MAT 311 Solutions for Midterm II Practice Problems

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.

Review Topics.
The following are the most important new skills not already tested on Midterm I.

(1) Know the statement of quadratic reciprocity, including the criteria for when -1 is a quadratic residue and when 2 is a quadratic residue. Be able to use quadratic reciprocity and the Chinese Remainder Theorem to find necessary and sufficient conditions for a given integer m to be a quadratic residue modulo a varying odd prime p in terms of the value of p modulo a fixed integer.

(2) Using elementary row and column operations over the integers, transform a given integer matrix into "block diagonal" form. Use this to find conditions for consistency of a linear system $AX = B$ in terms of linear congruences on the entries of B. For a consistent system, find the form of the general integer solution of the system.

(3) Know a necessary and sufficient condition for the existence of an integral, binary quadratic form with a given discriminant d and properly representing a given integer m.

(4) Using quadratic reciprocity and the Chinese Remainder Theorem, determine all odd primes p which are properly represented by some integral, binary quadratic form with a given discriminant d (but possibly depending on p).

(5) Use integral linear variable changes with determinant $+1$ to find a reduced form of an integral, binary quadratic form with non-square discriminant d.

(6) Find all integral, binary quadratic forms with given non-square discriminant d which are reduced.

(7) Know the general form of a Pythagorean triple. Be able to use this to prove non-existence of a triple (a, b, c) of integers with both $a^4 + b^4 = c^2$ and $abc \neq 0$. Similarly, be able to use Pythagorean triples to find the general solution of equations such as $a^2 + b^2 = c^4$ or $a^2 + b^2 = c^8$.

(8) For a ternary quadratic form with rational coefficients and nonzero discriminant, using an invertible linear variable change with rational coefficients, transform the quadratic form to "diagonal form" $g(ax^2 + by^2 + cz^2)$ where a, b, c are integers with $\gcd(a, b, c) = 1$.

(9) For a diagonal ternary quadratic form as above, use a further variable change to tranform to "Legendre diagonal form", $g(ax^2 + by^2 + cz^2)$ where a, b, c are integers such that abc is square-free.

(10) Use Legendre's theorem to determine when a Legendre diagonal ternary quadratic form has a nontrivial rational solution.

MAT 311 Number Theory | **Jason Starr**
Midterm II | **Spring 2011**
Thursday April 14th, 2011

Practice Problems.

(1) In each of the following cases, determine the value of the given Legendre symbol.

$$\text{(i) } \left(\frac{3}{151}\right), \quad \text{(ii) } \left(\frac{151}{157}\right), \quad \text{(iii) } \left(\frac{-1}{157}\right), \quad \text{(iv) } \left(\frac{2}{157}\right), \quad \text{(v) } \left(\frac{6}{101}\right).$$

(2) Find all prime integers p such that -14 is a square modulo p. Do not forget about $p = 2$ and $p = 7$. For each prime where -14 is a square modulo p, is it also a square modulo p^2, resp. modulo p^3?

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

(i)
$$5x + 17y = 6$$

(ii)
$$112x - 35y = 41$$

(iii)
$$112x - 35y = 42$$

(iv)
$$112x - 35y = b, \quad b \text{ arbitrary}$$

(v)
$$6x + 10y + 15z = 29$$

(4) 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.

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

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

(5) For each of the matrices A from **Problem 4**, 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.

(6) 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 -7. What if the discriminant equals -9?

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

$$\text{(i) } 5x^2 - 4xy + 3y^2, \quad \text{(ii) } 3x^2 - xy - 3y^2, \quad \text{(iii) } 16x^2 - 17xy + 4x^2.$$

(8) Find all the positive definite, reduced, integral, binary quadratic forms which have discriminant -7. Next find all the positive definite, reduced, integral, binary quadratic forms which have discriminant -23. What is the class number $H(-23)$?

(9) Find the general form of a positive Pythagorean triple whose smallest coordinate is a prime integer.

(10) Find the general form of a primitive solution of the integral, Diophantine equation

$$x^4 + y^2 = z^2$$

such that x is odd.

(11) Find an invertible linear change of coordinates (with rational coefficients) that transforms the following ternary quadratic form to diagonal form.

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

Then use Legendre's theorem to determine whether or not this ternary quadratic form has a solution.

(12) Find an invertible linear change of coordinates (with rational coefficients) that transforms the following ternary quadratic form to diagonal form.

$$f(x, y, z) = (x^2 + yz) + 5(y^2 + xz) + 5(z^2 + xy).$$

Then use Legendre's theorem to determine whether or not this ternary quadratic form has a solution.

Solutions to Problems.

