ON A THEOREM OF LEGENDRE

W. DUKE

Abstract. It is shown that the primitive zeros of certain indefinite ternary quadratic forms fall into a single orbit under automorphs of the form. Zeros of the ternary form consisting of triples of Gaussian binary quadratic forms are characterized. The number of orbits of these triples under the extended modular group is determined.

1. Introduction

Let $a, b, c$ be integers such that $q = abc$ is nonzero and square-free. One of Legendre’s most elegant theorems states that nonzero $x = (x_1, x_2, x_3) \in \mathbb{Z}^3$ exists so that

\begin{equation}
ax_1^2 + bx_2^2 + cx_3^2 = 0
\end{equation}

if and only if $a, b, c$ are not all of the same sign and $-bc, -ac, -ab$ are quadratic residues modulo $|a|, |b|, |c|$, respectively. The necessity of these solvability conditions is easy to show, while their sufficiency follows from the Hasse principle (see e.g. [32, p. 343]), which applies more generally to

\begin{equation}
S(x) := xSx^t = x\begin{pmatrix} a & d & f \\ d & b & e \\ f & e & c \end{pmatrix} x^t = ax_1^2 + bx_2^2 + cx_3^2 + 2dx_1x_2 + 2ex_2x_3 + 2fx_1x_3 = 0,
\end{equation}

with fixed integers $a, b, c, d, e, f$ such that $q := \text{det} S \neq 0$. Hasse’s principle implies that $S$ is isotropic, that is (1.2) has non-zero integral solutions, if and only if it is nontrivially solvable over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes $p$.

For indefinite $S(x)$ when one non-zero integral solution to (1.2) exists so do infinitely many primitive ones, where a solution $x$ is primitive if it is nonzero and

\[ \gcd(x) := \gcd(x_1, x_2, x_3) = 1. \]

The group $G$ of automorphs of $S$, which consists of those $A \in \text{GL}(3, \mathbb{Z})$ such that $S[A] = S$, acts on such solutions by $x \mapsto Ax^t$ and splits them into finitely many classes. Similarly, the subgroup $G^+ := G \cap \text{SL}(3, \mathbb{Z})$ splits them into finitely many proper classes.

Siegel’s main theorem applied to ternary forms gives a quantitative form of the Hasse principle for the non-homogeneous quadratic equation

\[ S(x) = n \]

when $-qn$ is not a square. In this situation rational solvability is not equivalent to integral solvability. For $S$ in a genus with one class Siegel’s theorem [27] yields a formula that counts the number of $G$-classes of solutions (these are still preserved) as a product of local densities. Each class in the count is weighted by a measure of the size of the subgroup of $G$ that fixes a solution contained in the class. A classical theorem of Meyer [22] shows that the genus of

$^1$Smith [30] gave explicit congruence conditions for $S$ to be isotropic that generalize those of Legendre.

$^2$Siegel’s theorem in the general ternary case gives a formula for a certain average of the number of weighted classes, where the averaging is over the genus. Kneser [19] refined Siegel’s theorem by employing the spinor genus, which is especially useful when dealing with definite ternary forms (c.f. [8]).
S contains only one class if \( q \) is square-free. For example, when applied to
\[
S(x) = 2x_1x_3 - 2x_2^2 = n,
\]
for which \( q = 2 \), Siegel’s formula yields Dirichlet’s class number formula for binary quadratic forms (see [28, p.114]).

However, Siegel’s formula from [27] does not pertain to the homogeneous equation (1.2) (see [28, p.108]). The main purpose of this paper is to show that a result like Siegel’s still holds for (1.2) and that the (proper) class number is one when non-trivial solutions exist, at least if we assume that \( q \) is odd and square-free.

**Theorem 1.** Suppose that \( S(x) \) given in (1.2) is isotropic and has an odd square-free determinant \( q \). Then all primitive integral solutions to (1.2) are equivalent under \( G^+ \).

It is important that the transformations of \( G^+ \) are integral and not simply rational. Surprisingly, the one-orbit conclusion of Theorem 1 appears to be well-known only for a few specific equations, in particular the Pythagorean
\[
x_1^2 - x_2^2 - x_3^2 = 0,
\]
where it goes back at least to 1934 [1]. For a discussion of the explicit “descent” proofs in this case and further references see [3]. The method behind the proof of Theorem 1 in this special case is also made explicit in an example near the end of §4.

Besides Legendre’s equation, another interesting special case of (1.2) is
\[
(1.3) \quad f(x_1, x_2) = x_3^2,
\]
where \( f \) is the (Gaussian) binary quadratic form
\[
f(x_1, x_2) = (a, b, c) = ax_1^2 + 2bx_1x_2 + cx_2^2.
\]
Suppose that \( f \) has non-square determinant \( q = b^2 - ac \) and is properly primitive, meaning that \( \gcd(a, 2b, c) = 1 \). When applied to (1.3), Smith’s congruence conditions for (1.2) to be nontrivially solvable, or Legendre’s if \( b = 0 \), amount to those of Gauss for \( f \) to belong to the principal genus of properly primitive forms of determinant \( q \). Such a form will properly represent squares. Gauss’s theorem on duplication gives more information; under these conditions \( f \) arises as the composition with itself of another properly primitive form \( f_3(x, y) = (a_3, b_3, c_3) \) of determinant \( q \). This means that
\[
f_3^2(x_1, x_2) = f(f_1(x_1, x_2), f_2(x_1, x_2))
\]
for two other binary quadratic forms \( f_1 \) and \( f_2 \). It follows that \( f \) represents the squares of the numbers represented by \( f_3 \). A formula for the number of \( \text{SL}(2, \mathbb{Z}) \)-classes of such forms \( f_3 \) follows from the genus theory of [11].

It is therefore natural to consider the solvability of the more general (1.2) in triples
\[
F = (f_1, f_2, f_3)
\]
of integral binary quadratic forms \( f_j = (a_j, b_j, c_j) \) for \( j = 1, 2, 3 \). Say a triple \( F \) is primitive if the values \( \gcd(a_j, b_j, c_j) \) for \( j = 1, 2, 3 \) are relatively prime in pairs. Let \( g = (\alpha, \beta, \gamma, \delta) \in \text{GL}(2, \mathbb{Z}) \) act on \( f = (a, b, c) = au_1^2 + 2bu_1u_2 + cu_2^2 \) by
\[
(1.4) \quad f|g(u) = f(\alpha u_1 + \beta u_2, \gamma u_1 + \delta u_2)
\]
and on a triple \( F = (f_1, f_2, f_3) \) by
\[
F|g = (f_1|g, f_2|g, f_3|g).
\]
Clearly if $S(F) = 0$ then $S(F | g) = 0$ for $g \in \text{GL}(2, \mathbb{Z})$. Also if $F$ is primitive so is $F | g$. Let $\nu(q)$ denote the number of distinct prime divisors of $q$.

