\pm}(x,y) = 2(x^2 \pm xy + 4y^2),\ f_2(x,y) = 2(2x^2+xy+2y^2),\ f_3(x,y) = x^2+15y^2,\ f_4(x,y) = 3x^2+5y^2.$$

Since $d \equiv 0 \pmod 8$, $\boxed{\text{2 is represented}}$; explicitly $f_{1,pm}(1,0) = 2$. For $p = 3, 5$, since p divides d, $\boxed{\text{3 and 5 are represented}}$; explicitly $f_4(1,0) = 3$ and $f_4(0,1) = 5$. And for an odd prime $p \neq 3, 5$, by quadratic reciprocity, $\left(\frac{-60}{p}\right) = \left(\frac{-15}{p}\right)$ equals $+1$, i.e, p is represented, if and only if $\boxed{p \equiv 1, 4, 2, -7 \pmod{15}}$; more explicitly, p is represented by f_3 if and only if $p \equiv 1, 4 \pmod{15}$ and p is represented by f_4 if and only if $p \equiv 2, -7 \pmod{15}$.

Solution to (18) This is similar to problems discussed on the review sheet for Midterm 2. So I will only list the answer.

(i) For the admissible linear change of coordinates $(x,y) = \boxed{(\tilde{y}, -\tilde{x} + \tilde{y})}$, the new form is reduced,

$$\tilde{f}(\tilde{x},\tilde{y}) = \boxed{3\tilde{x}^2 - \tilde{x}\tilde{y} + 4\tilde{y}^2}.$$

(ii) For the admissible linear change of coordinates $(x,y) = \boxed{(\tilde{y}, -\tilde{x})}$, the new form is reduced,

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

(iii) For the admissible linear change of coordinates $(x,y) = \boxed{(-\tilde{x}, -\tilde{y} - 2\tilde{x})}$, the new form is reduced,

$$\tilde{f}(\tilde{x},\tilde{y}) = \boxed{-3\tilde{x}^2 - 2\tilde{x}\tilde{y} + 4\tilde{y}^2}.$$

Solution to (19) This is similar to problems discussed on the review sheet for Midterm 2. So I will only list the answer.

(i) There is a $\boxed{\text{unique reduced}}$ positive definite form of discriminant -3,

$$f(x,y) = \boxed{x^2 + xy + y^2}.$$

In particular, $\boxed{H(-3) = 1}$.

(ii) There is a $\boxed{\text{unique reduced}}$ positive definite form of discriminant -4,

$$f(x,y) = \boxed{x^2 + y^2}.$$

In particular, $\boxed{H(-4) = 1}$.

(iii) There is a unique reduced positive definite form of discriminant -8,

$$f(x,y) = x^2 + 2y^2.$$

In particular, $H(-8) = 1$.

(iv) The class number is $H(-11) = 1$, although there are two distinct reduced positive definite forms of discriminant -3:

$$f_+(x,y) = x^2 + xy + 3y^2 \text{ and } f_-(x,y) = x^2 - xy + 3y^2$$

In fact these are equivalent: $f_+(x-y,y)$ equals $f_-(x,y)$. This is a highly subtle point which the textbook does not directly address.

Solution to (20) This is similar to **Problem 17**. In fact the cases $d = -3$ and $d = -4$ were solved in the **Solution to Problem 17**. So I will only record the answer for $d = -8$ and $d = -11$.

(i) For $d = -8$, since $d \equiv 0^2 \pmod 8$, the prime 2 is represented; explicitly $f(0,1) = 2$. For an odd prime p, by quadratic reciprocity $\left(\frac{-8}{p}\right) = \left(\frac{-2}{p}\right)$ equals $+1$, i.e., p is represented, if and only if $p \equiv 1, 3 \pmod 8$.

(ii) For $d = -11$, since $d \not\equiv 0, 1, 4 \pmod 8$, the prime 2 is not represented. Since 11 divides d, 11 is represented; explicitly $f_+(-1,2) = f_-(1,2) = 11$. For an odd prime $p \neq 11$, by quadratic reciprocity $\left(\frac{-8}{p}\right) = \left(\frac{-2}{p}\right)$ equals $+1$, i.e., p is represented, if and only if $p \equiv 1, 3 \pmod 8$.

