# THE HASSE–MINKOWSKI THEOREM OVER $\mathbb{Q}$

STEPHEN ZHOU

Abstract. We give a relatively elementary proof of the Hasse–Minkowski Theorem over $\mathbb{Q}$, developing some of the theory of quadratic forms along the way. We then use the Hasse–Minkowski Theorem to derive the theorems of sums of two and three squares.

## 1. Introduction

Say we want to solve a diophantine equation $f(\mathbf{x}) = 0$ over $\mathbb{Z}$ or $\mathbb{Q}$. If we suspect the equation has no solutions, we can try proving it in two ways. We can show that $f(\mathbf{x}) = 0$ can't be solved in $\mathbb{R}$ with analysis, or we can show that $f(\mathbf{x}) = 0 \pmod{p^n}$ doesn't have a solution for some $n$ and prime $p$. This corresponds to proving $f(\mathbf{x}) = 0$ doesn't have a solution in $\mathbb{Q}_p$.

The Hasse principle, or the local–global principle, suggests that we can do the reverse. If we have solutions in $\mathbb{R}$ and every $\mathbb{Q}_p$, we can often stitch them together into a solution in $\mathbb{Q}_p$. The goal of this paper is to prove a particularly nice example of the local-global principle.

**Definition 1.1.** A quadratic form of rank $n$ is a function $f : R^n \to R$ defined by

$$f(\mathbf{x}) = f(x_1, x_2, \ldots, x_n) = \sum_{i,j} a_{i,j} x_i x_j$$

for some constants $a_{ij} \in R$.

**Definition 1.2.** Let $R$ be a ring. A quadratic form $f : R^n \to R$ *represents* $y \in R$ over $R$ if there exists $\mathbf{x} \in R^n$ such that $f(\mathbf{x}) = y$.

The question of what numbers a quadratic form represents is a generalization of the question "What numbers are a sum of $n$ squares?". In 1890, Minkowski proved the Hasse–Minkowski Theorem over $\mathbb{Q}$. [5]

**Theorem 1.3** (Hasse–Minkowski)**.** *Let $f : \mathbb{Q}^n \to \mathbb{Q}$ be a quadratic form. Then $f$ represents $a$ in $\mathbb{Q}$ if and only if $f$ represents $a$ in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes $p$.*

We assume basic familiarity with quadratic reciprocity and the $p$-adic numbers $\mathbb{Q}_p$, particularly Hensel's Lemma. A good introduction is [3] For notational convenience, we will sometimes use $\mathbb{Q}_\infty$ as a synonym for $\mathbb{R}$, and $|\cdot|_\infty$ as a synonym for the regular absolute value $|\cdot|$. We will also refer to $\mathbb{Q}$

*Date*: June 8, 2026.

as the *global* field, and $\mathbb{R}$ and $\mathbb{Q}_p$ as the *local* fields. The set of primes and $\infty$ will then be denoted $V$, the set of *places* of $\mathbb{Q}$.

In Section 2, we develop a basic theory of quadratic forms, entirely avoiding the idea of an invariant. In Section 3, we develop the properties of the Hilbert symbol, which explains the behavior of a rank 3 quadratic form. This prepares us for Section 4, where the Hasse–Minkowski Theorem is finally proved. We then apply this theorem in Section 5 to give relatively simple proofs of the theorems on sums of two and three squares. We conclude with other resources in Section 6. Our exposition broadly follows that of Serre [7] or Cassels [2], with some proofs simplified and theory omitted.

## 2. Quadratic Forms

Squares are simplest quadratic forms, and the simplest case of the local–global principle totally working.

**Theorem 2.1.** *If $x \in \mathbb{Q}$ is a square in $\mathbb{Q}_v$ for all $v \in V$ , then it is a square in $\mathbb{Q}$.*

*Proof.* If $x$ is a square in $\mathbb{R}$, then $x > 0$. If $x$ is a square in $\mathbb{Q}_p$, say $x = y^2$, then $|x|_p = |y|_p^2$, and $v_p(x) = 2v_p(y)$. Specifically, $v_p(x)$ is even for all $p$. And since $x > 0$, $x$ must be a square in $\mathbb{Q}$. □

But the local global principle can fail too.

