Quadratic Forms and the Three-Square Theorem

1500723

April 21, 2018

Contents

1 Introduction

The question of whether an integer can be written as a sum of three squares dates back to Diophantus, who investigated whether or not integers of the form $3n + 1$ could be represented in such a way. Throughout history, many other mathematicians (Fermat, Euler, Lagrange, Legendre, and Dirichlet, to name but a few) have investigated this problem, as well as the related two-square and four-square problems. The three-square theorem, which states that a positive integer can be written as a sum of three squares if and only if it is not of the form $4^k(8m + 7)$, proved to be the hardest to solve, and the first proof was published in 1798 by Legendre in his *Essai sur la théorie des nombres* [12]. A more comprehensive proof using Dirichlet's theorem on primes in arithmetic progressions was given by Dirichlet in 1850 and presented by Landau in [11]. This is the proof we follow here. Although the question of whether an integer can be written as a sum of two or four squares can be solved by first answering the question for prime numbers, the same technique does not work for three squares: we see that $3 = 1^2 + 1^2 + 1^2$ and $5 = 2^2+1^2+0^2$, but it is easily checked that $15 = 3\times5$ cannot be expressed as a sum of three squares, so a different approach is necessary. Dirichlet's proof of the three-square theorem is based on the theory of binary and ternary

quadratic forms, which was mainly developed by Gauss in his *Disquisitiones Arithmeticae* [6].[1]

We start by introducing the theory behind binary quadratic forms in Section 2 and we show that each class of binary quadratic forms has a unique reduced representative. In Section 3 we develop this theory further in order to prove a simplified version of the *Gauss class number problem*. We use this to identify which primes can be written in the form x^2+ny^2 for $n = 1, 2, 3, 4$, and 7, and as a consequence, give a classification of integers which can be written as a sum of two squares. In Section 4 we look at ternary forms and show that every ternary form with determinant 1 is equivalent to a sum of three squares. Finally, in Section 5, assuming Dirichlet's theorem on primes in arithmetic progressions, we prove the three-square theorem.

2 Binary Quadratic Forms

In this section we introduce the main definitions and results concerning binary quadratic forms.

Definition 2.1. A *binary quadratic form over* $\mathbb{Z}$ is a polynomial of the form

$$f(x, y) = ax^2 + bxy + cy^2,$$

where $a, b, c \in \mathbb{Z}$.

So $2x^2+5xy-11y^2$, $9xy$, and x^2+y^2 are all examples of binary quadratic forms over $\mathbb{Z}$. It is possible to also insist that b be even. The two definitions are described as *collaborators* in [3, p. 355] since they are closely related. Gauss notably insisted that b be even, but we prefer to work in a slightly more general setting. Binary quadratic forms may sometimes be referred to simply as *binary forms*, or even just as *forms* if there is no possible confusion. We will also assume from now on that all of the binary quadratic forms we consider are over $\mathbb{Z}$.

Definition 2.2. The *matrix* of a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is denoted M_f, and is defined as

$$M_f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

We choose this matrix because

$$f(x, y) = \begin{pmatrix} x & y \end{pmatrix} M_f \begin{pmatrix} x \\ y \end{pmatrix}.$$

It will be often useful to work with the matrix of a binary form, rather than with the form itself.

[1] A full historical overview can be found in [5, §§ 6–8].

Definition 2.3. An integer n is said to be *represented* by a given form f if there exist integers x and y such that $f(x, y) = n$.

Using this definition, asking whether a positive integer n is the sum of two squares can be rewritten as: *does the binary quadratic form* $x^2 + y^2$ *represent* n*?* Our sums-of-squares problem is now a quadratic form problem.

Definition 2.4. Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form. The *discriminant* of f is denoted D, or $D(f)$, and is given by the formula $D = b^2 - 4ac$.

The *determinant* of f is denoted d_2, or $d_2(f)$, and is given by the formula $d_2(f) = \det M_f = ac - b^2/4$.

The important point to note is that for a binary form f, we have that $D(f) = -4d_2(f)$, so these two definitions are closely related.[2] We will tend to use the discriminant D when looking at binary forms. We also see that $D \equiv b^2 \equiv 0$ or $1 \pmod 4$. This fact will be important later.

Another concept where definitions differ is that of equivalent forms. We would like to group quadratic forms which share similar properties together, ideally into equivalence classes. Gauss defined two notions of equivalence: proper and improper. Here, we only concern ourselves with proper equivalence, and simply refer to it as equivalence, because the notion of improper equivalence is not needed.

Definition 2.5. Let f and g be two binary quadratic forms. We say that f *is equivalent to* g, and write $f \sim g$, if there exists a matrix $P \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$M_g = P^T M_f P.$$

Alternatively, we can say that $f \sim g$ if there exist integers p, q, r, and s with $ps - qr = 1$, such that $g(x, y) = f(px + qy, rx + sy)$. If two forms are equivalent then we say that they belong to the same *class*.

These two definitions are the same because if we assume the matrix version of the definition using $P = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then

$$\begin{aligned} g(x, y) &= \begin{pmatrix} x & y \end{pmatrix} M_g \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} P^T M_f P \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} px + qy & rx + sy \end{pmatrix} M_f \begin{pmatrix} px + qy \\ rx + sy \end{pmatrix} = f(px + qy, rx + sy). \end{aligned}$$

[2] *A Notational Nightmare!* Some authors use the determinant, others the discriminant. Unfortunately, many use the determinant and call it the discriminant, and some even use the discriminant and call it the determinant! Fortunately, for ternary forms we will only have a determinant.

Conversely, if we assume that $g(x,y) = f(px+qy, rx+sy)$, with $ps-qr = 1$, then we can set $P = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, and

$$\begin{pmatrix} x & y \end{pmatrix} M_g \begin{pmatrix} x \\ y \end{pmatrix} = g(x,y) = f(px+qy, rx+sy) = \begin{pmatrix} x & y \end{pmatrix} P^T M_f P \begin{pmatrix} x \\ y \end{pmatrix},$$

so we do indeed have that $M_g = P^T M_f P$. Since these two definitions are equivalent we will use them interchangeably. Saying that two binary forms are equivalent is effectively just saying that one can be obtained from the other by a linear transformation.

Proposition 1. *Equivalence of quadratic forms is an equivalence relation.*

Proof. [2, p. 5]. Let f, g, and h be binary quadratic forms. We have reflexivity since the identity matrix $I_2 \in \mathrm{SL}_2(\mathbb{Z})$ and $M_f = I_2^T M_f I_2$. For symmetry, suppose $f \sim g$, and let $P \in \mathrm{SL}_2(\mathbb{Z})$ be such that $M_g = P^T M_f P$. Then $P^{-1} \in \mathrm{SL}_2(\mathbb{Z})$, and $(P^T)^{-1} = (P^{-1})^T$, so $g \sim f$ because

$$M_f = (P^{-1})^T M_g P^{-1}.$$

Finally, for transitivity, suppose $f \sim g$ and $g \sim h$. Let $P, S \in \mathrm{SL}_2(\mathbb{Z})$ be such that $M_g = P^T M_f P$ and $M_h = S^T M_g S$. Then

$$M_h = S^T M_g S = S^T P^T M_f P S = (PS)^T M_f P S,$$

so $f \sim h$, since $PS \in \mathrm{SL}_2(\mathbb{Z})$. □

Alternatively, it could be shown that the group $\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms, and that the orbits are precisely the equivalence classes of the quadratic forms, see [14, pp. 7–9] for example.

Equivalent forms share some important properties, as we can see from the following propositions.

Proposition 2. *Equivalent forms have the same discriminant.*

Proof. [11, p. 153]. Let f and g be two equivalent quadratic forms. Let $P \in \mathrm{SL}_2(\mathbb{Z})$ be such that $M_g = P^T M_f P$. Then

$$\det M_g = \det\left(P^T M_f P\right) = (\det P^T)(\det M_f)(\det P) = \det M_f$$

because $\det(P^T) = \det(P) = 1$. So $d_2(g) = d_2(f)$, giving $D(g) = -4d_2(g) = -4d_2(f) = D(f)$. Hence f and g have the same discriminant. □

Proposition 3. *Equivalent forms represent the same integers. That is, if f and g are equivalent binary quadratic forms, then an integer n is represented by f if and only if it is represented by g.*

Proof. [14, p. 9]. Let f and g be our equivalent binary quadratic forms and let $P \in \mathrm{SL}_2(\mathbb{Z})$ be such that $M_g = P^T M_f P$. Let n be an integer represented by g, so $n = g(x, y)$ for some $x, y \in \mathbb{Z}$. Then,

$$\begin{aligned} n &= \begin{pmatrix} x & y \end{pmatrix} M_g \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} P^T M_f P \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \left(P \begin{pmatrix} x \\ y \end{pmatrix} \right)^T M_f \left(P \begin{pmatrix} x \\ y \end{pmatrix} \right) = \begin{pmatrix} u & v \end{pmatrix} M_f \begin{pmatrix} u \\ v \end{pmatrix}, \end{aligned}$$

where $\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) = P\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$. So $n = f(u, v)$, and n is represented by f. The converse follows since our equivalence of forms is an equivalence relation, and therefore symmetric. □

We could also simply note that $n = g(x, y) = f(px+qy, rx+sy)$, and see straight away that n is also represented by f. The above proof is presented since it will immediately generalise to ternary forms in Section 4.

Since we are interested in representing positive integers by quadratic forms, we restrict our attention to *positive definite* forms.

