

Number Theory
 McGill 189-346/377 B
 Solutions to Problem Set #7

- 2.1. If $f(x, y)$ represents m , then by definition there are integers r, s such that $f(r, s) = m$. Let $d = \text{GCD}(r, s)$, and write $r = dr', s = ds'$. Then

$$m = f(r, s) = f(dr', ds') = d^2 f(r', s') = d^2 m'$$

where $m' = f(r', s')$. Since $\text{GCD}(r', s') = 1$, by definition f properly represents m' , and we obtain the desired conclusion.

- 2.3. Recall that the discriminant of a quadratic form $g = aX^2 + bXY + cY^2$ is equal to -4 times the determinant of the associated matrix

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

Recall also that g is given by the expression

$$g(X, Y) = \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Now suppose that $f(x, y)$ is defined as $f(x, y) = g(px + qy, rx + sy)$. Then we have

$$f(x, y) = \begin{pmatrix} px + qy & rx + sy \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} px + qy \\ rx + sy \end{pmatrix}.$$

Since

$$\begin{pmatrix} px + qy \\ rx + sy \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

it follows that the matrix associated to $f(x, y)$ is

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

The determinant of this matrix is equal to $(ps - qr)^2(ac - b^2/4)$, and the desired result follows.

- 2.6. Following the proof of Theorem 2.8 in Cox, the idea is to make the middle coefficient as small as possible. We know that a substitution of the form $x = X, y = Y - mX$ is a proper equivalence, and will subtract $2m$ (the coefficient of y^2) from the middle coefficient. Witness: $126x^2 + 74xy + 13y^2 = 126X^2 + 74X(Y - mX) + 13(Y - mX)^2 = (126 - 74m + 13m^2)X^2 + (74 - 26m)XY + 13Y^2$. To minimize $74 - 26m$, take $m = 3$. Then $126 - 74 \cdot 3 + 13 \cdot 3^2 = 21$, and so we find that our form is properly equivalent to $21X^2 - 4XY + 13Y^2$. This form is not quite reduced yet, since reduced forms have $a \leq c$. So we must interchange X and Y ; however, since we must be careful to use proper equivalence, we should set $x = Y$ and $y = -X$. (Simply swapping X and Y has determinant -1 .) This substitution changes the sign of the middle coefficient, and we obtain the reduced form $13x^2 + 4xy + 21y^2$. To double-check our arithmetic, it does not hurt to confirm that our new form has the same discriminant as the original: and indeed, they both have discriminant -1076 .
- 2.11. (a) Table 2.14 shows that the only reduced form of discriminant -4 is $x^2 + y^2$. Hence theorem 2.16 of Cox tells us that an odd prime p is represented by $x^2 + y^2$ if and only if $\left(\frac{-4}{p}\right) = 1$. But $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)$, and we know that this is 1 if and only if $p \equiv 1 \pmod{4}$. Hence an odd prime p is of the form $x^2 + y^2$ if and only if $p \equiv 1 \pmod{4}$.

- (b) Table 2.14 shows that the only reduced form of discriminant -8 is $x^2 + 2y^2$. Hence an odd prime p is represented by this quadratic form if and only if $\left(\frac{-8}{p}\right) = 1$. Now $\left(\frac{-8}{p}\right) = \left(\frac{-2}{p}\right)$. This occurs if and only if both or neither of $-1, 2$ are squares $(\text{mod } p)$. Now -1 is a square $(\text{mod } p)$ if and only if $p \equiv 1 \pmod{4}$, and 2 is a square $(\text{mod } p)$ if and only if $p \equiv \pm 1 \pmod{8}$. So both -1 and 2 are squares if and only if $p \equiv 1 \pmod{8}$, while neither are squares if and only if $p \equiv 3 \pmod{8}$. Therefore an odd prime p is of the form $x^2 + 2y^2$ if and only if $p \equiv 1, 3 \pmod{8}$.
- (c) From table 2.14, $x^2 + 3y^2$ is the only reduced form of discriminant -12 . This time, we wish to determine the odd primes p such that $\left(\frac{-12}{p}\right) = \left(\frac{-3}{p}\right) = 1$. Using the formulation of quadratic reciprocity in equation (1.12) in Cox, we see $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$, and so we are after the primes p such that p is square $(\text{mod } 3)$. In other words, $p \equiv 1 \pmod{3}$. Therefore an odd prime p other than 3 (which divides $D = -12$, so is excluded in Theorem 2.16!) is of the form $x^2 + 3y^2$ if and only if $p \equiv 1 \pmod{3}$.
- (d) From table 2.14, $x^2 + 7y^2$ is the only reduced form of discriminant -28 . We wish to determine the odd primes p such that $\left(\frac{-28}{p}\right) = \left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right)$. This happens if and only if p is square $(\text{mod } 7)$, i.e., $p \equiv 1, 2, 4 \pmod{7}$. One may check that for p odd, this is the same as statement (2.17).

2.12 (a) Factor $m = p_1^{b_1} \cdots p_r^{b_r}$, with the p_i distinct and $b_i > 0$. Choose k such that $p_k^{b_k}$ is minimal, and set $a = p_k^{b_k}$, $c = m/a$. Certainly $(a, c) = 1$. Since m is assumed not to be a prime power, there is some $j \neq k$ such that $1 < p_j^{b_j} | c$, and by the minimality of $p_k^{b_k}$ we have $a < c$, as desired.