*Example.* Consider the polynomial $f(x) = (x^2 - 2)(x^2 - 17)(x^2 - 34)$. We claim that $f(x) = 0$ has a solution in every $\mathbb{Q}_v, v \in V$, but not $\mathbb{Q}$ itself.

$f$ clearly has zeroes in $\mathbb{R}$.

We calculate that $f'(x) = 2x[(x^2-2)(x^2-17)+(x^2-17)(x^2-34)+(x^2-34)(x^2-2)]$, which is $\neq 0$ unless $2 \equiv 0$.

Notice that at least one of $2, 17, 34$ is a residue modulo $p$ for all $p$, since

$$\left(\frac{2}{p}\right)\left(\frac{17}{p}\right)\left(\frac{34}{p}\right) = \left(\frac{34}{p}\right)\left(\frac{34}{p}\right) = (\pm 1)^2 = 1,$$

so at least one of the residue symbols must be 1.

Hensel's Lemma allows us to lift this solution $\mod p$ into a solution in $\mathbb{Q}_p$.

But there is no solution in $\mathbb{Q}$, since none of $2, 17, 34$ are squares.

We can simplify our statement of the Hasse–Minkowski Theorem.

**Definition 2.2.** A quadratic form $f$ is *isotropic* if there exists $\mathbf{x} \neq \mathbf{0}$ such that $f(\mathbf{x}) = 0$ and *anisotropic* otherwise.

Notice that if $f$ represents $a$, then $ay^2 - f$ is isotropic. So the Hasse–Minkowski Theorem can be restated as follows. Also notice that a quadratic form that is isotropic over $\mathbb{R}$ is also indefinite, or not strictly nonnegative or nonpositive.

**Theorem 2.3** (Hasse-Minkowski)**.** *Let $f : \mathbb{Q}^n \to \mathbb{Q}$ be a quadratic form. If $f$ is isotropic in $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime $p$, then $f$ is isotropic in $\mathbb{Q}$.*

Notice that if we take an invertible linear transformation of a quadratic form, the new form represents the same numbers. We call this relation equivalence.

**Definition 2.4.** Two quadratic forms $f, g$ are equivalent if there exists an invertible linear transformation $A$ such that $f(\mathbf{x}) = g(A\mathbf{x})$.

We can make any quadratic form a sum of squares under equivalence. These forms have a special name.

**Definition 2.5.** A quadratic form $\sum a_{ij}x_ix_j$ is *diagonal* if $i \neq j$ implies $a_{ij} = 0$.

**Theorem 2.6.** *Any rational quadratic form is equivalent to a diagonal quadratic form.*

*Proof.* Let $f$ be a quadratic form. We induct on the rank $n$ of $f$

If $n = 1$, then $f(x) = ax^2$ is clearly diagonal.

Assume that all quadratic forms of rank $n-1$ are equivalent to a diagonal form. Let

$$f(x_1, \ldots, x_n) = \sum_{i,j \leq n} a_{i,j}x_i^2$$

be a quadratic form of rank $n$.

First assume that some $a_{i,i}$ is nonzero. Without loss of generality, say $a_{1,1} \neq 0$. Then by scaling the coefficients of $f$, we can assume that $a_{1,1} = 1$. Then we can write

$$f = x_1^2 + x_1 g + h,$$

where $g(x_2, \ldots, x_n)$ is a linear function in $n-1$ variables, and $h(x_2, \ldots, x_n)$ is a quadratic form of rank $n-1$.

Completing the square, we see that

$$f = \left(x_1 + \frac{g}{2}\right)^2 + (h - g^2)$$

Define the substitution $x_1' = x_1 + \frac{1}{2}g(x_2, \ldots, x_n)$, which is invertible since $x_1 = x_1' - \frac{1}{2}g(x_2, \ldots, x_n)$.

Then we have that

$$f(x_1, \ldots, x_n) = x_1^2 + h - g^2.$$

By induction, $h - g^2$ is equivalent to a diagonal form as a quadratic form of rank $n-1$. Thus, $f$ is equivalent to a diagonal form. □

From now on, we will assume all quadratic forms are diagonal.

Before we analyze quadratic forms in $\mathbb{Q}_p$, we need to analyze them in finite fields $\mathbb{F}_p$ for prime $p$. The following theorem will be useful.