Definition 2.6. A binary quadratic form f is said to be *positive definite* if $f(x, y) \geqslant 0$ for all integers x and y, and $f(x, y) = 0$ if and only if $x = y = 0$.

Although this is the natural way to define positive definite forms, it is not a definition that is very easy to work with. The following proposition gives a simple way of checking positive definiteness.

Proposition 4. *A binary quadratic form $f(x, y) = ax^2+bxy+cy^2$ is positive definite if and only if $D < 0$ and $a > 0$.*

Proof. Similar to [11, p. 154]. For the forward direction, we prove the contrapositive. Suppose $a \leqslant 0$. Then $f(1, 0) = a \leqslant 0$, and so f is not positive definite. Now suppose that $a > 0$, but $D \geqslant 0$. We consider the following important identity (which is easily verified), essentially obtained by completing the square:

$$f(x, y) = \frac{(2ax + by)^2}{4a} - \frac{Dy^2}{4a}.$$

This identity is well defined since $a > 0$ by assumption. We see that $f(b, -2a) = 0 - aD = -aD \leqslant 0$, so f is not positive definite.

Conversely, if we assume $a > 0$ and $D < 0$, then using the above identity again, it is clear that $f(x, y) \geqslant 0$ for all $x, y \in \mathbb{Z}$, and $f(x, y) = 0$ if and only if $2ax + by = 0$ and $y = 0$, which holds if and only if $x = y = 0$. So f is positive definite. □

Proposition 5. *Let f and g be equivalent binary quadratic forms. Then f is positive definite if and only if g is positive definite.*

Proof. Let f and g be equivalent binary quadratic forms, let $P \in \mathrm{SL}_2(\mathbb{Z})$ be such that $M_g = P^T M_f P$, and suppose that f is positive definite. By Proposition 3, we know that f and g represent the same integers, meaning that g must represent only non-negative integers. To confirm that g is positive definite, we need only verify that $g(x, y) = 0$ if and only if $x = y = 0$. If $x = y = 0$, we clearly have that $g(x, y) = 0$. If $g(x, y) = 0$, then using Proposition 3 again, we have that

$$\left(P\begin{pmatrix}x\\y\end{pmatrix}\right)^T M_f \left(P\begin{pmatrix}x\\y\end{pmatrix}\right) = 0,$$

and since f is positive definite, $P\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) = \left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)$. Then since P is invertible, we have that $x = 0$ and $y = 0$. □

Example 2.1. Having seen all these definitions we will look at an example involving them. Consider the binary quadratic form over $\mathbb{Z}$:

$$f(x, y) = 13x^2 - 36xy + 25y^2.$$

First of all, this has matrix $M_f = \left(\begin{smallmatrix}13 & -18\\ -18 & 25\end{smallmatrix}\right)$. The discriminant of f is $D(f) = (-36)^2 - 4(13)(25) = -4$, so the determinant of f is $d_2(f) = 1$. Since $13 > 0$ and $D(f) = -4 < 0$, f is positive definite by Proposition 4. Next, $f(-4, 6) = 1972$, so 1972 is represented by f.

Furthermore we calculate that $f(3x + 4y, 2x + 3y) = x^2 + y^2$, so f is equivalent to $g(x, y) := x^2 + y^2$ since $\left(\begin{smallmatrix}3 & 4\\ 2 & 3\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. We note that g is positive definite and that $D(g) = -4$ as expected. Proposition 3 tells us that g also represents 1972, so 1972 is a sum of two squares! Using the method from Proposition 3 we can even find two squares which sum to give 1972: we have that $g(x, y) = f(3x + 4y, 2x + 3y)$, so inverting this relation we have $f(x, y) = g(3x - 4y, -2x + 3y)$. So

$$1972 = f(-4, 6) = g(3(-4) - 4(6), -2(-4) + 3(6)) = g(-36, 26),$$

giving $36^2 + 26^2 = 1972$.

Definition 2.7. A positive definite binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is said to be *reduced* if $|b| \leqslant a \leqslant c$, and $b \geqslant 0$ if either $|b| = a$ or $a = c$.

As we are about to see, reduced forms are important because they are representatives of our equivalence classes. Many authors define a reduced form to be one simply satisfying $|b| \leqslant a \leqslant c$, without the extra conditions. However, these extra conditions will guarantee uniqueness as the next theorem shows, and this will be important in the next section.

Theorem 6. *Any positive definite binary quadratic form is equivalent to a unique reduced form.*

Proof. Adapted from [2, p. 14] and [13, pp. 90–91]. We prove this theorem in two parts, first showing existence and then uniqueness. First let $f_0(x, y) = a_0x^2 + b_0xy + a_1y^2$ be a positive definite binary quadratic form. Our goal is to apply a reduction algorithm to create a sequence of forms $f_0, f_1, \ldots$ in which each form in the sequence is equivalent to the next (and hence to all of the others), and such that the sequence necessarily terminates with a reduced form f_n.

Using a slight variation on the standard division algorithm with b_0 and $2a_1$, we know that we can find integers q_1 and b_1 such that

$$b_0 = 2a_1q_1 - b_1 \quad \text{and} \quad -a_1 < b_1 \leqslant a_1.$$

Alternatively, this can be viewed as taking the least residue of b_0 modulo $2a_1$. We now transform f_0 to f_1 using the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -q_1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Using our second definition of equivalence:

$$\begin{aligned} f_1(x, y) &= f_0(y, -x - q_1y) = a_0y^2 + b_0y(-x - q_1y) + a_1(x + q_1y)^2 \\ &= a_1x^2 + (-b_0 + 2a_1q_1)xy + (a_0 - b_0q_1 + a_1q_1^2)y^2 \\ &= a_1x^2 + b_1xy + a_2y, \end{aligned}$$

where we have defined $a_2 := a_0 - b_0q_1 + a_1q_1^2$. If $a_2 \geqslant a_1$, then we stop; otherwise we repeat the process to find $f_2(x, y) = a_2x^2 + b_2xy + a_3y^2$, with $-a_2 < b_2 \leqslant a_2$. This process must terminate eventually, because $a_1 > a_2 > a_3 > \ldots$ and each $a_i > 0$ since each form is positive definite by Proposition 5. We therefore eventually reach a form f_n given by

$$f_n(x, y) = a_nx^2 + b_nxy + a_{n+1}y^2, \quad \text{where } -a_n < b_n \leqslant a_n, \text{ and } a_{n+1} \geqslant a_n.$$

If $a_{n+1} > a_n$, then f_n is reduced, and we are done. If $a_{n+1} = a_n$, then our form is also reduced if $b_n \geqslant 0$, so assume $b_n < 0$. Then set

$$g(x, y) = f_n(y, -x) = a_{n+1}x^2 - b_nxy + a_ny^2.$$

Then $g \sim f$, because the transformation matrix is $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Since $a_{n+1} = a_n$, all we have done is flipped the sign of the xy coefficient of f_n, so g is reduced, completing the existence part of the proof.

Now for uniqueness: let $f(x, y) = ax^2 + bxy + cy^2$ and $F(x, y) = Ax^2 + Bxy + Cy^2$ be reduced positive definite binary quadratic forms, and suppose that $f \sim F$, under the transformation matrix $P = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then using our alternative definition of form equivalence again, we have that

$$\begin{aligned} F(x, y) &= f(px + qy, rx + sy) \\ &= a(px + qy)^2 + b(px + qy)(rx + sy)xy + c(rx + sy)^2 \\ &= (ap^2 + bpr + cr^2)x^2 + (2apq + b(ps + qr) + 2crs)xy \\ &\quad + (aq^2 + bqs + cs^2)y^2, \end{aligned}$$

and then comparing coefficients gives:

$$A = ap^2+bpr+cr^2, \quad B = 2apq+b(ps+qr)+2crs, \quad C = aq^2+bqs+cs^2. \tag{1}$$

Our aim is to show that $f = F$. Let us start by showing that $A = a$. We know that $|b| \leqslant a \leqslant c$ because f is reduced. Also, $\big(|p| - |r|\big)^2 \geqslant 0$, so $p^2 + r^2 \geqslant 2|pr|$. Using these inequalities, we obtain the following:

$$\begin{aligned} A = ap^2 + bpr + cr^2 &\geqslant ap^2 - |b||pr| + cr^2 \geqslant ap^2 - a|pr| + cr^2 \\ &\geqslant ap^2 - a|pr| + ar^2 = a(p^2 + r^2 - |pr|) \geqslant a|pr|\,. \end{aligned} \tag{2}$$

By the symmetry of the problem, we can assume without loss of generality that $a \geqslant A$. By (2), $A \geqslant a|pr|$, so $|pr| = 0$ or 1. If $|pr| = 1$ then $A \geqslant a$, so $A = a$ in this case. Suppose instead that $|pr| = 0$. Then from (1)

$$A = ap^2 + cr^2 \geqslant ap^2 + ar^2 = a(p^2 + r^2) \geqslant a, \tag{3}$$

where the last inequality holds because we cannot have $p = r = 0$, since $\det P = 1$. So in this case too, $A = a$.