Solution to (21) There does not exist a nontrivial Pythagorean triple (x,y,z) such that xy is a square integer. First of all, if there exists a nontrivial Pythagorean triple such that xy is a square integer, then by factoring also there exists a primitive Pythagorean triple such that xy is a square, say w^2. Up to changing (x,y,z) to $(-x,-y,-z)$, assume that both x and y are positive. For a primitive Pythagorean triple, $\gcd(x,y)$ equals 1. If a product of two positive, relatively prime integers is a square, then each factor is a square, i.e., $x = u^2$ and $y = v^2$. Since (x,y,z) is a Pythagorean triple, this gives $u^4 + v^4 = z^2$. But, in the course of proving Fermat's Last Theorem for $n = 4$, we proved there are no triples $(u,v,z) \neq (0,0,0)$ such that $u^4 + v^4 = z^2$.

Solution to (23) This is similar to problems from the review sheet for Midterm 2. So I am not including the solutions to this problem.

Solution to (24) **(a)** Here $c(x) = 1$, $u(x) = \frac{2}{3} + q(x)g(x)$, and $v(x) = \frac{-1}{3} - q(x)f(x)$, where $q(x)$ is an arbitrary polynomial with rational coefficients. So $f(x)/c(x)$ equals $f(x)$, and $g(x)/c(x)$ equals $g(x)$. So $F_1(X)$ equals $f(x)$ and $G_1(x)$ equals $g(x)$.

(b) Here $c(x) = x + 1$, $u(x) = q(x)f(x)$, and $v(x) = 1 - q(x)g(x)$, where $q(x)$ is an arbitrary polynomial with rational coefficients. So $f(x)/c(x)$ equals $F_1(x)$ equals $x^2 + 1$, and $g(x)/c(x)$ equals $G_1(x)$ equals 1.

(c) Also in this case $c(x) = \boxed{x+1}$, $u(x) = \boxed{1+q(x)f(x)}$, and $v(x) = \boxed{-x^2 - q(x)f(x)}$, where $q(x)$ is an arbitrary polynomial with rational coefficients. So $f(x)/c(x)$ equals $F_1(x)$ equals $\boxed{x^2+1}$, and $g(x)/c(x)$ equals $G_1(x)$ equals $\boxed{x^4+x^2+1}$.

(d) In this case $c(x) = \boxed{(x^3+x)^2}$, $u(x) = \boxed{-\frac{27}{6}(x) + q(x)g(x)}$, and $v(x) = \boxed{\frac{1}{6}(3x^2+2) - q(x)f(x)}$, where $q(x)$ is an arbitrary polynomial with rational coefficients. So $f(x)/c(x)$ equals $F_1(x)$ equals $\boxed{x^3+x}$, and $g(x)/c(x)$ equals $G_1(x)$ equals $\boxed{9x^2+3}$.

Solution to (24) Let α be a nonzero algebraic number. Write the minimal polynomial of α as

$$m_\alpha(x) = x^d - c_1x^{d-1} + \cdots + (-1)^e c_e x^{d-e} + \cdots + (-1)^{d-1}c_{d-1}x + (-1)^d c_d = xg(x) + (-1)^d c_d.$$

Since the polynomial $m_\alpha(x)$ has minimal degree among polynomials satisfied by α, c_d is nonzero; otherwise $\alpha g(\alpha) = 0$ so that $g(x)$ is a polynomial satisfied by α of smaller degree than $m_\alpha(x)$. Since c_d is nonzero, the equation $m_\alpha(\alpha) = 0$ is equivalent to

$$\alpha \cdot \frac{(-1)^{d-1}}{c_d} g(\alpha) = 1.$$

In other words $1/\alpha = (-1)^{d-1}g(\alpha)/c_d$. And to find the minimal polynomial of $\beta = 1/\alpha$, use the fact that $(-1)^d\beta^d/c_d \cdot m_\alpha(1/\beta) = 0$, i.e., β satisfies the polynomial

$$\frac{(-1)^d}{c_d}x^d m_\alpha(1/x) = x^d - \frac{c_{d-1}}{c_d} + \cdots + (-1)^{d-e}\frac{c_e}{c_d}x^e + \cdots + (-1)^{d-1}\frac{c_1}{c_d}x + (-1)^d\frac{1}{c_d}.$$

If the minimal polynomial $m_\beta(x)$ of β had degree r strictly smaller than d, then by the same argument also α satisfies the polynomial $x^r m_\beta(1/x)$ which has degree $r < d$, contradicting that $m_\alpha(x)$ has degree d. Therefore $m_\beta(x)$ has degree d, from which it follows that $m_\beta(x)$ is the polynomial above, $m_{1/\alpha}(x) = \frac{(-1)^d}{c_d}x^d m_\alpha(1/x)$. Finally, to find the minimal polynomial of $\gamma = \alpha - (1/\alpha)$, it is usually best to combine the above observations with the technique of computing the characteristic polynomial of the matrix representative A_γ of the $\mathbb{Q}$-linear operator $L_\gamma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ by $v \mapsto \gamma \cdot v$.