**Theorem 2.** Primitive Gaussian triples $F = (f_1, f_2, f_3)$ exist that satisfy $S(F) = 0$ identically if and only if $S$ is isotropic. If $S$ has an odd square-free determinant $q$ these triples, when any exist, fall into

$$H = 2^{\nu(q)+2}$$

orbits under the action of $\text{GL}(2, \mathbb{Z})$.

In the case of Legendre’s equation (1.1) this result is due to Georg Cantor in his little-known 1867 dissertation [2].

Binary quadratic forms (positive if definite) may be represented by special points or hyperbolic geodesics in the upper half-plane

$$\mathcal{H} = \{ z \in \mathbb{C}; \text{Im } z > 0 \}.$$ 

Solvability of Legendre’s equation has the following geometric formulation.

**Proposition 1.** Let $a, b, c$ be integers that are relatively prime in pairs with $a, c > 0$ and $b < 0$. Then the following two statements are equivalent. There exists a pair of geodesics in $\mathcal{H}$, each having endpoints that are Galois conjugates in the real quadratic fields $\mathbb{Q}(\sqrt{|ab|})$ and $\mathbb{Q}(\sqrt{|bc|})$, respectively, which are such that the geodesics intersect at right angles at a point in the imaginary quadratic field $\mathbb{Q}(i \sqrt{|ac|})$. The numbers $-bc, -ac, -ab$ are quadratic residues modulo $|a|, |b|, |c|$, respectively.

![Figure 1](https://via.placeholder.com/150)

**Figure 1.** A pair of geodesics associated to $(7, -15, 23)$.

**Example.** Gauss illustrated his proof of Legendre’s theorem with the example [11, p. 346]

$$7x_1^2 - 15x_2^2 + 23x_3^2 = 0.$$ 

Here

$$-7 \cdot 23 \equiv 2^2 \pmod{15}, \quad 15 \cdot 23 \equiv 3^2 \pmod{7}, \quad 15 \cdot 7 \equiv 6^2 \pmod{23}$$

gives rise to the solution $(3, 7, 6)$. Figure 1 illustrates two orthogonal geodesics with endpoints at

$$\frac{1}{4} \left(\pm \sqrt{15 \cdot 7} - 9\right) \quad \text{and} \quad \frac{1}{11} \left(\pm \sqrt{15 \cdot 23} + 9\right)$$

that intersect at the point $\frac{1}{6} \left(-1 + \sqrt{-23 \cdot 7}\right) \in \mathcal{H}$. 

2. Triples of binary quadratic forms

When they exist, all nonzero rational solution to (1.2) can be obtained by evaluating a single triple of binary quadratic forms at rational points. This has been known for a long time. However, Cantor [2] pointed out that in order to get primitive integral solutions we need to control the common denominator, which is not automatic. Similar remarks were made by Dickson [4]. Such control is needed to make analytic use of the parameterization to count primitive integral solutions. One way to overcome this difficulty is to use a finite number of triples, as was done for (1.3) using genus theory. This makes it possible to impose the condition \( \gcd(x) = 1 \) upon an integer solution to (1.2) by requiring that the variables of the parameterizing quadratic forms lie in certain arithmetic progressions, which is an analytically friendly process. In this section I will review the general parameterization given by Hooley [15], which makes use of the arithmetic invariant theory of triples of binary quadratic forms.3

This parameterization will be used in the proofs of Theorems 1 and 2.

For a pair of (Gaussian) binary quadratic forms \( f_j = (a_j, b_j, c_j) \) with integers \( a_j, b_j, c_j \) for \( j = 1, 2 \), define the bilinear form

\[
\langle f_1, f_2 \rangle = b_1 b_2 - \frac{1}{2}(a_1 c_2 + a_2 c_1).
\]

We have that \( \langle f_1|g, f_2|g \rangle = \langle f_1, f_2 \rangle \) where \( g = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \text{GL}(2, \mathbb{Z}) \) acts as in (1.4). In particular, \( \langle f, f \rangle = b^2 - ac \), called by Gauss the determinant of \( f = (a, b, c) \), is an invariant.

Define the discriminant matrix of \( F \) by

\[
disc(F) = \begin{pmatrix} \langle f_1, f_1 \rangle & \langle f_1, f_2 \rangle & \langle f_1, f_3 \rangle \\ \langle f_2, f_1 \rangle & \langle f_2, f_2 \rangle & \langle f_2, f_3 \rangle \\ \langle f_3, f_1 \rangle & \langle f_3, f_2 \rangle & \langle f_3, f_3 \rangle \end{pmatrix},
\]

which is a symmetric matrix with integral diagonal and half-integral off-diagonal entries. The set of all primitive \( F \) with a fixed \( disc(F) \) is preserved \( \text{GL}(2, \mathbb{Z}) \). Assuming that \( disc(F) \) is non-singular, this set splits into finitely many classes under this action (see [15, p.474]).

For any \( 3 \times 3 \) matrix \( A \) the adjoint is defined by

\[
A^* = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}^* = \begin{pmatrix} ce-fi & fg-di & dh-ce \\ ch-bi & ai-cg & bg-ah \\ bf-ec & cd-af & ae-bd \end{pmatrix}.
\]

The following is from [15]4

**Proposition 2.** Suppose that \( S(x) \) is isotropic. The general primitive solution of \( S(x) = 0 \) is given by

\[
x = (f_1(u), f_2(u), f_3(u))
\]

where \( F = (f_1, f_2, f_3) \) runs through a full set of \( \text{GL}(2, \mathbb{Z}) \)-representatives of triples with discriminant form

\[
disc(F) = -S^*
\]

and where \( u = (u_1, u_2) \) is restricted so that \( \gcd(x) = 1 \). Each solution is obtained exactly twice through \( \pm u \).