Next we prove the following claim: *if $c > a$, then $B = b$ and also $C = c$.* Suppose $c > a$. We still have that $|pr| = 0$ or 1. If $|pr| = 1$, then $r \neq 0$, so $cr^2 > ar^2$, meaning that the first inequality on the second line of (2) becomes strict, such that $A > a|pr| = a$, a contradiction since $A = a$. This leaves us with $|pr| = 0$. If $p = 0$, then $r \neq 0$ (because $\det P = 1$) and from (3) we have that $A = cr^2 > ar^2 \geqslant a$, a contradiction again, so we must in fact have that $p \neq 0$ and $r = 0$. Then $1 = ps - qr = ps$, so using (1), $B = 2apq + b$, so $B - b = 2apq$; that is $B - b$ is a multiple of $2a$. Then since both f and F are reduced and $A = a$, we have that $-a < b \leqslant a$ and $-a < B \leqslant a$. Multiplying the first inequality through by -1, and then adding the two inequalities together gives

$$-2a < B - b < 2a.$$

Since $B - b$ is a multiple of $2a$, we must have $B - b = 0$, so $B = b$. Also, $0 = B - b = 2apq$, and since $a > 0$ and $p \neq 0$ we must have $q = 0$, so $C = cs^2$ by (1). Then using the fact that $ps = 1$, we either have that $p = s = 1$, or $p = s = -1$; either way, $s^2 = 1$, so $C = c$, proving the claim.

With this claim, we can can now prove that $C = c$. Since $A = a$, our problem is still symmetrical, so let us assume that $c \geqslant C$. If $c > C$ then $c > C \geqslant A = a$, (where $C \geqslant A$ because F is reduced), so $c > a$, and by our claim $C = c$, which is a contradiction. This means that in fact $C = c$, so to complete our proof we must show that $B = b$.

Since $f \sim F$, we know that $D(f) = D(F)$; that is

$$b^2 - 4ac = B^2 - 4AC = B^2 - 4ac,$$

so $b^2 = B^2$, giving $b = B$ or $-B$. Suppose that $b \neq B$. This means that $b = -B$, but also that $b \neq 0$. If $b < 0$ then we must have $c > a$, because if $c = a$ then $b \geqslant 0$ by our definition of a reduced form. Then by our claim $B = b$, a contradiction. Similarly, if $b > 0$, then $B < 0$, so $c = C > A = a$, giving the same contradiction. We conclude that $B = b$, and hence $f = F$. □

Example 2.2. Here we carry out the reduction algorithm with $f(x, y) = 13x^2 - 36xy + 25y^2$ from Example 2.1, so we expect to end up with $x^2 + y^2$ (by uniqueness). We start with $a_0 = 13, b_0 = -36$, and $a_1 = 25$. By reducing -36 modulo 50, we have that $-36 = 50(-1) + 14$, so $b_1 = -14$ and $q_1 = -1$ giving

$$f_1(x, y) = 25x^2 - 14xy + (13 - 36 + 25)y^2 = 25x^2 - 14xy + 2y^2.$$

Then, reducing -14 modulo 4, we see that $-14 = 4(-3) - 2$, so $b_2 = 2$ and $q_2 = -3$ and we obtain

$$f_2(x, y) = 2x^2 + 2xy + (25 - (-14)(-3) + 2(-3)^2) = 2x^2 + 2xy + y^2.$$

Repeating the algorithm once more, $2 = 2(1) - 0$, so $b_3 = 0$ and $q_3 = 1$ and $f_3(x, y) = x^2 + 0xy + (2 - 2 + 1)y^2 = x^2 + y^2$ as expected.

Reduced forms satisfy the following important inequality.

Lemma 7. *If $f(x, y) = ax^2 + bxy + cy^2$ is a reduced positive definite quadratic form with discriminant D, then*

$$0 < a \leqslant \sqrt{\frac{-D}{3}}.$$

Proof. [11, p. 156]. Let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced positive definite binary quadratic form with discriminant D. Since f is positive definite we must have $a > 0$ (and $D < 0$). Then $c \geqslant a$, so $ac \geqslant a^2$. Also $b^2 \leqslant a^2$ because $-a < b \leqslant a$. Using these inequalities,

$$-D = 4ac - b^2 \geqslant 4a^2 - a^2 = 3a^2.$$

Then rearranging produces the desired inequality. □

We have now covered all of the necessary theory on binary quadratic forms. We develop more in the following section, but it will be not needed to prove the three-square theorem. We present here one more result which links quadratic forms with sums of squares.

Theorem 8. *Every positive definite binary quadratic form with discriminant $D = -4$ is equivalent to a sum of two squares.*

Proof. [11, p. 156]. Let $f(x, y)$ be a positive definite binary quadratic form with discriminant $D(f) = -4$. Then we know that f is equivalent to a reduced form $g(x, y) = ax^2 + bxy + cy^2$ with discriminant $D(g) = -4$ and

$$a \leqslant \sqrt{\frac{-D(g)}{3}} = \frac{2}{\sqrt{3}} < 2.$$

Since f is positive definite, so is g (by Proposition 5), so $a > 0$, which together with the above inequality implies that $a = 1$. Then we also know, since g is a reduced form, that $-a < b \leqslant a$; so $b = 0$ or $b = 1$. Since $b^2 \equiv D \equiv 0 \pmod 4$, b is even, so $b = 0$. Then from the discriminant equation $D(g) = b^2 - 4ac$, we obtain $c = 1$, so $g(x, y) = x^2 + y^2$, and f is indeed equivalent to a sum of two squares. □

Returning to our quadratic form $f = 13x^2 - 36xy + 25y^2$ from Examples 2.1 and 2.2, we now see that as soon as we know that f is positive definite, $D(f) = -4$, and $f(-4, 6) = 1972$, we can conclude that 1972 is a sum of two squares.

3 Class Numbers and Primes of the Form $x^2 + ny^2$

In this section we take a short detour from our path of proving the three-square theorem and discuss binary forms in more depth. In particular, we look at class numbers of binary quadratic forms and representations of prime numbers.

Theorem 9. *The number of classes of positive definite forms of a given discriminant D is finite.*

Proof. [11, p. 176]. Let $D < 0$, and let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced positive definite form with discriminant D. By the previous lemma $0 < a \leqslant \sqrt{-D/3}$, so we have only finitely many choices for a. Once a is chosen, we have only finitely many choices for b because $-a < b \leqslant a$; and then a and b uniquely determine c from the formula $D = b^2 - 4ac$, so we have finitely many reduced forms with discriminant D. Since each class must have a reduced representative, the number of classes must also be finite. □

The concept of *primitivity* will also be important in this section.

Definition 3.1. A binary form $f(x, y) = ax^2 + bxy + cy^2$ is said to be *primitive* if a, b, and c are coprime, and *imprimitive* otherwise.

Proposition 10. *Let f and g be two equivalent binary quadratic forms. If f is primitive, then g is primitive. Equivalently, if f is imprimitive, so is g.*

Proof. Let f and g be equivalent binary quadratic forms, suppose f is imprimitive and let $\delta > 1$ be the greatest common divisor of the coefficients of f. Let m be an arbitrary integer represented by f (and hence also by g). Since δ divides each of the coefficients of f, we have that $\delta \mid m$ also. In particular, if $g = ax^2 + bxy + cy^2$, then

$$\delta \mid a = g(1,0), \quad \delta \mid c = g(0,1), \quad \text{and} \quad \delta \mid a+b+c = g(1,1).$$

From this, $\delta \mid b = (a+b+c) - a - c$. So $\gcd(a,b,c) \geqslant \delta > 1$, so g is imprimitive. The two statements in the theorem are equivalent because a binary quadratic form is either primitive or imprimitive, so one statement is the contrapositive of the other. □

From this, we conclude that each class of binary quadratic forms is either made up of primitive or imprimitive forms.

Definition 3.2. Given some integer $D < 0$, the number of classes of primitive positive definite quadratic forms with discriminant D is denoted $h(D)$.

Since we know that every positive definite binary quadratic form is equivalent to a unique reduced form, we can view $h(D)$ as the number of reduced primitive binary forms with discriminant D. By Theorem 9, $h(D)$ is finite for any $D < 0$.

Next, we introduce the idea of principal forms. We saw earlier that a discriminant D (of a binary form) is either congruent to 0 or 1 modulo 4. In fact, given any integer D congruent to 0 or 1 modulo 4, we can construct a binary form with discriminant D.

Definition 3.3. Let D be a negative integer such that $D \equiv 0$ or $1 \pmod 4$.

- If $D \equiv 0 \pmod 4$, then $x^2 - (D/4)y^2$ is the *principal form of discriminant D.*
- If $D \equiv 1 \pmod 4$, then $x^2 + xy - ((D-1)/4)y^2$ is the *principal form of discriminant D.*

Checking that each of these principal forms does indeed have discriminant D is simple. We also see that these principal forms are reduced, so given a negative integer $D \equiv 0$ or $1 \pmod 4$, we have that $h(D) \geqslant 1$.

One of the important questions that Gauss formulated was *when does $h(D) = 1$?* That is: when is the principal form the only primitive reduced form with discriminant D? Since Gauss was working with the slightly less general quadratic forms $f(x,y) = ax^2 + \mathbf{2}bxy + cy^2$ with determinant $d = b^2 - ac$, the conjecture that Gauss made actually corresponds to the following theorem, which he was unable to prove. The theorem was first proven by Landau in 1903 in [10].

Theorem 11. *If $n \in \mathbb{N}$, then $h(-4n) = 1$ if and only if $n \in \{1,2,3,4,7\}$.*

Proof. Based on [13, pp. 92–93]. For the forward direction, suppose that $n \notin \{1, 2, 3, 4, 7\}$. The principal form of discriminant $-4n$ is $x^2 + ny^2$. Our aim is to construct a *non-principal* primitive reduced form with the same discriminant. If we can do this, then $h(-4n) > 1$, which is what we want to show. We split the proof up into different cases.

