REPRESENTATION OF INTEGERS BY TERNARY QUADRATIC FORMS: A GEOMETRIC APPROACH

Gabriel Durham
Department of Mathematics, University of Georgia, Athens, Georgia
gjdurham@uga.edu

Received: 9/11/15, Revised: 2/22/16, Accepted: 8/1/16, Published: 8/26/16

Abstract

In 1957 N.C. Ankeny provided a new proof of the three squares theorem using geometry of numbers. This paper generalizes Ankeny's technique, proving exactly which integers are represented by $x^2 + 2y^2 + 2z^2$ and $x^2 + y^2 + 2z^2$ as well as proving sufficient conditions for an integer to be represented by $x^2 + y^2 + 3z^2$ and $x^2 + y^2 + 7z^2$.

1. Introduction

A natural question in the study of quadratic forms concerns the representation of integers by certain quadratic forms. Given an n-ary quadratic form Q and an integer m, does there exist a vector $\vec{x} \in \mathbb{Z}^n$ such that $Q(\vec{x}) = m$? This paper considers this question for four ternary quadratic forms: $x^2+2y^2+2z^2$, $x^2+y^2+2z^2$, $x^2+y^2+3z^2$, and $x^2+y^2+7z^2$. We are able to prove exactly which integers are represented by the first two forms and provide sufficient conditions for an integer m to be represented by the final two forms.

In 1931, Burton Jones [3] provided one of the key breakthroughs in the study of positive definite ternary quadratic forms when he proved that the forms of a given genus collectively represent all positive integers not ruled out by certain congruence conditions. As a result, if a quadratic form is alone in its genus then one can show it represents an integer m by showing that it locally represents m. While Jones' work made the task of determining which integers are represented by our first three forms[1] more straightforward, the proofs presented in this paper make no use of Jones' result. Furthermore, Jones' result tells us little about forms with one or more "genus-mates." While ternary quadratic forms have been studied for centuries, relatively little is known about the representation of integers by forms not alone in their genus. In particular, the question of exactly which integers are

[1] As well as all other "class number one" forms (i.e. forms which are alone in their genus).

represented by $x^2+y^2+7z^2$ remains open, despite the fact that this form has the smallest determinant (and thus, in a sense, is the most simple) of any classically integral ternary quadratic form not alone in its genus. While this paper does not fully answer the question, we do provide a new proof of a result of Kaplansky [4] in our proof of Theorem 3(a). For a more comprehensive list of what is known about the representation of integers by $x^2+y^2+7z^2$ the reader may consult Wang and Pei [5].

To prove our results we generalize a method developed by N.C. Ankeny [1], which he used to provide a new proof of the Gauss-Legendre three squares theorem. Ankeny began with a positive integer m not of the form $4^k(8\ell+7)$ for some $k,\ell\in\mathbb{Z}$ and, using Dirichlet's theorem on primes in an arithmetic progression, defined a prime q based on the prime factors of m. He then defined a linear map, $\vec{\Phi}:(x,y,z)\mapsto(R,S,T)$. By considering the body $\Omega=\{(R,S,T)\in\mathbb{R}^3|R^2+S^2+T^2<2m\}$, he was able to invoke Minkowski's convex body theorem to guarantee integer values of x,y,z such that $\vec{\Phi}(x,y,z)\in\Omega$. By the properties of the transformation $\vec{\Phi}$, he shows that $R^2+S^2+T^2=m$ and $R\in\mathbb{Z}$. To complete the proof of the three squares theorem Ankeny showed that S^2+T^2 is a sum of two integer squares by showing that for all primes p dividing S^2+T^2 to an odd power, $\left(\frac{-1}{p}\right)=1$.

We alter this method by changing the transformation $\vec{\Phi}$ to show that S^2+T^2 is represented by other binary forms. We obtain the following results:

Theorem 1. *The quadratic form $x^2+2y^2+2z^2$ represents a positive integer m if and only if m is not of the form $4^k(8\ell+7)$ for some $k,\ell\in\mathbb{Z}$.*

Theorem 2. *The quadratic form $x^2+y^2+2z^2$ represents a positive integer m if and only if m is not of the form $4^k(16\ell+14)$ for some $k,\ell\in\mathbb{Z}$.*

Theorem 3. (a) *If m is a positive integer of the form $4^k(8\ell+5)$ for some $k,\ell\in\mathbb{Z}$ and $\mathrm{ord}_7(m)$ is even then m is represented by the quadratic form $x^2+y^2+7z^2$.*
(b) *If m is a positive integer of the form $4^k(8\ell+1)$ for some $k,\ell\in\mathbb{Z}$ and $\mathrm{ord}_3(m)$ is even then m is represented by the quadratic form $x^2+y^2+3z^2$.*

2. Background

The following section serves as a brief introduction to the material presented in the paper.

Let $n\in\mathbb{N}$. An *$n-$ary integral quadratic form*, Q, is a homogeneous polynomial

of degree two, i.e.,

$$Q : \mathbb{Z}^n \to \mathbb{Z}$$
$$Q : (\vec{x}) \mapsto \sum_{1 \le i \le j \le n} a_{i,j} x_i x_j,$$

where $a_{i,j} \in \mathbb{Z}$ for all $1 \le i \le j \le n$. We say Q *represents* an integer m if there exists an $\vec{x} \in \mathbb{Z}^n$ such that $Q(\vec{x}) = m$.