Solution to (1) Recall that by quadratic reciprocity, for odd primes p and q we have

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

Also we have

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

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

(i) Notice that 151 is an odd prime. Set q to be 3, and set p to be 151. Then $(p-1)/2$ equals 1 and $(q-1)/2$ equals 75. Thus $(p-1)/2 \cdot (q-1)/2$ is odd, so that $(-1)^{(p-1)/2\cdot(q-1)/2}$ equals -1. Therefore we have
$$\left(\frac{3}{151}\right) = -\left(\frac{151}{3}\right).$$
Since $151 \equiv 1 \pmod 3$, which is a quadratic residue modulo 3, we have
$$\left(\frac{3}{151}\right) = -\left(\frac{151}{3}\right) = -(+1) = \boxed{-1}.$$
So 3 is not a quadratic residue modulo 151.

(ii) Notice that 157 is an odd prime. Set q to be 151, and set p to be 157. Then $(q-1)/2$ equals 76, which is even. Hence also $(p-1)/2 \cdot (q-1)/2$ is even. Thus by quadratic reciprocity,
$$\left(\frac{151}{157}\right) = +\left(\frac{157}{151}\right).$$
Of course $157 \equiv 6 \pmod{151}$. Thus we have
$$\left(\frac{157}{151}\right) = \left(\frac{6}{151}\right).$$
Since 6 equals $2 \cdot 3$, we have
$$(frac2 \cdot 3151) = \left(\frac{2}{151}\right) \cdot \left(\frac{3}{151}\right).$$
As computed above,
$$\left(\frac{3}{151}\right) = -1.$$
And for any odd prime q, $\left(\frac{2}{p}\right)$ equals $+1$ if and only if $p^2 - 1$ is divisible by 16, i.e., if and only if $p \equiv \pm 1 \pmod 8$. In this case $151 \equiv -1 \pmod 8$. Thus we have
$$\left(\frac{2}{151}\right) = +1.$$
This gives
$$\left(\frac{6}{151}\right) = (-1)(+1) = -1.$$

So by quadratic reciprocity,

$$\left(\frac{151}{157}\right) = \boxed{-1},$$

i.e., 151 is not a quadratic residue modulo 157.

(iii) As used above, 157 is congruent to -1 modulo 8, and hence it is congruent to 1 modulo 4. Therefore we have

$$\left(\frac{-1}{157}\right) = \boxed{+1},$$

i.e., -1 is a quadratic residue modulo 157.

(iv) As also used above, since 157 is congruent to -1 modulo 8, we have

$$\left(\frac{2}{157}\right) = \boxed{+1},$$

i.e., 2 is a quadratic residue modulo 157.

(v) Denote the odd prime 101 by p. Notice that 6 equals $3 \cdot 2$. Therefore we have,

$$\left(\frac{6}{101}\right) = \left(\frac{2}{101}\right) \cdot \left(\frac{3}{101}\right)$$

Recall that for an odd prime p such as 101, 2 is a quadratic residue modulo p if and only if p is congruent to ± 1 modulo 8. In this case, $p \equiv 3 \pmod 8$. Thus $\left(\frac{2}{101}\right)$ equals -1.

Since $(p-1)/2 = 50$ is even, also $(p-1)/2 \cdot (q-1)/2$ is even for every odd prime q such as 3. Thus, by quadratic reciprocity,

$$\left(\frac{q}{101}\right) = \left(\frac{101}{q}\right).$$

In particular, we have

$$\left(\frac{3}{101}\right) = \left(\frac{101}{3}\right).$$

And 101 is congruent to -1 modulo 3. This is not a quadratic residue modulo 3. Thus we have

$$\left(\frac{3}{101}\right) = -1.$$

Multiplying gives

$$\left(\frac{6}{101}\right) = \left(\frac{2}{101}\right) \cdot \left(\frac{3}{101}\right) = (-1)(-1) = \boxed{+1}.$$

Thus 6 is a quadratic residue modulo 101.

Solution to (2) First of all, for $p = 2$ and $p = 7$, $-14 \equiv 0 = 0^2 \pmod p$. Thus -14 is a quadratic residue modulo 2 and 7. Next consider the case where p is an odd prime different from 7. Since -14 equals $(-1) \cdot 2 \cdot 7$, we have

$$\left(\frac{-14}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{7}{p}\right).$$

As discussed in the **Solution to Problem 1**, -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$ and 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 (\mathrm{mod}\ 8)$. Thus both $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ equal $+1$ if and only if $p \equiv 1 \pmod 8$. And both $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ equal -1 if and only if $p \equiv 3 \pmod 8$. Therefore we conclude that

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

Next, $(7-1)/2$ equals 3. Thus for an odd prime p, $(p-1)/2 \cdot (7-1)/2$ is even if and only if $p \equiv 1 \pmod 4$. So if $p \equiv 1 \pmod 4$, then by quadratic reciprocity we have

$$\left(\frac{7}{p}\right) = +\left(\frac{p}{7}\right) = \begin{cases} +1, & p \equiv 1, -3, 2 \pmod 7, \\ -1, & p \equiv -1, 3, -2 \pmod 7 \end{cases}$$