The fact that \( S(f_1(u), f_2(u), f_3(u)) = 0 \) when \( disc(F) = -S^* \) is a syzygy and can be verified through a direct calculation. The converse, that all solutions arise this way, is deeper and requires the more intricate proof given in detail in [15].

---

3The invariant theory of such triples over \( \mathbb{C} \) can be found in Hilbert’s lectures [14, Lecture XLIII, p.155] and also in [26].

4The statement of Theorem 1 of [15] needs a correction; \( A, B, C, 2F, 2G \) and \( 2H \) should be replaced by their negatives.
In order to apply the parameterization of Proposition 2 quantitatively we need to be able to restrict \( u = (u_1, u_2) \) so that \( \gcd(x) = 1 \). The following lemma shows that the only primes that can divide \( \gcd(x) \) must also divide \( 2 \det S \).

**Lemma 1.** Given a triple \( F = (f_1, f_2, f_3) \) with \( \text{disc}(F) = -S^* \) and a prime \( p \) where \( f_1, f_2, f_3 \) share a non-trivial common zero in \((\mathbb{Z}/p\mathbb{Z})^2\) we must have that \( p|\det S \).

**Proof.** The resultant of \( f_1 \) and \( f_2 \) is given by

\[
\text{result}(f_1, f_2) = (a_1 c_2)^2 - 4(a_1 b_2)(b_1 c_2) = 4(f_1, f_2)^2 - 4\langle f_1, f_1 \rangle \langle f_2, f_2 \rangle,
\]

where we are using the convenient notation from [26]:

\[
(a, b) = a_ib_j - a_jb_i.
\]

Now \( (f_1, f_2)^2 - \langle f_1, f_1 \rangle \langle f_2, f_2 \rangle = D_{3,3} \) is a principal minor of the discriminant matrix \( \text{disc}(F) \). Thus for a prime \( p > 2 \), if \( p|f_1(u) \) and \( p|f_2(u) \) for \( \gcd(u) = 1 \) then \( p|D_{3,3} \). Thus if \( f_1, f_2, f_3 \) share a non-trivial common zero in \((\mathbb{Z}/p\mathbb{Z})^2\) we must have that \( p|\det(\text{disc } F) \) and

\[
\det S^* = (\det S)^2.
\]

\[\square\]

I turn now to the geometric interpretation of triples of binary quadratic forms and give a proof of Proposition 1. Associated to a binary quadratic form \((a, b, c)\) with \( b^2 - ac > 0 \) is the hyperbolic geodesic in the upper half-plane \( \mathcal{H} \) with endpoints at the roots of \( ax^2 + 2bx + c = 0 \) (including \( i\infty \) when \( a = 0 \)). The geodesic comes with an orientation. If \( b^2 - ac < 0 \) there is a CM point \( z \in \mathcal{H} \), which is a root of \( az^2 + 2z + c = 0 \). Distances or angles between corresponding geodesics or points are determined by the entries in disc \( F \) and the values of \( \gcd(a_j, 2b_j, c_j) \).

For example, if \( f_1 \) and \( f_2 \) are both properly primitive (meaning that \( \gcd(a_j, 2b_j, c_j) = 1 \) for \( j = 1, 2 \)) and correspond to intersecting geodesics then the angle of intersection is given by \( \theta \) where

\[
\cos \theta = \frac{\langle f_1, f_2 \rangle}{\sqrt{|\langle f_1, f_1 \rangle \langle f_2, f_2 \rangle|}}.
\]

For two nonsingular indefinite binary quadratic forms \( f_1 \) and \( f_2 \), we have that \( \langle f_1, f_2 \rangle = 0 \) if and only if the associated geodesics are orthogonal. For \( f_1 \) nonsingular and indefinite and \( f_2 \) positive definite \( \langle f_1, f_2 \rangle = 0 \) if and only if the CM point associated to \( f_2 \) lies on the geodesic associated to \( f_1 \). Therefore triples with a diagonal discriminant form have an especially simple geometric interpretation.

**Proof of Proposition 1.** The “if” part of the statement is clear from Legendre’s theorem, the discussion above and Proposition 2, since the parameterizing \( F \) satisfies

\[
\text{disc}(F) = \left( \begin{array}{ccc} -bc & 0 & 0 \\ 0 & -ac & 0 \\ 0 & 0 & -ab \end{array} \right) = - \left( \begin{array}{ccc} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{array} \right)^*.
\]

For the converse we need to observe that the assumed existence of the geodesics implies that there is an \( F \) with

\[
\text{disc}(F) = \left( \begin{array}{ccc} -\ell_1^2bc & 0 & 0 \\ 0 & -\ell_2ac & 0 \\ 0 & 0 & -\ell_3ab \end{array} \right),
\]

for some positive integers \( \ell_1, \ell_2, \ell_3 \). Then

\[
\text{disc}(\ell_1\ell_2\ell_3 F) = -S_1^*,
\]

where

\[
S_1 = \left( \begin{array}{ccc} \ell_1^2\ell_3a & 0 & 0 \\ 0 & \ell_2^2\ell_3b & 0 \\ 0 & 0 & \ell_1^2\ell_2c \end{array} \right).
\]
By Proposition 2 there exist integers \((x_1, x_2, x_3)\) not all zero with
\[ a(\ell_2\ell_3 x_1)^2 + b(\ell_1\ell_3 x_2)^2 + c(\ell_1\ell_2 x_3)^2 = 0. \]

\[\square\]

3. The class number of triples

In this section I will prove Theorem 2. First I give a simplification.