**Theorem 2.7** (Chevalley's Theorem)**.** *Let $f(x_1, \ldots, x_n)$ be a polynomial of degree $d$ over the finite field $\mathbb{F}_p$ for a prime number $p$. Let $S = \{\mathbf{x} \in \mathbb{F}_q : f(\mathbf{x}) = 0\}$. If $\deg f < n$, then $|S| \equiv 0 \pmod{p}$.*

*Proof.* Notice that

$$|S| = \sum_{\mathbf{x} \in \mathbf{F}_p^n} (1 - f(\mathbf{x})^{p-1}),$$

since $a^{p-1} \equiv 1 \pmod{p}$ if $a \not\equiv 0 \pmod{p}$ and $0^{p-1} \equiv 0 \pmod{p}$.

We will evaluate the sum modulo $p$. 1 is summed $p^n$ times and contributes 0 to the sum, while $f(\mathbf{x})^{p-1}$ can be written as a sum of monomials. The degree of $f(\mathbf{x})^{p-1}$ is less than $n(p-1)$, so at least one variable of the monomial has degree less than $p-1$. Since $\sum_{x=0}^{p-1} x^a \equiv 0 \pmod{p}$, the whole sum is $0 \pmod{p}$, so $|S| \equiv 0 \pmod{p}$. □

As a corollary, we see that

**Theorem 2.8.** *Let $f$ be a quadratic form of rank $\geq 3$. Then $f$ has a nontrivial root in $\mathbb{F}_p$ for all primes $p$.*

*Proof.* A quadratic form has the trivial solution. But the total number of solutions is $0 \pmod{p}$, so there must be at least $p-1$ other zeros in $\mathbb{F}_p$. □

Recall Hensel's Lemma.

**Theorem 2.9** (Hensel's)**.** *Let $f(x)$ be a polynomial over $\mathbb{Q}_p$. Say that*

$$f(a) \equiv 0 \pmod{p^{2s+1}}.$$

*Then if*

$$f'(a) \not\equiv 0 \pmod{p^{s+1}}$$

*There exists $\alpha$ such that $f(\alpha) = 0$ in $\mathbb{Q}_p$, and $\alpha \equiv a \pmod{p}^s$.*

Applying this to quadratic forms, we get the following theorem.

**Theorem 2.10.** *Let $f(x, y, z) = ax^2 + by^2 + cz^2$, and let $p$ be an odd prime. Then, if $p \nmid a, b, c$, then $f$ is isotropic over $\mathbb{Q}_p$.*

*Proof.* By Theorem 2.8, we see that there exists $(x, y, z)$ not all divisible by $p$ such that $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$. Without loss of generality, assume $x \neq 0 \pmod{p}$. Fix $y, z$ and view $f$ as a function of solely $x$. Then since

$$\frac{\partial f}{\partial x} = 2ax \not\equiv 0 \pmod{p},$$

Hensel's Lemma allows us to lift to a solution $\mathbb{Q}_p$. □

This further implies

**Theorem 2.11.** *Let $f$ be a quadratic form of rank $n \geq 5$, and $p \neq 2$ be an odd prime. Then $f$ is isotropic over $\mathbb{Q}_p$.*

*Proof.* Let $f(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i^2$ be a quadratic form. We may assume the $a_i$ are squarefree. So we can write

$$f(\mathbf{x}) = \sum_{i=1}^{m} a_i x_i^2 + p \sum_{i=m+1}^{n} b_i x_i^2,$$

where none of the $a_i, b_i$ are divisible by $p$.

If $n \geq 5$, at least one of $\sum_{i=1}^{m} a_i x_i^2$ and $\sum_{i=m+1}^{n} b_i x_i^2$ has rank greater than 3, and thus is isotropic over $\mathbb{Q}_p$ by Theorem 2.10. Thus $f(\mathbf{x})$ is isotropic over $\mathbb{Q}_p$ as well. □

The $p = 2$ case is also true, although the details are a little more complicated.

**Theorem 2.12.** *Let $f$ be a quadratic form of rank $n \geq 5$. Then $f$ is isotropic over $\mathbb{Q}_2$.*

*Proof.* It suffices to consider the case $n = 5$. Let $f(\mathbf{x}) = \sum_{i=1}^{5} a_i x_i^2$ be a quadratic form. By scaling, we can assume that no $a_i$ is divisible by 4, and that at least three are odd, say $a_1, a_2, a_3$.