A quadratic form Q is *positive definite* if both of the following hold:

$$(i)\ Q(\vec{x}) \ge 0 \text{ for all } \vec{x} \in \mathbb{Z}^n,$$
$$(ii)\ Q(\vec{x}) = 0 \text{ if and only if } \vec{x} = \vec{0}.$$

Henceforth, by "form" we mean "positive definite ternary integral quadratic form."

Throughout the paper $\left(\frac{a}{b}\right)$ refers to the Jacobi symbol.

Furthermore, a quadratic form Q is *multiplicative* if the following holds: for all integers a and b, if Q represents a and b, then Q represents ab.

The following proofs rely on three external theorems, two of which, Dirichlet's theorem on primes in an arithmetic progression and Minkowski's theorem on convex symmetric bodies, are some of the more powerful and well-known results of nineteenth century number theory. The third theorem comes from the theory of binary quadratic forms and was reproved using the geometry of numbers by Clark, Hicks, Parshall, and Thompson in 2013 and states the following:

Theorem 4. *([2]): For $c = 2, 3$ and 7, $x^2 + cy^2$ represents a positive integer m if and only if $\left(\frac{-c}{p}\right) = 1$ for all primes p dividing m to an odd power.*

3. Proofs of Theorems

For Theorems 1 and 2 we can look at these forms (mod 8) and (mod 16) and see that they do not represent any positive integer congruent to 7 (mod 8) and 14 (mod 16), respectively. Thus, the proofs of these theorems will provide necessary and sufficient conditions for a positive integer to be represented by these forms.

We can also see that for any positive $m \in \mathbb{Z}$, if $x^2 + 2y^2 + 2z^2$ represents m, then $x^2 + y^2 + 2z^2$ represents $2m$, and if $x^2 + y^2 + 2z^2$ represents m, then $x^2 + 2y^2 + 2z^2$ represents $2m$. Thus, Theorems 1 and 2 can be proven simply by showing which positive odd integers are represented by these forms; however, the purpose of this paper is to display the manner in which Ankeny's technique can be generalized. In the spirit of this purpose we completely prove Theorem 1 using Ankeny's technique. We also use Ankeny's technique to show which positive odd integers are represented by the form $x^2+y^2+2z^2$, but, for brevity's sake, we refer to Theorem 1 when proving

which even integers are represented by the form and leave the "Ankeny-style" proof to the reader.

3.1. $x^2 + 2y^2 + 2z^2$

Here we wish to prove that the quadratic form $x^2+2y^2+2z^2$ represents all positive integers not of the form $4^k(8\ell+7)$ for some $k, \ell \in \mathbb{Z}$.

Proof of Theorem 1. Let m be a positive integer which cannot be written as $m = 4^k(8\ell+7)$ for any $k, \ell \in \mathbb{Z}$. Without loss of generality we can assume that m is squarefree. We will first consider the case where $m \equiv 3 \pmod 8$.

Let q be an odd prime such that $q > m$, $q \equiv 1 \pmod 8$, and $\left(\frac{-2q}{p}\right) = 1$ for all primes $p|m$ (we know such a q exists by Dirichlet's theorem on primes in an arithmetic progression). This construction of q guarantees that there exists a $t \in \mathbb{Z}$ with $t^2 \equiv \frac{-1}{2q} \pmod m$. This construction of q also guarantees

$$1 = \prod_{p|m}\left(\frac{-2q}{p}\right) = \left(\frac{-2}{m}\right)\prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{p}{q}\right) = \left(\frac{m}{q}\right) = \left(\frac{-m}{q}\right).$$

Thus there exists a $b \in \mathbb{Z}$, where b is odd, such that $b^2 \equiv -m \pmod q$. As a result, there is an $h_1 \in \mathbb{Z}$ such that $b^2 - qh_1 = -m$. Looking at this statement modulo 2 we get $-qh_1 \equiv 0 \pmod 2$. Thus $h_1 = 2h$ for some $h \in \mathbb{Z}$. Therefore we have that

$$b^2 - 2qh = -m.$$

We now consider the body, Ω, defined by

$$\Omega = \{(R,S,T) \in \mathbb{R}^3 | 2R^2 + S^2 + T^2 < 2m\},$$

where

$$\begin{aligned} R &= tqx + bty + mz \\ S &= \sqrt{q}x + \tfrac{b}{\sqrt{q}}y \\ T &= \tfrac{\sqrt{m}}{\sqrt{q}}y. \end{aligned}$$

Note that $vol(\Omega) = (\frac{4}{3})(\pi)(\frac{1}{\sqrt{2}})(\sqrt{2m}^3) = \frac{8\pi m^{3/2}}{3}$.

Let $\vec{\Phi} : \mathbb{R}^3 \to \mathbb{R}^3$ where $\vec{\Phi} : (x,y,z) \mapsto (R,S,T)$ be the function associated to the above transformation. We see that $\vec{\Phi}(\vec{x}) = M_{\vec{\Phi}}\vec{x}$ where $M_{\vec{\Phi}} =$

$$\begin{bmatrix} tq & bt & m \\ \sqrt{q} & \frac{b}{\sqrt{q}} & 0 \\ 0 & \frac{\sqrt{m}}{\sqrt{q}} & 0 \end{bmatrix}.$$

By looking at $\vec{\Phi}$ as a linear map we see that $M_{\vec{\Phi}}$ is the standard matrix of $\vec{\Phi}$. Furthermore, $\det(M_{\vec{\Phi}}) = (m)(\sqrt{q})(\frac{\sqrt{m}}{\sqrt{q}}) = m^{3/2}$.