And if $p \equiv -1 \pmod 4$, then by quadratic reciprocity we have

$$\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = \begin{cases} -1, & p \equiv 1, -3, 2 \pmod 7, \\ +1, & p \equiv -1, 3, -2 \pmod 7 \end{cases}$$

Putting the pieces together, we conclude that

$$\left(\frac{-14}{p}\right) = \begin{cases} +1, & p \equiv \pm 1 \pmod 8 \text{ and } p \equiv 1, -3, 2 \pmod 7, \\ -1, & p \equiv \pm 3 \pmod 8 \text{ and } p \equiv 1, -3, 2 \pmod 7, \\ -1, & p \equiv \pm 1 \pmod 8 \text{ and } p \equiv -1, 3, -2 \pmod 7, \\ +1, & p \equiv \pm 3 \pmod 8 \text{ and } p \equiv -1, 3, -2 \pmod 7. \end{cases}$$

Combined with the Chinese Remainder Theorem, we conclude that

$$\boxed{\left(\frac{-14}{p}\right) = \begin{cases} +1, & p \equiv 1, 3, 5, 9, -11, 13, 15, -17, -19, 23, 25, -27 \pmod{56}, \\ -1, & p \equiv -1, -3, -5, -9, 11, -13, -15, 17, 19, -23, -25, 27 \pmod{56} \end{cases}}$$

By Hensel's Lemma, for a prime p and for an integer x_s such that $x_s^2 + 14 \equiv 0 \pmod{p^s}$, if $2x_s \not\equiv 0 \pmod p$ then there exists an integer x_{s+1} such that $x_{s+1}^2 + 14 \equiv 0 \pmod{p^{s+1}}$ and such that $x_{s+1} \equiv x_s (\mathrm{mod}\ p^s)$. Thus, inductively, if there exists an integer x_0 such that $x_0^2 + 14 \equiv 0 \pmod p$ and such that $2x_0 \not\equiv 0\ (\mathrm{mod} p)$, then for every integer $s \geq 1$, there exists an integer x_s such that $x_s^2 + 14 \equiv 0 \pmod p$ and such that $x_s \equiv x_0 \pmod p$. For every prime integer $p \neq 2, 7$, if $x_0^2 + 14 \equiv 0 \pmod p$, then automatically $x_0 \not\equiv 0 \pmod p$. Thus, for a prime $p \neq 2, 7$, for every integer $s \geq 1$, -14 is a quadratic residue modulo p^s if and only if -14 is a quadratic residue modulo p.

On the other hand, it is straightforward to check that $-14 \equiv -2 \pmod 4$ is not a quadratic residue modulo 4. Similarly -14 is not a quadratic residue modulo 49.

Solution to (3) A single linear equation over the integers

$$a_1x_1 + \cdots + a_nx_n = b$$

is consistent if and only if $g := \gcd(a_1, \dots, a_n)$ divides b. In this case, using the Euclidean algorithm we can find integers $c_{i,j}$ such that the linear change of variables,

$$X = VX', \ X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \ V = \begin{bmatrix} c_{1,1} & c_{1,2} & \dots & c_{1,n} \\ c_{2,1} & c_{2,2} & \dots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n,1} & c_{n,2} & \dots & c_{n,n} \end{bmatrix}, \ X' = \begin{bmatrix} x_1' \\ x_2' \\ \vdots \\ x_n' \end{bmatrix},$$

has $\det(V) = \pm 1$ and gives a new linear equation

$$gx_1' = b.$$

So the general solution is $x_1' = (b/g)$ and all other variables x_i' are arbitrary. By back-substituting, this gives the general integer solution of the original linear equation.

(i) The Euclidean algorithm leads to the following change of variables,

$$X = VX', \ X = \begin{bmatrix} x \\ y \end{bmatrix}, \ V = \begin{bmatrix} 7 & -17 \\ -2 & 5 \end{bmatrix}, \ X' = \begin{bmatrix} x' \\ y' \end{bmatrix}.$$

With respect to the new variables, the linear equation reads

$$x' = 6.$$

This system is $\boxed{\text{consistent}}$ with general solution $x' = 6$ and y' is an arbitrary integer t. Back-substituting gives the general solution in the original variables

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -17 \\ -2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ t \end{bmatrix} = \boxed{\begin{bmatrix} 42 - 17t \\ -12 + 5t \end{bmatrix}} = \boxed{\begin{bmatrix} 8 - 17s \\ -2 + 5s \end{bmatrix}}$$

where $t = 3 + s$.