By computation, notice that there exists $\mathbf{y}$ such that one of $y_1, y_2, y_3$ is odd, and $f(\mathbf{y}) = 0 \pmod 8$. The partial derivative with respect to $y_i$ is then $2 \pmod 4$, so Hensel's Lemma lifts the solution modulo 8 to one modulo $\mathbb{Q}_2$. □

This should give us some intuition as to why the Local Global principle is so nice for quadratic forms. If a quadratic form has rank $\geq 5$, it is isotropic over all $\mathbb{Q}_p$, so we need to show that all indefinite quadratic forms of rank $\geq 5$ are isotropic. Then we only need to consider the cases of rank $< 5$. Theorem 2.10 further tells us that there are only finitely many primes $p$ for which a quadratic form is anisotropic, specifically those dividing it's coefficients.

## 3. The Hilbert Symbol

The proof of the $n = 3$ case of the Hasse-Minkowski Theorem turns out to be especially important. We introduce some machinery for it here. Recall that we only need to care about the diagonal case up to equivalence. We can also scale, so the only quadratic forms that matter are of the form $x^2 - ay^2 - bz^2$.

**Definition 3.1.** The Hilbert symbol $(a, b)_p$ is 1 if $f(x, y, z) = x_1^2 - ay^2 - bz^2$ is isotropic in $\mathbb{Q}_p$, and $-1$ if $f(\mathbf{x})$ is anisotropic.

We have a simple characterization of the Hilbert symbol.

**Theorem 3.2.** *$(a, b)_p = 1$ if and only if $a$ is the norm of an element in $\mathbb{Q}_p[\sqrt{b}]$.*

*Proof.* If $b$ is the square of $c$ in $\mathbb{Q}_p$, then $\mathbb{Q}_p[\sqrt{b}] = \mathbb{Q}_p$, and $(a, b)_p = 1$ since $x^2 - ay^2 - c^2z^2$ has the nontrivial root $(x, y, z) = (c, 0, 1)$.

If $b$ is not a square in $\mathbb{Q}_p$, let $\beta$ be a square root of $b$. Then every element of $\mathbb{Q}_p[\sqrt{b}]$ can be written as $x + \beta z$, where $x, z \in \mathbb{Q}_p$. The norm of $x + \beta z$ is $x^2 - bz^2$. So $a$ being the norm of an element of $\mathbb{Q}_p[\sqrt{b}]$ is equivalent to there existing $x, z$ such that $a = x^2 - bz^2$ implying $x^2 - ay^2 - bz^2$ has the nontrivial root $(x, 1, z)$. Conversely, say $x^2 - ay^2 - bz^2 = 0$. Notice that $y \neq 0$, since $b$ is not a square. Then $a$ is the norm of $\frac{x}{y} + \beta\frac{z}{y}$ . □

Even more surprisingly, the Hilbert symbol is bilinear. More specifically, we have the following formula for the Hilbert symbol.

**Theorem 3.3.** *Let $a, b$ be elements of some $\mathbb{Q}_p$.*

*If $p = \infty$, then $(a, b)_\infty = 1$ if $a > 0$ or $b > 0$, and $(a, b)_\infty = -1$ if $a < 0$ and $b < 0$.*

*If $p < \infty$, write $a = p^\alpha u, , b = p^\beta v$, where $u, v \in \mathbf{U}_p$. Then, if $p$ is odd,*

$$(a, b)_p = (-1)^{\alpha\beta \frac{p-1}{2}} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$$

*and if $p = 2$,*

$$(a, b)_2 = (-1)^{\frac{u-1}{2}\frac{v-1}{2} + \alpha\frac{u^2-1}{8} + \beta\frac{v^2-1}{8}}.$$

We need a lemma first.