We now wish to examine $\vec{\Phi}^{-1}(\Omega)$. Since Ω is a convex symmetric body and $\vec{\Phi}$ is invertible, we know that $\vec{\Phi}^{-1}(\Omega)$ is convex and symmetric as well. We see that

$$vol(\vec{\Phi}^{-1}(\Omega)) = \frac{1}{|\det(M_{\vec{\Phi}})|} vol(\Omega) = \frac{1}{m^{3/2}} vol(\Omega) = \frac{8\pi}{3} > 2^3.$$

By Minkowski's theorem on convex symmetric bodies there exist $x_1, y_1, z_1 \in \mathbb{Z}$, not all zero, such that $\vec{\Phi}(x_1, y_1, z_1) \in \Omega$. Let $(R_1, S_1, T_1) := \vec{\Phi}(x_1, y_1, z_1)$.

We see that

$$\begin{aligned} 2R_1^2 + S_1^2 + T_1^2 &\equiv 2(tqx_1 + bty_1)^2 + (\sqrt{q}x_1 + \frac{by_1}{\sqrt{q}})^2 + (\frac{\sqrt{m}y_1}{\sqrt{q}})^2 \\ &\equiv 2t^2(qx_1 + by_1)^2 + \frac{1}{q}((qx_1 + by_1)^2 + my_1^2) \\ &\equiv \frac{-2}{2q}(qx_1 + by_1)^2 + \frac{1}{q}(qx_1 + by_1)^2 \\ &\equiv 0 \pmod{m}, \end{aligned}$$

and also that

$$\begin{aligned} S_1^2 + T_1^2 &= \frac{1}{q}(q^2x_1^2 + 2qbx_1y_1 + (b^2 + m)y_1^2) \\ &= \frac{1}{q}(q^2x_1^2 + 2qbx_1y_1 + 2qhy_1^2) \\ &= qx_1^2 + 2bx_1y_1 + 2hy_1^2. \end{aligned}$$

While $S_1, T_1 \notin \mathbb{Z}$, we can see that $S_1^2 + T_1^2 \in \mathbb{Z}$. Thus $2R_1^2 + S_1^2 + T_1^2 \in \mathbb{Z}$, $0 < 2R_1^2 + S_1^2 + T_1^2 < 2m$, and $2R_1^2 + S_1^2 + T_1^2 \equiv 0 \pmod{m}$. We can now conclude that $2R_1^2 + S_1^2 + T_1^2 = m$.

Our goal now is to show that $2R_1^2 + S_1^2 + T_1^2$ is represented by the quadratic form $x^2 + 2y^2 + 2z^2$. Since $R_1 \in \mathbb{Z}$ we wish to show that $S_1^2 + T_1^2$ is of the form $a^2 + 2b^2$ for some $a, b \in \mathbb{Z}$. By the theorem of Clark, Hicks, Parshall, and Thompson, it will suffice to show that $\left(\frac{-2}{p}\right) = 1$ for all primes p dividing $S_1^2 + T_1^2$ to an odd power [2]. We note here that $x^2 + 2y^2$ is multiplicative and represents 2, so we need not consider $p = 2$; furthermore, $S_1^2 + T_1^2 \leq m < q$, and so we need not consider $p = q$. Thus, it will suffice to show $\left(\frac{-2}{p}\right) = 1$ for all odd primes $p|v$, where $v := q(S_1^2 + T_1^2)$. We will do this in two cases.

`Case 1` $p \nmid m$: We see that $0 \not\equiv m \equiv 2R_1^2 \pmod{p}$; it follows that $-m \equiv -2R_1^2 \pmod{p}$ and so $\left(\frac{-2}{p}\right) = \left(\frac{-m}{p}\right)$. Furthermore, $0 \equiv v \equiv (qx_1 + by_1)^2 + my_1^2 \pmod{p}$ so $(qx_1 + by_1)^2 \equiv (-m)y_1^2 \pmod{p}$. Since p divides v to an odd power we know $y_1 \not\equiv 0 \pmod{p}$ and thus we can conclude $1 = \left(\frac{-m}{p}\right) = \left(\frac{-2}{p}\right)$.

`Case 2` $p|m$: Since m is assumed squarefree, we can assume $p \nmid \frac{m}{p}$. Since $2R_1^2 + S_1^2 + T_1^2 = m$, we know $2R_1^2 \equiv 0 \pmod{p}$ and $p|R_1$. Furthermore, $(qx_1 + by_1)^2 + my^2 \equiv (qx_1 + by_1)^2 \equiv 0 \pmod{p}$, so $p|(qx_1 + by_1)$. Hence, $\frac{2R_1^2}{p} + \frac{S_1^2+T_1^2}{p} = \frac{2R_1^2}{p} + \frac{1}{q}(\frac{(qx_1+by_1)^2}{p} + \frac{m}{p}y_1^2) = \frac{m}{p}$. It follows that $y_1^2 \equiv q \pmod{p}$. Thus, $\left(\frac{-2}{p}\right) = \left(\frac{-2q}{p}\right) = 1$.

In both cases $\left(\frac{-2}{p}\right) = 1$, thus there exist $a, b \in \mathbb{Z}$ such that $S_1^2 + T_1^2 = a^2 + 2b^2$. Therefore, m is represented by the form $x^2 + 2y^2 + 2z^2$, as required.

