Amir Jafari; Farhood Rostamkhani
On ternary quadratic forms over the rational numbers

Czechoslovak Mathematical Journal, Vol. 72 (2022), No. 4, 1105–1119

Persistent URL: http://dml.cz/dmlcz/151133

Czechoslovak Mathematical Journal, 72 (147) (2022), 1105–1119

ON TERNARY QUADRATIC FORMS OVER THE RATIONAL NUMBERS

Amir Jafari, Farhood Rostamkhani, Tehran

Received September 26, 2021. Published online October 7, 2022.

Abstract. For a ternary quadratic form over the rational numbers, we characterize the set of rational numbers represented by that form over the rational numbers. Consequently, we reprove the classical fact that any positive definite integral ternary quadratic form must fail to represent infinitely many positive integers over the rational numbers. Our proof uses only the quadratic reciprocity law and the Hasse-Minkowski theorem, and is elementary.

Keywords: ternary quadratic forms; Gauss reciprocity law; Hasse-Minkowski theorem

MSC 2020: 11A15, 11D09

1. Introduction

It is a well-known theorem of Lagrange that any positive integer is a sum of at most four squares. In other words, the quadratic form $x^2+y^2+z^2+t^2$ represents any positive integer over the integers. However, the quadratic form $x^2+y^2+z^2$ cannot represent any number of the form $8k+7$ even when we allow x, y, and z to be rational numbers. One may wonder if $ax^2+by^2+cz^2$ for some carefully chosen positive integers a, b, and c will represent all positive integers that are large enough over the integers. Indeed, if we allow having negative coefficients, then a ternary quadratic form such as $x^2+y^2-z^2$ can represent any integer over the integers since for an integer n, we have

$$(n+1)^2+0^2-n^2=2n+1, \quad n^2+1^2-(n-1)^2=2n.$$

However, it is a classical result that any positive definite integral ternary quadratic form must fail to represent infinitely many positive integers even over the rationals, see [2], page 142.

DOI: 10.21136/CMJ.2022.0359-21

One of the aims of this note is to characterize all rational numbers represented by a rational ternary quadratic form over the rationals. For nonzero rational numbers a, b and c let us denote by $R(a,b,c)$ the set of rational numbers represented by $ax^2 + by^2 + cz^2$ over the rational numbers. The following theorem determines this set in the case when a, b, and c are square-free pairwise relatively prime nonzero integers. The more general case is explained after the statement of the theorem. The symbol $\left(\frac{\cdot}{p}\right)$ denotes Legendre's symbol.

Theorem 1.1. *Let a, b and c be square-free and pairwise relatively prime nonzero integers, let N be a nonzero rational number, and let $N = nn_0^2$, where n is a uniquely determined square-free integer and n_0 is a rational number uniquely determined up to a sign. Then, $N \in R(a,b,c)$ if and only if the following conditions hold.*

(1) *If a, b and c are positive (or negative) then n is positive (or negative, respectively).*

(2) *If $a \equiv b \equiv c \equiv 1$ or $3 \pmod 4$ then $n \not\equiv -abc \pmod 8$.*

(3) *If a is even and $b + c \equiv a$ or $2a \pmod 8$ then $n \not\equiv -abc \pmod{16}$. Similarly, if b is even and $a + c \equiv b$ or $2b \pmod 8$ then $n \not\equiv -abc \pmod{16}$. Finally, if c is even and $a + b \equiv c$ or $2c \pmod 8$ then $n \not\equiv -abc \pmod{16}$.*

(4) *If p is an odd prime divisor of n and a then $(\frac{-bc}{p}) = 1$ or $(\frac{na/p^2}{p}) = 1$. Similarly, if p is an odd prime divisor of n and b then $(\frac{-ac}{p}) = 1$ or $(\frac{nb/p^2}{p}) = 1$. Finally, if p is an odd prime factor of n and c then $(\frac{nc/p^2}{p}) = 1$ or $(\frac{-ab}{p}) = 1$.*

We prove this theorem in Section 2 using the Hasse-Minkowski theorem and a delicate analysis of the congruence classes represented by $ax^2+by^2+cz^2$ modulo powers of 2 and powers of odd prime numbers.

In fact, Theorem 1.1 can be used to determine the set of all rational numbers represented by any rational ternary quadratic form over the rational numbers. Indeed, any rational ternary quadratic form $Q(x,y,z)$ can be transformed into a diagonal rational ternary quadratic form $ax^2+by^2+cz^2$ by a linear change of variables with rational coefficients, see [11], Chapter 1, Section 3. Since $Q(x,y,z)$ and $ax^2+by^2+cz^2$ represent the same rational numbers over the rationals, hence we need to determine $R(a,b,c)$. To do this, find unique positive rational numbers r, s, and t such that $a = r^2a_1$, $b = s^2b_1$, and $c = t^2c_1$, where a_1, b_1, and c_1 are square-free integers. Also, let d be the greatest common divisor of a_1, b_1, and c_1 and write $a_1 = da_2$, $b_1 = db_2$, and $c_1 = dc_2$. It is clear that

$$R(a,b,c) = R(a_1,b_1,c_1) = dR(a_2,b_2,c_2).$$

Finally, let d_1 (or d_2 or d_3) be the greatest common divisors of b_2 and c_2 (or a_2 and c_2 or a_2 and b_2, respectively). Therefore, one can find integers a_3, b_3, and c_3

such that $a_2 = d_2d_3a_3$, $b_2 = d_1d_3b_3$, and $c_2 = d_1d_2c_3$. Hence,

$$R(a_2, b_2, c_2) = d_1d_2d_3R(d_1a_3, d_2b_3, d_3c_3).$$

So, we have the formula

$$R(a, b, c) = dd_1d_2d_3R(d_1a_3, d_2b_3, d_3c_3). \tag{1.1}$$

Note that d_1a_3, d_2b_3 and d_3c_3 are square-free pairwise relatively prime nonzero integers. So, Theorem 1.1 can be used to determine $R(d_1a_3, d_2b_3, d_3c_3)$ and formula (1.1) will determine all rational numbers represented by $Q(x, y, z)$ over the rationals.

