ON THE HASSE–MINKOWSKI THEOREM AND APPLICATIONS TO SUMS OF SQUARES

THANH CAN

Abstract. In this paper, we present a proof of the Hasse–Minkowski theorem in the cases $n \leq 3$. We then discuss Selmer's cubic as a counterexample to the Hasse principle for higher-degree forms, and conclude with applications to the theorems on integer representations as sums of two, three, and four squares.

1. Introduction

The Hasse principle is the idea that a given property holds over $\mathbb{Q}$ if and only if it holds over $\mathbb{R}$ and every $\mathbb{Q}_p$. In other words, the principle connects solvability in local fields and solvability in global fields, allowing for the reduction of an infinite arithmetic problem over $\mathbb{Q}$ to a collection of local computations in $\mathbb{R}$ and $\mathbb{Q}_p$. The Hasse–Minkowski theorem (Theorem 3.1) in particular establishes the Hasse principle for quadratic forms (Definition 2.1), thus illustrating their well-behavedness as opposed to higher-degree forms.

In Section 2, we recall some background definitions and results in p-adic analysis. In Section 3, we state the Hasse–Minkowski theorem and provide the proof for $n \leq 3$. In Section 4, we demonstrate a counterexample to the Hasse principle for cubic forms. Finally, in Section 5, we use the Hasse–Minkowski theorem to derive some classical results in elementary number theory on sums of squares.

2. Preliminaries

We briefly recall some definitions and the generalized Hensel's lemma, which will be central to our discussion in later sections.

Definition 2.1 (Quadratic form)**.** Let k be a field. A *quadratic form* over k is a function

$$f(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j$$

where $a_{ij} \in k$. A quadratic form f over k is said to be *diagonal* if

$$f(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i \leq n} a_i x_i^2$$

where $a_i \in k$.

Proposition 2.2. *Every quadratic form over $\mathbb{Q}$ is equivalent to a diagonal quadratic form under an invertible linear change of variables.*

Date: May 2026.

Example 2.3. Let $f(x_1, x_2, x_3) = x_1^2 + 4x_1x_2 + 6x_1x_3 + 5x_2^2 + 8x_2x_3 + x_3^2$ be a quadratic form in three variables. Observe that

$$\begin{aligned} f &= (x_1 + 2x_2 + 3x_3)^2 + x_2 - 4x_2x_3 - 8x_3^2 \\ &= (x_1 + 2x_2 + 3x_3)^2 + (x_2 - 2x_3)^2 - 12x_3^2, \end{aligned}$$

so defining the new variables

$$y_1 = x_1 + 2x_2 + 3x_3, \quad y_2 = x_2 - 2x_3, \quad y_3 = x_3,$$

we get the diagonal form $f = y_1^2 + y_2^2 - 12y_3^2$.

In particular, there exists an invertible matrix $(c_{ij}) \in \mathrm{GL}_n(\mathbb{Q})$ such that under the linear substitution $x_i = \sum_{j=1}^n c_{ij}y_j$, the form $f(x_1, \ldots, x_n)$ becomes diagonal in the variables $y_1, \ldots, y_n$. We now recall the generalized Hensel's lemma, which will be extensively used in Sections 4 and 5.

Theorem 2.4 (Generalized Hensel's lemma)**.** *If $f(x) \in \mathbb{Z}_p[x]$ and $a_0 \in \mathbb{Z}_p$ satisfies*

$$f(a_0) \equiv 0 \pmod{p^{2k+1}}, \quad f'(a_0) \not\equiv 0 \pmod{p^{k+1}},$$

where k is a nonnegative integer, then there is a unique $a \in \mathbb{Z}_p$ with $f(a) = 0$ and $a \equiv a_0 \pmod{p^{2k+1}}$.

Remark 2.5. Setting $k = 0$ in the above theorem recovers the classical Hensel's lemma.

Example 2.6. Let $b \equiv 1 \pmod 8$ be an element in $\mathbb{Z}_2$. We will show that b is a square in $\mathbb{Z}_2$, or equivalently, there exists $x \in \mathbb{Z}_2$ such that $x^2 = b$. Let $f(x) = x^2 - b$. We have $f(1) \equiv 0 \pmod{2^3}$ and $f'(1) = 2 \not\equiv 0 \pmod{2^2}$, so applying Theorem 2.4 with $k = 1$, there is $x \in \mathbb{Z}_2$ such that $x^2 = b$ and $x \equiv 1 \pmod{2^3}$, as desired.