**Lemma 3.4.** *Let $a, a', b$ be elements of a field. Then*

1. $(a, b)_p = (b, a)_p$
2. $(a, c^2)_p = 1$
3. $(a, -a)_p = 1$
4. $(a, 1 - a)_p = 1$
5. $(a, b)_p = 1$ *implies that* $(aa', b)_p = (a', b)_p$
6. $(a, b)_p = (a, -ab)_p = (a(1 - a)b)_p$

*Proof.* 1) follows from the commutativity of addition. $x^2 - ay^2 - c^2z^2$ has the nontrivial root $(x, y, z) = (c, 0, 1)$, proving 2). $x^2 - ay^2 + az^2$ has the nontrivial root $(x, y, z) = (0, 1, 1)$, proving 3). $x^2 - ay^2 + (a - 1)z^2$ has the nontrivial root $(x, y, z) = (1, 1, 1)$, proving 4). By Theorem 3.2, $(a, b)_p = 1$ is equivalent to $a$ being the norm of an element of $\mathbb{Q}[\sqrt{b}]$. But the norms of $\mathbb{Q}[\sqrt{b}]$ form a group, so $aa'$ is a norm if and only if $a'$ is. 6. Then follows from 5., 4. and 3. □

Now we are ready to prove Theorem 3.3.

*Proof of Theorem 3.3.* We may assume $a, b$ are square free by factoring, so $\alpha, \beta \leq 1$. We will do casework on the possible values of $\alpha, \beta$.

First, assume $p$ is odd.

Then if $\alpha = \beta = 0$, we need to prove that $(a, b)_p = 1$, which follows by Theorem 2.10.

If $\alpha = 1, \beta = 0$, we need to show that

$$(a, b)_p = \left(\frac{b}{p}\right).$$

Let $a = pu$, where $p \nmid u$. By the previous paragraph, $(u, b)_p = 1$, so by Lemma 3.4 we see that $(a, b)_p = (p, b)_p$. If $b$ is a square modulo $p$, it is clear that $(p, b)_p = 1 = \left(\frac{b}{p}\right)$. If $b$ is not a square, then $x^2 - py^2 - bz^2 \equiv x^2 - bz^2 \pmod{p}$ has no nontrivial zeroes in $\mathbb{F}_p$. But if a nontrivial solution in $\mathbb{Q}_p$ exists, there must be one where $z, x \not\equiv 0 \pmod{p}$. Thus $(p, b)_p = -1 = \left(\frac{b}{p}\right)$.

The case $\alpha = 0, \beta = 1$ is symmetric.

Now consider the case $\alpha = \beta = 1$. Let $a = pu, b = pv$, where $p \nmid u, v$. We need to show that

$$(pu, pv)_p = (-1)^{(p-1)/2} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right).$$

Using Lemma 3.4, we calculate that

$$(pu, pv)_p = (pu, -p^2uv)_p = (pu, -uv)_p.$$

By the $\alpha = 1, \beta = 0$ case, we see that

$$(pu, -uv) = \left(\frac{-uv}{p}\right).$$

Since $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ and the Legendre symbol is multiplicative, we get the desired result.

The case $p = 2$ follows by similar casework on $\alpha, \beta$. □

The Hilbert principle also has some nice properties globally, when $v$ is allowed to vary and $a, b \in \mathbb{Q}$ fixed.

**Theorem 3.5.** *Let $a, b \neq 0$ and $\{primes\} \cup \{\infty\}$. Then for all but finitely many $v \in V$, we have $(a, b)_v = 1$, and*

$$\prod_{v \in V} (a, b)_v = 1.$$

*Proof.* All but finitely many primes will not divide $ab$. For these primes, $x^2 - ay^2 - bz^2$ has a nontrivial zero by Theorem 2.10, so $(a, b)_p = 1$ for all but finitely many primes.

It remains to prove that

$$\prod_{v \in V} (a, b)_v = 1.$$

Since the Hilbert symbol is bilinear, we can assume that $a$ or $b$ is either $-1$ or a prime. Now we divide into cases and apply Theorem 3.3.

Say $a = -1, b = -1$. By Theorem 3.3, $(-1, -1)_\infty = -1 = (-1, -1)_2$, and $(-1, -1)_p = 1$ for all odd $p$, so the product is equal to 1.

Now let $a = -1$ and $b = q$ is a prime. If $q = 2$, $(-1, 2)_v = 1$ for all $v$. If $p$ is odd, $(-1, q)_v = 1$ if $v \neq 2, q$ by Theorem 2.10, and $(-1, q)_2 = (-1)^{(p-1)/2} = (-1, q)_q$ by Theorem 3.3, so the product is 1.