As a corollary to Theorem 1, we can extend the following result of Doyle and Williams, see [5], Theorem 1.

Theorem 1.2 (Doyle-Williams)**.** *Let $a, b, c \in \mathbb{N}$. Then the ternary form $ax^2 + by^2 + cz^2$ does not represent over the integers any positive integer $\equiv -4abc \pmod{32(abc)^2}$.*

Using the notation introduced after the statement of Theorem 1.1, we present the following theorem that generalizes the Doyle-Williams theorem.

Theorem 1.3. *Let a, b and c be positive rational numbers and $abc = R^2S$, where S is a uniquely determined square-free integer and R is a rational number uniquely determined up to a sign. Then the ternary form $ax^2 + by^2 + cz^2$ does not represent any positive integer congruent to $-S \pmod{8d_1d_2d_3S^2}$ over the rationals. In particular, if a, b and c are integers then $ax^2+by^2+cz^2$ does not represent any positive integer congruent to $-abc \pmod{8abcS}$ over the rationals and more particularly it does not represent any number $\equiv -abc \pmod{8(abc)^2}$ over the rationals.*

As a consequence of Theorem 1.3 and the fact that any rational ternary quadratic form is equivalent to a rational diagonal quadratic form, we can state the following version of the classical result mentioned in [2], page 142.

Theorem 1.4. *Any positive definite ternary quadratic form over the rational numbers fails to represent an infinite progression of positive integers over the rational numbers.*

We also prove an assertion in the converse direction of the Doyle-Williams theorem. Namely, we prove the following.

Theorem 1.5. *Let a, b and c be square-free and pairwise relatively prime nonzero integers. Then the form $ax^2 + by^2 + cz^2$ represents all integers over the integers if and only if the congruence*

$$ax^2 + by^2 + cz^2 \equiv -abc \pmod{8(abc)^2}$$

is solvable.

The history of the problems studied in this article is very rich. It was Fermat, who in 1638 first stated without proof that any number is a sum of at most four squares. After some unsuccessful tries by Euler, Lagrange proved it in 1770. Gauss proved in 1796 another conjecture of Fermat that any number is a sum of at most three triangular numbers (i.e., numbers of the form $\frac{1}{2}n(n+1)$) by showing that the only numbers not represented by $x^2+y^2+z^2$ over the integers are of the form $4^m(8k+7)$. He published this result in his famous Disquisitiones Arithmeticae in 1801. In 1748, Euler conjectured that the ternary quadratic form $x^2+y^2+2z^2$ represents every odd integer over the integers and Lebesgue in 1857 in Théorème 1 of [12] proved this conjecture. Dickson in [4], Theorems X and VII in 1927 showed that the forms $x^2+2y^2+3z^2$ and $x^2+2y^2+4z^2$ also represent all odd integers over the integers. In 1995 Kaplansky in [10], page 212 gave a list of 23 integral positive definite ternary quadratic forms that he claimed to be the only such forms (up to equivalence) that represent all odd integers over the integers. He showed the validity of his claim for 19 of these forms. Interestingly, the three forms found by Euler and Dickson were the only diagonal ternary quadratic forms in this list. Another interesting historical result is due to Ramanujan. In 1916, he wrote a paper (see [17], page 220), in which, among other things, he studied the ternary form $x^2+y^2+10z^2$. He showed that the only even numbers not represented by this form over the integers are of the form $4^m(16k+6)$, and observed the following list of odd numbers are not represented over the integers

$$3,\ 7,\ 21,\ 31,\ 33,\ 43,\ 67,\ 79,\ 87,\ 133,\ 217,\ 219,\ 223,\ 253,\ 307,\ 391,\ \ldots$$

He mentioned that they do not seem to follow any simple law. It is not clear if Ramanujan believed this list was complete or not or if the set was finite or infinite. In 1927 Jones and Pall in [9], page 168 showed that 679 is in the list as well. In 1941 Gupta in [8], page 519 found that 2719 is also in the list. Computer searches for numbers up to 2×10^{10} have not produced any new odd numbers. It was proved in 1990 by Duke and Schulze-Pillot in [6], page 56 that $x^2+y^2+10z^2$ represents all large enough odd integers, and hence this list is finite. Also, in 1997 Ono and Soundararajan in [16], page 416 conjectured that Ramanujan's list with the two extra numbers 679 and 2719 is complete. They showed the validity of their conjecture, assuming the generalized Riemann hypothesis.

The study of representability over the integers by ternary quadratic forms is a very active research theme. For example, besides odd numbers, one may be tempted to study other arithmetic progressions $dk+r$ for $k \in \{0,1,\ldots\}$. A form representing all numbers in this progression over the integers is called (d,r)*-universal*. Sun in [19], Theorem 1.7 proved that the forms $x^2+3y^2+24z^2$, $4x^2+3y^2+6z^2$, and $x^2+12y^2+6z^2$ are $(6,1)$-universal. In [20], Theorems 1.1 and 1.2 Wu and Sun were able to show that $2x^2+3y^2+10z^2$ is $(8,5)$-universal. Also, they showed that $x^2+3y^2+14z^2$ and $2x^2+3y^2+7z^2$ are $(14,7)$-universal.