3. Hasse–Minkowski Theorem

In this section, we state the Hasse–Minkowski Theorem. We provide a proof for $n \leq 3$; for the proofs for the cases $n = 4$ and $n \geq 5$, one can refer to [Ser93, Chapter IV].

Theorem 3.1 (Hasse–Minkowski)**.** *Let $Q(x_1, \ldots, x_n)$ be a quadratic form with coefficients in $\mathbb{Q}$. The equation $Q(x_1, \ldots, x_n) = 0$ has a nontrivial solution in $\mathbb{Q}$ if and only if it has a nontrivial solution in $\mathbb{R}$ and every $\mathbb{Q}_p$.*

The only if direction is clear: since $\mathbb{Q}$ embeds into $\mathbb{R}$ and every $\mathbb{Q}_p$, every nontrivial rational solution to the equation produces a solution in $\mathbb{R}$ and $\mathbb{Q}_p$. We now provide a partial proof of the if direction, which uses induction on the dimension n of the quadratic form. In this paper, we resolve the cases $n \leq 3$.

If $n = 1$, then $Q(x_1) = ax_1^2$ for some $a \in \mathbb{Q}^\times$. Obseve that if $ax_1^2 = 0$ in $\mathbb{R}$ and $\mathbb{Q}_p$, then we have $x_1 = 0$, so the equation $Q(x_1) = 0$ has no nontrivial solutions in $\mathbb{R}$ and $\mathbb{Q}_p$. Thus, the Hasse–Minkowski theorem is vacuously true in this case.

3.1. The $n = 2$ case.

By Proposition 2.2, we can write any 2-dimensional quadratic form as $ax^2 + by^2$ for some $a, b \in \mathbb{Q}^\times$. The Hasse–Minkowski theorem for this case thus states that if the equation $ax^2 + by^2 = 0$ has a nontrivial solution in $\mathbb{R}$ and every $\mathbb{Q}_p$, then it has a nontrivial solution in $\mathbb{Q}$.

For a given prime p, suppose that $ax_0^2 + by_0^2 = 0$ in $\mathbb{Q}_p$, where x_0 and y_0 are non-zero elements of $\mathbb{Q}_p$. Rearranging the equation, we obtain

$$-\frac{a}{b} = \frac{y_0^2}{x_0^2}.$$

It follows that $-\frac{a}{b}$ is a square in $\mathbb{Q}_p$, so $\nu_p(-\frac{a}{b})$ is even. Furthermore, since the equation has a nontrivial real solution, $-\frac{a}{b}$ is positive, so we can write

$$-\frac{a}{b} = \prod_p p^{\nu_p(-\frac{a}{b})}$$

where each $\nu_p(-\frac{a}{b})$ is even. This means that $-\frac{a}{b}$ is a square in $\mathbb{Q}$ and the equation admits a nontrivial rational solution.

3.2. **The $n = 3$ case.** We follow [Ser93, Theorem 8, p. 42]. We must show that if the quadratic form $f = ax^2 + by^2 + cz^2$ has a nontrivial zero in $\mathbb{R}$ and every $\mathbb{Q}_p$, then f also has a nontrivial zero in $\mathbb{Q}$.

We begin by making some simplifications. By clearing denominators, we may assume that a, b, c are in $\mathbb{Z}_p$. Moreover, for a given prime p, if p^2 divides one of the coefficients, say a, then we can substitute x with $\frac{x}{p}$ and eventually reduce $\nu_p(a)$ to 0 or 1. As a result, we may suppose that a, b, c are squarefree. Finally, by multiplying f by $-c$ and making suitable linear substitutions (which doesn't change the fact that f admits a nontrivial zero), we obtain an equivalent quadratic form of the form $ax^2 + by^2 - z^2$ (which we also call f) where a, b are squarefree integers.

Without loss of generality, suppose that $|a| \leq |b|$. We proceed by induction on $|a| + |b|$. For the base case $|a| + |b| = 2$, we have $|a| = |b| = 1$. Since f has a nontrivial zero in $\mathbb{R}$, we have the list of possibilities

$$f \in \{x^2 + y^2 - z^2, -x^2 + y^2 - z^2, x^2 - y^2 - z^2\}.$$

Each of these possibilities of f have a nontrivial zero, namely $(1, 0, 1)$, $(0, 1, 1)$, $(1, 1, 0)$, respectively, so the theorem holds for the base case.