Suppose n is not a prime power. Let p be a prime factor of n, and set $d = \mathrm{ord}_p(n)$. Now set

$$a = \min\left(p^d, \frac{n}{p^d}\right) \quad \text{and} \quad c = \max\left(p^d, \frac{n}{p^d}\right).$$

Then $ac = n$ and $\gcd(a, c) = 1$. Furthermore, $1 < a < c$ because $n \neq p^d$ (as n is not a prime power by assumption). Let $f(x, y) = ax^2 + cy^2$. This form is non-principal since $a > 1$, it is primitive because $\gcd(a, 0, c) = \gcd(a, c) = 1$, it is reduced as $0 < a < c$, and finally $D(f) = -4ac = -4n$. All this together means that $h(-4n) > 1$.

Next, suppose $n = 2^l$, where $l \geqslant 3$. If $l = 3$, then $n = 8$, and $-4n = -32$. Set $f(x, y) = 3x^2 + 2xy + 3y^2$, which is clearly non-principal, primitve, reduced, and $D(f) = -4n$, so $h(-4n) > 1$. If $l \geqslant 4$, then we follow a very similar method. Let

$$g(x, y) = 4x^2 + 4xy + (2^{l-2} + 1)y^2.$$

Clearly g is non-principal and primitive. Also, g is a reduced form because $|4| \leqslant 4 \leqslant 2^{l-2} + 1$, where we have used the fact that $l \geqslant 4$. Finally,

$$D(g) = 4^2 - 4(4)(2^{l-2} + 1) = -4(-4 + 4(2^{l-2} + 1)) = -4(2^l) = -4n$$

as required, so $h(-4n) > 1$.

Our final possibility is when $n = p^r$ for an odd prime p and an integer $r \geqslant 1$. Consider $n + 1$, which is even. Suppose $n + 1$ is not a power of 2; that is, not a prime power. Then as we did earlier we can write $n + 1 = ac$ where $1 < a < c$ and $\gcd(a, c) = 1$. This time, set $f(x, y) = ax^2 + 2xy + cy^2$. Then f is non-principal, reduced because $|2| \leqslant a < c$, and primitive since $\gcd(a, c) = 1$. We then simply check the discriminant of f to see that $D(f) = -4n$, so we have again that $h(-4n) > 1$. Otherwise, suppose $n + 1 = 2^t$ for some $t \geqslant 1$. We cannot have $t = 1, 2$, or 3 because $n \neq 1, 3$, or 7. Also $t = 4$ would imply that $n = 15$, but this is not a prime power, so this is impossible. If $t = 5$, then $n = 31$, and we set $g(x, y) = 5x^2 + 4xy + 7y^2$. We have here that $h(-4n) > 1$ because g is non-principal, primitive, reduced, and $D(g) = -4n$ again. For $t \geqslant 6$, let

$$k(x, y) = 8x^2 + 6xy + (2^{t-3} + 1)y^2.$$

We see straight away that k is non-principal and primitive. Since $t \geqslant 6$, We have that $|6| < 8 < 2^{t-3} + 1$, so k is reduced, and

$$D(k) = 6^2 - 4(8)(2^{t-3} + 1) = -4(-9 + 2^t + 8) = -4(2^t - 1) = -4n,$$

so yet again $h(-4n) > 1$. We have exhausted all positive integers n other than $n \in \{1, 2, 3, 4, 7\}$, so we have completed one direction of the proof.

For the converse, we assume $n \in \{1, 2, 3, 4, 7\}$, and we would like to show that $h(-4n) = 1$. Suppose $f(x, y) = ax^2 + bxy + cy^2$ is a reduced form with discriminant $D(f) = -4n$. Then $b^2 = D + 4ac \equiv 0 \pmod 4$, so b must be even. Recall that we have the two inequalities:

$$-a < b \leqslant a \quad \text{and} \quad 0 < a \leqslant \sqrt{\frac{-D(f)}{3}} = 2\sqrt{\frac{n}{3}}.$$

Suppose $a = 1$, then $b = 0$ as b is even, and $-4c = -4n$ from the discriminant equation, so $c = n$. We have our principal form $f(x, y) = x^2 + ny^2$.

Suppose $a = 2$. This will only occur when $n \geqslant 3$. We have $b = 0$ or 2 and $b^2 - 8c = -4n$, which gives

$$c = \frac{b^2 + 4n}{8}.$$

If $n = 3$ or 7, we must have $b = 2$ for c to be an integer. If $b = 2$, then $c = 2$ or 4 depending on whether $n = 3$ or 7. Either way a, b, and c are all even, so f is imprimitive, meaning it does not increase $h(-4n)$. Similarly, if $n = 4$, then $b = 0$, and so $c = 2$ meaning that f is imprimitive.

We are now in a position to quickly complete the proof using the inequality $0 < a \leqslant 2\sqrt{n/3}$. If $n = 1$ or 2, then $a = 1$, and the principal form is the only reduced primitive form, so $h(-4n) = 1$. If $n = 3$ or 4, then $a = 1$ or 2, and the principal form is the only reduced primitive form, because the reduced forms obtained when $a = 2$ are imprimitive, so $h(-4n) = 1$. Finally, if $n = 7$, we can have $a = 1, 2$, or 3. We need only check that the case $a = 3$ does not produce a non-principal primitive reduced form. If $a = 3$, then $b = -2, 0$, or 2. After rearranging the discriminant equation $b^2 - 12c = -28$, we have that

$$c = \frac{b^2 + 28}{12},$$

which is not an integer for $b = -2, 0$, or 2. We therefore conclude that $h(-4n) = 1$ when $n = 7$ also. □

This gives a complete answer to the question posed by Gauss, but it does not tell the whole story. Since $D \equiv 0$ or $1 \pmod 4$, this theorem tells us which negative *even* discriminants have class number 1, namely $D = -4, -8, -12, -16$, and -28. What about the odd discriminants? This question led to the formation of the *Gauss class number problem*, concerning *fundamental discriminants*[3], which states that $h(D) = 1$ if and only

[3]If $D \neq 1$ is an integer such that $D \equiv 1 \pmod 4$ and D is square-free, or $D = 4m$ where $m \equiv 2$ or $3 \pmod 4$ and m is square-free, then D is said to be a *fundamental discriminant*.

if $D = -3, -4, -7, -8, -11, -19, -43, -67$, or -163, where D is a negative fundamental discriminant. The problem is usually stated in terms of imaginary quadratic fields. This problem is much deeper and was eventually solved by Heegner in 1952, although his proof contained some minor mistakes and was not accepted at the time. Stark formally completed and corrected the proof in 1969 (see [17]). A full discussion of the class number problem, as well as its proof, can be found in [4].

Another important problem in number theory is the representation of primes of the form $x^2 + ny^2$. Fermat investigated the cases $n = 1, 2$, and 3, and formulated conjectures which were later proved by Euler, even though Fermat claimed he had an *irrefutable* proof for $n = 1$ which he did not write down! [5, p. 228]. Using the previous theorem, we present our own proof for the cases $n = 1, 2, 3, 4$, and 7, which is based on ideas from [4, § 2A].

Theorem 12. *Let p be a prime number. Then*

(a) $p = x^2 + y^2$ *if and only if* $p \equiv 1 \pmod 4$ *or* $p = 2$.

(b) $p = x^2 + 2y^2$ *if and only if* $p \equiv 1, 3 \pmod 8$ *or* $p = 2$.

(c) $p = x^2 + 3y^2$ *if and only if* $p \equiv 1 \pmod 3$ *or* $p = 3$.

(d) $p = x^2 + 4y^2$ *if and only if* $p \equiv 1 \pmod 4$

(e) $p = x^2 + 7y^2$ *if and only if* $p \equiv 1, 2, 4 \pmod 7$ *or* $p = 7$.

Proof. Let us take p to be an odd prime, because dealing with the case $p = 2$ is trivial here. Proving that the given congruence conditions are necessary is straightforward. We simply consider each equation modulo the number used in the condition. For example, consider $p = x^2 + 2y^2$ modulo 8. We know that squares are congruent to $0, 1$, or 4 modulo 8. Since p is odd, x must be odd, so $x^2 \equiv 1 \pmod 8$ and $2y^2 \equiv 0$ or $2 \pmod 8$. Adding these together means $p = x^2 + 2y^2 \equiv 1$ or $3 \pmod 8$. The other cases are treated very similarly, and are in fact simpler.

We will now tackle the converse. Again we take p to be odd, and also we note that in (c), $3 = 0^2 + 3(1^2)$, and in (e), $7 = 0^2 + 7(1^2)$, so we can focus on the congruence conditions themselves, and not on any extra cases. The point is that the congruence conditions placed on p for $p = x^2 + ny^2$ (for $n \in \{1, 2, 3, 4, 7\}$) are equivalent to checking when the Legendre symbol $\left(\frac{-n}{p}\right) = +1$. Verifying this claim is simple using the law of quadratic reciprocity.

In (a), we know already that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$. In (b), we have that $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1$ or $3 \pmod 8$. Similarly, this equivalence of conditions holds in (c), (d), and (e). So rather

than assuming the congruence conditions in each case, we will assume that $\left(\frac{-n}{p}\right) = 1$, since this is equivalent.

Using our previous theorem, we know that if we can represent p by a primitive positive definite form of discriminant $-4n$, then p is also representable by $x^2 + ny^2$ because $h(-4n) = 1$. Since $\left(\frac{-n}{p}\right) = 1$, we can pick an integer t such that $t^2 \equiv -n \pmod{p}$; that is $t^2 = -n + kp$, where $k \in \mathbb{Z}$ and we also see that $k > 0$. Rearranging this gives $kp - t^2 = n$, or

$$\det \begin{pmatrix} k & t \\ t & p \end{pmatrix} = n.$$

Then it is natural to set $f(x, y) = kx^2 + 2txy + py^2$, as $D(f) = -4d_2(f) = -4n$, just as we wanted. Also f represents p because $f(0, 1) = p$, and f is positive definite since $k > 0$ and $D(f) < 0$. We just need to check that f is primitive in order to complete the proof.