According to [5], page 2, we do not know who was the first person to state that integral positive definite ternary quadratic forms must fail to represent infinitely many positive integers over the rationals. This statement goes back to at least 1933 when Albert (see [1], page 275) states it and also in Conway's beautiful book (see [2], page 142), where he gives a modern proof using p-adic equivalence of forms and isotropic forms. Finally, we mention two papers by Mordell (see [14], [15]) that study the solvability of the equation $ax^2+by^2+cz^2+dt^2=0$ when x, y, z and t are integers not all equal to zero. As this is related to the representability of an integer by $ax^2+by^2+cz^2$ over the rationals, some of his results overlap ours.

2. Proofs

In this section, we prove the results of the introduction. First, we state the following important lemma.

Lemma 2.1. *Let a, b and c be positive square-free pairwise relatively prime integers. If for all odd prime factors p of a, we have $(\frac{-bc}{p})=1$ and similarly, for all odd prime factors p' of b, we have $(\frac{-ac}{p'})=1$ and finally, for all prime factors p'' of c, we have $(\frac{-ab}{p''})=1$, then the conditions of parts* (2) *or* (3) *of Theorem* 1.1 *hold for a, b and c.*

Proof. The proof uses quadratic reciprocity for the Jacobi symbol

$$\Bigl(\frac{m}{n}\Bigr)=\prod_i\Bigl(\frac{m}{p_i}\Bigr)^{e_i},$$

where $n=p_1^{e_1}\ldots p_k^{e_k}$ is an odd number. We use the following well-known facts, see [7], Chapter 3.8.

$$(2.1)\quad \Bigl(\frac{-1}{n}\Bigr)=(-1)^{(n-1)/2},\quad \Bigl(\frac{2}{n}\Bigr)=(-1)^{(n^2-1)/8}\quad \text{when } n \text{ is odd.}$$

$$(2.2)\quad \Bigl(\frac{n}{m}\Bigr)\Bigl(\frac{m}{n}\Bigr)=(-1)^{((n-1)/2)(m-1)/2}\quad \text{when } n,\ m \text{ are odd and } (m,n)=1.$$

$$(2.3)\quad \Bigl(\frac{mm'}{n}\Bigr)=\Bigl(\frac{m}{n}\Bigr)\Bigl(\frac{m'}{n}\Bigr)\quad \text{when } n \text{ is odd.}$$

First assume that a, b and c are odd integers. By definition of the Jacobi symbol we have $(\frac{-bc}{a}) = \prod_{p|a}(\frac{-bc}{p}) = 1$. Similarly we have $(\frac{-ac}{b}) = (\frac{-ab}{c}) = 1$. Hence, if we use equation (2.3) and write these as

$$\Big(\frac{-1}{a}\Big)\Big(\frac{b}{a}\Big)\Big(\frac{c}{a}\Big) = 1, \quad \Big(\frac{-1}{b}\Big)\Big(\frac{a}{b}\Big)\Big(\frac{c}{b}\Big) = 1, \quad \Big(\frac{-1}{c}\Big)\Big(\frac{a}{c}\Big)\Big(\frac{b}{c}\Big) = 1,$$

and take the product of the three expressions and use equation (2.1) and the reciprocity law of equation (2.2) above, we get

$$(-1)^{\alpha+\beta+\gamma+\alpha\beta+\beta\gamma+\alpha\gamma} = 1, \tag{2.4}$$

where $\alpha = \frac{1}{2}(a-1)$, $\beta = \frac{1}{2}(b-1)$ and $\gamma = \frac{1}{2}(c-1)$. This implies that α, β, and γ have the same parity since if, for example, α is even and β is odd, the exponent in equation (2.4) is congruent to 1 modulo 2. Hence, $a \equiv b \equiv c \pmod 4$. It remains to prove the lemma when exactly one of a, b or c is even. So, let us assume that $a = 2a'$, where a' is an odd number. Then using equation (2.3), we have

$$\Big(\frac{-1}{a'}\Big)\Big(\frac{b}{a'}\Big)\Big(\frac{c}{a'}\Big) = 1, \quad \Big(\frac{-1}{b}\Big)\Big(\frac{2}{b}\Big)\Big(\frac{a'}{b}\Big)\Big(\frac{c}{b}\Big) = 1, \quad \text{and} \quad \Big(\frac{-1}{c}\Big)\Big(\frac{2}{c}\Big)\Big(\frac{a'}{c}\Big)\Big(\frac{b}{c}\Big) = 1.$$

So if we let $\alpha = \frac{1}{2}(a'-1)$, $\beta = \frac{1}{2}(b-1)$, $\gamma = \frac{1}{2}(c-1)$, $\beta' = \frac{1}{8}(b^2-1)$ and $\gamma' = \frac{1}{8}(c^2-1)$, it follows by multiplying this expressions and using the properties of the Jacobi symbol that

$$(-1)^{\alpha\beta+\alpha\gamma+\beta\gamma+\alpha+\beta+\gamma+\beta'+\gamma'} = 1.$$

Equivalently

$$8\alpha\beta + 8\alpha\gamma + 8\beta\gamma + 8\alpha + 8\beta + 8\gamma + 8\beta' + 8\gamma' = (a'+b+c)^2 - (a')^2 - 8$$

must be divisible by 16. This implies that $(b+c)(b+c+2a') = (b+c)(b+c+a)$ is divisible by 8 and not by 16. Since b and c are odd hence, $b+c \equiv 0, a, 2a$ or $3a \pmod 8$. Since $(b+c)(b+c+a)$ is divisible by 16 when $b+c \equiv 0$ or $3a \pmod 8$, this finishes the proof. □

In the following, we use the Hasse-Minkowski theorem (see [18], Chapter IV, Theorem 8) to prove Theorem 1.1. For an integral diagonal ternary quadratic form $ax^2+by^2+cz^2$, the Hasse-Minkowski theorem asserts that for an integer n the equation $ax^2+by^2+cz^2 = n$ has a solution in rational numbers if and only if it has a solution in real numbers and for any prime power p^m the congruence $ax^2+by^2+cz^2 \equiv n \pmod{p^m}$ has a solution in integers. This version of the Hasse-Minkowski theorem was essentially proved by Legendre, see [13].