`For` m `odd`: If $m \equiv 1, 5 \pmod{8}$ take q to be an odd prime such that $q > m$, $q \equiv 1 \pmod{8}$, and $\left(\frac{-q}{p}\right) = 1$ for all primes $p|m$. We see that

$$1 = \prod_{p|m}\left(\frac{-q}{p}\right) = \left(\frac{-1}{m}\right)\prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{p}{q}\right) = \left(\frac{m}{q}\right) = \left(\frac{-m}{q}\right).$$

We now proceed as before; however, we take $t^2 \equiv \frac{-1}{4q} \pmod{m}$ and take the following transformation

$$\begin{aligned} R &= 2tqx + bty + mz \\ S &= \sqrt{2q}x + \tfrac{b}{\sqrt{2q}}y \\ T &= \tfrac{\sqrt{m}}{\sqrt{2q}}y. \end{aligned}$$

`For` m `even`: Take $m = 2m_1$. Since m is assumed squarefree we can assume that m_1 is odd.

If $m_1 \equiv 1, 3 \pmod{8}$ take q to be an odd prime such that $q \equiv 1 \pmod{8}$, $q > m_1$, and $\left(\frac{-2q}{p}\right) = 1$ for all $p|m_1$. We see that

$$1 = \prod_{p|m_1}\left(\frac{-2q}{p}\right) = \left(\frac{-2}{m_1}\right)\prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m_1}\left(\frac{q}{p}\right) = \prod_{p|m_1}\left(\frac{p}{q}\right) = \left(\frac{m_1}{q}\right) = \left(\frac{-2m_1}{q}\right).$$

Now take $t, b \in \mathbb{Z}$ such that $t^2 \equiv \frac{-1}{2q} \pmod{m_1}$ and $b^2 \equiv -2m_1 \pmod{q}$, where b is even. Thus there exists an $h \in \mathbb{Z}$ such that

$$b^2 - 2qh = -2m_1.$$

We now consider the body defined by

$$\Omega = \{(R, S, T) \in \mathbb{R}^3 | R^2 + \frac{S^2 + T^2}{2} < 2m_1\}$$

(note that $vol(\Omega) = \frac{16\pi\sqrt{2}m_1^{3/2}}{3}$) where

$$\begin{aligned} R &= tqx + bty + m_1 z \\ S &= \sqrt{q}x + \tfrac{b}{\sqrt{q}}y \\ T &= \tfrac{\sqrt{2m_1}}{\sqrt{q}}y. \end{aligned}$$

We define $\vec{\Phi}$ to be the function associated to the above transformation. We see that $\vec{\Phi}$ is an invertible linear map and the determinant of its standard matrix is $\sqrt{2}m_1^{3/2}$, thus the volume of $\vec{\Phi}^{-1}(\Omega)$ is $\frac{16\pi}{3} > 16 = 2^3(2)$.

We now consider the lattice $\Lambda = \{(x, y, z) \in \mathbb{Z}^3 | x \equiv 0 \pmod 2\}$. Since $[\mathbb{Z}^3 : \Lambda] = 2$, we know the fundamental domain of Λ has volume 2 and thus we can invoke Minkowski's theorem on convex symmetric bodies to show there exists a nonzero point $(x_1, y_1, z_1) \in \Lambda$ such that $\vec{\Phi}(x_1, y_1, z_1) \in \Omega$. Let $(R_1, S_1, T_1) := \vec{\Phi}(x_1, y_1, z_1)$.

We see that

$$\begin{aligned} R_1^2 + \frac{S_1^2 + T_1^2}{2} &\equiv t^2(qx_1 + by_1)^2 + \frac{1}{2q}(qx_1 + by_1)^2 + \frac{1}{2q}(\sqrt{2m_1}y_1)^2 \\ &\equiv t^2(qx_1 + by_1)^2 + \frac{1}{2q}((qx_1 + by_1)^2 + 2my_1^2) \\ &\equiv \frac{-1}{2q}(qx_1 + by_1)^2 + \frac{1}{2q}(qx_1 + by_1)^2 \\ &\equiv 0 \pmod{m_1} \end{aligned}$$

and that

$$\begin{aligned} \frac{1}{2}(S_1^2 + T_1^2) &= \frac{1}{2q}((qx_1 + by_1)^2 + 2m_1y_1^2) \\ &= \frac{1}{2q}(q^2x_1^2 + 2qbx_1y_1 + 2qhy_1^2) \\ &= q\frac{x_1^2}{2} + bx_1y_1 + hy_1^2. \end{aligned}$$

Since x_1 is even, we see that $\frac{S_1^2+T_1^2}{2} \in \mathbb{Z}$. Moreover, $0 < R_1^2 + \frac{S_1^2+T_1^2}{2} < 2m_1$, and we conclude that $R_1^2 + \frac{S_1^2+T_1^2}{2} = m_1$.

We now define $v := 2q(S_1^2+T_1^2)$. We now wish to show that $\frac{S_1^2+T_1^2}{2}$ is represented by the binary quadratic form $x^2 + 2y^2$. As before, it will suffice to show $\left(\frac{-2}{p}\right) = 1$ for all odd primes p dividing v to an odd power [2]. We proceed in two cases.