(b) $D = -32$: a is bounded above by $\sqrt{32/3} < 4$, so $a \leq 3$. Since $b \leq a$ is even (as D is even), the possibilities are $b = 0, \pm 2$. Recall $b^2 - 4ac = D$, so $4ac = b^2 + 32$. If $b = 0$, then $4ac = 32$, so $ac = 8$, and we can have $a = 1, c = 8$ or $a = 2, c = 4$. We obtain the reduced form $x^2 + 8y^2$; but $2x^2 + 4y^2$ is not reduced, as it is not primitive. If $b = \pm 2$, we have $4ac = 36$, so $ac = 9$. This implies $a = c = 3$, as we require $a \geq |b|$. This yields the reduced form $3x^2 + 2xy + 3y^2$, as $a = c$ necessitates $b \geq 0$. Thus we find two forms, and $h(-32) = 2$.

$D = -124$: a is bounded above by $\sqrt{124/3} < 7$, so $a \leq 6$. Since $b \leq a$ is even, the possibilities are $|b| = 0, 2, 4, 6$. We test each option in turn. If $|b| = 0$, then $4ac = 124$, so $ac = 31$, and we obtain the form $x^2 + 31y^2$. If $|b| = 2$, then $4ac = 128$, so $ac = 32$. Since $2 \geq a \geq 8$, this forces a, b, c all even, and the forms so-obtained are not primitive. If $|b| = 4$, then $4ac = 140$, so $ac = 35$. This yields $a = 5, c = 7$, and the two reduced forms $5x^2 \pm 4xy + 7y^2$. If $|b| = 6$, then $4ac = 160$, so $ac = 40$. It is not possible to have $ac = 40$ with $6 \leq a \leq c$, so we obtain no forms. Thus, we obtain three forms and $h(-124) = 3$.

2.13 (a) The two reduced forms of discriminant -20 are $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$, and for p odd, $(-20/p) = (-5/p)$. If $p \equiv 1 \pmod{4}$, we have $(-5/p) = (5/p) = (p/5) = 1$ if and only if $p \equiv 1, 4 \pmod{5}$. Combining the two congruences, we get $p \equiv 1, 9 \pmod{20}$. If $p \equiv 3 \pmod{4}$, we have $(-5/p) = -(5/p) = -(p/5) = 1$ if and only if $p \equiv 2, 3 \pmod{5}$, and combining the two congruences we obtain $p \equiv 3, 7 \pmod{20}$. So by theorem 2.16, an odd prime p other than 5 is of one of the two forms $x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$ if and only if $p \equiv 1, 3, 7, 9 \pmod{20}$.

(b) For $D = -3$, the only reduced form is $x^2 + xy + y^2$; and $(-3/p) = (p/3) = 1$ if and only if $p \equiv 1 \pmod{3}$. So an odd prime p other than 3 is of the form $x^2 + xy + y^2$ if and only if $p \equiv 1 \pmod{3}$.

(c) $D = -15$: check that the reduced forms are $x^2 + xy + 4y^2$ and $2x^2 + xy + 2y^2$. By quadratic reciprocity, $(-15/p) = (-3/p)(5/p) = (p/3)(p/5) = 1$ if and only if $p \equiv 1 \pmod{3}$ and $p \equiv 1, 4 \pmod{5}$, or $p \equiv 2 \pmod{3}$ and $p \equiv 2, 3 \pmod{5}$. By the Chinese Remainder Theorem, these amount to $p \equiv 1, 2, 4, 8 \pmod{15}$. Thus an odd prime p other than $3, 5$

is of at least one of the forms $x^2 + xy + 4y^2, 2x^2 + xy + 2y^2$ if and only if $p \equiv 1, 2, 4, 8 \pmod{15}$.

- (d) $D = -24$: the reduced forms are $x^2 + 6y^2, 2x^2 + 3y^2$. Also $(-24/p) = (-3/p)(2/p) = (p/3)(2/p) = 1$ if and only if $p \equiv 1 \pmod{3}$ and $p \equiv \pm 1 \pmod{8}$, or $p \equiv 2 \pmod{3}$ and $p \equiv \pm 3 \pmod{8}$. This amounts to $p \equiv 1, 5, 7, 11 \pmod{24}$, so an odd prime p other than 3 is of at least one of the forms $x^2 + 6y^2, 2x^2 + 3y^2$ if and only if $p \equiv 1, 5, 7, 11 \pmod{24}$.
- (e) $D = -31$: boy, this problem set turned out to be long. The reduced forms are $x^2 + xy + 8y^2, 2x^2 \pm xy + 4y^2$. Now $(-31/p) = (p/31) = 1$ if and only if p is square $\pmod{31}$, so an odd prime p other than 31 is of at least one of the forms $x^2 + xy + 8y^2, 2x^2 \pm xy + 4y^2$ if and only if p is square $\pmod{31}$.
- (f) $D = -52$: the reduced forms are $x^2 + 13y^2, 2x^2 + 2xy + 7y^2$. Also $(-52/p) = (-13/p) = 1$ if and only if $p \equiv 1 \pmod{4}$ and $p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$ (squares), or $p \equiv -1 \pmod{4}$ and $p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$ (non-squares). Combining gives

$$p \equiv 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49 \pmod{52}.$$

2.16 If $D \equiv 1 \pmod{4}$, then $(1-D)/4$ is an integer. Then the discriminant of $x^2 + xy + (1-D)/4$ is $1 - 4 \cdot (1-D)/4 = D$. This is reduced, because $b = 1, a = 1, c = (1-D)/4$ and $0 \leq b \leq a \leq c$.