**Proposition 3.** Any two isotropic \(S\) in (1.2) with the same odd square-free determinant \(q\) are equivalent under \(\text{SL}(3, \mathbb{Z})\). In particular, for any such \(S\) there exists \(A \in \text{SL}(3, \mathbb{Z})\) so that

\[
S[A] := A^t SA = Q = \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & -q & 0 \\ 0 & 0 & -1 \end{array} \right).
\]

**Proof.** This follows by an extension of the standard reduction method taken further by using the assumptions on \(S\) and \(q\). Since \(S\) represents zero, there exists \(B \in \text{SL}(3, \mathbb{Z})\) so that

\[
S[B] = S_1 = \left( \begin{array}{ccc} b_1 & b_2 & 0 \\ b_1 a & b & 0 \\ b_2 & b & c \end{array} \right),
\]

where

\[
q = 2b_1 b_2 - a b_2^2 - c b_1^2.
\]

Since \(q\) is square-free there exist \(u, v \in \mathbb{Z}\) so that \(ub_1 + vb_2 = 1\). Then

\[
C = \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & b & u \\ 0 & -b_1 & v \end{array} \right) \in \text{SL}(3, \mathbb{Z})
\]

and

\[
S_2 = S_1[C] = \left( \begin{array}{ccc} 0 & 0 & 1 \\ 0 & -q & c_1 \\ 1 & c_1 & c_2 \end{array} \right),
\]

where

\[
c_1 = ab_2 u - b_1 c v - b + 2bb_2 v \quad \text{and} \quad c_2 = au^2 + cv^2 + 2buv.
\]

There are two cases. If \(au^2 + cv^2\) is odd choose

\[
D = \left( \begin{array}{ccc} 1 & -c_1 & d_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \in \text{SL}(3, \mathbb{Z})
\]

where

\[
d_2 = -buv - \frac{1}{2}(1 + au^2 + cv^2) \in \mathbb{Z}.
\]

Thus,

\[
S_3 = S[BCD] = S_2[D] = \left( \begin{array}{ccc} 0 & 0 & 1 \\ 0 & -q & 1 \\ 1 & 0 & -1 \end{array} \right).
\]

Since \(q\) is odd from (3.2) we know that \(ab_2^2 + cb_1^2\) is odd. If \(au^2 + cv^2\) is even choose

\[
D = \left( \begin{array}{ccc} 1 & d_1 & d_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \in \text{SL}(3, \mathbb{Z})
\]

where now

\[
d_1 = -c_1 - ab_2^2 - cb_1^2 \quad \text{and} \quad d_2 = (b + bb_1 b_2 - ab_2 u - 2bb_2 v + cb_1 v - buv) - \frac{1}{2}(1 + ab_2^2 + cb_1^2 + au^2 + cv^2) \in \mathbb{Z},
\]

and again a calculation shows that we have (3.3). Finally, since \(Q = S_3[E]\) where

\[
E = \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right),
\]

we have \(Q = S[A]\) for \(A = BCDE\). 

\[\square\]
In view of Proposition 3, Theorem 2 follows from the dissertation of Cantor, which implies it in the case of the Legendre equation. However, we now give an independent proof.

**Proof of Theorem 2.** The first statement follows from Proposition 2. If \( S(x) \) is isotropic and has odd square-free determinant, by Proposition 3 we may assume that \( S = Q \) from (3.1). Write \( q = q_1 q_2 \) with \( q_1, q_2 \in \mathbb{Z}^+ \). Clearly \( \gcd(q_1, q_2) = 1 \). Let \( F = \pm (f_1, f_2, f_3) \) when either

\[
(3.4) \quad f_1(u) = q_1 u_1^2 + q_2 u_2^2, \quad f_2(u) = 2 u_1 u_2 \quad \text{and} \quad f_3(u) = q_1 u_1^2 - q_2 u_2^2 \quad \text{or}
\]

\[
(3.5) \quad f_1(u) = \frac{1}{2} (q_1 + q_2) u_1^2 + (q_1 - q_2) u_1 u_2 + \frac{1}{2} (q_1 + q_2) u_2^2, \quad \quad f_2(u) = u_1^2 - u_2^2 \quad \text{and} \quad \quad f_3(u) = \frac{1}{2} (q_1 - q_2) u_1^2 + (q_1 + q_2) u_1 u_2 + \frac{1}{2} (q_1 - q_2) u_2^2.
\]

In either case \( F \) is primitive and

\[
(3.6) \quad \text{disc}(F) = \left( \begin{smallmatrix} -q & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & q \end{smallmatrix} \right) = \left( \begin{smallmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{smallmatrix} \right)^* = -Q^*.
\]

Also we have that

\[
f_1^2(u) - q f_2^2(u) - f_3^2(u) = 0.
\]

By Proposition 2 the proof is finished if we show that each triple \( F' \) with \( \text{disc}(F') = -Q^* \) is equivalent to a unique \( \pm (f_1, f_2, f_3) \) with \( f_1, f_2, f_3 \) given in (3.4) or (3.5) for some decomposition \( q = q_1 q_2 \). It follows from [11, Art 206–210] that any form \((a, b, c)\) that satisfies \( b^2 - ac = 1 \) is (properly or improperly) equivalent to exactly one of \((0, 1, 0)\) or \((1, 1, 0)\). Therefore, after making an obvious change of variables in \((1, 1, 0)\) we may assume that

\[
f_2(u) = \pm 2 u_1 u_2 \quad \text{or} \quad f_2(u) = \pm (u_1^2 - u_2^2).
\]

A straightforward argument shows that there is a unique (ordered) decomposition \( q = q_1 q_2 \) so that either \( f_1 \) and \( f_3 \) or \(-f_1\) and \(-f_3\) are given in the corresponding choice of (3.4) or (3.5). This completes the proof of Theorem 2. \( \square \)

Later we will need to impose that condition that

\[
\gcd(f_1(u), f_2(u), f_3(u)) = 1
\]

for a triple \( F = (f_1, f_2, f_3) \) with \( \text{disc}(F) = -Q^* \). As previously mentioned, this can be done by restricting the parameterizing variables \( u \) with \( \gcd(u) = 1 \) to suitable arithmetic progressions modulo \( 2q \). For a prime \( p \) and such a triple \( F \) let

\[
B_F(p) = \{ u \in (\mathbb{Z}/p\mathbb{Z})^2; f_1(u) \equiv f_2(u) \equiv f_3(u) \equiv 0 \pmod{p} \}.
\]

By Lemma 1 we have that \( B_F(p) = 1 \) unless \( p | 2q \). Define \( R_F \) to be the set of all \( r \in (\mathbb{Z}/2q\mathbb{Z})^2 \) which, when reduced modulo \( p \), are not in \( B_F(p) \) for any \( p | 2q \). The following lemma shows that \( \#R_F \) is independent of the class of \( F \) and is non-zero.