Since p is prime, $\gcd(k, 2t, p) = 1$ or p. Let us suppose that it is p. Since p is odd, $p \mid 2t$ implies that $p \mid t$. Then $p^2 \mid t^2$, and also $p^2 \mid kp$ because $p \mid k$ and $p \mid p$. So $p^2 \mid n = kp - t^2$, but this would imply that $9 \leqslant p^2 \leqslant n \leqslant 7$, a clear contradiction, so f is indeed primitive. □

As an application of this theorem, we can give a complete classification of the numbers that can be written as a sum of two squares. Since we have answered the question for primes, we have done most of the work thanks to the following identity, known as the *Brahmagupta-Fibonacci Identity*:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

for integers a, b, c, and d. This equation can be verified simply by expanding out the brackets and rearranging.

Theorem 13 (Two-Square Theorem)**.** *A positive integer n can be written as a sum of two squares if and only if n can be written in the form $n = ab^2$ where a and b are integers such that a has no prime factors $q \equiv 3 \pmod{4}$.*

Equivalently a positive integer n can be written as a sum of two squares if and only if in the prime factorisation of n every prime $q \equiv 3 \pmod{4}$ appears with an even exponent.

Proof. Adapted from [9, pp. 605–606]. Suppose first that n is of the form ab^2 where any prime factor of a is either equal to 2 or congruent to 1 (mod 4). Then by Theorem 12, each of these prime factors can be written as a sum of two squares, so a can be expressed as a sum of two squares using the Brahmagupta-Fibonacci identity, so $a = x^2 + y^2$ for some integers x and y. Hence $n = (bx)^2 + (by)^2$ can be expressed as a sum of two squares.

Conversely, suppose $n = x^2 + y^2$ for $x, y \in \mathbb{Z}$, and let q be a prime congruent to 3 modulo 4. Suppose $\mathrm{ord}_q(n)$ is odd (so $\mathrm{ord}_q(n) > 0$ and

$q \mid n$). Let $d = \gcd(x, y)$, then set $r = x/d$, $s = y/d$, and $m = n/d^2$. We have that $\gcd(r, s) = 1$ and

$$r^2 + s^2 = \frac{x^2}{d^2} + \frac{y^2}{d^2} = m.$$

Now, suppose $q \nmid m$, so $\operatorname{ord}_q(m) = 0$. Then we have that

$$\operatorname{ord}_q(n) = \operatorname{ord}_q(md^2) = \operatorname{ord}_q(m) + \operatorname{ord}_q(d^2) = 2\operatorname{ord}_q(d).$$

However, this is a contradiction as $\operatorname{ord}_q(n)$ is odd, so we must in fact have that $q \mid m$. Next, we cannot have $q \mid r$, as otherwise this would imply that $q \mid m - r^2 = s^2$, and hence that $q \mid s$, contradicting the corprimality of r and s. So $q \nmid r$ and $\gcd(r, q) = 1$. Using this, we know that we can pick an integer t satisfying the congruence $rt \equiv s \pmod{q}$. Then

$$0 \equiv m \equiv r^2 + s^2 \equiv r^2 + (rt)^2 \equiv (1 + t^2)r^2 \pmod{q},$$

so $q \mid (1+t^2)r^2$. Then $q \nmid r^2$, since $q \nmid r$, so $q \mid t^2+1$ as q is a prime; that is $t^2 \equiv -1 \pmod{q}$, contradicting the supplementary law of quadratic reciprocity, because $q \equiv 3 \pmod{4}$. This contradiction means that our assumption that $\operatorname{ord}_q(n)$ was odd is false, and hence $\operatorname{ord}_q(n)$ is even, completing the proof. □

In this section and the preceding one, we have only really scratched the surface of the theory of binary quadratic forms, and it is important to see what else there is to investigate. There exists a composition law for primitive classes of binary quadratic forms, and in fact Gauss showed that this set of primitive classes forms a finite abelian group with this binary operation, now called the *class group*, before the notion of a group was even formalised! This composition law was recently reconsidered by Manjul Bhargava, who came up with a concept now known as the Bhargava cube, to work with this binary operation. Bhargava and Hanke also recently proved the famous *290-theorem* [1], which states that if a positive definite binary quadratic form (as defined in Definition 1) represents all positive integers up to 290 (in fact even a certain subset will do), then it represents all positive integers!

4 Ternary Quadratic Forms

Asking whether a positive integer can be written as a sum of three squares is the same as asking whether it can be represented by the ternary form $x^2 + y^2 + z^2$, so just as we developed a theory for binary forms, we must do the same for ternary forms, although here we only go into as much detail as needed to prove the three-square theorem. Throughout this section, we follow the proofs by Landau, [11, pp. 156–160], with some slight adaptations and modernisations.

Definition 4.1. An *integral ternary quadratic form* is a polynomial of the form

$$f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j,$$

where $a_{ij} \in \mathbb{Z}$ and $a_{ij} = a_{ji}$ for all $i, j \in \{1, 2, 3\}$. We define the *matrix* of f to be the symmetric matrix of coefficients

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}.$$

We then define the *determinant* of f, denoted d_3, or $d_3(f)$, to be the determinant of its associated matrix: $d_3 = \det(a_{ij})$.

An important point to note is that in this definition, when $i \neq j$, the coefficient of x_{ij} is $a_{ij}+a_{ji} = 2a_{ij}$, which is even. So saying that a ternary form is *integral* as defined above is *stronger* than simply saying that the polynomial f has integer coefficients. In comparison, for binary quadratic forms, we did not insist that b be even (see Definition 2.1), which is why we did not refer to binary forms as integral in Section 2, but rather as binary forms over $\mathbb{Z}$. So $3x_1^2 - 4x_1x_2 + 2x_2^2 + 7x_2x_3 + x_3^2$ is *not* an integral ternary form (due to the $7x_2x_3$ term), but changing this 7, to say a 6, gives $3x_1^2 - 4x_1x_2 + 2x_2^2 + 6x_2x_3 + x_3^2$, which *is* an integral ternary form. Importantly, $x_1^2 + x_2^2 + x_3^2$ is an integral ternary form.

We will take all ternary forms to be *integral* (as defined above) from now on. Fortunately, a lot of the work we did with binary forms holds also for ternary forms. The definitions for *equivalent* ternary forms (see Definition 2.5), and *positive definite* ternary forms (see Definition 2.6) are the same as for binary forms, except that we take our matrices to be in $\mathrm{SL}_3(\mathbb{Z})$. Furthermore, the proofs that this equivalence is indeed an equivalence relation (Proposition 1), that equivalent forms represent the same integers (Proposition 3) and have the same determinant (Proposition 2), and that positive definiteness is preserved by equivalence (Proposition 5) are almost identical; the only difference being that we are now working with three by three matrices, and we use the determinant in Proposition 2 rather than the discriminant. On the other hand, the classification of positive definite ternary forms is somewhat different to Proposition 4, as we see in the following theorem.

Theorem 14. *A ternary quadratic form $f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j$ is positive definite if and only if the following three conditions hold:*

$$a_{11} > 0, \qquad b := \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix} > 0, \qquad d_3 > 0.$$

Furthermore, if f is positive definite, then

$$a_{11}f(x_1, x_2, x_3) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + g(x_2, x_3),$$

where g is the binary quadratic form

$$g(x_2, x_3) = (a_{11}a_{22} - a_{12}^2)x_2^2 + 2(a_{11}a_{23} - a_{12}a_{13})x_2x_3 + (a_{11}a_{33} - a_{13}^2)x_3^2,$$

and g is positive definite with determinant $d_2(g) = a_{11}d_3$.

Proof. Checking the identity and the fact that $d_2(g) = a_{11}d_3$ is simply done by direct calculation. Now, if $a_{11} \leqslant 0$, then $f(1, 0, 0) = a_{11} \leqslant 0$, and f is not positive definite, so let us assume that $a_{11} > 0$ for the remainder of the proof. By our classification of positive definite binary quadratic forms, g is positive definite if and only if $a_{11}a_{22} - a_{12}^2 > 0$ and $-(1/4)D(g) = d_2(g) = a_{11}d_3 > 0$, and since $a_{11} > 0$, this is if and only if $b = a_{11}a_{22} - a_{12}^2 > 0$ and $d_3 > 0$. So the three conditions in the theorem are equivalent to g being positive definite, and to complete the proof we must therefore show the following: *f is positive definite if and only if g is positive definite.*

Suppose that g is not positive definite, so there exist integers s_1 and t_1, not both zero, such that $g(s_1, t_1) \leqslant 0$. Set $s_2 = a_{11}s_1$ and $t_2 = a_{11}t_1$. We have that

$$g(s_2, t_2) = a_{11}^2 g(s_1, t_1) \leqslant 0.$$

Then set

$$r_2 = \frac{-a_{12}s_2 - a_{13}t_2}{a_{11}} \in \mathbb{Z}.$$

Then $a_{11}r_2 + a_{12}s_2 + a_{13}t_2 = 0$, so

$$a_{11}f(r_2, s_2, t_2) = 0^2 + g(s_2, t_2) \leqslant 0.$$

Since $a_{11} > 0$, we have that $f(r_2, s_2, t_2) \leqslant 0$, so f is not positive definite.