`Case 1` $p \nmid m$: Since $m_1 \equiv R_1^2 \pmod p$, we have $\left(\frac{m_1}{p}\right) = 1$. Furthermore, $(qx_1 + by_1)^2 \equiv -2m_1y_1^2 \pmod p$. It follows that $\left(\frac{-2}{p}\right) = \left(\frac{m_1}{p}\right) = 1$.

Case 2 $p|m$: By the same argument presented in the $m \equiv 3 \pmod 8$ case, we see that $-2y_1^2 \equiv -2q \pmod p$. By the construction of q, $\left(\frac{-2}{p}\right) = \left(\frac{-2q}{p}\right) = 1$.

In both cases we have $\left(\frac{-2}{p}\right) = 1$. Therefore there exist $a_1, b_1 \in \mathbb{Z}$ such that $\frac{S_1^2+T_1^2}{2} = a_1^2 + 2b_1^2$. Since the form $x^2 + 2y^2$ is multiplicative and represents 2 we also know there exist $a, b \in \mathbb{Z}$ such that $S_1^2 + T_1^2 = a^2 + 2b^2$. Furthermore, since $R_1^2 + \frac{S_1^2+T_1^2}{2} = m_1$, $2R_1^2 + S_1^2 + T_1^2 = m$. Noting that $R_1 \in \mathbb{Z}$ we see $m = 2R_1^2 + a^2 + 2b^2$.

Therefore m is represented by $x^2 + 2y^2 + 2z^2$, as required.

If $m_1 \equiv 5 \pmod 8$, take q to be an odd prime such that $q > m_1$, $q \equiv 5 \pmod 8$, and $\left(\frac{-2q}{p}\right) = 1$ for all primes $p|m_1$. We see that

$$1 = \prod_{p|m_1} \left(\frac{-2q}{p}\right) = \left(\frac{-2}{m_1}\right) \prod_{p|m} \left(\frac{q}{p}\right) = (-1) \prod_{p|m_1} \left(\frac{q}{p}\right)$$

$$= (-1) \prod_{p|m_1} \left(\frac{p}{q}\right) = (-1) \left(\frac{m_1}{q}\right) = \left(\frac{-2m_1}{q}\right).$$

The rest of the proof proceeds as above.

If $m_1 \equiv 7 \pmod 8$, take q to be an odd prime such that $q > m_1$, $q \equiv 3 \pmod 8$, and $\left(\frac{-2q}{p}\right) = 1$ for all primes $p|m_1$. We see that

$$1 = \prod_{p|m_1} \left(\frac{-2q}{p}\right) = \left(\frac{-2}{m_1}\right) \prod_{p|m} \left(\frac{q}{p}\right) = (-1) \prod_{p|m_1} \left(\frac{q}{p}\right) = \prod_{p|m_1} \left(\frac{p}{q}\right)$$

$$= \left(\frac{m_1}{q}\right) = \left(\frac{-2m_1}{q}\right).$$

The rest of the proof proceeds as above.

This completes the proof of Theorem 1. □

3.2. $x^2 + y^2 + 2z^2$

We now wish to prove that the quadratic form $x^2 + y^2 + 2z^2$ represents all positive integers not of the form $4^k(16\ell + 14)$ for some $k, \ell \in \mathbb{Z}$.

Proof of Theorem 2. Let m be a positive integer which cannot be written as $m = 4^k(16\ell + 14)$ for any $k, \ell \in \mathbb{Z}$. We wish to prove that m is represented by the form $x^2 + y^2 + 2z^2$. Without loss of generality we can assume that m is squarefree. As before we first consider the case where $m \equiv 3 \pmod 8$.

Let q be an odd prime where $q > m$, $q \equiv 1 \pmod 8$, and $\left(\frac{-2q}{p}\right) = 1$ for all primes $p|m$. Furthermore, this construction of q ensures that there exists a $t \in \mathbb{Z}$ such that $t^2 \equiv \frac{-1}{2q} \pmod m$. We also have

$$1 = \prod_{p|m}\left(\frac{-2q}{p}\right) = \left(\frac{-2}{m}\right)\prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{p}{q}\right) = \left(\frac{m}{q}\right) = \left(\frac{-2m}{q}\right).$$

Thus there exists a $b \in \mathbb{Z}$, where b is even, such that $b^2 \equiv -2m \pmod{q}$. As a result we know $b^2 - qh_1 = -2m$ for some $h_1 \in \mathbb{Z}$. We can thus write $h_1 = 2h$ for some $h \in \mathbb{Z}$ and see

$$b^2 - 2qh = -2m.$$

We now consider the body defined by

$$\Omega = \{(R, S, T) \in \mathbb{R}^3 | R^2 + S^2 + T^2 < 2m\}$$

(note that $vol(\Omega) = \frac{4}{3}\pi\sqrt{2m}^3 = \frac{8\sqrt{2}\pi m^{3/2}}{3}$) where

$$\begin{aligned} R &= 2tqx + bty + mz \\ S &= \sqrt{2q}x + \tfrac{b}{\sqrt{2q}}y \\ T &= \tfrac{\sqrt{2m}}{\sqrt{2q}}y. \end{aligned}$$

Let $\vec{\Phi} : \mathbb{R}^3 \to \mathbb{R}^3$, where $\vec{\Phi} : (x, y, z) \mapsto (R, S, T)$, be the function associated to the above transformation. Thus, $\vec{\Phi}(\vec{x}) = M_{\vec{\Phi}}\vec{x}$ where $M_{\vec{\Phi}} =$

$$\begin{bmatrix} 2tq & bt & m \\ \sqrt{2q} & \frac{b}{\sqrt{2q}} & 0 \\ 0 & \frac{\sqrt{2m}}{\sqrt{2q}} & 0 \end{bmatrix}.$$