(a) Of course $m_1(x) = \boxed{x-1}$, $1/\alpha = \boxed{1}$, $m_{1/\alpha}(x) = \boxed{x-1}$. And $\gamma = \alpha - (1/\alpha)$ equals 0, which has minimal polynomial $m_\beta(x) = \boxed{x}$.

(b) The algebraic number $\alpha = \sqrt{7}$ satisfies the monic polynomial $x^2 - 7$. By the criterion that a root u/v must have u dividing 7 and v dividing 1, it is straightforward to see this has no rational roots. Hence this polynomial is irreducible so that $m_\alpha(x) = \boxed{x^2-7}$. Thus $\beta = 1/\alpha$ equals $f(\alpha)$ for $f(x) = \boxed{x/7}$. And the minimal polynomial is $m_\beta(x) = \frac{(-1)^2}{7}x^2 m_\alpha(1/x) = \boxed{x^2 - \frac{1}{7}}$.

Finally $\gamma := \alpha - (1/\alpha)$ equals $\alpha - \frac{1}{7}\alpha = \frac{6}{7}\alpha$. For a nonzero algebraic number α and a nonzero rational number b, $\gamma = b\cdot\alpha$ satisfies the degree d polynomial $b^d m_\alpha(x/b)$. So the minimal polynomial $m_\gamma(x)$ has degree r at most d. But if $r < d$, then since also $\alpha = (1/b)\gamma = b_1\gamma$, also α satisfies the polynomial $b_1^d m_\gamma(x/b_1)$ which has degree $e < d$, contradicting that $m_\alpha(x)$ has degree d. Thus e equals d so that $m_{b\cdot\alpha}(x) = b^d m_\alpha(x/b)$. Therefore $m_\gamma(x) = (6/7)^2((7x/6)^2 - 7) = \boxed{x^2 - \frac{36}{7}}$.

(c) The algebraic number $\alpha = \sqrt[3]{7}$ satisfies the monic polynomial $x^3 - 7$. By the criterion that a rational root u/v must have u dividing 7 and v dividing 1, it is straightforward to see this has no rational roots. Hence this cubic polynomial is irreducible so that $m_\alpha(x) = \boxed{x^3 - 7}$. Thus $\beta = 1/\alpha$ equals $f(\alpha)$ for $f(x) = \boxed{x^2/7}$. And the minimal polynomial is $m_\beta(x) = \frac{(-1)^3}{7}x^3 m_\alpha(1/x) = \boxed{x^3 - \frac{1}{7}}$.

Finally $\gamma := \alpha - (1/\alpha)$ equals $\alpha - \frac{1}{7}\alpha^2$. With respect to the ordered $\mathbb{Q}$-basis $\mathcal{B} = (1, \alpha, \alpha^2)$ for $\mathbb{Q}(\alpha)$, the matrix representative A_γ of $L_\gamma(v) = \gamma \cdot v$ equals

$$A_\gamma = \begin{bmatrix} 0 & -1 & 7 \\ 1 & 0 & -1 \\ \frac{-1}{7} & 1 & 0 \end{bmatrix}.$$

The characteristic polynomial is $c_{L_\gamma}(x) = x^3 + 3x - (7 - \frac{1}{7}) = \frac{1}{7}(7x^3 + 21x - 48)$. Every rational root is of the form u/v where u divides 48 and v divides 7. It is straightforward to check none of these finitely many fractions is a root, hence $c_{L_\gamma}(x)$ is irreducible. Therefore this is the minimal polynomial,

$$m_\gamma(x) = c_{L_\gamma}(x) = \boxed{x^3 + 3x - \frac{48}{7}}.$$

(d) Denote $\sqrt[3]{7}$ by θ; this is the case considered in (c) above. Then $\alpha = \theta + 2\theta^2$. With respect to the ordered $\mathbb{Q}$-basis $\mathcal{B} = (1, \theta, \theta^2)$, the matrix representative A_α of $L_\alpha(v) = \alpha \cdot v$ equals

$$A_\alpha = \begin{bmatrix} 0 & 14 & 7 \\ 1 & 0 & 14 \\ 2 & 1 & 0 \end{bmatrix}.$$