Conversely, suppose that g is positive definite. From our identity, it is clear that $f(x_1, x_2, x_3) \geqslant 0$, and if $f(x_1, x_2, x_3) = 0$, then we must have

$$g(x_2, x_3) = 0 \quad \text{and} \quad a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = 0.$$

From the first equation, $x_2 = x_3 = 0$ because g is positive definite, and then from the second equation we obtain $a_{11}x_1 = 0$, which implies that $x_1 = 0$ because $a_{11} > 0$; so f is indeed positive definite. □

Just as for binary forms, we would like to find representatives for classes of ternary forms. We do not formally define these representatives as reduced, although the idea is the same. We first need the following lemma.

Lemma 15. *Given integers c_{11}, c_{21}, and c_{31} such that $\gcd(c_{11}, c_{21}, c_{31}) = 1$, the remaining six entries in the 3×3 matrix $C := (c_{ij})$ can be chosen such that $C \in \mathrm{SL}_3(\mathbb{Z})$*

Proof. Let $g = \gcd(c_{11}, c_{21})$. Then $\gcd(g, c_{31}) = 1$, as otherwise this would contradict the assumption that $\gcd(c_{11}, c_{21}, c_{31}) = 1$. Using Bezout's identity twice, we can pick integers c_{12}, c_{22} and integers u, v such that

$$c_{11}c_{22} - c_{21}c_{12} = g \quad \text{and} \quad gu - c_{31}v = 1.$$

Then, in the following matrix all entries are integers and expanding the determinant about the bottom row we find that:

$$\begin{aligned}\begin{vmatrix} c_{11} & c_{12} & \frac{c_{11}v}{g} \\ c_{21} & c_{22} & \frac{c_{21}v}{g} \\ c_{31} & 0 & u \end{vmatrix} &= \frac{c_{31}v}{g}(c_{21}c_{12} - c_{11}c_{22}) + u(c_{11}c_{22} - c_{21}c_{12}) \\ &= -c_{31}v + gu = 1,\end{aligned}$$

where we have used both of the above identities. □

Theorem 16. *Every positive definite ternary quadratic form, with determinant d_3, is equivalent to a form $h(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij}x_ix_j$, satisfying:*

$$0 < a_{11} \leqslant \frac{4}{3}\sqrt[3]{d_3}, \qquad 2|a_{12}| \leqslant a_{11}, \qquad 2|a_{13}| \leqslant a_{11}.$$

Proof. Let f be a positive definite ternary quadratic form and let a_{11} be the smallest positive integer representable by f, and hence by any form equivalent to f because forms in the same class represent the same set of integers. We have that $a_{11} = f(c_{11}, c_{21}, c_{31})$ for some integers $c_{11}, c_{21},$ and c_{31}. Furthermore, $\delta := \gcd(c_{11}, c_{21}, c_{31}) = 1$, because otherwise, if $\delta > 1$ we would have

$$f(\frac{c_{11}}{\delta}, \frac{c_{21}}{\delta}, \frac{c_{31}}{\delta}) = \frac{a_{11}}{\delta^2} < a_{11},$$

contradicting the minimality of a_{11}. Then by the previous lemma, we can pick the remaining six integers in the matrix $C := (c_{ij})$ such that $\det(C) = 1$. Now let g be the positive definite ternary quadratic form obtained by transforming f with the matrix C, so $M_g = C^T M_f C$, and write $g = \sum_{i,j=1}^{3} b_{ij}x_ix_j$. Using the ternary version of Proposition 3, we have that:

$$b_{11} = g(1, 0, 0) = f(c_{11}, c_{21}, c_{31}) = a_{11}.$$

So g is a form equivalent to f with first coefficient $b_{11} = a_{11}$. Next we will construct another matrix, N, which will transform g to a new form, h, which will satisfy the conditions given in the theorem. Set

$$N = \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & v & w \end{pmatrix} = (n_{ij}),$$

where r and s are arbitrary integers and t, u, v, and w are integers such that the matrix $B := \left(\begin{smallmatrix} t & u \\ v & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Expanding the determinant of N about the first column we see that $\det(N) = \det(B) = 1$, so $N \in \mathrm{SL}_3(\mathbb{Z})$. Let h be the form obtained by transforming g using N; so $M_h = N^T M_g N$, and

$$h(1,0,0) = g(n_{11}, n_{21}, n_{23}) = g(1,0,0) = a_{11},$$

so we can set $h = \sum_{i,j=1}^{3} a_{ij} y_i y_j$, and we also know that $\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}^T = N \begin{pmatrix} y_1 & y_2 & y_3 \end{pmatrix}^T$. Writing out the matrix equation, $M_h = N^T M_g N$, in full, we have that

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ r & t & v \\ s & u & w \end{pmatrix} \begin{pmatrix} a_{11} & b_{12} & b_{13} \\ b_{12} & b_{22} & b_{23} \\ b_{13} & b_{23} & b_{33} \end{pmatrix} \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & v & w \end{pmatrix},$$

and then by comparing matrix entries on each side of the equation we obtain the following two relations:

$$a_{12} = a_{11} r + t b_{12} + v b_{13} \quad \text{and} \quad a_{13} = a_{11} s + u b_{12} + w b_{13}. \tag{4}$$

Using these, we obtain the following:

$$\begin{aligned} \begin{pmatrix} b_{11} & b_{12} & b_{13} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &= \begin{pmatrix} b_{11} & b_{12} & b_{13} \end{pmatrix} \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & v & w \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \\ &= \begin{pmatrix} b_{11} & a_{12} & a_{13} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}, \end{aligned}$$

so $b_{11}x_1 + b_{12}x_2 + b_{13}x_3 = a_{11}y_1 + a_{12}y_2 + a_{13}y_3$, because $a_{11} = b_{11}$. To see why this equation is important we use the identity given in Theorem 14 for both g and h:

$$\begin{aligned} a_{11} g(x_1, x_2, x_3) &= (b_{11}x_1 + b_{12}x_2 + b_{13}x_3)^2 + k(x_2, x_3), \\ a_{11} h(y_1, y_2, y_3) &= (a_{11}y_1 + a_{12}y_2 + a_{13}y_3)^2 + l(y_2, y_3), \end{aligned}$$

where k and l are positive definite binary quadratic forms as in Theorem 14. Then subtracting one equation from the other, we have that

$$a_{11} \left(g(x_1, x_2, x_3) - h(y_1, y_2, y_3) \right) = k(x_2, x_3) - l(y_2, y_3).$$

The matrix N takes g to h, so applying the transformation $\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}^T = N \begin{pmatrix} y_1 & y_2 & y_3 \end{pmatrix}^T$ and rearranging, gives

$$k(ty_2 + uy_3, vy_2 + wy_3) = l(y_2, y_3),$$

so $k \sim l$ under the transformation matrix B. Since we have not yet chosen our integers t, u, v, and w, we can pick them (by Theorem 6) such that B takes our binary form k to l, such that l is a reduced form. By Theorem 14 again, the first coefficient of l is given by $a_{11}a_{22} - a_{12}^2$, and $d_2(l) = a_{11}d_3(h)$. Then since l is a reduced form, we know that

$$a_{11}a_{22} - a_{12}^2 \leqslant \frac{2}{\sqrt{3}}\sqrt{a_{11}d_3(h)}$$

by our classification of reduced positive definite binary forms (Lemma 7). Now that we have chosen t, u, v, and w, we can return to our two relations from (4) and write

$$a_{12} = a_{11}r + m_1 \quad \text{and} \quad a_{13} = a_{11}s + m_2,$$

where $m_1 = tb_{12} + vb_{13}$ and $m_2 = ub_{12} + wb_{13}$ are now just constants. In fact, $a_{12} = a_{11}r + m_1$ is the congruence class of m_1 modulo a_{11}, so we can choose r such that a_{12} lies in the system of least residues of this congruence class; that is, $|a_{12}| \leqslant a_{11}/2$. In the same way we can pick s such that $|a_{13}| \leqslant a_{11}/2$, and so we have satisfied two out of our three required inequalities. Finally, We know that $a_{11} > 0$, so to complete the proof, we must show that $a_{11} \leqslant \frac{4}{3}\sqrt[3]{d_3(h)}$. We first note that $a_{22} = h(0, 1, 0)$ is representable by h, so by the minimality of a_{11} (for all forms in the class), $a_{22} \geqslant a_{11}$. Using this,

$$a_{11}^2 \leqslant a_{11}a_{22} = (a_{11}a_{22} - a_{12}^2) + a_{12}^2 \leqslant \frac{2}{\sqrt{3}}\sqrt{a_{11}d_3(h)} + \frac{a_{11}^2}{4}.$$

Then simply rearranging this produces the desired inequality: for

$$\frac{3}{4}a_{11}^{\frac{3}{2}} \leqslant \frac{2}{\sqrt{3}}\sqrt{d_3(h)},$$

hence

$$a_{11} \leqslant \left(\frac{8}{3\sqrt{3}}\sqrt{d_3(h)}\right)^{\frac{2}{3}} = \frac{4}{3}\sqrt[3]{d_3(h)},$$

as required. □

We now prove the ternary version of Proposition 8.