**Lemma 2.** Given a triple \( F = (f_1, f_2, f_3) \) with \( \text{disc}(F) = -Q^* \) we have

\[
\#R_F = 2q \prod_{p | q} (p - 1).
\]

**Proof.** Given a prime \( p | 2q \) we claim that \( f_1, f_2, f_3 \) share exactly \( p \) common zeros in \((\mathbb{Z}/p\mathbb{Z})^2\), including \((0, 0)\). Suppose first that \( p > 2 \). By (3.6) if \( p | q \) we see that \( f_1(u_1, 1) \) and \( f_3(u_1, 1) \) each have a double root modulo \( p \). Using resultants from the proof of Lemma 1, we also have that each pair of \( f_j(u_1, 1) \) share a root modulo \( p \) so the result follows. A similar analysis works for \( p = 2 \). The claim may also be checked directly using the particular triples from (3.4) and (3.5). The result of the lemma now follows by the Chinese remainder theorem. \( \square \)
4. THE ASSOCIATED FUCHSIAN GROUP

I now turn to the proof of Theorem 1. By Proposition 3 we may assume that \( S = Q \) from (3.1). We may also assume that \( q > 0 \). We make use of a Fuchsian group \( \Gamma = \Gamma_Q \subset \text{PSL}(2, \mathbb{R}) \) that arises by a construction of Fricke-Klein [10]. Other useful references for this section are [20], [21] and [25].

Let \( O \) be the connected component of the identity of the special orthogonal group

\[
\{ C \in \text{SL}(3, \mathbb{R}); \; Q[C] := C'QC = Q \}.
\]

Then \( \Gamma \) is isomorphic to \( G_0 = G^+ \cap O \), where again

\[
G^+ = \{ A \in \text{SL}(3, \mathbb{Z}); \; Q[A] = Q \}.
\]

The matrix representatives of \( \Gamma \) are explicitly given in [10]. We will make use of their characterization and show that the conjugacy classes of primitive parabolic elements of \( \Gamma \) correspond to the \( G_0 \)-classes of primitive solutions to \( Q(x) = 0 \). This correspondence reduces the proof of Theorem 1 to showing that \( \Gamma \backslash \mathcal{H} \) has only one cusp.

Let

\[
S_0 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}
\]

and for \( g = \pm \left( \begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix} \right) \) let

\[
A_g = \begin{pmatrix} \alpha^2 & 2\alpha\beta & \beta^2 \\ \alpha\gamma & \alpha\delta + \beta\gamma & \beta\delta \\ \gamma^2 & 2\gamma\delta & \delta^2 \end{pmatrix}.
\]

We have that \( \det A_g = (\det g)^3 \) and \( \text{tr} A_g = (\text{tr} g)^2 - \det g \). Also, for \( g, h \in \text{PSL}(2, \mathbb{R}) \)

\[
A_{gh} = A_gA_h \quad \text{and} \quad S_0[A_g] = S_0.
\]

Let

\[
B_0 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}.
\]

Then \( S_0[B_0] = Q \) and for

\[
C_g = B_0^{-1}A_gB_0 = \begin{pmatrix} \frac{1}{2}(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) & \sqrt{\gamma}(\alpha\beta + \gamma\delta) & \frac{1}{2}(\alpha^2 - \beta^2 + \gamma^2 - \delta^2) \\ \sqrt{\gamma}(\alpha\gamma + \beta\delta) & \alpha\delta + \beta\gamma & \sqrt{\gamma}(\alpha\beta - \gamma\delta) \\ \frac{1}{2}(\alpha^2 + \beta^2 + \gamma^2 - \delta^2) & \sqrt{\gamma}(\alpha\gamma - \beta\delta) & \frac{1}{2}(\alpha^2 - \beta^2 - \gamma^2 + \delta^2) \end{pmatrix}
\]

we have that \( \det C_g = (\det g)^3 \) and \( \text{tr} C_g = (\text{tr} g)^2 - \det g \) as well as

\[
C_{gh} = C_gC_h \quad \text{and} \quad Q[C_g] = Q
\]

for \( g, h \in \text{PSL}(2, \mathbb{R}) \).

The map \( g \mapsto C_g \) gives a Lie group isomorphism from \( \text{PSL}(2, \mathbb{R}) \) to \( O \). Define

\[
\Gamma = \Gamma_Q = \{ g \in \text{PSL}(2, \mathbb{R}); \; C_g \in \text{Mat}_3(\mathbb{Z}) \}.
\]

Clearly \( \Gamma \) is isomorphic to \( G_0 \) through \( g \mapsto C_g \). As was shown in [10], \( \Gamma \) is Fuchsian of the first kind acting on \( \mathcal{H} \). Also, \( \Gamma \) has cusps if and only if \( Q \) is isotropic.

It is shown in [10, I p.537] that every element \( g \in \Gamma \) has one of the forms

\[
g_1 = g_1(n) = \pm \frac{1}{2} \left( \frac{(n_0+n_2)\sqrt{\eta}}{(n_0-n_2)\sqrt{\eta}} \frac{(n_1+n_3)\sqrt{\eta}}{(n_1-n_3)\sqrt{\eta}} \right) \quad g_2 = g_2(n) = \pm \frac{1}{2} \left( \frac{(n_0+n_2)\sqrt{\eta}}{(n_0-n_2)\sqrt{\eta}} \frac{(n_1+n_3)\sqrt{\eta}}{(n_1-n_3)\sqrt{\eta}} \right)
\]

with \( q = q_1q_2 \) and \( n = (n_1, n_2, n_3, n_4) \in \mathbb{Z}^4 \) such that \( \det g_j = 1 \) for \( j = 1, 2 \). In \( g_1 \) we also require that

\[
n_0 \equiv n_1 \equiv n_1 \equiv n_3 (\mod 2).
\]
Note that
\[(4.5) \quad (\text{tr} \, g_1)^2 = \frac{1}{4} n_0^2 q_1 \quad \text{and} \quad (\text{tr} \, g_2)^2 = \frac{1}{4} n_0^2 q_1.\]
The set of \(g_1\) with \(q_1 = 1\) comprise a distinguished subgroup \(\Gamma_0:\)
\[(4.6) \quad g = g(n) = \pm \frac{1}{2} \left( \begin{array}{cc} n_0 + n_2 & (n_1 + n_3)\sqrt{q} \\ (n_1 - n_3)\sqrt{q} & n_0 - n_2 \end{array} \right),\]
where (4.4) holds and
\[n_0^2 - qn_1^2 - n_2^2 + qn_3^2 = 4.\]

**Proposition 4.** Suppose that \(q\) is a positive odd square-free integer. Then there is a bijection between the \(G_0\)-classes of primitive solutions \(m \in \mathbb{Z}^3\) to \(Q(m) = 0\) and conjugacy classes of primitive parabolic elements in \(\Gamma\).

