MATH 115, SUMMER 2012
HOMEWORK 5
SOLUTION

JAMES MCIVOR

(1) (NZM 3.5.1) Find a reduced form equivalent to $7x^2 + 25xy + 23y^2$.

Solution: By applying step 2 with $k = 2$, and then step 1, we obtain the reduced form $x^2 + 3xy + 7y^2$.

(2) (NZM 3.5.4) Show that a binary quadratic form f properly represents an integer n if and only if there is a form equivalent to f in which the coefficient of x^2 is n.

Solution: First assume f is equivalent to a form $g(x, y) = nx^2 + kxy + my^2$ for some k, m. Then $g(1, 0) = n$ and this representation is proper since the gcd of 0 and 1 is 1. This means that f also represents n properly since equivalent forms properly represent the same integers.

For the other direction, suppose f properly represents n. Then there are coprime integers s, t such that $f(s, t) = n$. Since s and t are coprime, there exist integers α, β such that $\alpha s + \beta y = 1$. Now consider the matrix $\begin{pmatrix} s & -\beta \\ t & \alpha \end{pmatrix}$. It has determinant one, so it's in the moidular group. Therefore $f(x, y) = ax^2 + bxy + cy^2$ is equivalent to the form

$$\begin{aligned}
g(x,y) &= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} s & t \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} s & -\beta \\ t & \alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} s & t \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} as + bt/2 & * \\ bs/2 + ct & * \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} as^2 + bst + ct^2 & * \\ * & * \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} n & * \\ * & * \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},
\end{aligned}$$

where $*$ denotes something I'm too lazy to compute, but which doesn't matter anyway, because this equivalent form has x^2 coefficient equal to n, as desired.

(3) Find all reduced positive definite primitive forms of discriminant -7.

Solution: If $d = -7$, we have $7 = 4ac - b^2$, so b must be odd. Also the reduction theorem tells us that $|b| \le a \le \sqrt{7/3}$, so $|b| \le a \le 1$. Thus

$|b| = a = 1$, and since $b > -a$, b must be 1. Solving for c in the previous equation gives $c = 2$. This gives two reduced forms $x^2 \pm xy + 2y^2$.

(4) Find all reduced positive definite primitive forms of discriminant -8.

Solution: We have $8 = 4ac - b^2$ so b is even. By the reduction theorem, $|b| \leq a \leq 1$, so $|b| = 0$. Thus $4ac = 8$, so $a = 1$, $c = 2$, giving the reduced form $x^2 + 2y^2$.

(5) Find all reduced positive definite primitive forms of discriminant -27.

Solution: We have $27 = 4ac - b^2$, so b is odd, and $|b| \leq a \leq 3$ by the reduction theorem. If $|b| = a = 3$, then $36 = 12c$, so $c = 3$ also, so this form is not primitive. Thus $|b|$ must be 1, hence $28 = 4ac$ so one of a or c is 1, the other is 7. To be reduced, we must have $a \leq c$, so $a = 1$, $c = 7$. Since $b > -a$, b must be positive 1, giving the form $x^2 + xy + 7y^2$.

(6) Determine which prime numbers are represented by the form $2x^2 + 3y^2$.

Solution: Call this form f. Its discriminant is -24. First we determine whether there are any other reduced primitive forms of discriminant -24. For this we would have $24 = 4ac - b^2$, so b is even; also $|b| \leq a \leq 2$ by the reduction theorem. If $|b| = 2$, then $a = 2$ also and we get $28 = 4ac = 8c$, which is impossible. Thus $b = 0$, so $24 = 4ac$, hence $6 = ac$. Since we must have $a \leq c$ and $a \leq 2$, the only possibilities are $a = 2, c = 3$ and $a = 1, c = 6$. Thus there are two reduced forms of discriminant -24, namely $f = 2x^2 + 3y^2$ and $g = x^2 + 6y^2$.