Now, suppose that $|a|+|b| > 2$, so $|b| \geq 2$. We claim that if f has a nontrivial zero in every $\mathbb{Q}_p$ (in particular for each p dividing b), then a is a square (or zero) modulo b. Since b is squarefree, it suffices to show that a is a square modulo p for each p dividing b. Fix a prime p, and suppose that $(x_0, y_0, z_0) \in \mathbb{Q}_p^3$ is a nontrivial zero of f in $\mathbb{Q}_p$. We may scale f and further suppose that $\min(\nu_p(x_0), \nu_p(y_0), \nu_p(z_0)) = 0$. Taking f modulo p, we have

$$ax_0^2 + by_0^2 - z_0^2 \equiv ax_0^2 - z_0^2 \equiv 0 \pmod{p}.$$

If $z_0 \equiv 0 \pmod{p}$, then either $a \equiv 0 \pmod{p}$ or $x_0 \equiv 0 \pmod{p}$. The latter case, however, leads to $by_0^2 \equiv 0 \pmod{p^2}$; since b is squarefree, we must have $y_0 \equiv x_0 \equiv z_0 \pmod{p}$, contradicting the assumption that at least one of x_0, y_0, z_0 is a unit in $\mathbb{Z}_p$. If $z_0 \not\equiv 0 \pmod{p}$, then $x_0 \not\equiv 0 \pmod{p}$ and $a \equiv \frac{z_0^2}{x_0^2} \pmod{p}$ is a square in $\mathbb{Z}/p\mathbb{Z}$, as needed. Consequently, a is either 0 or a quadratic residue modulo p, from which the Chinese Remainder Theorem implies that a is a quadratic residue modulo b.

Using the claim, we can write $t^2 = a + bb'$ for integers t, b' such that $|t| \leq \frac{|b|}{2}$. In order to use the inductive hypothesis, we have the following lemma.

Lemma 3.2. *Let k be a field. The quadratic form $f = ax^2 + by^2 - z^2$ has a nontrivial zero in k if and only if $f' = ax^2 + b'y^2 - z^2$ has a nontrivial zero in k, where b' is defined as above.*

Proof. Suppose (x_0, y_0, z_0) is a nontrivial zero of f. This means that

$$ax_0^2 + by_0^2 - z_0^2 = 0$$

where x_0, y_0, z_0 are not all zero. Using the Brahmagupta–Fibonacci identity, we have

$$(z_0^2 - ax_0^2)(t^2 - a) = (z_0 t + ax_0)^2 - a(z_0 + x_0 t)^2.$$

Substituting $z_0^2 - ax_0^2 = by_0^2$ and $t^2 - a = bb'$, we obtain

$$b^2 b' y_0^2 = (z_0 t + ax_0)^2 - a(z_0 + x_0 t)^2.$$

Let $z_0 + x_0 t = x_1$, $by_0 = y_1$, and $z_0 t + ax_0 = z_1$, we have

$$b' y_1^2 = z_1^2 - ax_1^2,$$

implying that (x_1, y_1, z_1) is a nontrivial root of f', as desired.

The converse follows from an analogous application of the Brahmagupta–Fibonacci identity, yielding the lemma. □

The above result with $k = \mathbb{Q}$ and $\mathbb{Q}_p$ allows us to reduce the problem to the zeros of f'. However, since $|b| \geq 2$, we have

$$|b'| = \left| \frac{t^2 - a}{b} \right| \leq \frac{|b|^2 + 4|a|}{4|b|} \leq \frac{|b|}{4} + 1 < |b|.$$

Writing $b' = b''u$ such that u is an integer and b'' is squarefree, we obtain $|b''| \leq |b'| < |b|$. Applying the inductive hypothesis to $f'' = ax^2 + b''y_0^2 - z_0^2$, which is equivalent to f, finishes the induction.

4. A counterexample

While the Hasse–Minkowski theorem establishes the Hasse principle for quadratic forms, an analogous result does not necessarily hold for forms of higher power. A famous counterexample is the following.

Example 4.1 (Selmer's cubic)**.** The cubic equation

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a solution in $\mathbb{R}$ and every $\mathbb{Q}_p$, but not in $\mathbb{Q}$.

A nontrivial real solution is $\left(1/\sqrt[3]{3}, -1/\sqrt[3]{4}, 0\right)$. To find a solution in each $\mathbb{Q}_p$, we consider the cases $p = 3$, $p = 5$, and $p \neq 3, 5$.

