1 Proposition 4.1

$f = (a, b, c)$ is a quadratic form with discriminant $\Delta$ that represents $r$ \textit{primitively}. Then

$$s^2 - \Delta \equiv 0 \pmod{4r}$$

has an integer solution $s$. Conversely, if $\Delta$ is a discriminant to a set of binary forms, and a solution $s$ exists to the equation above, then $r$ is represented by some form.

2 Background

$r$ is \textit{represented} by $f$ if $r = ax^2 + bxy + cy^2$ for some $x, y$. This is a \textit{primitive representation} if $\gcd(x, y) = 1$.

3 Proof

First, we recognize that if $r = ax^2 + bxy + cy^2$ with $\gcd(x, y) = 1$, we can use the second statement to write that $1 = wx - zy$ for integers $w$ and $z$. This is the determinant of the matrix

$$M = \begin{bmatrix} x & z \\ y & w \end{bmatrix}$$

Now, let’s see how $M$ acts on our form $f$. When we take

$$M' = M^T \cdot \begin{bmatrix} a & b \\ b & c \end{bmatrix} \cdot M = \begin{bmatrix} r & \frac{s}{2} \\ \frac{s}{2} & t \end{bmatrix}$$

we see that the term $r$ emerges in the upper left corner. So $M'$ is the matrix of an equivalent form $f'$ of $f$. Because these two forms are equivalent, $f$ and $f'$ have the same discriminant $\Delta$. Then, we have that

$$s^2 - 4rt = \Delta \Rightarrow s^2 - \Delta \equiv 0 \pmod{4r}$$
The converse is quite obvious. If \( s^2 - \Delta \equiv 0 \ (mod \ 4r) \) we have that
\[
s^2 - 4rt = \Delta
\]
Then, the form \( f = (r, s, t) \) has discriminant \( \Delta \), and clearly represents \( r \) when \( x, y = 1, 0 \)

### 4 Bigger Picture

This is a basic result about when it is possible to represent an integer \( r \) with a form. So if a set of forms have discriminant \( \Delta \), all we need to check to see if it is possible to represent \( r \) is that \( \Delta \) is a quadratic residue mod \( 4r \). However, we won’t know which of the forms with that discriminant represent \( r \). In general, we still do not have the machinery to easily determine what the set of all \( r \) is given a form. Moreover, we don’t know which forms with discriminant \( \Delta \) represent \( r \).

Some interesting results have been shown in this area of mathematics:

**Theorem:** If a positive definite quadratic form over \( \mathbb{Z} \) represents the following numbers:
\[
1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290
\]
then it represents all integers.

From this theorem, we immediately see that there are quadratic forms over some number of variables greater than 2 that represent all integers. In fact, it can be shown that:

**Theorem:** For each of the aforementioned integers, there exists a quadratic form which represents every integer but that integer.

One might ask the question what’s the minimum number of variables needed to create a universal form that represents every integer. This question has been solved:

**Theorem:** Four is the minimum number of variables needed to represent every integer. The form \( f = a^2 + b^2 + c^2 + d^2 \) does this. There are exactly 6436 universal quadratic quaternary (over four variables) forms.