It's clear that $p = 2$ and $p = 3$ are both represented by f. From now on, consider $p > 3$. By our theorem from class (the"p-rep Thm"), we know that a prime p is represented by one of these forms if and only if -24 is a square mod p. We compute the Legendre symbol

$$\left(\frac{-24}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^3\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{2}{p}\right)\left(\frac{p}{3}\right)(-1)^{(p-1)/2} = \left(\frac{2}{p}\right)\left(\frac{p}{3}\right)$$

Notice we use that $p \neq 3$ in applying the QRL in the second equality. The quantity $\left(\frac{2}{p}\right)\left(\frac{p}{3}\right)$ is one iff either

$$\begin{cases} p \equiv \pm 1 \mod 8 \\ p \equiv 1 \mod 3 \end{cases}$$

or

$$\begin{cases} p \equiv \pm 3 \mod 8 \\ p \equiv 2 \mod 3 \end{cases}$$

We now show that the values of p satisfying the second conditions are *not* represented by g, because if $p = x^2 + 6y^2$ for some x, y, then reducing mod 3 gives $p \equiv x^2$, so $p \equiv 1 \mod 3$. Thus all primes $p > 3$ satisfying the second conditions are represented by f.

Conversely, we have to show also that any prime $p > 3$ represented by f satisfies $p \equiv \pm 3 \mod 8$ and $p \equiv 2 \mod 3$. The second condition is straightforward: if $p = 2x^2 + 3y^2$, then reducing mod p gives $p \equiv 2x^2$, and x^2 must be one, since 0,1 are the only squares mod 3 and $x \neq 0$ or else p would be a multiple of 3. For the mod 8 condition, if $p = 2x^2 + 3y^2$, then y must be odd, say $y = 2m + 1$. If x is even, say $x = 2k$, then

$$p = 8k^2 + 12m^2 + 12m + 3 \equiv 12m(m+1) + 3 \equiv 3 \mod 8,$$

since $m(m+1)$ must be even. If x is odd, say $x = 2k+1$, then

$$p = 8k^2 + 8k + 2 + 12m^2 + 12m + 3 \equiv 12m(m+1) + 5 \equiv -3 \mod 8,$$

using again that $m(m+1)$ is even. Thus we've proved that the primes represented by f are $p = 2, 3$, and those primes $p > 3$ such that $p \equiv \pm 3 \mod 8$ and $p \equiv 2 \mod 3$.

(7) Determine which prime numbers are represented by the form $x^2 + 7y^2$.

Solution: Call this form f. Its discriminant is -28. First we see whether there are other primitive reduced forms of discriminant -18. Such forms must have $28 = 4ac - b^2$ so b must be even, and $|b| \leq a \leq \sqrt{28/3}$, so $|b| \leq a \leq 3$. We cannot have $|b| = 2$, because then $a \geq 2$, and $32 = 4ac$, so a, c are also divisible by 2 and this is not primitive. So $b = 0$, hence $7 = 4ac$, so $a = 1$ and $c = 7$, and the only primitive reduced form of discriminant -28 is our f.

It's clear that 7 is represented by f, and $2, 3, 5$ are not, so from now on consider an odd prime $p > 7$ (this is to make sure we can use quadratic reciprocity). Such a prime p is represented by f iff

$$1 = \left(\frac{-28}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2\left(\frac{7}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}\frac{7-1}{2}} = \left(\frac{p}{7}\right)$$

This happens iff p is a square mod 7. The quadratic residues mod 7 are 1,2, and 4. So an odd prime p is represented by f iff $p = 7$ or $p \equiv 1, 2, 4 \mod 7$.

(8) Determine which prime numbers are represented by the form $x^2 + 8y^2$.

Solution: Call the form f; it has discriminant -32. What other primitive reduced forms have this discriminant? We would have $32 = 4ac - b^2$ and $|b| \leq a \leq 3$, and b must be even. If $b = 0$, then we have $ac = 8$, and a could be at most 2, but if so then $c = 4$ so we don't get a primitive form. Thus we get the form $a = 1$, $b = 0$, $c = 8$, which is our f.