Finally, consider the case where $a = q, b = r$ are both primes. If $q = r$, then $(r, r)_v = (-1, r)_v$, so we are reduced to the previous case. So assume $q \neq r$. Say that $q = 2$. Then $(2, r)_v = 1$ for $v \neq 2, r$ by Theorem 2.10. We calculate that $(2, r)_v = (-1)^{(l^2-1)/8}$, $(2, r)_r = \left(\frac{2}{r}\right) = (-1)^{(l^2-1)/8}$, so the product is 1. Now say that $q, r \neq 2$. Then $(q, r)_v = 1$ for $v \neq 2, q, r$, and Theorem 3.3 shows that

$$(q, r)_2 = (-1)^{((q-1)/2)\cdot((r-1)/2)}, (q, r)_q = \left(\frac{r}{q}\right), (q, r)_r = \left(\frac{q}{r}\right).$$

By quadratic reciprocity,

$$\left(\frac{q}{r}\right)\left(\frac{r}{q}\right) = (-1)^{((q-1)/2)\cdot((r-1)/2)},$$

so the product over all the places is 1. □

The following theorem will be used to prove the rank 4 case of the Hasse–Minkowski Theorem.

**Theorem 3.6.** *Let $a_i, 1 \leq i \leq n$ be a finite sequence in $\mathbb{Q}$, and let $\varepsilon_{i,v}, 1 \leq i \leq n, v \in V$ be all equal to $\pm 1$. Then there exists $x \in \mathbb{Q}$ such that $(x, a_i)_v = \varepsilon_{i,v}$ if and only if the following conditions are met.*

1. *All but finitely many of the $\varepsilon_{i,v}$ are 1.*
2. *For all $1 \leq i \leq n$, we have $\prod_{v \in V} \varepsilon_{i,v} = 1$.*
3. *For all $v \in V$, there exists $x_v \in \mathbb{Q}_v$ such that $(x_v, a_i)_v = \varepsilon_{i,v}$ for $1 \leq i \leq n$.*

The proof requires Dirichlet's Theorem on primes in arithmetic progression.

**Theorem 3.7.** *Let $m \in \mathbb{N}$, and let $a$ be coprime to $m$. Then there exist infinitely many primes $p$ such that $p \equiv a \pmod{m}$.*

Dirichlet's Theorem belongs in analytic number theory, so we will not prove it here. The curious reader is directed to [1].

*Proof of 3.6.* The necessity of conditions has already been proven. So we assume they are satisfied and construct a satisfactory $x$.

Multiplying the $a_i$ by squares, we can assume they are all integers. Let $S$ consist of $2, \infty$ and all the prime divisors of $\prod a_i$. Let $T$ consist of all $v \in V$ such that there exists $1 \leq i \leq n$ such that $\varepsilon_{i,v} = -1$. By assumption, $S, T$ are both finite sets.

First consider the case where $S \cap T = \varnothing$. Set

$$a = \prod_{p \in T \setminus \{\infty\}} p$$

and

$$m = 8 \prod_{p \in S \setminus \{2, \infty\}} p.$$

Since $S$ and $T$ are disjoint, $a$ and $m$ are relatively prime, so Dirichlet's Theorem gives us a prime $q \notin S \cup T$ such that $q \equiv a \pmod{m}$. We claim that $x = aq$ works.

Say that $v \in S$. Then $v \notin T$, so $\varepsilon_{i,v} = 1$ for all $i \leq n$. So we need to show that $(a_i, x)_v = 1$ for all $v \in S$. If $v = \infty$, this is obvious. If $v$ is a prime $p$, then $x \equiv a^2 \pmod{m}$. By the Chinese remainder theorem, we have $x \equiv a^2 \pmod{p}$ if $p$ is odd, and $x \equiv a^2 \pmod{8}$ if $p = 2$. Either way, $x$‘ is a square in $p$, so $(a_i, x)_p = 1$.

Now say that $v = p \notin S$. Then $p \nmid a_i$, and $p \neq 2$, so Theorem 3.3 gives

$$(a_i, b)_p = \left(\frac{a_i}{p}\right)^{v_p(b)}$$

for any $b$.