The characteristic polynomial is $c_{L_\alpha}(x) = x^3 - 42x - 7\cdot 3\cdot 19$. By the criterion that a rational root u/v must have u dividing $7\cdot 3\cdot 19$ and must have v dividing 1, it is straightforward to see this has no rational roots. Hence this cubic polynomial is irreducible so that $m_\alpha(x) = \boxed{x^3 - 42x - 7\cdot 3\cdot 19}$. Thus $\beta = 1/\alpha$ equals $f(\alpha)$ for $f(x) = \boxed{(x^2 - 42)/7} = (\theta^2 + 28\theta - 14)/7$. And the minimal polynomial is $m_\beta(x) = \frac{(-1)^3}{7\cdot 3\cdot 19}x^3 m_\alpha(x)$, i.e.,

$$m_\beta(x) = \boxed{x^3 + \frac{2}{19}x - \frac{1}{7\cdot 3\cdot 19}}.$$

Finally, $\gamma := \alpha - (1/\alpha)$ equals $\frac{13}{7}\theta^2 - 3\theta + 2$. So the matrix representative is

$$A_\gamma = \begin{bmatrix} 2 & 13 & -21 \\ -3 & 2 & 13 \\ \frac{13}{7} & -3 & 2 \end{bmatrix}.$$

The characteristic polynomial is

$$c_{L_\gamma}(x) = (x-2)^3 + 9\cdot 13(x-2) - \frac{1}{7}(13^3 - 7\cdot 3^3) = \boxed{x^3 - 2\cdot 3x^2 + 3\cdot 43x - \tfrac{2^2\cdot 3\cdot 11\cdot 29}{7}}.$$

(e) Denote $\mu = \sqrt{2}$ and $\nu = \sqrt{3}$. Then one ordered $\mathbb{Q}$-basis for $\mathbb{Q}(\mu,\nu)$ is $(1,\mu,\nu,\mu\nu)$. Since α equals $\mu+\nu$, the matrix representative A_α of $L_\alpha(v) = \alpha\cdot v$ is

$$A_\alpha = \begin{bmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

The characteristic polynomial is $c_{L_\alpha}(x) = x^4 - 10x^2 + 1$. A rational root must have the form u/v where both u and v divide 1. It is straightforward to see no such rational number is a root. Hence this quartic polynomial has no linear factor. So if it is reducible, it is the square of an irreducible quadratic polynomial which must have the form $x^2 \pm 1$ (since $c_{L_\alpha}(x)$ has trivial linear and cubic terms, this forces the linear term of the quadratic to be zero). It is easy to see that the square of both of these quadratics is different from $c_{L_\alpha}(x)$. Hence $c_{L_\alpha}(x)$ is irreducible. Thus the minimal polynomial is

$$m_\alpha(x) = \boxed{x^4 - 10x^2 + 1}.$$

Thus $\beta := 1/\alpha$ equals $f(\alpha)$ for $f(x) = \boxed{-x^3 + 10x} = \nu - \mu$. And the minimal polynomial is

$$m_\beta(x) = \frac{(-1)^4}{1}x^4 m_\alpha(1/x) = \boxed{x^4 - 10x^2 + 1}$$

Finally, $\gamma := \alpha - (1/\alpha)$ equals 2μ. So the matrix representative is

$$A_\gamma = \begin{bmatrix} 0 & 4 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 2 & 0 \end{bmatrix}.$$

Thus the characteristic polynomial is $c_{L_\gamma}(x) = (x^2-8)^2$. This is reducible. So it is *not* the minimal polynomial of γ. Instead the minimal polynomial is the unique irreducible factor,

$$m_\gamma(x) = \boxed{x^2 - 8}.$$

Solution to (25) (a) Of course $\gamma := \alpha + \beta$ equals 3, so $m_\gamma(x) = \boxed{x-3}$. And $\delta = \alpha\cdot\beta$ equals 2, so $m_\delta(x) = \boxed{x-2}$.

(b) Since $\gamma := \alpha+\beta$ equals $2\sqrt[3]{7}$, by the same technique as above, $m_\gamma(x) = \boxed{x^3 - 2^3\cdot 7}$. And since $\delta := \alpha\cdot\beta$ equals $\sqrt[3]{7}^2$, also $m_\delta(x) = \boxed{x^3 - 7^2}$.

