Theorem 1. If $F, G$ are equivalent integral binary quadratic forms, then $F$ and $G$ represent the same set of integers.

Proof. Write $G(x, y) = F(\alpha x + \beta y, \gamma x + \delta y)$ where
\[
\det \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = \pm 1
\]
Then $m = G(r, s) \Rightarrow m = F(\alpha r + \beta s, \gamma r + \delta s)$, so if $G$ represents $m$, so does $F$. Since the matrix has determinant 1, it is invertible and its inverse is another integer matrix, so the reverse statement follows as well. \hfill \Box

Lemma 2. $F$ properly represents an integer $m$ if and only if $F$ is properly equivalent to a form $mx^2 + Bxy + Cy^2$.

Proof. $\Leftarrow$: It is obvious by the above that $F$ represents $m$; the problem is to show that it represents $m$ properly. Write $G(x, y) = mx^2 + Bxy + Cy^2$; then $G(x, y) = F(\alpha x + \beta y, \gamma x + \delta y)$, where $\alpha \delta - \beta \gamma = 1$. Then $m = G(1, 0) = F(\alpha, \gamma)$. But clearly $(\alpha, \gamma) = 1$ since otherwise we cannot have $\alpha \delta - \beta \gamma = 1$. So $F$ represents $m$ properly.

$\Rightarrow$: Write $F(p, q) = m$, where $(p, q) = 1$. Since $(p, q) = 1$, we can find integers $r, s$ such that $ps - qr = 1$, and then
\[
F(px + ry, qx + sy) = a(px + ry)^2 + b(px + ry)(qx + sy) + c(qx + sy)^2
\]
\[
= (ap^2 + bpq + cq^2)x^2 + (2apr + bps + bqr + 2cqs)xy + (ar^2 + brs + cs^2)y^2
\]
\[
= F(p, q)x^2 + (2apr + bps + bqr + 2cqs)xy + F(r, s)y^2 = mx^2 + Bxy + Cy^2
\]
\hfill \Box
**Definition 1.** If $F$ is a binary quadratic form, its discriminant, $\Delta(F)$ is $b^2-4ac$.

Note that $\Delta(F)$ is always either congruent to 0 or 1 mod 4, and that $b$ is even (odd) exactly when $\Delta(F) \equiv 0(1) \pmod{4}$.

**Theorem 3.** If $F,G$ are equivalent integral quadratic forms, then $\Delta(F) = \Delta(G)$.

*Proof.* For any form $F$, define

$$M_F = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$$

Then

$$2F(x,y) = (x\ y)M_F \begin{pmatrix} x \\ y \end{pmatrix}$$

Note further that $\Delta(F) = -\det(M_F)$.

Now in our particular case, if $G(x,y) = F(\alpha x + \beta y, \gamma x + \delta y)$, then

$$2G(x,y) = (\alpha x + \beta y \ \gamma x + \delta y)M_F \begin{pmatrix} \alpha \ 
\beta \\
\gamma \\
\delta \end{pmatrix} = (x\ y)M_F \begin{pmatrix} \alpha & \beta \\
\gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Hence

$$M_G = \begin{pmatrix} \alpha & \gamma \\
\beta & \delta \end{pmatrix}M_F \begin{pmatrix} \alpha & \beta \\
\gamma & \delta \end{pmatrix}$$

But $\Delta(F) = -\det(M_F)$, so since $\det \begin{pmatrix} \alpha & \beta \\
\gamma & \delta \end{pmatrix} = \det \begin{pmatrix} \alpha & \beta \\
\gamma & \delta \end{pmatrix} = \pm 1$,

$$\Delta(G) = -\det(M_G) = -\det \begin{pmatrix} \alpha & \gamma \\
\beta & \delta \end{pmatrix} \det(M_F) \det \begin{pmatrix} \alpha & \beta \\
\gamma & \delta \end{pmatrix} = -\det(M_F) = \Delta(F)$$

\[\square\]

Note that this proof shows that applying a set of transformations amount to multiplying by the transform matrix on the left and its transpose on the right.

**Example:** In the previous example, note that $\Delta(F) = 1 - 4 \cdot 1 \cdot 6 = -23$, and $\Delta(G) = 51^2 - 4 \cdot 82 \cdot 8 = 2601 - 2624 = -23$.