If $p \notin T \cup \{q\}$, then $v_p(x) = 0$, so $(a_i, x)_p = 1 = \varepsilon_{i,p}$, where the last equality follows since $p \notin T$. If instead $p \in T$, we have that $v_p(x) = 1$. Condition 3. shows that there exists $x_p \in \mathbb{Q}_p$ such that $(a_i, x_p)_p = \varepsilon_{i,p}$ for $i \leq n$. Since $p \in T$, one of the $\varepsilon_{i,p}$ equals $-1$, so $v_p(a_i)$ must be odd, implying that

$$(a_i, x)_p = \left(\frac{a_i}{p}\right)^{v_p(x)} = (a_i, x_p)_p = \varepsilon_{i,p}$$

for all $i \leq n$. Finally, if $p = q$, we use Hilbert reciprocity and condition 2. to calculate that

$$(a_i, x)_q = \prod_{v \neq q} (a_i, x)_v = \prod_{v \neq q} \varepsilon_{i,v} = \varepsilon_{i,p}.$$

Now consider the case $S \cap T \neq \varnothing$. We will reduce to the case where $S \cap T = \varnothing$. The rationals are dense in $\mathbb{Q}_p$, so we can choose $x' \in \mathbb{Q}$ such that $x'/x_v$ is a square in $\mathbb{Q}_v$ for all $v \in S$, since $S$ is a finite set. By bilinearity, we see that $(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v}$ for all $v \in S$. Then set $\eta_{i,v} = \varepsilon_{i,v}(a_i, x')_v$. Then $\eta_{i,v}$ satisfies condition 1., 2.,3. The $S \cap T = \varnothing$ case then shows that there exists $y \in \mathbb{Q}$ such that $(a_i, y)_v = \eta_{i,v}$. Then set $x = yx'$. □

## 4. The Hasse–Minkowski Theorem

We are now ready to prove the Hasse–Minkowski theorem. We will split the theorem into cases based on the rank $n$ of $f$.

The rank 1 case is trivial, since $ax^2$ is always anisotropic.

The rank 2 case is nearly as simple.

**Theorem 4.1.** *Let $f(x_1, x_2)$ be a rank 2 quadratic form. Then $f$ is isotropic in $\mathbb{Q}$ if and only if $f$ is isotropic in $\mathbb{Q}_p$ for all $p \in V$.*

*Proof.* Let $f(x_1, x_2) = ax_1^2 - bx_2^2$. Then if $f(x_1, x_2) = 0$, it follows that $\frac{b}{a} = \frac{x_1^2}{x_2^2}$, $\frac{b}{a}$ must be a square. But Theorem 2.1 says that an element of $\mathbb{Q}$ is a square in $\mathbb{Q}$ if and only if it is a square in all $\mathbb{Q}_p$. □

The rank 3 case follows by induction.

**Theorem 4.2.** *Let $f(x_1, x_2, x_3)$ be a rank 3 quadratic form. Then $f$ is isotropic in $\mathbb{Q}$ if and only if $f$ is isotropic in $\mathbb{Q}_p$ for all $p \in V$.*

*Proof.* Let $f(\mathbf{x}) = x_1^2 - ax_2^2 - bx_3^2$, where $a, b$ are squarefree. We induct on $|a| + |b|$. When $|a| + |b| = 2$, we are reduced to an obvious finite case check. Without loss of generality, assume that $|a| \leq |b|$. Now write $b = \pm p_1 \dots p_k$. We will show that $a$ is a square modulo $p_i$ for all $i$, and thus is a square modulo $b$. We see that $x_1^2 - ax_2^2 \equiv 0 \pmod{p}$, and $x \neq 0$, so $a$ is a square

mod $p$. So there exists $t, |t| \leq |b|/2$ such that $t^2 = bb'$ for some integer $b'$. So $bb'$ is a norm of the extension $K[\sqrt{a}]$, where $K$ is either local or global. So $b$ and $b'$ are either both norms of $K[\sqrt{a}]$, or neither are norms of $K[\sqrt{a}]$. By Theorem 3.2, $f$ represents 0 if and only if

$$f' = x_1^2 - ax_2^2 - b'x_3^2$$

does. But

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

so our induction is complete. □

Rank 4 is the most complicated case.

**Theorem 4.3.** *Let $f(x_1, x_2, x_3, x_4)$ be a rank 4 quadratic form. Then $f$ is isotropic in $\mathbb{Q}$ if and only if $f$ is isotropic in $\mathbb{Q}_p$ for all $p \in V$.*

*Proof.* Write $f(\mathbf{x}) = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$.