(c) One ordered $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha, \beta)$ is $\mathcal{B} = (1, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2)$. For $\gamma := \alpha + \beta$, the matrix representative A_γ of $L_\gamma(v) = \gamma \cdot v$ with respect to this basis is

$$A_\gamma = \begin{bmatrix} 0 & 0 & 7 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & 0 & 7 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

The characteristic polynomial is

$$c_{L_\gamma}(x) = (x^2-3)^3 - 2^3 \cdot 7x^3 + 7^2 + 2 \cdot 3 \cdot 7x(x^2-3) = x^6 - 9x^4 + 14x^3 + 27x^2 - 22.$$

This is of the form $m_\gamma(x)^e$ where e is an integer $e \geq 1$. Since $c_{L_\gamma}(x)$ has integer coefficients, by Gauss's Lemma also $m_\gamma(x)$ has integer coefficients. And thus the constant coefficient $c_{L_\gamma}(0) = -22$ equals the e^{th} power of the constant coefficient, $m_\gamma(0)^e$. But -22 is squarefree, so e must equal 1. Therefore $c_{L_\gamma}(x)$ equals the minimal polynomial, i.e.

$$m_\gamma(x) = \boxed{x^6 - 9x^4 + 14x^3 + 27x^2 - 22}.$$

For $\delta = \alpha\beta$, we have

$$A_\delta = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 21 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 7 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix},$$

so that $c_{L_\delta}(x) = x^6 - 3^3 7^2$. As above, $c_{L_\delta}(x) = m_\delta(x)^e$ for some integer e. But the only integer e which divides the exponent 3 in the factor 3^3 and the exponent 2 in the factor 7^2 is $e = 1$. Thus $c_{L_\delta}(x)$ equals $m_\delta(x)$, i.e.,

$$m_\delta(x) = \boxed{x^6 - 3^3 7^2}.$$

Solution to (26) (a) The minimal polynomial is $m_\alpha(x) = x^2 - x - \frac{1}{4}$. Thus $\boxed{\alpha \text{ is not an algebraic integer}}$, since the coefficient $-1/4$ is not an integer.

(b) The minimal polynomial is $m_\alpha(x) = x^2 - x - \frac{1}{2}$. Thus $\boxed{\alpha \text{ is not an algebraic integer}}$, since the coefficient $-1/2$ is not an integer.

(c) By the **Solution to Problem 24**, the minimal polynomial of α is $m_\alpha(x) = x^4 - 10x^2 + 1$. Since the coefficients are all integers, $\boxed{\alpha \text{ is an algebraic integer}}$. Since the constant coefficient equals 1, $\boxed{\alpha \text{ is a unit}}$ and a formula for the inverse is $\beta = 1/\alpha = \boxed{-\alpha^3 + 10\alpha}$. Since 1 equals $\alpha \cdot \beta$, $\boxed{n_1 = 1}$. And $\boxed{\text{every integer } n}$ is a multiple of α and the algebraic integer $n\beta$.

(d) Note that $\alpha = \sqrt[3]{3}$. So the minimal polynomial is $m_\alpha(x) = x^3 - 3$. Thus $\boxed{\alpha \text{ is an algebraic integer}}$. Since the norm equals 3, $\boxed{n_1 = 3}$. And $\alpha \cdot \beta = 3$ for $\beta = 3/\alpha = \boxed{\alpha^2}$.

Solution to (27) For a squarefree integer $m \neq 1$, if $m \not\equiv 1 \pmod 4$ then $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ equals

$$\{a + b\sqrt{m} | a, b \in \mathbb{Z}\}.$$

And if $m \equiv 1 \pmod 4$, then $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ equals

$$\{\frac{1}{2}(a + b\sqrt{m}) | a, b \in \mathbb{Z}\ a \equiv b \pmod 2\}.$$

So for $m = 2, -1, -5$, we have the first case, and for $m = -3$ we have the second case. For $m = -5$, the units are precisely $U_{\mathbb{Q}(\sqrt{-5})} = \{-1, +1\}$. For $m = -1$, the units are

$$U_{\mathbb{Q}(\sqrt{-1})} = \{\sqrt{-1}, -1, -\sqrt{-1}, 1\}.$$

And for $m = -3$, the units are

$$U_{\mathbb{Q}(\sqrt{-3})} = \{\frac{1}{2}(1 - \sqrt{-3}), \frac{1}{2}(-1 - \sqrt{-3}), -1, \frac{1}{2}(-1 + \sqrt{-3}), \frac{1}{2}(1 + \sqrt{-3}), 1\}.$$