The following two lemmas characterize numbers represented modulo 8 or 16 by $ax^2+by^2+cz^2$.

Lemma 2.2. *Let a, b and c be square-free pairwise relatively prime integers. Then the ternary quadratic form $ax^2 + by^2 + cz^2 \pmod 8$ represents all congruence classes $\pmod 8$ unless $a \equiv b \equiv c \pmod 4$, in which case the only congruence class that is not represented is $-abc \pmod 8$.*

Proof. We consider three cases.

Case 1: If one of the coefficients a, b or c is even, for example $a \equiv 2 \pmod 4$, then since the square of any number is $\equiv 0$ or $1 \pmod 4$, one sees that $ax^2 + by^2 \pmod 4$ represents all congruence classes $\pmod 4$. Note that $4c \equiv 4 \pmod 8$. So if $ax^2 + by^2$ represents $n \pmod 8$ then $ax^2 + by^2 + 4c$ represents $n + 4 \pmod 8$ and hence all congruence classes $\pmod 8$ are represented in this case.

Case 2: If $a \equiv b \equiv c \pmod 4$, then without loss of generality we may assume that our form is one of the two ternary quadratic forms $a(x^2+y^2+z^2)$ or $a(x^2+y^2+5z^2)$. They represent all congruence classes modulo 8 except $-a \pmod 8$ and $-5a \pmod 8$, respectively, which are the same as $-abc \pmod 8$ in each case.

Case 3: If all the coefficients are odd and two of them, for example, a and b, are not congruent modulo 4, then clearly $ax^2+by^2 \pmod 4$ represents 1 and 3 $\pmod 4$ and in this representation one of x or y is even. If we replace the even variable, for example x, with $x + 2$, we see that this form represents $1, 3, 5$ and $7 \pmod 8$. Since c is odd letting $z = 1$, we see that $ax^2 + by^2 + c$ represents $0, 2, 4, 6 \pmod 8$. Hence, all congruence classes modulo 8 are represented. □

Lemma 2.3. *Let a, b and c be square-free pairwise relatively prime integers and one of them be even. The ternary quadratic form $Q(x, y, z) = ax^2 + by^2 + cz^2 \pmod{16}$ represents all congruence classes unless a (possibly b, possibly c) is even and $b + c \equiv a$ or $2a \pmod 8$ (possibly $a + c \equiv b$ or $2b \pmod 8$, possibly $a + b \equiv c$ or $2c \pmod 8$, respectively), in which case the only congruence class that is not represented is $-abc \pmod{16}$.*

Proof. Without loss of generality, we may assume that $a = 2a'$ is even and since a is square-free hence, a' is odd. First, we show that $n \pmod{16}$ is represented by $ax^2 + by^2 + cz^2$ for any odd integer n. By Lemma 2.2, one can find x_0, y_0 and z_0 such that $ax_0^2 + by_0^2 + cz_0^2 \equiv n \pmod 8$. Since n is odd, one of y_0 or z_0 is odd. Assume for example that y_0 is odd, then $9by_0^2 \equiv by_0^2 + 8 \pmod{16}$. Hence, replacing y_0 with $3y_0$, if needed, we may represent $n \pmod{16}$. Since $a' \pmod{16}$ and $3a' \pmod{16}$ are represented, hence replacing x, y and z with $2x$, $2y$ and $2z$ one can represent $4a'$ and $12a'$ that is $2a$ and $6a$ modulo 16. Also clearly 0, a and $4a$ are represented. The only congruence classes modulo 16 that remain are $3a, 5a$ and $7a$. Depending on the congruence of $b + c$ modulo 8, we have four cases.

Case 1: If $b+c\equiv 0 \pmod 8$ then $b\not\equiv c \pmod 4$, that is one of them is congruent to a' (mod 4) and the other one to $3a'$ (mod 4). Hence, $Q(1,2,0)=a+4b$ and $Q(1,0,2)=a+4c$ are $3a$ and $7a$ modulo 16. If $b+c\equiv 4a \pmod{16}$ then $Q(1,1,1)\equiv 5a \pmod{16}$ and if $b+c\equiv 0 \pmod{16}$ then $9b+c\equiv 8\equiv 4a \pmod{16}$ and therefore, $Q(1,3,1)\equiv 5a \pmod{16}$. So in this case all congruence classes modulo 16 are represented.

Case 2: If $b+c\equiv 3a \pmod 8$ then $Q(0,1,1)=b+c$ and $Q(0,3,1)=9b+c\equiv b+c+8 \pmod{16}$ are $3a$ and $7a$ (mod 16). Also $Q(1,2,2)=a+4(b+c)\equiv 13a\equiv 5a$ (mod 16). Again all congruence classes modulo 16 are represented.

Case 3: If $b+c\equiv 2a\equiv 4 \pmod 8$ then since b and c are odd it follows that $bc\equiv 3 \pmod 8$ and hence $-abc\equiv -3a\equiv 5a \pmod{16}$. So we need to show that $3a$ and $7a$ are represented modulo 16 but $5a$ is not. Note that $Q(1,1,1)=a+b+c$ and $Q(1,3,1)=a+9b+c\equiv a+b+c+8 \pmod{16}$. These are $3a$ and $7a$ (mod 16). The only even congruence classes modulo 16 that are represented by by^2+cz^2 are 0, $4b$, $4c$, $4(b+c)$, $b+c$ and $b+c+8\equiv b+c+4a \pmod{16}$, so if $Q(x,y,z)\equiv 5a \pmod{16}$, since $ax^2\equiv 0, a$ or $4a$ (mod 16), hence $by^2+cz^2\equiv 5a, 4a$ or a (mod 16). Comparing with the possible even congruence values of by^2+cz^2 shows that this is impossible.