(ii) The Euclidean algorithm leads to the following change of variables,

$$X = VX', \ X = \begin{bmatrix} x \\ y \end{bmatrix}, \ V = \begin{bmatrix} 1 & 5 \\ 3 & 16 \end{bmatrix}, \ X' = \begin{bmatrix} x' \\ y' \end{bmatrix}.$$

With respect to the new variables, the linear equation reads

$$7x' = 41.$$

Since 7 does not divide 41, this system is $\boxed{\text{inconsistent}}$.

(iii) The Euclidean algorithm leads to the following change of variables,

$$X = VX',\ X = \begin{bmatrix} x \\ y \end{bmatrix},\ V = \begin{bmatrix} 1 & 5 \\ 3 & 16 \end{bmatrix},\ X' = \begin{bmatrix} x' \\ y' \end{bmatrix}.$$

With respect to the new variables, the linear equation reads

$$7x' = 42.$$

Since 7 divides 42, this system is $\boxed{\text{consistent}}$ with general solution $x' = 6$ and y' is an arbitrary integer t. Back-substituting gives the general solution in the original variables

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 5 \\ 3 & 16 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ t \end{bmatrix} = \boxed{\begin{bmatrix} 6+5t \\ 18+16t \end{bmatrix}} = \boxed{\begin{bmatrix} 1+5s \\ 2+16s \end{bmatrix}}$$

where $t = -1 + s$.

(iv) The Euclidean algorithm leads to the following change of variables,

$$X = VX',\ X = \begin{bmatrix} x \\ y \end{bmatrix},\ V = \begin{bmatrix} 1 & 5 \\ 3 & 16 \end{bmatrix},\ X' = \begin{bmatrix} x' \\ y' \end{bmatrix}.$$

With respect to the new variables, the linear equation reads

$$7x' = b.$$

Thus the system is $\boxed{\text{consistent if and only if 7 divides } b}$. In this case, write $b = 7c$. Then the general solution is $x' = c$ and y' is an arbitrary integer t. Back-substituting gives the general solution in the original variables

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 5 \\ 3 & 16 \end{bmatrix} \cdot \begin{bmatrix} c \\ t \end{bmatrix} = \boxed{\begin{bmatrix} c+5t \\ 3c+16t \end{bmatrix}}$$

where $c = b/7$.

(v) The Euclidean algorithm leads to the following change of variables,

$$X = VX',\ X = \begin{bmatrix} x \\ y \\ z \end{bmatrix},\ V = \begin{bmatrix} -4 & -5 & 10 \\ 1 & 3 & -3 \\ 1 & 0 & -2 \end{bmatrix},\ X' = \begin{bmatrix} x' \\ y' \\ z' \end{bmatrix}.$$

With respect to the new variables, the linear equation reads

$$x' = 29.$$

Thus the system is $\boxed{\text{consistent}}$ with general solution $x' = 29$ and with y', z' being arbitrary integers s, t. Back-substituting gives the general solution in the original variables

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} -4 & -5 & 10 \\ 1 & 3 & -3 \\ 1 & 0 & -2 \end{bmatrix} \begin{bmatrix} 29 \\ s \\ t \end{bmatrix} = \boxed{\begin{bmatrix} -116 & -5s & +10t \\ 29 & +3s & -3t \\ 29 & & -2t \end{bmatrix}} = \boxed{\begin{bmatrix} -1 & -5u & +10v \\ 2 & +3u & -3v \\ 1 & & -2v \end{bmatrix}}$$

where $t = 14 + u$ and where $s = 5 + v$.

Solution to (4) Let A be an $m \times n$ matrix with integer entries. By performing elementary row and column operations with integer coefficients, the original augmented matrix

$$\left[\begin{array}{c|c} A & I_{m\times m} \\ \hline I_{n\times n} & \end{array}\right]$$

is elementary equivalent to an augmented matrix

$$\left[\begin{array}{c|c} A' & U \\ \hline V & \end{array}\right]$$

where U, resp. V, is an invertible matrix with integer entries of size $m \times m$, resp. $n \times n$, and where A' is a matrix in "block diagonal" form,

$$A' = \left[\begin{array}{ccccc|ccc} a'_{1,1} & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & a'_{2,2} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & a'_{3,3} & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a'_{r,r} & 0 & \dots & 0 \\ \hline 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{array}\right],$$

for an integer $0 \leq r \leq \min(m, n)$ and for nonzero integers $a'_{1,1}, \dots, a'_{r,r}$. In fact one can even arrange that the matrix is in "Smith normal form", i.e., every $a'_{i,i}$ is positive and $a'_{i,i}$ divides $a'_{i+1,i+1}$ for $i = 1, \dots, r-1$. Because these augmented matrices are elementary equivalent, we have

$$A' = UAV.$$

(i) The original augmented matrix is

$$\left[\begin{array}{cc|cc} -2 & 3 & 1 & 0 \\ 3 & -1 & 0 & 1 \\ \hline 1 & 0 & & \\ 0 & 1 & & \end{array}\right].$$