**Proof.** It is easy to check using (4.5) that \(g \in \Gamma\) is parabolic if and only if \(g = g(n) \in \Gamma_0\) where \(n = (\pm 2, m_1, m_2, m_3)\) satisfies
\[-qm_1^2 - m_2^2 + qm_3^2 = 0.\]
Now since all of these \(m_j\) must be even by (4.4), we can characterize the parabolic elements of \(\Gamma\) to be those of the form
\[(4.7) \quad h(m) = \pm \left( \begin{array}{cc} 1-qm_2 & (m_1+m_3)\sqrt{q} \\ (-m_1+m_3)\sqrt{q} & 1+qm_2 \end{array} \right),\]
where \(m = (m_1, m_2, m_3) \in \mathbb{Z}^3\) is not zero and \(Q(m) = 0\). The primitive parabolics will be those with \(\gcd(m) = 1\). A computation shows that for \(g \in \Gamma\) and \(C_g\) from (4.2) we have
\[gh(m)g^{-1} = h(C_gm'),\]
and this establishes the correspondence. \(\square\)

**Example.** In the Pythagorean triple case where \(q = 1\), the group \(\Gamma\) was determined by Gauss and Schering [12, p.311.]. It is generated by
\[g = \pm \left( \begin{array}{cc} 1 & -2 \\ 0 & 1 \end{array} \right), \quad g' = \pm \frac{1}{\sqrt{2}} \left( \begin{array}{cc} 1 & -3 \\ 1 & 1 \end{array} \right), \quad g'' = \pm \frac{1}{\sqrt{2}} \left( \begin{array}{cc} 1 & -1 \\ 1 & 1 \end{array} \right),\]
which have orders \(\infty, 2\) and 4, respectively, and satisfy the Fuchsian relation
\[gg'g'' = \pm \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right).\]
Their images in \(G_0\) are
\[
\left( \begin{array}{cc} 3 & -2 & -2 \\ -2 & 1 & -1 \\ 2 & -1 & 1 \end{array} \right), \quad \left( \begin{array}{cc} 3 & -2 & -2 \\ 2 & -1 & 1 \\ 2 & -1 & -1 \end{array} \right), \quad \left( \begin{array}{cc} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{array} \right).
\]
Since \(\Gamma \backslash \mathcal{H}\) has only one cusp we see that, up to sign changes, these matrices will produce all Pythagorean triples from \((1,1,0),\) say.

**Remark.** It should be possible, using the methods of [20], to show that \(\Gamma\) has only one cusp by relating it to the normalizer of \(\Gamma_0\) in \(\text{PSL}(2, \mathbb{R})\), where \(\Gamma_0\) was defined in (4.6). However, in this paper we proceed by an analytic method that combines the results of Proposition 2 and Theorem 2 with basic properties of Eisenstein series and Epstein zeta functions. This approach has the advantage of relating the result of Theorem 1 directly to the problem of asymptotically counting solutions to \(S(x) = 0\) with a norm constraint on the size of \(x\). For more on this see the Remarks at the end of the paper.
5. A VOLUME COMPUTATION

Next we will compute \( \text{vol}(\Gamma_Q \backslash \mathcal{H}) \) for \( Q \) in (3.1) with \( q \) odd and square-free. For this we apply Siegel’s main theorem, which expresses the covolume of the group of automorphs of an indefinite integral ternary quadratic form, whose genus consists of a single class, as a product of local densities. In [28, Lecture 15] Siegel explains this purely arithmetic means of calculating the covolume. He uses \( G \) and does the volume computation in the Cayley-Klein projective model of the hyperbolic plane. This translates directly to the more usual Poincaré model using the upper half-plane \( \mathcal{H} \) with the invariant measure

\[
d\mu = \frac{dx
d y}{y^2}
\]

and the covolume of \( \Gamma \) is twice that computed by Siegel for \( G \).

By Proposition 3 and the Hasse principle (or Meyer’s theorem), the genus of \( Q \) contains a single class. Together with the local density calculations given in [23]\(^5\), Siegel’s result implies that the covolume of \( \Gamma \) is

\[
\text{vol}(\Gamma \backslash \mathcal{H}) = \pi \alpha_2^{-1} \prod_{p|q} \frac{1}{2}(p + 1).
\]

Here \( \alpha_2 \) is the local density at 2, which is more difficult to compute in general but is given in [23]. For odd \( q \) it is simpler and may be expressed in terms of the Hasse invariant \( c_2(Q) \) as

\[
\alpha_2 = \frac{6}{2 + c_2(Q)}.
\]

Using [18, p.36] we have \( c_2(Q) = 1 \) so \( \alpha_2 = 2 \). Thus we have

**Proposition 5.** Let \( q \) be square-free and odd and \( Q \) be given in (3.1). Then for \( \Gamma_Q \) from (4.3) we have that

\[
\text{vol}(\Gamma \backslash \mathcal{H}) = \pi \prod_{p|q} \frac{p+1}{2}.
\]

6. EISENSTEIN SERIES

In this section I will explicitly evaluate the sum of all the Eisenstein series for \( \Gamma \). For the spectral theory of Fuchsian groups consult the masterly treatment [17]. In the notation of [17], let \( a \) be a cusp for \( \Gamma \) and \( g_a \in \Gamma \) be a parabolic transformation of \( \Gamma \) that generates \( \Gamma_a \), the subgroup of \( \Gamma \) that fixes \( a \). Let \( \sigma_a \in \text{PSL}(2, \mathbb{R}) \) be a scaling matrix for \( a \) so that

\[
\sigma_a(i\infty) = a \quad \text{and} \quad \sigma_a^{-1}g_a\sigma_a = \pm \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right).
\]

The Eisenstein series for the cusp \( a \) is defined by

\[
E_a(z, s) = \sum_{g \in \Gamma_a \backslash \Gamma} (\text{Im} \ \sigma_a^{-1}gz)^s,
\]

convergent for \( \text{Re} \ s > 1 \). Each \( E_a(z, s) \) has a meromorphic continuation in \( s \) with a simple pole at \( s = 1 \) and

\[
\text{res}_{s=1} E_a(z, s) = \frac{1}{\text{vol}(\Gamma \backslash \mathcal{H})}.
\]