Since Ω is a convex symmetric body, $\vec{\Phi}^{-1}(\Omega)$ is as well. We see that

$$vol(\vec{\Phi}^{-1}(\Omega)) = \frac{vol(\Omega)}{|\det(M_{\vec{\Phi}})|} = \frac{8\pi}{3} > 8.$$

Minkowski's theorem on convex symmetric bodies guarantees the existence of $x_1, y_1, z_1 \in \mathbb{Z}$ (not all zero) such that $\vec{\Phi}(x_1, y_1, z_1) \in \Omega$. Let $(R_1, S_1, T_1) := \vec{\Phi}(x_1, y_1, z_1)$. We see that

$$\begin{aligned} R_1^2 + S_1^2 + T_1^2 &\equiv (2tqx_1 + bty_1)^2 + (\sqrt{2q}x_1 + \frac{by_1}{\sqrt{2q}})^2 + (\frac{\sqrt{2m}y_1}{\sqrt{2q}})^2 \\ &\equiv t^2(2qx_1 + by_1)^2 + \frac{1}{2q}((2qx_1 + by_1)^2 + 2my_1^2) \\ &\equiv t^2(2qx_1 + by_1)^2 + \frac{1}{2q}(2qx_1 + by_1)^2 \\ &\equiv 0 \pmod{m}, \end{aligned}$$

and that

$$\begin{aligned} S_1^2 + T_1^2 &= \frac{1}{2q}(4q^2x_1^2 + 4qbx_1y_1 + (b^2+2m)y_1^2) \\ &= \frac{1}{2q}(4q^2x_1^2 + 4qbx_1y_1 + 2qhy_1^2) \\ &= 2qx_1^2 + 2bx_1y_1 + hy_1^2. \end{aligned}$$

We now see that $S_1^2+T_1^2 \in \mathbb{Z}$ and, as before, we can conclude that $R_1^2+S_1^2+T_1^2 = m$.

Let $v := 2q(S_1^2 + T_1^2)$. We wish to show that $S_1^2 + T_1^2$ is of the form $a^2 + 2b^2$ for some $a, b \in \mathbb{Z}$. As was the case in our proof of Theorem 1, it will suffice to show $\left(\frac{-2}{p}\right) = 1$ for all odd primes p dividing v to an odd power (and we need not consider $p = q$) [2]. We will do so in two cases.

`Case 1` $p \nmid m$: Since $m \equiv {R_1}^2 \pmod{p}$, $\left(\frac{m}{p}\right) = 1$. Furthermore, $(2qx_1 + by_1)^2 \equiv -2my_1^2 \pmod{p}$. Thus $\left(\frac{-2}{p}\right) = \left(\frac{m}{p}\right) = 1$.

`Case 2` $p|m$: Since m is assumed squarefree we know that $p \nmid \frac{m}{p}$. Since $R_1^2 + S_1^2 + T_1^2 = m$, $R_1^2 \equiv 0 \pmod{p}$ and so $p|R_1$. Moreover, we know that $(2qx_1 + by_1)^2 - 2my_1^2 \equiv (2qx_1 + by_1)^2 \equiv 0 \pmod{p}$. Thus $p|(2qx_1 + by_1)$. Noting that $\frac{R_1^2}{p}+\frac{1}{2q}(\frac{(2qx_1+by_1)^2}{p} + 2\frac{m}{p}y_1^2)= \frac{m}{p}$, we see that $\frac{1}{2q}(2\frac{m}{p}y_1^2) \equiv \frac{m}{p} \pmod{p}$, and so $-2y_1^2 \equiv -2q \pmod{p}$. Thus $\left(\frac{-2}{p}\right) = \left(\frac{-2q}{p}\right) = 1$.

In both cases we have $\left(\frac{-2}{p}\right) = 1$ for all odd primes p dividing v to an odd power. We now know there exist $a, b \in \mathbb{Z}$ such that $S_1^2 + T_1^2 = a + 2b^2$.
Therefore, m is represented by the quadratic form $x^2 + y^2 + 2z^2$, as required.

For m odd we consider two situations.

For $m \equiv 7 \pmod{8}$, take q to be an odd prime such that $q > m$, $q \equiv 3 \pmod{8}$, and $\left(\frac{-2q}{p}\right) = 1$ for all primes $p|m$. We see that

$$1=\prod_{p|m}\left(\frac{-2q}{p}\right)=\left(\frac{-2}{m}\right)\prod_{p|m}\left(\frac{q}{p}\right) = (-1)\prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{p}{q}\right)=\left(\frac{m}{q}\right)=\left(\frac{-2m}{q}\right).$$

The rest of the proof proceeds as above.

For $m \equiv 1, 5 \pmod{8}$, take q to be an odd prime such that $q > m$, $q \equiv 1 \pmod{8}$, and $\left(\frac{-q}{p}\right) = 1$ for all primes $p|m$. We see that

$$1 = \prod_{p|m}\left(\frac{-2q}{p}\right) = \left(\frac{-1}{m}\right)\prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{p}{q}\right) = \left(\frac{m}{q}\right) = \left(\frac{-2m}{q}\right).$$

We let $t^2 \equiv \frac{-1}{q} \pmod{m}$ and take the following transformation

$$\begin{aligned} R &= tqx + bty + mz \\ S &= \sqrt{q}x + \tfrac{b}{\sqrt{q}}y \\ T &= \tfrac{\sqrt{2m}}{\sqrt{q}}y. \end{aligned}$$

The rest of the proof proceeds as above.