By performing elementary row and column operations with integer coefficients, this is elementary equivalent to the following augmented matrix

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 7 & 3 & 2 \\ \hline 1 & -2 & & \\ 0 & 1 & & \end{array}\right].$$

Thus we have

$$A' = UAV,\ U = \boxed{\begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix}},\ A' = \boxed{\begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}},\ V = \boxed{\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}}.$$

(ii) The original augmented matrix is

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & -3 & 0 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right].$$

By performing elementary row and column operations with integer coefficients, this is elementary equivalent to the following augmented matrix

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 & -1 & 0 \\ 0 & 0 & 3 & -2 & 0 & -1 \\ \hline 1 & 0 & -2 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right].$$

Thus we have

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

(iii) The original augmented matrix is

$$\left[\begin{array}{cc|ccc} 5 & 10 & 1 & 0 & 0 \\ 9 & 3 & 0 & 1 & 0 \\ 4 & 3 & 0 & 0 & 1 \\ \hline 1 & 0 & & & \\ 0 & 1 & & & \end{array}\right].$$

By performing elementary row and column operations with integer coefficients, this is elementary equivalent to the following augmented matrix

$$\left[\begin{array}{cc|ccc} 1 & 0 & -1 & -2 & 6 \\ 0 & 5 & 2 & 2 & -7 \\ 0 & 0 & 3 & 5 & -15 \\ \hline 1 & -2 & & & \\ 0 & 1 & & & \end{array}\right].$$

Thus we have

$$A' = UAV,\ U = \boxed{\begin{bmatrix} -1 & -2 & 6 \\ 2 & 2 & -7 \\ 3 & 5 & -15 \end{bmatrix}},\ A' = \boxed{\begin{bmatrix} 1 & 0 \\ 0 & 5 \\ 0 & 0 \end{bmatrix}},\ V = \boxed{\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}}.$$

(iv) The original augmented matrix is

$$\left[\begin{array}{cccc|ccc} 1 & 1 & -3 & 0 & 1 & 0 & 0 \\ 5 & 5 & -3 & 0 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \end{array}\right].$$

By performing elementary row and column operations with integer coefficients, this is elementary equivalent to the following augmented matrix

$$\left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 6 & 0 & 0 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 1 & -2 \\ \hline 1 & 3 & -1 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \end{array}\right].$$

Thus we have

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

(v) The original augmented matrix is

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 3 & 1 & 2 & 0 & 1 & 0 \\ 2 & 3 & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right].$$

By performing elementary row and column operations with integer coefficients, this is elementary equivalent to the following augmented matrix

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -3 & 0 & 2 \\ 0 & 1 & 0 & 2 & 0 & -1 \\ 0 & 0 & 18 & 7 & 1 & -5 \\ \hline 1 & 0 & 7 & & & \\ 0 & 1 & -5 & & & \\ 0 & 0 & 1 & & & \end{array}\right].$$

Thus we have

$$A' = UAV,\ U = \boxed{\left[\begin{array}{ccc} -3 & 0 & 2 \\ 2 & 0 & -1 \\ 7 & 1 & -5 \end{array}\right]},\ A' = \boxed{\left[\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 18 \end{array}\right]},\ V = \boxed{\left[\begin{array}{ccc} 1 & 0 & 7 \\ 0 & 1 & -5 \\ 0 & 0 & 1 \end{array}\right]}.$$

Solution to (5) Let A be an $m \times n$ matrix. Let U, resp. V, be an invertible matrix with integer entries of size $m \times m$, resp. $n \times n$, such that the $m \times n$ integer matrix

$$A' = UAV$$

is in "block-diagonal" form,

$$A' = \left[\begin{array}{ccccc|ccc} a'_{1,1} & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & a'_{2,2} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & a'_{3,3} & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a'_{r,r} & 0 & \dots & 0 \\ \hline 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{array}\right],$$

for an integer $0 \leq r \leq \min(m,n)$ and for nonzero integers $a'_{1,1}, \dots, a'_{r,r}$. Make the change of variables,

$$X = VX',\ X = \left[\begin{array}{c} x_1 \\ \vdots \\ x_n \end{array}\right],\ X' = \left[\begin{array}{c} x'_1 \\ \vdots \\ x'_n \end{array}\right].$$