Case 4: If $b+c\equiv a \pmod 8$ then we have two subcases.

Subcase 4.1: If $b\equiv c\equiv a' \pmod 4$ then either $b\equiv c\equiv a' \pmod 8$ or $a\equiv b\equiv 5a' \pmod 8$, in both cases $bc\equiv 1 \pmod 8$ and hence $-abc\equiv 7a \pmod{16}$. Hence, we need to show that $Q(x,y,z)$ represents $3a$ and $5a$ (mod 16) but it does not represent $7a$ (mod 16). Note that $Q(1,2,2)=a+4b+4c\equiv 5a \pmod{16}$ and $Q(1,2,0)=a+4b\equiv a+4a'=3a \pmod{16}$. If $Q(x,y,z)\equiv 7a \pmod{16}$ then $by^2+cz^2\equiv 7a$, $6a$ or $3a$ (mod 16). Note that $4b\equiv 4c\equiv 2a \pmod{16}$. Hence, the even congruence classes of by^2+cz^2 listed in Case 3 cannot represent $7a$, $6a$ or $3a$ (mod 16).

Subcase 4.2: If $b\equiv c\equiv 3a' \pmod 4$ then one of them is congruent to $3a'$ and the other one is congruent to $5a'$ modulo 8 so $bc\equiv 5 \pmod 8$ and hence $-abc\equiv -5a\equiv 3a \pmod{16}$. Hence, we need to show that $Q(x,y,z)$ represents $5a$ and $7a$ (mod 16) but it does not represent $3a$ (mod 16). Note that $Q(1,2,2)=a+4b+4c\equiv 5a$ (mod 16), $Q(1,2,0)=a+4b\equiv a+12a'=7a \pmod{16}$. If $Q(x,y,z)\equiv 3a \pmod{16}$ then $by^2+cz^2\equiv 3a$, $2a$ or $7a$ (mod 16). Note that $4b\equiv 4c\equiv 6a \pmod{16}$. Hence, the even congruence classes of by^2+cz^2 listed in Case 3 cannot represent $3a$, $2a$ or $7a$ (mod 16). □

In Lemmas 2.4 and 2.5, we classify all the congruence classes modulo 2^m for $m\geqslant 3$ when the coefficients a, b and c are odd and modulo 2^m for $m\geqslant 4$ when one of a, b or c is even, that are represented by $ax^2+by^2+cz^2$.

Lemma 2.4. *If a, b and c are odd pairwise relatively prime and square-free integers and an integer n is represented by $ax^2+by^2+cz^2 \pmod 8$ then it is represented $\pmod{2^m}$ for any $m \geqslant 3$.*

Proof. It is enough to show this for the case, where n is not divisible by 4, since we can replace x, y and z by 2^lx, 2^ly and 2^lz for some l. We prove the claim by induction on m. Suppose that we can find x, y, z such that $ax^2+by^2+cz^2=n+k2^m$ for $m \geqslant 3$. Since n is not a multiple of 4 hence at least one of x, y or z is odd. Without loss of generality, we can assume that x is odd. Put $x'=x+k_1 2^{m-1}$. Then

$$a(x')^2+by^2+cz^2=n+k2^m+2^m ak_1x+ak_1^2 2^{2m-2}.$$

Since $2m-2 \geqslant m+1$, we only need to take $k_1=k$ to make the induction work. □

Lemma 2.5. *Let a, b and c be square-free pairwise relatively prime integers. If one of a, b or c is even and an integer n is represented by $ax^2+by^2+cz^2 \pmod{16}$ then it is represented $\pmod{2^m}$ for any $m \geqslant 4$.*

Proof. As in the previous part, we may assume that n is not divisible by 4. Assume $ax^2+by^2+cz^2=n+k2^m$ for some $m \geqslant 4$. Since n is not a multiple of 4 one of x, y or z is odd. Assume x is odd. If a is odd as well, then the same proof as before makes the induction work. Assume $a=2a'$, where a' is an odd integer. Let $x'=x+k_1 2^{m-2}$ then

$$a(x')^2+by^2+cz^2=n+k2^m+2^m a'k_1x+a'k_1^2 2^{2m-3}.$$

Since $2m-3 \geqslant m+1$, we only need to take $k_1=k$ to make the induction work. □

We summarize the previous lemmas in the following corollary that will be used in the proof of Theorem 1.1.

Corollary 2.6. *Let a, b and c be square-free pairwise relatively prime integers. A number n is represented by $ax^2+by^2+cz^2$ modulo all powers of 2 if and only:*

(1) *if a, b and c are odd and $a \equiv b \equiv c \pmod 4$ then $n \not\equiv -abc \pmod 8$.*

(2) *if a (possibly b, possibly c) is even and $b+c \equiv a$ or $2a \pmod 8$ (possibly $a+c \equiv b$ or $2b \pmod 8$, possibly $a+b \equiv c$ or $2c \pmod 8$, respectively) then $n \not\equiv -abc \pmod{16}$.*

Proof. It follows directly from Lemmas 2.2, 2.3, 2.4 and 2.5. □

Lemma 2.7. *If p is an odd prime number that does not divide bc, then any integer n prime to p is represented by $ax^2+by^2+cz^2 \pmod{p^m}$ for any $m \geqslant 1$. If p does not divide a, then all numbers are represented modulo p^m.*