Theorem 17. *Every positive definite ternary quadratic form with determinant* 1 *is equivalent to a sum of three squares.*

Proof. Given a positive definite ternary quadratic form with determinant 1, we know by Theorem 16 that it is equivalent to a positive definite form $f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij}x_ix_j$, satisfying:

$$0 < a_{11} \leqslant \frac{4}{3}, \qquad 2|a_{12}| \leqslant a_{11}, \qquad 2|a_{13}| \leqslant a_{11}.$$

From this we have that $a_{11} = 1, a_{12} = a_{13} = 0$, and so by the identity in Theorem 14,

$$f(x_1, x_2, x_3) = x_1^2 + g(x_2, x_3),$$

where $g(x_2, x_3) = a_{22}x_2^2 + 2a_{23}x_2x_3 + a_{33}x_3^2$ is positive definite and $d_2(g) = a_{11}d_3(f) = 1$. So g is a positive definite binary quadratic form with discriminant $D(g) = -4d_2(g) = -4$, and hence equivalent to a sum of two squares by Proposition 8. So there exists a matrix $S \in \mathrm{SL}_2(\mathbb{Z})$ such that $S^T M_g S = I_2$, where I_2 is the 2×2 identity matrix; that is the matrix of the sum of two squares. Now setting $P = I_1 \oplus S$, where $\oplus$ denotes the direct sum, we have that:

$$\begin{aligned} P^T M_f P &= (I_1 \oplus S)^T (I_1 \oplus M_g)(I_1 \oplus S) = (I_1 \oplus S^T)(I_1 \oplus M_g)(I_1 \oplus S) \\ &= I_1 \oplus (S^T M_g S) = I_1 \oplus I_2 = I_3, \end{aligned}$$

meaning that f, and hence also our original form, is equivalent to a sum of three squares. □

5 Sums of Three Squares

Having covered some theory on ternary quadratic forms, we are almost ready to prove our main theorem. We first need to introduce *Jacobi Symbols*, which are an extension of Legendre symbols.

Definition 5.1. Let $b > 0$ be an odd integer, and $b = \prod_{r=1}^{k} p_r$ a factorisation of m into (possibly repeated) prime numbers. Let a be any integer. We define the *Jacobi symbol* $\left(\frac{a}{b}\right)$ as

$$\left(\frac{a}{b}\right) = \prod_{r=1}^{k} \left(\frac{a}{p_r}\right),$$

where $\left(\frac{a}{p_r}\right)$ is the usual Legendre symbol.

It is important to note that $\left(\frac{a}{b}\right) = +1$ does not necessarily mean that a is a quadratic residue modulo b. For example, $\left(\frac{2}{15}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{3}\right) = +1$, but it can be checked that 2 is not a quadratic residue modulo 15. So, *why are Jacobi symbols useful?* The point is that (at least in our case) we will use them in intermediary steps to evaluate Legendre symbols. Jacobi symbols have properties which are very similar to those of Legendre symbols.

Proposition 18. *Let b, b_1 and b_2 be odd integers, and a, a_1 and a_2 integers. Then the following statements hold:*

(i) $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$ *if* $a_1 \equiv a_2 \pmod{b}$.

(ii) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$.

(iii) $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.

(iv) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.

(v) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.

(vi) If a and b are odd positive integers, then

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

Proof. The first three statements follow directly from the definition of the Jacobi symbol and the corresponding properties of the Legendre symbol. Statements (iv), (v), and (vi) require a little more work (although the proofs are also straightforward) and we refer to [8, p. 57] for the details. □

An alternative way of stating (vi) is the following: if a and b are odd positive integers, then

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{if } a \equiv 1 \pmod 4 \quad \text{or} \quad b \equiv 1 \pmod 4 \\ -\left(\frac{b}{a}\right) & \text{if } a \equiv b \equiv 3 \pmod 4 \end{cases}.$$

As was mentioned in the introduction, we also need Dirichlet's famous theorem on primes in arithmetic progressions. The proof is long and requires complex analysis; a proof is presented in [15, pp. 61–76].

Theorem 19 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *Let a and d be positive coprime integers. Then there are infinitely many primes congruent to a modulo d.*

We are finally ready to prove the three-square theorem. We follow Dirichlet's classical proof, presented by Landau.

Theorem 20 (Legendre's Three-Square Theorem)**.** *A positive integer n can be expressed as a sum of three squares if and only if n is not of the form $4^k(8m+7)$ where k and m are non negative integers.*

Proof. Adapted from [11, pp. 161–164]. The forward direction of this proof is relatively straightforward. First we will show that a number of the form $8m+7$ cannot be expressed as a sum of three squares. Suppose it can, and that for integers x, y, and z we have that $8m+7 = x^2+y^2+z^2$. Considering this equation modulo 8, we have

$$x^2 + y^2 + z^2 \equiv 7 \pmod 8,$$

and simply checking the possibilities shows that this is impossible because squares are congruent to $0, 1$, or 4 modulo 8. Now in the more general case, suppose $n = 4^k(8m+7) = x^2+y^2+z^2$ for $x, y, z \in \mathbb{Z}$ and $k \geqslant 1$ (as we have already treated the case $k = 0$). Then considering this equation modulo 4, we have that

$$x^2 + y^2 + z^2 \equiv 0 \pmod 4,$$

so we must have that x, y, and z are all even. This means that we can divide through by 4 to get

$$4^{k-1}(8m+7) = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2.$$

If $k - 1 = 0$, then this is a contradiction since $8m + 7$ is not a sum of three squares. Otherwise we divide by 4 again. This process must terminate eventually, giving us the same contradiction. We conclude that n is not a sum of three squares.

Now for the converse: we start by eliminating some possibilities. Suppose $n = 4^k n_1$, where $4 \nmid n_1$ (so $n_1 \not\equiv 0 \pmod 4$) and $n_1 = x^2 + y^2 + z^2$ is a sum of three squares. Then $n = (2^k x)^2 + (2^k y)^2 + (2^k z)^2$ is also a sum of three squares, so we can assume that $n \not\equiv 0 \pmod 4$; as otherwise we could keep dividing by 4 to reduce the problem to a new number (n_1) not congruent to 0 modulo 4. We also know that $n \equiv 7 \pmod 8$ is not a sum of three squares, so we will just consider the cases $n \equiv 1, 2, 3, 5, \text{ or } 6 \pmod 8$.

In order to prove our theorem, we will construct a positive definite ternary quadratic form which has determinant 1 and which represents n. If we can construct such a form, then we know that it will be equivalent to a sum of three squares which must also represent n; that is n is a sum of three squares. With this knowledge, we must pick six integers $a_{11}, a_{12}, a_{13}, a_{22}, a_{23}, a_{33}$ such that the ternary form they determine (namely $f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j$) represents n, and such that the form is positive definite, which by Theorem 14, occurs when the following three conditions hold:

$$a_{11} > 0, \qquad b := a_{11}a_{22} - a_{12}^2 > 0, \qquad d_3(f) = 1.$$

We start by setting $a_{13} = 1, a_{23} = 0$, and $a_{33} = n$, so that

$$f(x_1, x_2, x_3) = a_{11}x_1^2 + 2a_{12}x_1x_2 + 2x_1x_3 + a_{22}x_2^2 + nx_3^2.$$

Then $f(0, 0, 1) = n$ meaning that the condition that f must represent n is satisfied. Next, we have that

$$d_3(f) = \begin{vmatrix} a_{11} & a_{12} & 1 \\ a_{12} & a_{22} & 0 \\ 1 & 0 & n \end{vmatrix} = nb - a_{22},$$

so the three conditions still left to satisfy are equivalent to the following three:

$$a_{11} > 0, \qquad b = a_{11}a_{22} - a_{12}^2 > 0, \qquad a_{22} = bn - 1.$$

If $n = 1$ it is clearly a sum of three squares, so let us assume that $n > 1$. The first condition is now implied by the remaining two, as we now show. From our second condition, $b > 0$, and using the fact that $n > 1$,

$$a_{22} = bn - 1 > b - 1 \geqslant 0.$$

Using our second condition again, we have that

$$a_{11}a_{22} = b + a_{12}^2 > 0,$$

so $a_{11} > 0$ because $a_{22} > 0$ by our previous equation, eliminating our first condition and leaving us with

$$b = a_{11}a_{22} - a_{12}^2 > 0 \quad \text{and} \quad a_{22} = bn - 1.$$

In order to satisfy these two conditions, we need a $b > 0$, such that

$$a_{11} = \frac{b + a_{12}^2}{a_{22}} \in \mathbb{Z}, \tag{5}$$

which is saying that we must find a $b > 0$ such that $b + a_{12}^2 \equiv 0 \pmod{a_{22}}$; that is $-b \equiv a_{12}^2 \pmod{bn-1}$, because if we can find an integer b satisfying these conditions, we can set $a_{22} = bn - 1$, we can let a_{12} be the integer whose square is congruent to $-b$ modulo $bn - 1$, and we can finally define a_{11} as in (5), and all the necessary conditions will be satisfied. So we have finally reduced our conditions down to needing to find a positive integer b such that $-b$ is a quadratic residue modulo $bn - 1$. We now split into two cases depending on whether n is odd or even.

First suppose $n \equiv 2$ or $6 \pmod 8$. We aim to find a prime $p = bn - 1$ such that $\left(\frac{-b}{p}\right) = 1$. Let $g = \gcd(4n, n-1)$. Then $g \mid 4n - 4(n-1) = 4$, so $g = 1, 2$, or 4. Since $n - 1$ is odd, $g = 1$, so by Dirichlet's theorem there exists an integer $v \geqslant 0$ such that

$$p := 4nv + n - 1 = (4v + 1)n - 1$$

is prime. Set $b = 4v + 1 > 0$, so $p = bn - 1$. Then $b \equiv 1 \pmod 4$ and $p \equiv n - 1 \equiv 1 \pmod 4$, so

$$\left(\frac{-b}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{p}{b}\right) = \left(\frac{bn-1}{b}\right) = \left(\frac{-1}{b}\right) = 1,$$

using the Jacobi symbol properties from Proposition 1.8, meaning that b satisfies our conditions as $-b$ is a quadratic residue modulo $p = bn - 1$.