And let B be a column m-vector,

$$B = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

Then the original linear system, $AX = B$, is equivalent to the new linear system $A'X' = UB$. Denoting UB by B',

$$B' = UB, \ B' = \begin{bmatrix} b'_1 \\ \vdots \\ b'_m \end{bmatrix},$$

the new system is simply

$$\left\{ \begin{array}{ccc} a'_{1,1}x'_1 & = & b'_1 \\ a'_{2,2}x'_2 & = & b'_2 \\ \vdots & \vdots & \vdots \\ a'_{r,r}x'_r & = & b'_r \\ 0 & = & b'_{r+1} \\ \vdots & \vdots & \vdots \\ 0 & = & b'_m \end{array} \right.$$

Thus the system is consistent if and only if both $b'_j = 0$ for every $j = r+1, \dots, m$ and $b'_i \equiv 0 \pmod{a'_{i,i}}$ for every $i = 1, \dots, r$. In this case, the general solution is given by $x'_i = b'_i / a'_{i,i}$ for $i = 1, \dots, r$, and every x'_j is an arbitrary integer for $j = r+1, \dots, m$. We can back-substitute for the original variables using $X = VX'$.

(i) The new linear system is

$$A'X' = B'$$

where

$$A' = \begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}, \ X' = \begin{bmatrix} x'_1 \\ x'_2 \end{bmatrix}, \ B' = UB = \begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} b_1 + b_2 \\ 3b_1 + 2b_2 \end{bmatrix}.$$

In other words, the system is

$$\left\{ \begin{array}{ccc} 1x'_1 & = & b_1 + b_2 \\ 7x'_2 & = & 3b_1 + 2b_2 \end{array} \right.$$

Therefore the system is consistent if and only if

$$\boxed{3b_1 + 2b_2 \equiv 0 \pmod{7}},$$

i.e., $3b_1 + 2b_2 = 7c$ for some integer c. And then the general solution is

$$X' = \begin{bmatrix} x'_1 \\ x'_2 \end{bmatrix} = \begin{bmatrix} b_1 + b_2 \\ c \end{bmatrix}.$$

Back-substituting gives the general solution in the original variables

$$X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 + b_2 \\ c \end{bmatrix} = \boxed{\begin{bmatrix} b_1 + b_2 - 2c \\ c \end{bmatrix}},$$

where $3b_1 + 2b_2 = 7c$.

(ii) The new linear system is

$$A'X' = B'$$

where

$$A' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix},\ X' = \begin{bmatrix} x_1' \\ x_2' \\ x_2' \end{bmatrix},\ B' = UB = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ -2 & 0 & -1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ -b_2 \\ -2b_1 - b_3 \end{bmatrix}.$$

In other words, the system is

$$\begin{cases} 1x_1' &= b_1 \\ 3x_2' &= -b_2 \\ 3x_3' &= -2b_1 - b_3 \end{cases}$$

Therefore the system is consistent if and only if

$$\boxed{-b_2 \equiv 0 \pmod 3 \text{ and } -2b_1 - b_3 \equiv 0 \pmod 3},$$

i.e., $-b_2 = 3c_1$ and $-2b_1 - b_3 = 3c_2$ for some integers c_1 and c_2. And then the general solution is

$$X' = \begin{bmatrix} x_1' \\ x_2' \\ x_3' \end{bmatrix} = \begin{bmatrix} b_1 \\ c_1 \\ c_2 \end{bmatrix}.$$

Back-substituting gives the general solution in the original variables

$$X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ c_1 \\ c_2 \end{bmatrix} = \boxed{\begin{bmatrix} b_1 - 2c_2 \\ c_1 \\ c_2 \end{bmatrix}},$$

where $-b_2 = 3c_1$ and $-2b_1 - b_3 = 3c_2$.

(iii) The new linear system is

$$A'X' = B'$$

where

$$A' = \begin{bmatrix} 1 & 0 \\ 0 & 5 \\ 0 & 0 \end{bmatrix},\ X' = \begin{bmatrix} x_1' \\ x_2' \end{bmatrix},\ B' = UB = \begin{bmatrix} -1 & -2 & 6 \\ 2 & 2 & -7 \\ 3 & 5 & -15 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} -b_1 - 2b_2 + 6b_3 \\ 2b_1 + 2b_2 - 7b_3 \\ 3b_1 + 5b_2 - 15b_3 \end{bmatrix}.$$

In other words, the system is

$$\begin{cases} 1x_1' &= -b_1 - 2b_2 + 6b_3 \\ 5x_2' &= 2b_1 + 2b_2 - 7b_3 \\ 0 &= 3b_1 + 5b_2 - 15b_3 \end{cases}$$

Therefore the system is consistent if and only if

$$\boxed{3b_1 + 5b_2 - 15b_3 = 0 \text{ and } 2b_1 + 2b_2 - 7b_3 \equiv 0 \pmod 5},$$

i.e., $2b_1 + 2b + 2 - 7b_3 = 5c$. And then the general solution is

$$X' = \begin{bmatrix} x_1' \\ x_2' \end{bmatrix} = \begin{bmatrix} -b_1 - 2b_2 + 6b_3 \\ c \end{bmatrix}.$$

Back-substituting gives the general solution in the original variables

$$X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -b_1 - 2b_2 + 6b_3 \\ c \end{bmatrix} = \boxed{\begin{bmatrix} -b_1 - 2b_2 + 6b_3 - 2c \\ c \end{bmatrix}},$$

where $2b_1 + 2b + 2 - 7b_3 = 5c$.