For m even we let $m = 2m_1$. By Theorem 1 we know, for $m_1 \equiv 1, 3, 5 \pmod 8$, there exist $x, y, z \in \mathbb{Z}$ such that $m_1 = x^2+2y^2+2z^2$. Thus $2m_1 = 2x^2+(2y)^2+(2z)^2$. Therefore, m is represented by $x^2 + y^2 + 2z^2$.

This completes the proof of Theorem 2. □

3.3. $x^2 + y^2 + 7z^2$ and $x^2 + y^2 + 3z^2$

Here we wish to show that if m is a positive integer of the form $4^k(8\ell + 5)$ for some $k, \ell \in \mathbb{Z}$ and $\text{ord}_7(m)$ is even then m is represented by the quadratic form $x^2 + y^2 + 7z^2$ and if m is a positive integer of the form $4^k(8\ell + 1)$ for some $k, \ell \in \mathbb{Z}$ and $\text{ord}_3(m)$ is even then m is represented by the quadratic form $x^2 + y^2 + 3z^2$.

Proof of Theorem 3. We first seek to prove Theorem 3(a). Let m be a positive integer of the form $4^k(8\ell + 5)$ for some $k, \ell \in \mathbb{Z}$ with $\text{ord}_7(m)$ even. Without loss of generality we can assume m is squarefree (and consequently that $7 \nmid m$), and $m \equiv 5 \pmod 8$.

Let q be an odd prime such that $q > m$, $q \equiv 1 \pmod{28}$, and $\left(\frac{-q}{p}\right) = 1$ for all primes $p|m$. By this construction of q, there exists a $t \in \mathbb{Z}$ such that $t^2 \equiv \frac{-1}{4q} \pmod m$. Additionally we see that

$$1 = \prod_{p|m}\left(\frac{-q}{p}\right) = \left(\frac{-1}{m}\right)\prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{p}{q}\right) = \left(\frac{m}{q}\right) = \left(\frac{-7m}{q}\right).$$

Thus there is a $b \in \mathbb{Z}$, where b is odd, such that $b^2 \equiv -7m \pmod q$. This shows us that $b^2 - qh_1 = -7m$ for some $h_1 \in \mathbb{Z}$. Looking at this statement modulo 4 we see that $h_1 \equiv 0 \pmod 4$. Therefore $h_1 = 4h$ for some $h \in \mathbb{Z}$ and so

$$b^2 - 4qh = -7m.$$

Looking at the above statement modulo 8 we see $4qh \equiv 4 \pmod 8$, thus h is odd.

We now consider the body defined by

$$\Omega = \{(R, S, T) \in \mathbb{R}^3 | R^2 + S^2 + T^2 < 2m\}$$

(note that $vol(\Omega) = \frac{4}{3}\pi\sqrt{2m}^3 = \frac{8\sqrt{2}\pi m^{3/2}}{3}$) where

$$\begin{aligned} R &= 2tqx + bty + mz \\ S &= \sqrt{q}x + \tfrac{b}{2\sqrt{q}}y \\ T &= \tfrac{\sqrt{7m}}{2\sqrt{q}}y. \end{aligned}$$

Let $\vec{\Phi} : \mathbb{R}^3 \to \mathbb{R}^3$, where $\vec{\Phi} : (x, y, z) \mapsto (R, S, T)$, be the function associated to the above transformation. Thus, $\vec{\Phi}(\vec{x}) = M_{\vec{\Phi}}\vec{x}$ where $M_{\vec{\Phi}} =$

$$\begin{bmatrix} 2tq & bt & m \\ \sqrt{q} & \frac{b}{2\sqrt{2q}} & 0 \\ 0 & \frac{\sqrt{7m}}{2\sqrt{q}} & 0 \end{bmatrix}.$$

We see that $\det(M_{\vec{\Phi}}) = \frac{\sqrt{7}m^{3/2}}{2}$. Since Ω is a convex symmetric body, $\vec{\Phi}^{-1}(\Omega)$ is as well. It follows that

$$vol(\vec{\Phi}^{-1}(\Omega)) = \frac{vol(\Omega)}{|\det(M_{\vec{\Phi}})|} = \frac{16\sqrt{2}\pi}{3\sqrt{7}} > 8.$$

Minkowski's theorem on convex symmetric bodies guarantees that there exist $x_1, y_1, z_1 \in \mathbb{Z}$, not all zero, with $\vec{\Phi}(x_1, y_1, z_1) \in \Omega$. Let $(R_1, S_1, T_1) := \vec{\Phi}(x_1, y_1, z_1)$. We see that

$$\begin{aligned} R_1^2 + S_1^2 + T_1^2 &\equiv (2tqx_1 + bty_1)^2 + (\sqrt{q}x_1 + \frac{by_1}{2\sqrt{q}})^2 + (\frac{\sqrt{7m}y_1}{2\sqrt{q}})^2 \\ &\equiv t^2(2qx_1 + by_1)^2 + \frac{1}{4q}((2qx_1 + by_1)^2 + 7my_1^2) \\ &\equiv t^2(2qx_1 + by_1)^2 + \frac{1}{4q}(2qx_1 + by_1)^2 \\ &\equiv 0 \pmod{m}, \end{aligned}$$

and that

$$\begin{aligned} S_1^2 + T_1^2 &= \frac{1}{4q}(4q^2x_1^2 + 4qbx_1y_1 + (b^2 + 7m)y_1^2) \\ &= \frac{1}{4q}(4q^2x_1^2 + 4qbx_1y_1 + 4qhy_1^2) \\ &= qx_1^2 + bx_1y_1 + hy_1^2. \end{aligned}$$