On the other hand, if $|b| = 2$, we have $9 = ac$. Since $a \geq |b| = 2$, a must be 3, hance $c = 3$. Since $a = c$, b must be positive, and we get the form $g = 3x^2 + 2xy + 3y^2$.

So there are two primitive reduced forms of discriminant -32, namely $f = x^2 + 8y^2$ and $g = 3x^2 + 2xy + 3y^2$. A prime p is represented by f or g iff

$$1 = \left(\frac{-32}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^5 = (-1)^{(p-1)/2}\left(\frac{2}{p}\right),$$

which happens iff either

$$\begin{cases} p \equiv 1 \mod 4 \\ p \equiv \pm 1 \mod 8 \end{cases}$$

or

$$\begin{cases} p \equiv 3 \mod 4 \\ p \equiv \pm 3 \mod 8 \end{cases}$$

But if $p \equiv -1 \mod 8$, then it can't be congruent to 1 mod 4, and similarly if $p \equiv -3$ mod 8, it can't be congruent to 3 mod 4, so actually the conditions are just

$$p \equiv 1 \mod 8 \quad \text{or} \quad p \equiv 3 \mod 8$$

So primes represented by f or g must be congruent to 1 or 3 mod 8. We now show that those congruent to 1 mod 8 are *not* represented by g. For if

$$p = 3x^2 + 2xy + 3y^2,$$

then x and y have opposite parity, say x even and y odd, so xy is even and reducing mod 4 gives

$$p \equiv 3(x^2 + y^2) \mod 4$$

Now the only squares mod 4 are 0 and 1, depending on whether the integer is even or odd respectively, so $x^2 \equiv 0 \mod 4$ and $y^2 \equiv 1 \mod 4$, so the above shows that if p is represented by g then $p \equiv 3 \mod 4$. Thus p is represented by f iff $p \equiv 1 \mod 8$.

(9) Prove that if $a = 0$, the form $ax^2 + bxy + cy^2$ is not definite.

Solution: If $a = 0$, our form looks like $bxy + cy^2 = (bx + cy)y$. By fixing $y = 1$ and varying x, we can obtain both positive and negative values, so the form is indefinite. In particular, it's not definite.

(10) Prove that if $f(x, y) = ax^2 + bxy + cy^2$ is a reduced positive definite form, then the smallest positive integer represented by f is a.

Solution: Suppose that f represents k, where $0 < k < a$. Then $f(x, y) = k$ for some $x, y \in \mathbb{Z}$. We seek a contradiction. If $x = 0$, then $cy^2 = k < a$, so $a > c$, contradicting the fact that f is reduced. If $y = 0$ then $ax^2 = k < a$, which forces $x = 0$, but then $k = 0$, contradiction. So x and y must both be nonzero. If $0 < |x| \leq |y|$, then since $|b| \leq c$, we have $|by| \leq cy$ and hence $|bxy| \leq cy^2$. This means $bxy + cy^2 \geq 0$, so $ax^2 + bxy + cy^2 \geq ax^2$. Then we get

$$k = ax^2 + bxy + cy^2 \geq ax^2 \geq a,$$

contradicting the fact that $k < a$. The final case, when x, y are nonzero and $|x| \geq |y|$, is handled similarly.

(11) (NZM 5.2.2) For what integers a, b, c does the system

$$x_1 + 2x_2 + 3x_3 + 4x_4 = a$$
$$x_1 + 4x_2 + 9x_3 + 16x_4 = b$$
$$x_1 + 8x_2 + 27x_3 + 64x_4 = c$$

have a solution in integers? What are the solutions if $a = b = c = 1$?