Proof. We prove this by induction on $m = 1$. Let n be an integer which is not divisible by p. Since the classes of by^2 and $n - cz^2$ modulo p are each of size $\frac{1}{2}(p+1)$ so they intersect and hence one can find y and z not both divisible by p (since n is prime to p) such that $by^2 + cz^2 \equiv n \pmod{p}$. Suppose that we have y and z not both multiples of p, such that $by^2 + cz^2 = n + kp^m$ for $m \geqslant 1$ and some integer k. Without loss of generality, we assume that y is not a multiple of p. Let $y' = y + k_1 p^m$. Then

$$b(y')^2 + cz^2 = n + kp^m + 2byk_1p^m + bk_1^2p^{2m}.$$

Since $2m \geqslant m + 1$, we need to take $k_1 = -(2by)^{-1}k \pmod{p}$ for the induction to work. So we even showed that $by^2 + cz^2 \pmod{p^m}$ represents all integers that are prime to p. If p does not divide a and n is a multiple of p then $n - a$ is prime to p and is therefore, represented by $by^2 + cz^2 \pmod{p^m}$. Hence, if we let $x = 1$ we have $n \equiv a + by^2 + cz^2 \pmod{p^m}$. □

Lemma 2.8. *If p is an odd prime number that divides a then for any integer n prime to p, np is represented by $ax^2 + by^2 + cz^2 \pmod{p^m}$ for any $m \geqslant 1$, unless $(\frac{-bc}{p}) = (\frac{na/p}{p}) = -1$, where it is not represented $\pmod{p^2}$.*

Proof. Note that if $(\frac{-bc}{p}) = 1$ then $by^2 + cz^2 \equiv np \equiv 0 \pmod{p}$ has a solution (y, z) such that not both y and z are divisible by p, so the above proof works again. If $(\frac{na/p}{p}) = 1$, let $a = pa'$, then we can find z such that $a'x^2 \equiv n \pmod{p}$ or $ax^2 \equiv np \pmod{p^2}$. Suppose that $ax^2 = np + kp^m$ for some $m \geqslant 2$ and k. Then since n is prime to p, x is also prime to p. Let $x' = x + k_1p^{m-1}$, then

$$a(x')^2 = np + kp^m + 2a'xk_1p^m + k_1^2a'p^{2m-1}.$$

Since $2m - 1 \geqslant m + 1$, it is enough to take $k_1 \equiv -(2a'x)^{-1}k \pmod{p}$ for the induction to work. So, even ax^2 alone represents np modulo p^m. We now show that if $(\frac{-bc}{p}) = (\frac{-na/p}{p}) = -1$ then np is not represented modulo p^2. In contrary, assume that for integers x, y and z, we have

$$ax^2 + by^2 + cz^2 \equiv np \pmod{p^2}.$$

If y or z is not divisible by p, then by considering the above equation modulo p, it follows that $-bc$ is a quadratic residue modulo p, contrary to the assumption. So y and z are divisible by p. Simplifying the equation, it follows that

$$\frac{a}{p}x^2 \equiv n \pmod{p}.$$

Therefore, na/p is a quadratic residue modulo p, again contrary to the assumption. □

Corollary 2.9. *A number n is represented by $ax^2 + by^2 + cz^2$ modulo all powers of an odd prime number p unless $p \mid n$ and p divides a (or b, or c) and $(\frac{-bc}{p}) = (\frac{na/p^2}{p}) = -1$ (or $(\frac{-ac}{p}) = (\frac{nb/p^2}{p}) = -1$, or $(\frac{-ab}{p}) = (\frac{nc/p^2}{p}) = -1$, respectively) in which case n is not represented modulo p^2.*

Proof. It follows directly from Lemmas 2.7 and 2.8. □

Now, we prove Theorem 1.1.

Proof of Theorem 1.1. Note that N is represented over the rationals by $ax^2 + by^2 + cz^2$ if and only if n is represented by the rationals. Because, it is enough to replace x, y and z with n_0x, n_0y and n_0z. Condition (1) is equivalent to the representability over the real numbers. Conditions (2) and (3) are equivalent to the representability modulo powers of 2 according to Corollary 2.6. Finally, Condition (4) is equivalent to the representability modulo powers of odd primes according to Corollary 2.9. So by the Hasse-Minkowski theorem, our proof is complete. □

Example 2.10. For instance, consider the Ramanujan ternary form $x^2 + y^2 + 10z^2$. Since $(\frac{-1}{5}) = 1$ and $a + b \equiv c \pmod 8$, i.e., $2 \equiv 10 \pmod 8$, the only positive numbers up to a square factor not represented over the rational numbers are those $\equiv -10 \pmod{16}$. That is numbers of the form $16k + 6$. If we take the square factor into the account, the only positive integers not represented by this form are of the form $l^2(16k + 6)$. If we write $l = 2^m r$ for some odd number r and a nonnegative integer m then numbers of the form $4^m(16k + 6)r^2$ are the only positive integers not represented by this form over the rationals. But since $r^2 \equiv 1$ or $9 \pmod{16}$, hence $(16k+6)r^2$ is of the form $16k' + 6$. Therefore, the only positive integers not represented by this form are of the form $4^m(16k' + 6)$ for some integer k'. This is different from representing numbers over integers. It was mentioned in the introduction that without assuming the generalized Riemann hypothesis, we do not know all the odd integers not represented by this form over the integers. All odd positive integers are represented over the rational numbers by this form. For example $3 = (\frac{1}{2})^2 + (\frac{1}{2})^2 + 10(\frac{1}{2})^2$, although 3 is not represented over the integers.

Next, let us prove Theorem 1.3.

Proof of Theorem 1.3. First, we prove that if a, b, c are positive square-free pairwise relatively prime integers, then any positive integer congruent to $-abc$ $(\mathrm{mod}\ 8(abc)^2)$ is not represented by $ax^2 + by^2 + cz^2$ over the rationals.