(iv) The new linear system is

$$A'X' = B'$$

where

$$A' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ X' = \begin{bmatrix} x_1' \\ x_2' \\ x_3' \\ x_4' \end{bmatrix}, \ B' = UB = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ -1 & 1 & -2 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ -2b_1 + b_3 \\ -b_1 + b_2 - 2b_3 \end{bmatrix}.$$

In other words, the system is

$$\begin{cases} 1x_1' &= b_1 \\ 6x_2' &= -2b_1 + b_3 \\ 0 &= -b_1 + b_2 - 2b_3 \end{cases}$$

Therefore the system is consistent if and only if

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

i.e., $-2b_1 + b_3 = 6c$ for some integer c. And then the general solution is

$$X' = \begin{bmatrix} x_1' \\ x_2' \\ x_3' \\ x_4' \end{bmatrix} = \begin{bmatrix} b_1 \\ c \\ s \\ t \end{bmatrix}$$

for arbitrary integers s and t. Back-substituting gives the general solution in the original variables

$$X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 1 & 3 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ c \\ s \\ t \end{bmatrix} = \boxed{\begin{bmatrix} b_1 + 3c - s \\ s \\ c \\ t \end{bmatrix}},$$

where $-2b_1 + b_3 = 6c$ and where s, t are arbitrary integers.

(v) The new linear system is

$$A'X' = B'$$

where

$$A' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 18 \end{bmatrix}, \ X' = \begin{bmatrix} x_1' \\ x_2' \\ x_3' \end{bmatrix}, \ B' = UB = \begin{bmatrix} -3 & 0 & 2 \\ 2 & 0 & -1 \\ 7 & 1 & -5 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} -3b_1 + 2b_3 \\ 2b_1 - b_3 \\ 7b_1 + b_2 - 5b_3 \end{bmatrix}.$$

In other words, the system is

$$\begin{cases} 1x_1' & = & -3b_1 + 2b_3 \\ 1x_2' & = & 2b_1 - b_3 \\ 18x_3' & = & 7b_1 + b_2 - 5b_3 \end{cases}$$

Therefore the system is consistent if and only if

$$\boxed{7b_1 + b_2 - 5b_3 \equiv 0 \pmod{18}},$$

i.e., $7b_1 + b_2 - 5b_3 = 18c$ for some integer c. And then the general solution is

$$X' = \begin{bmatrix} x_1' \\ x_2' \\ x_3' \end{bmatrix} = \begin{bmatrix} -3b_1 + 2b_3 \\ 2b_1 - b_3 \\ c \end{bmatrix}.$$

Back-substituting gives the general solution in the original variables

$$X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 7 \\ 0 & 1 & -5 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -3b_1 + 2b_3 \\ 2b_1 - b_3 \\ c \end{bmatrix} = \boxed{\begin{bmatrix} -3b_1 + 2b_3 + 7c \\ 2b_1 - b_3 - 5c \\ c \end{bmatrix}},$$

where $7b_1 + b_2 - 5b_3 = 18c$.

Solution to (6) For an integer d and for an integer n, there exists an integral, binary quadratic form of disciminant d which properly represents n if and only if d is congruent to a square modulo $4|n|$. First of all for $n = p = 2$, $-7 \equiv 1 = 1^2 \pmod{8}$, hence there exists an integral, binary quadratic form of discriminant -7 which properly represents 2. Next, $-7 \equiv 49 \pmod{28}$, hence there exists an integral, binary quadratic form of discriminant -7 which properly represents 7.

Finally, assume that p is an odd prime different from 7. Since $-7 \equiv 1 = 1^2 \pmod 4$, there exists an integral, binary quadratic form which properly represents p if and only if $\left(\frac{-7}{p}\right)$ equals 1. And by quadratic reciprocity,

$$\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right) = \begin{cases} +1 & = & p \equiv 1, 2, -3 \pmod 7, \\ -1 & = & p \equiv -1, -2, 3 \pmod 7, \end{cases}$$

Since -9 is not congruent to a square modulo 4, there exists no integral, binary quadratic form with discriminant equal to -9.