Solution: We write the system in matrix form:

$$A\mathbf{x} = \mathbf{b},$$

where

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 9 & 16 \\ 1 & 8 & 27 & 64 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

By subtracting off copies of the first row, one gets

$$I_3 A I_4 \sim \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 6 & 12 \\ 0 & 6 & 24 & 60 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

By subtracting off copies of the second row,

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 2 & -3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 6 & 12 \\ 0 & 0 & 6 & 24 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now we subtract off copies of the first column:

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 2 & -3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 6 & 12 \\ 0 & 0 & 6 & 24 \end{pmatrix} \begin{pmatrix} 1 & -2 & -3 & -4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Finally subtract off copies of the second and third columns:

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 2 & -3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \end{pmatrix} \begin{pmatrix} 1 & -2 & 3 & -4 \\ 0 & 1 & -3 & 6 \\ 0 & 0 & 1 & -4 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now we replace $\mathbf{b}$ by $\mathbf{c} = L\mathbf{b}$, where L is the 3×3 matrix on the left above:

$$\mathbf{c} = \begin{pmatrix} a \\ b - a \\ 2a - 3b + c \end{pmatrix}$$

Since the given system is equivalent to the system $D\mathbf{y} = \mathbf{c}$, where D is the diagonal matrix in the middle above, we have a solution if and only if $2 | b - a$ and $6 | 2a - 3b + c$. Thus a and b can be any integers of the same parity, and $c \equiv 3b - 2a \mod 6$.

In case $a = b = c = 1$, our solution for $\mathbf{y}$ is $y_1 = 1$, $y_2 = y_3 = 0$, and $y_4 = k$ is arbitrary. Since $\mathbf{x} = R\mathbf{y}$, where R is the 4×4 matrix on the right above, we have

$$\mathbf{x} = \begin{pmatrix} 1 & -2 & 3 & -4 \\ 0 & 1 & -3 & 6 \\ 0 & 0 & 1 & -4 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ k \end{pmatrix} = \begin{pmatrix} 1-4k \\ 6k \\ -4k \\ k \end{pmatrix}$$

(12) (NZM 5.3.2) Prove that if x, y, z is a Pythagorean triple then at least one of x, y is divisible by 3 and at least one of x, y, z is divisible by 5.

Solution: By Thm 5.5, x, y, z have the form

$$\begin{aligned} x &= a^2 - b^2 \\ y &= 2ab \\ z &= a^2 + b^2, \end{aligned}$$

Assume 3 doesn't divide y. Then $2ab \not\equiv 0 \mod 3$, so $ab \not\equiv 0 \mod 3$ since 2 is a unit mod 3. Thus 3 doesn't divide a or b. But then by Fermat's Little Thm $a^2 - b^2 \equiv 1 - 1 = 0 \mod 3$, so $3 \mid x$.

Now assume 5 doesn't divide y, so it deosn't divide a or b. Since $xz = a^4 - b^4 \equiv 1 - 1 = 0 \mod 5$ (using Fermat's Little Thm), 5 divides xz and since 5 is prime, 5 divides x or 5 divides z.

(13) (NZM 5.3.12) Show that if x, y satisfy $x^4 - 2y^2 = 1$, then $x = \pm 1$, $y = 0$. [Hint: Imitate the proof of the Pythagorean Triples Theorem]

Solution: Write the equation as

$$2y^2 = x^4 - 1 = (x^2 + 1)(x^2 - 1)$$

Clearly x is odd, so both $x^2 + 1$ and $x^2 - 1$ are even, hence 4 divides $2y^2$, so y is even, and hence 8 divides $2y^2$. Now since x is odd, $x^2 \equiv 1 mod 4$, so $x^2 + 1 \equiv 2 \mod 4$. Thus 2 divides $x^2 + 1$ but 4 does not. Also, $x^2 + 1$ and $x^2 - 1$ do not share any prime factors besides 2, since if p divides both, then p divides their difference, which is 2, so p must be 2. So we rewrite our equation as

$$y^2 = \frac{x^2 + 1}{2}(x^2 - 1)$$

where the two factors are coprime. Hence by Lemma 5.4 they are both perfect squares. So we can write $x^2 - 1 = r^2$ for some integer r. But then

$$x^2 + r^2 = 1,$$

and the only solutions for x and r are 0 or ± 1. $x = 0$ doesn't satisfy our original equation, since $-2y^2 = 1$ has no solution. Thus $x = \pm 1$, from which we see that y must be zero.