Thus $S_1^2 + T_1^2 \in \mathbb{Z}$ and, as before, we conclude $R_1^2 + S_1^2 + T_1^2 = m$. Since $R_1 \in \mathbb{Z}$ we wish to show $S_1^2 + T_1^2$ is of the form $a^2 + 7b^2$ for some $a, b \in \mathbb{Z}$. It will be sufficient to show that $\left(\frac{-7}{p}\right) = 1$ for all primes p dividing $S_1^2 + T_1^2$ to an odd power [2].

Note that $p \leq m < q$, so we can assume $p \neq q$. Furthermore, if $2|S_1^2 + T_1^2 = qx_1^2 + bx_1y_1 + hy_1^2$ then $2|x, y$ (since h and b are odd), thus 2 divides $S_1^2 + T_1^2$ to an even power and so we need not consider $p = 2$. We also need not consider $p = 7$, as the form $x^2 + 7y^2$ represents 7 and is multiplicative. As a result it will suffice to show $\left(\frac{-7}{p}\right) = 1$ for all primes $p|v$, where $p \neq 2, 7, q$ and $v := 4q(S_1^2 + T_1^2)$. We proceed in two cases.

`Case 1` $p \nmid m$: We see that $(2qx_1 + by_1)^2 \equiv -7my_1^2 \pmod{p}$ and $m \equiv {R_1}^2 \pmod{p}$. It follows that $\left(\frac{-7}{p}\right) = \left(\frac{m}{p}\right) = 1$.

`Case 2` $p|m$: Note that since m is assumed squarefree, $p \nmid \frac{m}{p}$. Thus, $R_1^2 \equiv 0 \pmod{p}$ and so $p|R_1$. Additionally, $(2qx_1 + by_1)^2 + 7my_1^2 \equiv (2qx_1 + by_1)^2 \equiv 0 \pmod{p}$ so $p|(2qx_1 + by_1)$. We now see that $\frac{R_1^2}{p} + \frac{1}{4q}(\frac{(2qx_1+by_1)^2}{p} + 7\frac{m}{p}y_1^2) = \frac{m}{p}$. Thus $\frac{1}{4q}(7\frac{m}{p}y_1^2) \equiv \frac{m}{p} \pmod{p}$. It follows that $-7y_1^2 \equiv -4q \pmod{p}$. By the construction of q, $\left(\frac{-7}{p}\right) = \left(\frac{-q}{p}\right) = 1$.

In both cases we see $\left(\frac{-7}{p}\right) = 1$. Thus there exist $a, b \in \mathbb{Z}$ such that $m = a^2 + 7b^2$. Therefore, m is represented by $x^2 + y^2 + 7z^2$, as required.

This completes the proof of Theorem 3(a).

The proof of Theorem 3(b) follows the above proof; however, we take q to be an odd prime such that $q > m$, $q \equiv 1 \pmod{12}$, and $\left(\frac{-q}{p}\right) = 1$ for all primes $p|m$. It follows that

$$1 = \prod_{p|m}\left(\frac{-q}{p}\right) = \left(\frac{-1}{m}\right)\prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{q}{p}\right) = \prod_{p|m}\left(\frac{p}{q}\right) = \left(\frac{m}{q}\right) = \left(\frac{-3m}{q}\right)$$

and we take the following transformation

$$\begin{aligned} R &= 2tqx + bty + mz \\ S &= \sqrt{q}x + \tfrac{b}{2\sqrt{q}}y \\ T &= \tfrac{\sqrt{3m}}{2\sqrt{q}}y. \end{aligned}$$

This completes the proof of Theorem 3. □

Acknowledgement: This research was supported by the National Science Foundation (DMS-1461189). I would additionally like to thank Dr. Katherine Thompson, Dr. Jeremy Rouse, Dr. Pete Clark, Sarah Blackwell and Tiffany Treece for their support. I would finally like to thank Dr. Theodore Shifrin for his guidance over the last three years and his decades of service to the University of Georgia and its students.

References

[1] N.C. Ankeny. Sums of three squares, *Proceedings of the American Mathematical Society* **8** (1957), 316-319.

[2] P.L. Clark, J. Hicks, H. Parshall, and K. Thompson. GoNI: Primes represented by binary quadratic forms, *Integers* **13** (2013), A37, 18pp.

[3] B. Jones. The regularity of a genus of positive ternary quadratic forms, *Trans. Amer. Math. Soc.* **33** (1931), 111-124.

[4] I. Kaplansky. The first nontrivial genus of positive definite ternary forms, *Mathematics of Computation* **64** (1995), 341-345.

[5] X. Wang and D. Pei. Eisenstein series of 3/2 weight and one conjecture of Kaplansky, *Sci. China Ser. A* **44** (2001) *no.* 10, 1278-1283.