If for an odd prime p that divides a (or b, or c) we have $(\frac{-bc}{p}) = -1$ (or $(\frac{-ac}{p}) = -1$, or $(\frac{-ab}{p}) = -1$, respectively) then if $n \equiv -abc \pmod{(abc)^2}$ we conclude that $n \equiv -abc \pmod{p^2}$ and hence $n/p \equiv -abc/p \pmod p$ and so $(\frac{na/p^2}{p}) = (\frac{(a/p)^2bc}{p}) = (\frac{-bc}{p}) = -1$ (or $(\frac{nb/p^2}{p}) = (\frac{-ac}{p}) = -1$, or $(\frac{nc/p^2}{p}) = (\frac{-ab}{p}) = -1$, respectively). By part (4) of Theorem 1.1, n is not representable over the rationals. If such a prime factor does not exist then according to Lemma 2.1, we are either in part (2) or part (3) of Theorem 1.1. In part (2), any $n \equiv -abc \pmod 8$ is not representable and in part (3) any $n \equiv -abc \pmod{16}$ is not representable over the rationals.

According to the formula (1.1) we have

$$R(a,b,c) = dd_1d_2d_3R(d_1a_3, d_2b_3, d_3c_3).$$

Since d_1a_3, d_2b_3 and d_3c_3 are positive square-free relatively prime integers, hence, any positive integer congruent to

$$-d_1d_2d_3a_3b_3c_3 \pmod{8(d_1d_2d_3a_3b_3c_3)^2}$$

is not in $R(d_1a_3, d_2b_3, d_3c_3)$. Therefore, any positive number congruent to

$$-dd_1^2d_2^2d_3^2a_3b_3c_3 \pmod{8d(d_1d_2d_3)^3(a_3b_3c_3)^2}$$

is not in $R(a,b,c)$. Since $S = da_3b_3c_3$ so any positive integer congruent to

$$-(d_1d_2d_3)^2S \pmod{8(d_1d_2d_3)^3S^2}$$

is not in $R(a,b,c)$. We can divide by a square, here $(d_1d_2d_3)^2$, without changing the representability over the rationals. Hence, any positive integer congruent to $-S \pmod{8d_1d_2d_3S^2}$ is not in $R(a,b,c)$. This proves the first statement of Theorem 1.3.

If a, b and c are positive integers, then $d_1d_2d_3S$ divides abc. Therefore, any positive integer congruent to $-S \pmod{8abcS}$ is not in $R(a,b,c)$. Notice that R is an integer, so any number congruent to $-R^2S \pmod{8abcR^2S}$ or equivalently congruent to $-abc \pmod{8(abc)^2}$ is not in $R(a,b,c)$. □

We finish this section by proving Theorem 1.5.

Proof of Theorem 1.5. Suppose that the congruence $ax^2 + by^2 + cz^2 \equiv -abc \pmod{8(abc)^2}$ is solvable. Then by Theorem 1.3, a, b and c are not of the same signs. If for a prime $p \mid c$, we have $(\frac{-ab}{p}) = -1$ then according to part (4) of Theorem 1.1, $-abc$ is not represented by $ax^2 + by^2 + cz^2 \pmod{p^2}$, because $(\frac{(-abc/p)(c/p)}{p}) = (\frac{-ab}{p}) = -1$. This implies that for any prime $p \mid c$, we have $(\frac{-ab}{p}) = 1$. By the Chinese remainder theorem, this implies that $-ab$ is a quadratic residue modulo c. Similarly $-bc$ and $-ac$ are quadratic residues modulo a and b, respectively. Now, we use a well-known theorem proved by Legendre in 1785 (see [13], pages 509–513) that states that if a, b and c are pairwise relatively prime integers not of the same sign, such that $-bc$, $-ac$ and $-ab$ are quadratic residues modulo a, b and c, respectively, then the equation

$$ax_0^2 + by_0^2 + cz_0^2 = 0$$

has solution in integers, where not all the three numbers x_0, y_0 and z_0 are zero. We may assume that the greatest common divisor of x_0, y_0, z_0 is one. This implies that these numbers are pairwise relatively prime, since we have assumed that the coefficients a, b and c are square free and if a prime factor divides x_0 and y_0 (for example) then it must divide z_0 as well. From this fact, it follows that the greatest common divisor of ax_0, by_0 and cz_0 is one. Therefore, there are integers x_1, y_1 and z_1 such that

$$ax_0x_1 + by_0y_1 + cz_0z_1 = 1.$$

Now, it follows that

$$a(kx_0 + x_1)^2 + b(ky_0 + y_1)^2 + c(kz_0 + z_1)^2 = 2k + (ax_1^2 + by_1^2 + cz_1^2). \tag{2.5}$$

Assume that a, b and c are odd. Then one of x_0, y_0 or z_0 is even and the other two are odd. Without loss of generality, we assume x_0 is even. Note that $x_2 = x_1 + by_0$, $y_2 = y_1 - ax_0$ and $z_2 = z_1$ satisfy

$$ax_0x_2 + by_0y_2 + cz_0z_2 = 1.$$

Hence,

$$a(kx_0 + x_2)^2 + b(ky_0 + y_2)^2 + c(kz_0 + z_2)^2 = 2k + (ax_2^2 + by_2^2 + cz_2^2). \tag{2.6}$$