In $\mathbb{Q}_3$, let $x = 0$ and $z = -1$; we thus have the equation $4y^3 - 5 = 0$. Let $f(y) = 4y^3 - 5$. Note that $f(2) = 27 \equiv 0 \pmod{3^3}$ and $f'(2) = 48 \not\equiv 0 \pmod{3^2}$, so we can apply the generalized version of Hensel's lemma (Theorem 2.4) with $a_0 = 2$ and $k = 1$ to obtain $a \in \mathbb{Z}_3$ such that $f(a) = 0$ and $a \equiv 2 \pmod{3^3}$. Consequently, a solution to Selmer's cubic in $\mathbb{Q}_3$ is $(0, y, -1)$ where $y^3 = \frac{5}{4}$ in $\mathbb{Z}_3$.

In $\mathbb{Q}_5$, let $y = z = -1$; we thus have the equation $3x^3 - 9 = 0$, or $x^3 - 3 = 0$. Let $f(x) = x^3 - 3$. Observe that $f(2) = 5 \equiv 0 \pmod 5$ and $f'(2) = 12 \not\equiv 0 \pmod 5$, so by Hensel's lemma, there is $a \in \mathbb{Z}_5$ such that $f(a) = 0$ and $a \equiv 2 \pmod 5$. Consequently, a solution to Selmer's cubic in $\mathbb{Q}_5$ is $(x, -1, -1)$ where $x^3 = 3$ in $\mathbb{Z}_5$.

To address the $p \neq 3, 5$ case, we introduce the following lemma.

Lemma 4.2. *Let p be a prime, and H be the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ containing all cubes. If $p \equiv 1 \pmod 3$, then H is a subgroup of index 3; otherwise, $H = (\mathbb{Z}/p\mathbb{Z})^\times$.*

Proof. Let g be a primitive root mod p. We have $(\mathbb{Z}/p\mathbb{Z})^\times = \{g, g^2, \ldots, g^{p-1}\}$, where $g^{p-1} \equiv 1 \pmod{p}$. If $p \not\equiv 1 \pmod{3}$, then we claim that every element in $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cube. Indeed, for any element $m = g^k$ where $1 \leq k \leq p-1$, take $l \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $3l \equiv k \pmod{p-1}$. It follows that $(g^l)^3 \equiv g^{3l} \equiv g^k \pmod{p}$, as needed. If $p \equiv 1 \pmod{3}$, then we claim that H consists of exactly the elements of the form g^{3k} for a positive integer k. Again, let g^u be an element in $(\mathbb{Z}/p\mathbb{Z})^\times$. We have $g^u \equiv g^{3k} \pmod{p}$ iff $u \equiv 3k \pmod{p-1}$. Since $p-1$ is a multiple of 3, such a k exists iff u is also a multiple of 3, which implies the conclusion. □

First, if 3 is a cube in $(\mathbb{Z}/p\mathbb{Z})^\times$, then there exists some x such that $x^3 \equiv 3 \pmod{p}$, so we can again use Hensel's lemma to lift x to a cube root of 3 in $\mathbb{Z}_p$ and obtain the solution $(x, -1, -1)$ to Selmer's cubic.

If 3 is not a cube in $(\mathbb{Z}/p\mathbb{Z})^\times$, then Lemma 4.2 implies that the set of cubes in $(\mathbb{Z}/p\mathbb{Z})^\times$ forms a subgroup of index 3 with coset representatives $\{1, 3, 9\}$. In particular, every element m of $(\mathbb{Z}/p\mathbb{Z})^\times$ is congruent to k^3, $3k^3$, or $9k^3$ modulo p for some $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. For concreteness, we consider $m = 5 \in (\mathbb{Z}/p\mathbb{Z})^\times$.

- If $5 \equiv k^3 \pmod{p}$, then by Hensel's lemma, k lifts to an element $x \in \mathbb{Z}_p$ such that $x^3 = 5$. In particular, $(-x, x, -1)$ is a solution to Selmer's cubic in $\mathbb{Q}_p$.
- If $5 \equiv 3k^3 \pmod{p}$, then k lifts to $x \in \mathbb{Z}_p$ such that $3x^3 = 5$. Here, $(x, 0, -1)$ is a solution to Selmer's cubic in $\mathbb{Q}_p$.
- If $5 \equiv 9k^3 \pmod{p}$, then $15 \equiv 27k^3 \equiv (3k)^3 \pmod{p}$, so $3k$ lifts to $x \in \mathbb{Z}_p$ such that $x^3 = 15$, and we find that $(3x, 5, -7)$ is a solution to Selmer's cubic in $\mathbb{Q}_p$.