Now suppose $n \equiv 1, 3, \text{ or } 5 \pmod 8$. Set $c = 1$ if $n \equiv 3 \pmod 8$ and set $c = 3$ if $n \equiv 1 \text{ or } 5 \pmod 8$. In both cases, $cn \equiv 3 \pmod 4$, so $(cn-1)/2$ is odd. Let $h = \gcd(4n, (cn-1)/2)$. If $c = 1$, then $h \mid 4n - 8((n-1)/2)) = 4$. If $c = 3$, then $h \mid 3(4n) - 8((3n-1)/2)) = 4$. Either way, $h \mid 4$, so $h = 1$ as $(cn-1)/2$ is odd. Then by Dirichlet's theorem, we can find an integer $v \geqslant 0$ such that

$$p := 4nv + \frac{cn-1}{2} = \frac{(8v+c)n-1}{2}$$

is prime. Now set $b = 8v + c$. We have that $b > 0$ and $2p = bn - 1$, so we want to show that b is a quadratic residue modulo $2p$. First we show that $\left(\frac{-2}{b}\right) = 1$. We have that

- If $n \equiv 1 \pmod 8$ then $b \equiv 3 \pmod 8$ and $p \equiv 1 \pmod 4$.
- If $n \equiv 3 \pmod 8$ then $b \equiv 1 \pmod 8$ and $p \equiv 1 \pmod 4$.
- If $n \equiv 5 \pmod 8$ then $b \equiv 3 \pmod 8$ and $p \equiv 3 \pmod 4$.

In each case, $\left(\frac{-2}{b}\right) = \left(\frac{-1}{b}\right)\left(\frac{2}{b}\right) = 1$ by parts (iv) and (v) of Proposition 18. Secondly, by parts (iv) and (vi) (or its reformulation) of Proposition 18, in all three cases we have that

$$\left(\frac{-b}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{p}{b}\right).$$

Using these two results,

$$\left(\frac{-b}{p}\right) = \left(\frac{p}{b}\right) = \left(\frac{p}{b}\right)\left(\frac{-2}{b}\right) = \left(\frac{-2p}{b}\right) = \left(\frac{1-bn}{b}\right) = \left(\frac{1}{b}\right) = 1,$$

so $-b$ is a quadratic residue modulo p, which is almost what we need. We can now pick an integer r_0 such that $r_0^2 \equiv -b \pmod p$. Set $r = r_0$ if r_0 is odd, and set $r = r_0 + p$ if r_0 is even. In both cases, r is odd, so $r^2 + b$ is even, and also $r \equiv r_0 \pmod p$. Therefore

$$r^2 + b \equiv 0 \pmod p \qquad \text{and} \qquad r^2 + b \equiv 0 \pmod 2.$$

Since $\gcd(2, p) = 1$, we have that $r^2 + b \equiv 0 \pmod{2p}$, so $-b$ is indeed a quadratic residue modulo $2p$, completing the proof. □

It is important to note that this proof is constructive, here we give an outline of the general method: given an integer $n \neq 4^k(8m+7)$, we divide n by 4 as many times as possible to obtain $n_1 \not\equiv 0 \pmod 4$. We then find a positive integer b such that $-b$ is a quadratic residue modulo $bn - 1$ using the same method as in the proof. This allows us to obtain a positive definite integral ternary quadratic form f of determinant 1, which is therefore equivalent to a sum of three squares, and with f representing n_1 as

$f(0,0,1) = n_1$ (from the proof again). We then find the matrix, $M = (m_{ij})$, which transforms $x_1^2 + x_2^2 + x_3^2$ into f; then (as in Proposition 3) we have that $n_1 = m_{13}^2 + m_{23}^2 + m_{33}^2$ and then we can easily express n as a sum of three squares. However, finding such a matrix M is not a simple task, we refer to [7, pp. 49–51] for some detailed examples.

To end this section, we look at two results which follow from the three-square theorem. The first is a result commonly known as the Eureka theorem, after Gauss famously wrote in his diary EΥΡΗΚΑ! num $= \Delta + \Delta + \Delta$ after finding a proof that every positive integer is a sum of three triangular numbers [18, p. 7]. The second is the celebrated four-square theorem by Lagrange, which can of course also be proved without the three-square theorem.

Theorem 21 (Gauss)**.** *Every positive integer n can be expressed as the sum of three triangular numbers.*

Proof. [7, pp. 25–26]. By the three-square theorem, given $n > 0$, we know that we can write

$$8n + 3 = x^2 + y^2 + z^2$$

for non-negative integers x, y, and z. Then considering this equation modulo 8 gives $x^2 + y^2 + z^2 \equiv 3 \pmod 8$, and since squares are congruent to $0, 1$, or $4 \pmod 8$, we must have that $x^2 \equiv y^2 \equiv z^2 \equiv 1 \pmod 8$, so x, y, and z are all odd. Hence there exist integers $r, s, t \geqslant 0$ such that

$$x = 2r + 1, \qquad y = 2s + 1, \qquad z = 2t + 1.$$

Now simply substituting in these values for x, y, and z gives:

$$\begin{aligned} 8n + 3 &= (2r + 1)^2 + (2s + 1)^2 + (2t + 1)^2 \\ &= 4r(r + 1) + 4s(s + 1) + 4t(t + 1) + 3. \end{aligned}$$

Then by subtracting 3 from each side and subsequently dividing by 8 on each side we have:

$$n = \frac{r(r+1)}{2} + \frac{s(s+1)}{2} + \frac{t(t+1)}{2}.$$

So n is the sum of three triangular numbers. □

Theorem 22 (Lagrange's Four-Square Theorem)**.** *Every positive integer n can be expressed as a sum of four squares.*

Proof. Based on [11, p. 164]. If n is not of the form $4^k(8m + 7)$ then we know that we can write n as a sum of three squares and simply appending 0^2 gives n as a sum of four squares, so suppose n is of the form $4^k(8m + 7)$. We have that

$$n = 4^k(8m + 7) = 4^k(8m + 6) + (2^k)^2.$$

Then, by the three-square theorem we can certainly write $4^k(8m+6) = x^2+y^2+z^2$ for integers x, y, and z, and simply setting $w = 2^k$ gives $n = x^2+y^2+z^2+w^2$, a sum of four squares. □

These two theorems form the first steps in the proof of *Fermat's polygonal number theorem*, an important result in additive number theory which states that ever positive integer can be written as a sum of n n-gonal numbers. The proof would require some more theory and can be found in [14].

It is also important to note that investigating representations of integers as sums of squares actually fits into a bigger picture: *Waring's problem*, concerning representations of integers as sums of squares and higher powers. The two, three and four-square theorems that we have proven here give a complete solution for the case of squares. For higher powers it is known, for example, that every positive integer can be written as the sum of nine cubes, or that every positive integer can be written as the sum of nineteen fourth powers! [14, p. 71]. Waring's problem is an active area of research (see [16] for a recent example of progress in this area), and alongside Goldbach's conjecture, one of the cornerstones of additive number theory.

References

[1] M. Bhargava and J. Hanke. Universal quadratic forms and the 290-theorem. Preprint, available at `http://math.stanford.edu/~vakil/files/290-Theorem-preprint.pdf` [Accessed 28 January 2018], 2005.

[2] D. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computation*. Springer-Verlag, New York, 1989.

[3] J. Conway and N. Sloane. *Sphere Packings, Lattices and Groups*, chapter 15. Springer-Verlag, New York, 1999.

[4] D. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. John Wiley & Sons, Hoboken, 2nd edition, 2013.

[5] L. Dickson. *History of the Theory of Numbers*, volume 2. Carnegie Institution of Washington, Washington, 1920.

[6] C. Gauss. *Disquisitiones Arithmeticae*. Yale University Press, 1965. Translated by A. Clarke. (Originally published in 1801).

[7] E. Grosswald. *Representations of Integers as Sums of Squares*. Springer-Verlag, New York, 1985.

[8] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, New York, 2nd edition, 1990.

[9] T. Koshy. *Elementary Number Theory with Applications.* Academic Press, 2nd edition, 2007.

[10] E. Landau. Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante. *Mathematische Annalen*, 56:671–676, 1903.

[11] E. Landau. *Elementary Number Theory.* Chelsea Publishing Company, New York, 2nd revised edition, 1998. Translated by J. Goodman. (Originally published in 1947).

[12] A. Legendre. *Essai sur la Théorie des Nombres.* Duprat, Paris, 1798.

[13] R. Mollin. *Algebraic Number Theory.* Chapman and Hall/CRC, 2nd edition, 2011.

[14] M. Nathanson. *Additive Number Theory: The Classical Bases.* Springer-Verlag, New York, 1996.

[15] J-P. Serre. *A Course in Arithmetic.* Springer-Verlag, New York, 1973.

[16] S. Siksek. Every integer greater than 454 is the sum of at most seven positive cubes. *Algebra & Number Theory*, 10(10):2093–2119, 2016.

[17] H. Stark. On the "gap" in a theorem of Heegner. *Journal of Number Theory*, 1(1):16–27, 1969.

[18] V. Varadarajan. *Algebra in Ancient and Modern Times.* American Mathematical Society, 1998.