Since $ax_1^2 + by_1^2 + cz_1^2$ and $ax_2^2 + by_2^2 + cz_2^2$ have different parities, equations (2.5) and (2.6) above represent all integers. Next, assume that all of a, b, and c are not odd. Without loss of generality, we can assume that a is even and b and c are odd. Then since y_0 and z_0 are coprime, they need to be odd. Hence y_1 and z_1 must be of different parities and this implies that $ax_1^2 + by_1^2 + cz_1^2$ is odd. So equation (2.5) represents all odd integers. To represent all even integers, it is enough to represent numbers of the form $4k+2$, since other numbers are of the form $4^m n$, where n is either odd or $\equiv 2 \pmod 4$, which has been represented. Now choose x_1, y_1, z_1 such that

$$ax_0x_1 + by_0y_1 + cz_0z_1 = 2$$

and hence

$$a(kx_0 + x_1)^2 + b(ky_0 + y_1)^2 + c(kz_0 + z_1)^2 = 4k + (ax_1^2 + by_1^2 + cz_1^2). \tag{2.7}$$

As before, we may replace (x_1, y_1, z_1) with $(x_1 + by_0, y_1 - ax_0, z_1)$ if needed to assume x_1 is odd. Since y_1 and z_1 are of the same parity, if we replace (x_1, y_1, z_1) with $(x_1, y_1 + cz_0, z_1 - by_0)$ we may assume that y_1 and z_1 are even. Hence,

$$ax_1^2 + by_1^2 + cz_1^2 \equiv a \equiv 2 \pmod 4$$

and equation (2.7) represents all numbers equivalent to 2 (mod 4). □

Remark 2.11. Inspecting the proof given above, one sees that the ternary quadratic form $ax^2+by^2+cz^2$ with abc square-free represents all integers over the integers if and only if it represents zero nontrivially. For example $x^2+by^2-cz^2$ with $b,c>0$ square-free and coprime represents all integers if and only if c is of the form x^2+by^2, where x and y are rational numbers. This implies that c must divide x^2+by^2 with x and y being nonzero relatively prime integers. If x^2+by^2 is the only binary quadratic form of the discriminant $-4b$ up to equivalence, which by a theorem of Landau happens only when $b=1,2,3,7$ (see [3], page 28) then we can conclude that c must be of the form x^2+by^2 for two relatively prime nonzero integers x and y. For example, the form $x^2+3y^2-pz^2$ for a prime number p represents all integers over the integers if and only if $p\equiv 1 \pmod 3$.

Acknowledgments. The authors wish to express their acknowledgment to the referee for providing very constructive remarks that improved the quality of this paper considerably.

References

[1] *A. A. Albert*: The integers represented by sets of ternary quadratic forms. Am. J. Math. *55* (1933), 274–292. zbl MR doi

[2] *J. H. Conway*: The Sensual (Quadratic) Form. The Carus Mathematical Monographs 26. Mathematical Association of America, Washington, 1997. zbl MR doi

[3] *D. A. Cox*: Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication. Pure and Applied Mathematics. A Wiley Series of Texts, Monographs, and Tracts. John Wiley & Sons, Hoboken, 2013. zbl MR doi

[4] *L. E. Dickson*: Integers represented by positive ternary quadratic forms. Bull. Am. Math. Soc. *33* (1927), 63–70. zbl MR doi

[5] *G. Doyle, K. S. Williams*: A positive-definite ternary quadratic form does not represent all positive integers. Integers *17* (2017), Article ID A.41, 19 pages. zbl MR

[6] *W. Duke, R. Schulze-Pillot*: Representations of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids. Invent. Math. *99* (1990), 49–57. zbl MR doi

[7] *D. E. Flath*: Introduction to Number Theory. AMS, Providence, 2018. zbl MR doi

[8] *H. Gupta*: Some idiosyncratic numbers of Ramanujan. Proc. Indian Acad. Sci., Sect. A *13* (1941), 519–520. zbl MR doi

[9] *B. W. Jones, G. Pall*: Regular and semi-regular positive ternary quadratic forms. Acta Math. *70* (1939), 165–191. zbl MR doi

[10] *I. Kaplansky*: Ternary positive quadratic forms that represent all odd positive integers. Acta Arith. *70* (1995), 209–214. zbl MR doi

[11] *I. Kaplansky*: Linear Algebra and Geometry: A Second Course. Dover Publications, Mineola, 2003. zbl MR

[12] *V. A. Lebesgue*: Tout nombre impair est la somme de quatre carrés dont deux sont égaux. J. Math. Pures Appl. (2) *2* (1857), 149–152. (In French.)

[13] *A. M. Legendre*: Essai sur la théorie des nombres. Duprat, Paris, 1798. (In French.) zbl

[14] *L. J. Mordell*: The condition for integer solutions of $ax^2+by^2+cz^2+dt^2=0$. J. Reine Angew. Math. *164* (1931), 40–49. zbl MR doi

[15] *L. J. Mordell*: Note on the diophantine equation $ax^2 + by^2 + cz^2 + dt^2 = 0$. Bull. Am. Math. Soc. *38* (1932), 277–282. zbl MR doi

[16] *K. Ono, K. Soundararajan*: Ramanujan's ternary quadratic form. Invent. Math. *130* (1997), 415–454. zbl MR doi

[17] *S. Ramanujan*: On the expression of a number in the form $ax^2 + by^2 + cz^2 + du^2$. Proc. Camb. Philos. Soc. *19* (1917), 11–21. zbl

[18] *J.-P. Serre*: A Course in Arithmetic. Graduate Texts in Mathematics 7. Springer, New York, 1973. zbl MR doi

[19] *Z.-W. Sun*: On universal sums of polygonal numbers. Sci. China, Math. *58* (2015), 1367–1396. zbl MR doi

[20] *H.-L. Wu, Z.-W. Sun*: Arithmetic progressions represented by diagonal ternary quadratic forms. Available at `https://arxiv.org/abs/1811.05855v1` (2018), 16 pages.

Authors' address: Amir Jafari (corresponding author), Farhood Rostamkhani, Department of Mathematical Sciences, Sharif University of Technology, P.O. Box 11155-9415, Tehran, Iran, e-mail: `amirjafa@gmail.com`, `farhood.rostamkhani@gmail.com`.