\(^5\)In [23] note the corrections: \( n_a - 1 \) in (23) should be \( n_a + 1 \) and in the formula for \( z_i \) below (47), the number 8 should be 3 and 4 should be 2.
Proposition 6. For $Q$ in (3.1) with $q$ odd and square-free we have the identity

\begin{equation}
\sum_a E_a(z, s) = \frac{1}{2} \left( \frac{\text{Im} z}{\sqrt{q}} \right)^{s} \sum_{m \in \mathbb{Z}^3 \atop Q(m) = 0}^* \left| (m_1 - m_3) |z|^2 - 2m_2 \sqrt{q} \text{Re}(z) + (m_1 + m_3) \right|^{-s},
\end{equation}

the first sum being over the inequivalent cusps of $\Gamma \backslash \mathcal{H}$ and where the star in the second sum indicates that we sum over $m = (m_1, m_2, m_3) \in \mathbb{Z}^3$ with $\gcd(m) = 1$.

Proof. As $g$ runs over $\Gamma_a \backslash \Gamma$ we have that $g^{-1} g a g$ runs over primitive parabolics in the $\Gamma$ conjugacy class of $g_a$. By the above (see around (4.7)) we get all such through

$$
\begin{align*}
g^{-1} g a g &= \pm \begin{pmatrix}
1 - m_2 q \\
-2m_2 \sqrt{q}
\end{pmatrix} \\
&\quad \times \begin{pmatrix}
(m_1 + m_3) \sqrt{q} \\
1 + m_2 q
\end{pmatrix},
\end{align*}
$$

where $m$ runs over $G_0$-association classes of solutions of $Q(m) = 0$ with $\gcd(m) = 1$ and one choice of $\pm m$ is made. This is done since changing the sign of $m$ amounts to taking the inverse of $g^{-1} g a g$.

We have

$$
\begin{align*}
g^{-1} g a g &= \pm \left( \sigma_a^{-1} g \right)^{-1} \begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},
\end{align*}
$$

If

$$
\sigma_a^{-1} g = \pm \begin{pmatrix}
a & b \\ c & d
\end{pmatrix}
$$

then

$$
\left( \sigma_a^{-1} g \right)^{-1} \begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm \begin{pmatrix}
1 + cd & d^2 \\
-c^2 & 1 - cd
\end{pmatrix},
$$

so a choice of $\pm m$ can be made so that we may take

$$
cd = -m_2 q, \quad c^2 = \sqrt{q}(m_1 - m_3) \quad \text{and} \quad d^2 = \sqrt{q}(m_1 + m_3).
$$

Since

$$
\text{Im}(\sigma_a^{-1} g z) = \frac{y}{|x + d|^2} = \frac{y}{c^2(x^2 + y^2) + 2cxd + d^2},
$$

comparison of (6.3) with (6.1) finishes the proof. 

For future reference set

\begin{equation}
\Phi(z, s) = \frac{1}{2} \left( \frac{\text{Im} z}{\sqrt{q}} \right)^{s} \sum_{m \in \mathbb{Z}^3 \atop Q(m) = 0}^* \left| (m_1 - m_3) |z|^2 - 2m_2 \sqrt{q} \text{Re}(z) + (m_1 + m_3) \right|^{-s}.
\end{equation}

Since the number of conjugacy classes of primitive parabolic elements in $\Gamma$ equals the number of inequivalent cusps of $\Gamma \backslash \mathcal{H}$, by Proposition 6 and (6.2) we have that

$$
\# \text{conjugacy classes of primitive parabolic elements in } \Gamma = \text{vol}(\Gamma \backslash \mathcal{H}) \text{res}_{s=1} \Phi(z; s).
$$

Hence by Propositions 4 and 5, the proof of Theorem 1 is reduced to showing that

\begin{equation}
\text{res}_{s=1} \Phi(z; s) = \frac{2}{\pi} \prod_{p/q} \frac{2}{p+1},
\end{equation}

ON A THEOREM OF LEGENDRE
7. Epstein zeta functions

Recall that $H$ is the number of $\text{GL}(2, \mathbb{Z})$ orbits of triples $F$ that satisfy $S(F) = 0$. By (6.5) and Theorem 2, Theorem 1 is a consequence of the following Proposition.

**Proposition 7.** We have the identity

$$\text{res}_{s=1} \Phi(z; s) = \frac{H}{2\pi} \prod_{p|q} \frac{1}{p+1}. $$

The remainder of the paper is devoted to the proof of Proposition 7. For a fixed $z \in \mathcal{H}$ let

$$N(m) = \sqrt{q} (\text{Im } z)^{-1} ((m_1 - m_3)|z|^2 - 2m_2 \sqrt{q} \text{Re } z + m_1 + m_3).$$

For any triple $F = (f_1, f_2, f_3)$ with $\text{disc}(F) = -Q^*$, which was given in (3.6), define

$$N_F(u) = |N(f_1(u), f_2(u), f_3(u))|.$$

This is a positive definite binary quadratic form since a calculation shows that the determinant of the $2 \times 2$ matrix $N_F$, when $N_F(u) = u N_F u^t$, is given by

(7.1) \[ \det N_F = 4q^2. \]

Now define for $r = (r_1, r_2) \in \left( \mathbb{Z}/2q\mathbb{Z} \right)^2$

(7.2) \[ Z^*_F(z, s; r) = \frac{1}{2} \sum_{\gcd(u) = 1}^{\prime} N_F(u)^{-s}. \]

Recall the definition of $R_F$ from above Lemma 2. By (6.4), Proposition 2 and Theorem 2 we have the expansion

(7.3) \[ \Phi(z, s) = \frac{1}{2} \sum_{[F]} \sum_{r \in R_F} Z^*_F(z, s; r), \]

where the sum over $[F]$ is over a full set of $H$ representatives of triples $F$ with $Q(F) = 0$, for instance $F = \pm (f_1, f_2, f_3)$ with $f_1, f_2, f_3$ given in (3.4) and (3.5).

Proposition 7 is now a consequence of (7.3), Lemma 2 and the following result.