The converse of this theorem is not true - that is, there are forms of the same discriminant that represent different numbers. For example, $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ both have discriminant $-20$, yet the second form represents 2 while the first clearly does not. However, equivalence classes of forms under arbitrary (proper or improper) equivalence represent disjoint sets of primes:

**Theorem 4.** Let $p$ be an odd prime. Suppose $F,G$ both represent $p$ and $\Delta(F) = \Delta(G)$. Then $F$ and $G$ are equivalent (but perhaps not properly equivalent).
Proof. Since \( p \) is prime, \( F \) obviously represents \( p \) properly. So \( F \sim px^2 + bxy + cy^2 \). Note that the transformation \((x, y) \mapsto (x + dy, y)\) results in a form whose middle term is \( 2pd + b \), so by an appropriate choice of \( d \) we can arrange that \( -p < b \leq p \). Similarly, \( G \sim px^2 + b'xy + c'y^2 \) with \( -p < b' \leq p \). Note also that since \( b^2 - 4pc = b'^2 - 4pc' \), it follows that \( b \equiv b' \pmod{2} \) (i.e. \( b, b' \) have the same parity).

Since \( \Delta(F) = \Delta(G) \), we see that \( b^2 - 4pc = b'^2 - 4pc' \iff b^2 \equiv b'^2 \pmod{p} \iff b \equiv \pm b' \pmod{p} \), so \( b = \pm b' + kp \) for some \( k \). Since \( b, b' \) have the same parity and \( p \) is odd, \( k \) is even; since \( -p < b, b' \leq p \), \( k = 0 \) (since otherwise \( b, b' \) would be separated by at least \( 2p \), which is impossible).

We are left with two cases. If \( b = b' \), then \( \Delta(F) = \Delta(G) \) implies that \( c = c' \) and hence \( F \sim G \). If \( b = -b' \), then again \( \Delta(F) = \Delta(G) \) implies that \( c = c' \).

Then \( F \) and \( G \) are equivalent via the transformation \((x, y) \mapsto (x, -y)\). \( \square \)

Note that \( F(x, y) = ax^2 + bxy + cy^2 \) and \( G(x, y) = ax^2 - bxy + cy^2 \) are always improperly equivalent via the transformation \((x, y) \mapsto (x, -y)\). They are sometimes properly equivalent, and sometimes not. For example, \( 2x^2 + 2xy + 3y^2 \) and \( 2x^2 - 2xy + 3y^2 \) are properly equivalent while \( 3x^2 + 2xy + 5y^2 \) and \( 3x^2 - 2xy + 5y^2 \) are not. (See the article on reduced integral binary quadratic forms for details).

In summary, we have proved the following:

\[
F, G \text{ equivalent } \Rightarrow F, G \text{ represent the same set of integers} \\
F, G \text{ equivalent } \Rightarrow \Delta(F) = \Delta(G) \\
\Delta(F) = \Delta(G) \text{ and } F, G \text{ both represent some odd prime } p \Rightarrow F \text{ and } G \text{ are equivalent}
\]

We conclude with the following lemma and corollary, which provide concrete criteria for when an integer is representable by a class of forms.

**Lemma 5.** If \( D \equiv 0, 1 \pmod{4} \) is an integer, and \( m \) is an odd integer relatively prime to \( D \), then \( m \) is properly represented by a primitive form of discriminant \( D \) if and only if \( D \) is a quadratic residue \( \text{mod } m \).

**Proof.** If \( F(x, y) \) properly represents \( m \), then by the preceding lemma, we may assume that \( F(x, y) = mx^2 + bxy + cy^2 \). Then \( D = b^2 - 4mc \), being the discriminant of \( F \), so that \( D \equiv b^2 \pmod{D} \). Conversely, if \( D \equiv b^2 \pmod{D} \), we may assume \( D \equiv b \pmod{2} \) (if they have different parities, replace \( b \) by \( b + m \); since \( m \) is odd, the condition now holds and \( D \equiv (b + m)^2 \pmod{D} \) as well). Since \( D \equiv 0, 1 \pmod{4} \), it follows that \( D \equiv b^2 \pmod{4} \) and thus \( D \equiv b^2 \pmod{4m} \). Hence \( D = b^2 - 4mc \) for some integer \( c \). But then \( mx^2 + bxy + cy^2 \) represents \( m \) and has discriminant \( D \); it is primitive since \( \gcd(m, b) = \gcd(m, D) = 1 \). \( \square \)

**Corollary 6.** Let \( n \) be an integer, and \( p \) an odd prime not dividing \( n \). Then \( \left( \frac{-n}{p} \right) = 1 \) if and only if \( p \) is represented by a primitive form of discriminant \( -4n \).\]
Proof. By the preceding lemma, \( p \) is represented by a primitive form of discriminant \(-4n\) if and only if

\[
1 = \left( \frac{-4n}{p} \right) = \left( \frac{-n}{p} \right)
\]

\[\square\]