Having exhausted all cases, we conclude that $3x^3 + 4y^3 + 5z^3 = 0$ always has a local solution. The proof that the cubic does not have any rational zeros uses more advanced techniques beyond the scope of this paper (such as elliptic curves), which the reader can refer to in [Cas91].

5. Applications to sums of squares

In this section, we showcase interesting applications of the Hasse–Minkowski theorem to sums of squares in $\mathbb{Z}$.

Recall a classical fact in elementary number theory:

Theorem 5.1 (Sum of two squares)**.** *A positive integer n can be written as a sum of two squares if and only if for every prime p dividing n such that $p \equiv 3 \pmod{4}$, the value of $\nu_p(n)$ is even.*

There exist various proofs of the above theorem, including an elementantary approach based on the unique factorization of $\mathbb{Z}[i]$, the Gaussian integers [Con17]. We instead provide a proof using the Hasse–Minkowski theorem to illustrate the power of working in $\mathbb{Q}_p$ and the utility of Hensel's lemma.

The theorem is a result in $\mathbb{Z}$, so in order to work in $\mathbb{Q}$ and its completions, we need the following result.

Lemma 5.2. *Let $f(x_1, x_2, \ldots, x_m)$ be a quadratic form over $\mathbb{Q}$. If there is $m \in \mathbb{Z}$ such that $f(x_1, \ldots, x_m) = n$ for $x_1, \ldots, x_m \in \mathbb{Q}$, then there is $x_1', \ldots, x_m' \in \mathbb{Z}$ such that $f(x_1', \ldots, x_m') = n$.*

This is a corollary of the Davenport–Cassels theorem that we state without proof; see [Cas78] for further details. We are now ready to prove Theorem 5.1.

Proof of Theorem 5.1. First, suppose that there are integers x, y such that $n = x^2 + y^2$. For a contradiction, suppose that there is p dividing n where $p \equiv 3 \pmod 4$ and $\nu_p(n)$ is odd. Since $\nu_p(x^2 + y^2) = \nu_p(n)$ is odd, while $\nu_p(x^2)$ and $\nu_p(y^2)$ are even, we must have $\nu_p(x^2) = \nu_p(y^2)$, or $\nu_p(x) = \nu_p(y)$. Let $x = p^u c$ and $y = p^u d$ where $p \nmid c, d$. It follows that $n = p^{2u}(c^2 + d^2)$, and $c^2 + d^2 \equiv 0 \pmod p$. This means that $c^2 \equiv -d^2 \pmod p$, so -1 is a quadratic residue modulo p, which is impossible as $p \equiv 3 \pmod 4$. We thus obtain the desired contradiction, and every prime $p \mid n$ with $p \equiv 3 \pmod 4$ must have even valuation.

On the other hand, suppose that if $p \mid n$ with $p \equiv 3 \pmod 4$, then $\nu_p(n)$ is even. We can write $n = P^2 n'$ where n' is squarefree and every prime dividing n' is congruent to $1 \pmod 4$. If there exist integers a', b' such that $n' = a'^2 + b'^2$, then $n = (Pa')^2 + (Pb')^2$ is a sum of two squares, so it suffices to show that n' can be written as a sum of two squares. Using Lemma 5.2, we let

$$f(x, y, z) = x^2 + y^2 - n'z^2,$$

and seek rational numbers x, y, z such that $f = 0$. By the Hasse–Minkowski Theorem, this is equivalent to f having a zero in $\mathbb{R}$ and every $\mathbb{Q}_p$. In $\mathbb{R}$, we can take $(x, y, z) = (\sqrt{n'}, 0, 1)$; we now find a zero of f in each $\mathbb{Q}_p$.

Suppose p is an odd prime. If $p \mid n'$, then pick nonzero $x_0, y_0 \in \mathbb{Z}/p\mathbb{Z}$ such that $x_0^2 \equiv -y_0^2 \pmod p$; note that this is only possible because $p \equiv 1 \pmod 4$. Letting $y = y_0$ and $z = 1$, we can treat f as a quadratic in x where $f(x) = x^2 + y_0^2 - n'$. Observe that $f(x_0) \equiv 0 \pmod p$ and $f'(x_0) = 2x_0 \not\equiv 0 \pmod p$, so by Hensel's lemma, x_0 lifts to a root $x \in \mathbb{Z}_p$. Consequently, $(x, y_0, 1)$ is a root of f in $\mathbb{Q}_p$.