Solution to (7) (i) The admissible linear change of coordinates $(x, y) = (-y_1, x_1 - y_1)$ gives a reduced form,

$$\boxed{3x_1^2 - 2x_1y_1 + 4y_1^2}.$$

(ii) The admissible linear change of coordinates $(x, y) = (-y_1, x_1)$ gives a reduced form,

$$\boxed{-3x_1^2 + x_1y_1 + 3y_1^2}.$$

(iii) The admissible linear change of coordinates $(x, y) = (-x_1, -2x_1 - y_1)$ gives a reduced form,

$$\boxed{-2x_1^2 - x_1y_1 + 4y_1^2}.$$

Solution to (8) There is only one positive definite, integral, binary quadratic form of discriminant -7 which is reduced, namely

$$\boxed{x^2 + xy + 2y^2}.$$

There are three positive definite, integral, binary quadratic form of discriminant -23 which is reduced, namely

$$\boxed{x^2 + xy + 6y^2}, \quad \boxed{2x^2 - xy + 3y^2}, \quad \boxed{2x^2 + xy + 3y^2}.$$

Therefore the class number is $\boxed{H(-23) = 3}$.

Solution to (9) Up to permuting x and y, every positive, primitive, Pythagorean triple has the form

$$\begin{cases} x & = & r^2 - s^2, \\ y & = & 2rs, \\ z & = & r^2 + s^2 \end{cases}$$

for relatively prime integers $r > s > 0$ such that $r \not\equiv s \pmod 2$. If one of x or y equals the prime $p = 2$, then it must be y, since x is odd. But this then implies $r = s = 1$, which contradicts the conditions on r and s. Hence 2 cannot be one of x or y for a positive, primitive, Pythagorean triple. For an odd prime $p \geq 3$, if one of x or y equals p, then it must be x, since y is even. Since

$p = (r+s)(r-s)$, it must be that $r-s$ equals 1 and $r+s$ equals p. This quickly leads to the general form of a primitive, Pythagorean triple with smallest entry equal to a prime,

$$\boxed{\begin{cases} x &= p, \\ y &= 4\cdot((p^2-1)/8), \\ z &= 1+4\cdot((p^2-1)/8) \end{cases}}$$

for an odd prime $p \geq 3$.

Solution to (10) Without loss of generality, change the signs of x, y and z if necessary so that all three are nonnegative. By considering the equation modulo 4, if x is odd then y must be even. Of course there is the trivial solution $(x,y,z) = (x,0,x^2)$. But if $y > 0$, then (x^2,y,z) is a Pythagorean triple of the form

$$\begin{cases} x^2 &= r^2-s^2), \\ y &= 2rs, \\ z &= r^2+s^2 \end{cases}$$

for integers $r > s > 0$ with $r \not\equiv s \pmod 2$. Then (x,s,r) is a Pythagorean triple. And since x is odd, s must be even. Thus (x,s,r) is a Pythagorean triple of the form

$$\begin{cases} x &= u^2-v^2, \\ s &= 2uv, \\ r &= u^2+v^2 \end{cases}$$

for integers $u > v > 0$ with $u \not\equiv v \pmod 2$. Back-substituting gives the general solution of the equation $x^4 + y^2 = z^2$ such that x is odd,

$$\boxed{\begin{cases} x &= u^2-v^2, \\ y &= 4uv(u^2+v^2), \\ z &= u^4+6u^2v^2+v^4 \end{cases}}$$

for integers $u > v > 0$ with $u \not\equiv v \pmod 2$.

Solution to (11) With respect to the linear change of variables,

$$X = VX_1, \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 & -3 & -19 \\ 0 & 2 & 11 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$$

the quadratic polynomial is

$$f_1(x_1,y_1,z_1) = f(x,y,z) = 2(x_1^2 + y_1^2 - 35z_1^2).$$

This is in Legendre diagonal form. And it does have a real point. But it does not have a primitive solution at 7, since $x_1^2 + y_1^2 \equiv 0 \pmod 7$ has no nontrivial solution. Thus there is $\boxed{\text{no nontrivial solution}}$ to $f(x,y,z) = 0$ in integers.

Solution to (12)

$$X = VX_1, \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{15} \begin{bmatrix} 15 & -15 & 5 \\ 0 & 6 & -7 \\ 0 & 0 & 5 \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$$

the quadratic polynomial is

$$f_1(x_1, y_1, z_1) = f(x, y, z) = \frac{2}{5}(5x_1^2 - 3y_1^2 + 2z_1^2).$$

This is in Legendre diagonal form. And it does have a real point. But it does not have a primitive solution at 3, since $5x_1^2 + 2z_1^2 \equiv 2(x_1^2 + z_1^2) \equiv 0 \pmod 3$ has no nontrivial solution. Thus there is $\boxed{\text{no nontrivial solution}}$ to $f(x, y, z) = 0$ in integers.