**Lemma 3.** $Z^*_F(z, s; r)$ has a meromorphic continuation to $\mathbb{C}$ and that it is holomorphic for $\Re(s) > \frac{1}{2}$, except for a simple pole at $s = 1$ with

$$\text{Res}_{s=1} Z^*_F(z, s; r) = \frac{1}{2q^2} \prod_{p|q} (p^2 - 1)^{-1}. $$

To prove Lemma 3 we require two more lemmas. First we will express $Z^*_F(z, s; r)$ in terms of the Epstein zeta function

$$Z_F(z, s; r) = \frac{1}{2} \sum_{u \equiv r \pmod{2q}}' N_F(u)^{-s},$$

where as usual the prime in the sum means omit $(0, 0)$.

**Lemma 4.** For $\Re(s) > 1$ and $r \in R_F$

(7.4) \[ Z^*_F(z, s; r) = \frac{1}{\phi(2q)} \sum_{\chi} L(2s, \chi)^{-1} \sum_{\ell \pmod{2q}} \frac{\chi(\ell)}{\gcd(\ell, 2q) = 1} Z_F(z, s; \ell r), \]

where $L(s, \chi)$ is the Dirichlet $L$-function, and the sum over $\chi$ is over all Dirichlet characters modulo $2q$. 
Proof. Since the Möbius function $\mu$ satisfies the identity
\[
\sum_{d|n} \mu(d) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if } n \neq 1 \n\end{cases}
\]
we have by (7.2) that
\[
Z_F^*(z, s; r) = \frac{1}{2} \sum_{u \in \mathbb{Z}^2} \sum_{d \mid \gcd(u_1, u_2)} \mu(d) N_F(u)^{-s}
\]
\[
= \frac{1}{2} \sum_{d \geq 1} \sum_{u \in \mathbb{Z}^2} \mu(d) N_F(du)^{-s}.
\]
Since $r \in R_F$ the only $d$ that occur are prime to $2q$. Thus
\[
Z_F^*(z, s; r) = \frac{1}{2} \sum_{\ell \equiv r \pmod{2q}} N_F(\ell)^{-s}.
\]
Now Lemma 4 follows from the easily proven evaluation
\[
\sum_{d \equiv \ell \pmod{2q}} \mu(d)d^{-2s} = \frac{1}{\phi(2q)} \sum_{\chi} \chi(\ell) L(2s, \chi)^{-1},
\]
where the sum on the right hand side is over all Dirichlet characters modulo $2q$.

The next result is well-known and follows from (7.1) and e.g. [29, Theorem 3 p.69].

**Lemma 5.** $Z_F(z, s; r)$ has analytic continuation in $s$ to an entire function except for a simple pole at $s = 1$. The residue there is given by
\[
\text{Res}_{s=1} Z_F(z, s; r) = \frac{\pi}{16q^2}.
\]

**Proof of Lemma 3.** By Lemma 4 and standard properties of Dirichlet $L$ functions we see that $Z_F^*(z, s; r)$ has a meromorphic continuation to $\mathbb{C}$ and that it is holomorphic for $\text{Re}(s) > \frac{1}{2}$, except for a simple pole at $s = 1$. By Lemma 5 the residue at $s = 1$ of $Z_F(z, s; \ell r)$ is independent of $\ell$, so in (7.4) only the term in the sum over $\chi$ with $\chi = \chi_0$, the trivial character modulo $2q$, contributes to the residue. Since
\[
L(2s, \chi_0) = \prod_{p \mid 2q} (1 - p^{-2s})^{-1},
\]
by (7.4) and Lemma 5 again we have
\[
\text{Res}_{s=1} Z_F^*(z, s; r) = \frac{\pi}{16q^2} \prod_{p \mid 2q} (1 - p^{-2})^{-1} = \frac{\pi}{16q^2} \prod_{p \mid 2q} (1 - p^{-2})^{-1} = \frac{1}{2q^2} \prod_{p \mid q} (p^2 - 1)^{-1}.
\]

This completes the proof of Lemma 3 and so also of Proposition 7 and Theorem 1. \qed
Remarks. The argument given in this section is similar to, but simpler than, one used in [5], where a class number formula for certain binary quartic forms was obtained by using an explicit parameterization of integral points on twists of an elliptic curve.

Although here we only made use of the constant in the leading term, it is clear that an asymptotic formula counting primitive solutions to $Q(x) = 0$ with a norm constraint on $x$ can be given using the formulas of this section, even one with an explicit remainder estimate. The proof of Theorem 1 compares this asymptotic with a similar count for each orbit of the group $G_0$, which is accomplished using Eisenstein series for a Fuchsian group. The spectral method of counting within an orbit was developed in some generality in [7]. By combining this orbit count with the full count obtained by the circle method, a new proof of Siegel’s mass formula in some cases was given in [9]. The circle method gives the constant in the asymptotic formula as a product of local densities, but it is not immediately applicable in the ternary case. By using a refinement of the circle method, asymptotics with a constant of this form for the full count in the isotropic ternary case were obtained in [13].6 A computation of primitive local densities for $Q(x) = 0$ (for finite primes) is, at least in some sense, implicit in our proof of Theorem 1.

Acknowledgements. I want to thank Peter Sarnak for sharing valuable insights on the general subject of this paper and for several specific comments and suggestions.

References

1. Berggren, B. Pytagoreiska trianglar, Tidskrift för Elementär Matematik, 17 (1934), 129–139.
5. Duke, W. On elliptic curves and binary quartic forms, IMRN 2021

6For more on the history of this method see [6] and [16]. See [24] and [31] for other approaches to the asymptotic in the isotropic ternary case.
27. Siegel, C.L. Über die analytische Theorie der quadratischen Formen. II. Ann. of Math. (2) 37 (1936), no. 1, 230–263, also in Gesammelte Abhandlungen I
29. Siegel, C. L. Lectures on advanced analytic number theory, Tata Institute, Bombay.
30. Smith, H.J.S. On the criterion of resolvability in Integral Numbers of the Indeterminate Equation \( f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'x'x'' + 2b''x'x = 0 \). Pr. Royal Soc. XIII, 100-111 (1864), in Collected Papers I.

UCLA MATHEMATICS DEPARTMENT, BOX 951555, LOS ANGELES, CA 90095-1555

Email address: wdduke@ucla.edu