If $p \nmid n'$, again let $z = 1$; we need x, y such that $x^2 + y^2 - n' = 0$. Consider the sets

$$S = \{x^2 \pmod p : x \in \mathbb{Z}/p\mathbb{Z}\}, \quad T = \{n' - y^2 \pmod p : y \in \mathbb{Z}/p\mathbb{Z}\}.$$

Since $|S| = |T| = \frac{p+1}{2}$, we have $|S| + |T| = p + 1 > |\mathbb{Z}/p\mathbb{Z}|$, so $S \cap T \neq \varnothing$. In other words, there exist x_0, y_0 such that $x_0^2 + y_0^2 - n' \equiv 0 \pmod p$. If $x_0 \equiv 0 \pmod p$, then n' is a quadratic residue modulo p, and we can set $x = 0$ and apply Hensel's lemma on $f(y) = y^2 - n'$ with $y = y_0$. Otherwise, we set $y = y_0$ and use Hensel's lemma on $f(x) = x^2 + y_0^2 - n'$ with $x = x_0$. In either case, we obtain a root of f in $\mathbb{Q}_p$.

Finally, if $p = 2$, note that $\frac{n'}{2^{\nu_2(n')}} \pmod 8 \in \{1, 5\}$, so $n' \pmod 8 \in \{1, 2, 5\}$ (since n' is squarefree). Let $z = 1$. Recall that if $n' \equiv 1 \pmod 8$, then n' is a square in $\mathbb{Z}_2$ (Example 2.6), so we can take $(x, 0, 1)$ is a zero of f in $\mathbb{Q}_2$ where $x^2 = n'$ in $\mathbb{Z}_2$. Similarly, if $n' \equiv 2 \pmod 8$ then $f(x, 1, 1) = 0$ in $\mathbb{Q}_2$; if $n' \equiv 5 \pmod 8$ then $f(x, 2, 1) = 0$ in $\mathbb{Q}_2$, and we have exhausted all cases. By the Hasse–Minkowski theorem, f has a zero in $\mathbb{Q}$, so n' can be written as a sum of two squares of rationals. This means that n can be written as a sum of two squares of integers, as desired. □

The above proof demonstrates a typical roadmap to finding roots of quadratic forms in $\mathbb{Q}$: find a root in $\mathbb{Z}/p\mathbb{Z}$, lift it to a root in $\mathbb{Q}_p$ with Hensel's lemma, and apply Hasse–Minkowski to obtain a root in $\mathbb{Q}$. Due to the conditions of Hensel's lemma, it is important to handle the cases where p divides a coefficient of the quadratic form or $p = 2$ separately. Following an analogous approach, we have another classical result.

Theorem 5.3 (Sum of three squares)**.** *A positive integer n can be written as the sum of three squares if and only if n is not of the form $4^a(8b+7)$ for nonnegative integers a and b.*

Assuming that n is squarefree, the above theorem is equivalent to showing that n can be written as a sum of three squares iff $n \not\equiv 7 \pmod 8$. If we attempted to mimic the approach in the proof of Theorem 5.1, we notice that the obstruction for when $n \equiv 7 \pmod 8$ occurs in $\mathbb{Q}_2$: by reducing modulo 8, we obtain

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

for positive integers x, y, z. The only squares modulo 8 are $0, 1, 4$, so three squares cannot sum to 7 (mod 8), yielding the desired contradiction. For a proof of the other direction using the Hasse–Minkowski theorem, one can refer to [Ser93, Appendix, p. 45]. We can finally complete the classification sums of squares in $\mathbb{Z}$ with the following result.

Theorem 5.4 (Sum of four squares)**.** *Every positive integer is a sum of four squares.*

Proof. Let n be a positive integer, and write $n = 4^a m$ for $a, m \geq 0$ and $4 \nmid m$. If $m \not\equiv 7 \pmod 8$, then m is a sum of three squares, and so is n. If $m \equiv 7 \pmod 8$, then $m - 1 \equiv 6 \pmod 8$, so $m - 1$ is a sum of three squares, implying that m is a sum of four squares, and so is n. □

References

[Cas78] John William Scott Cassels, *Rational quadratic forms*, L.M.S. Monographs, vol. 13, Academic Press, London and New York, 1978.

[Cas91] J. W. S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.

[Con17] Keith Conrad, *The Gaussian integers*, Expository notes, Moscow Center for Continuous Mathematical Education (MCCME) Summer School, Dubna, 2017, Accessed: 2026-05-28.

[Ser93] Jean-Pierre Serre, *A course in arithmetic*, Springer, 1993.