Notice that $f$ is isotropic in $\mathbb{Q}_v$ if and only if there exists $x_v \in \mathbb{Q}_v$ such that

$$ax_1^2 + bx_2^2 = x_v$$

and

$$cx_3^2 + dx_4^2 = -x_v$$

for some $\mathbf{x}$.

This is equivalent to saying that $(x_v, -ab)_v = (a, b)_v$ and $(x_v, -cd)_v = (c, d)_v$, for $v$ prime or infinite. Since all these terms are 1 for all but finitely many of the $v$, Theorem 3.6 shows that there exists some $x \in \mathbb{Q}$ such that $(x, -ab)_v = (a, b)_v$ and $(x, -cd)_v = (c, d)_v$ for all $v \in V$. Thus $ax_1^2 + bx_2^2$ represents $x$ and $cx_3^2 + dx_4^2$ represents $-x$, proving $f$ is isotropic in $\mathbb{Q}$. □

Now we induct to prove the Hasse–Minkowski Theorem for all $n \geq 5$.

**Theorem 4.4.** *Let $f(\mathbf{x})$ be a rank $n \geq 5$ quadratic form. Then $f$ is isotropic in $\mathbb{Q}$ if and only if $f$ is isotropic in $\mathbb{Q}_p$ for all $p \in V$.*

*Proof.* Induct on $n$. We write

$$f(\mathbf{x}) = a_1x_1^2 + a_2x_2^2 - (a_3x_3^2 + \cdots a_nx_n^2)$$

and

$$g(x_1, x_2) = a_1x_1^2 + a_2x_2^2, h(\mathbf{x}) = a_3x_3^2 + \cdots a_nx_n^2$$

so that $f = g - h$.

Let $S \subset V$ be the finite set consisting of all primes dividing at least one $a_i$. Let $p \in S$. There exists some $a_p \in \mathbb{Q}_p$ that is represented by both $g$ and $h$, and $\mathbf{x}_p = (x_{1,p}, \ldots, x_{n,p})$ such that

$$h(x_{1,p}, x_{2,p}) = a_p = g(x_{3,p}, \ldots, x_{n,p}).$$

The rational numbers are dense in all $\mathbb{Q}_p$, and the squares are an open set, so there exists $x_1, x_2 \in \mathbb{Q}$ such that $a/a_p$ is a square in $\mathbb{Q}_p$, where $h(x_1, x_2) = a$. Consider $f' = ay^2 - g$. Notice that $f'$ represents $a$ in $\mathbb{Q}_p$ for all $p \in S$. For

other primes $p$, Theorem 2.10 proves $f'$ is isotropic. So $f'$ is isotropic in $\mathbb{Q}_v$ for all $v \in V$, and thus $f'$ represents 0 by induction. Thus $g$ represents $a$ in $\mathbb{Q}$, so $f$ represents 0, completing the induction. □

Combining all the previous cases, we have proven the entire Hasse–Minkowski Theorem.

We showed in Section 2 that all quadratic forms with rank $\geq 5$ are isotropic over $\mathbb{Q}_p$, so the following follows as a consequence of the Hasse–Minkowski Theorem.

**Theorem 4.5** (Meyer's)**.** *Let $f$ be an indefinite quadratic form of rank $n \geq 5$. Then $f$ is isotropic in $\mathbb{Q}$.*

## 5. Sums of Squares

Quadratic forms were motivated by sums of squares. Here we use the Hasse–Minkowski thoerem to give simple proofs of the sums of squares theorems.

But we have been dealing with rational quadratic forms, and we are studying sums of integer squares. Fortunately, the following general theorem lets us turn rational solutions into integer solutions.

**Theorem 5.1** (Davenport–Cassels)**.** *Let $f$ be a quadratic form of rank $n$ with integer coefficients. Assume that for all $\mathbf{x} \in \mathbb{Q}^n$, there exists some $\mathbf{y} \in \mathbb{Z}^n$ such that $f(\mathbf{x} - \mathbf{y})$. Then if $n \in \mathbb{Z}$ is represented by $f$ over $\mathbb{Q}$, it is also represented by $f$ over $\mathbb{Z}$.*

*Proof.* Say $f$ represents $n$ in $\mathbb{Q}$. Then there exists $t \in \mathbb{N}$ and $x \in \mathbb{Z}^n$ such that $t^2 n = f(x)$. Choose the minimum such $t$. We want to show $t = 1$. By hypothesis, we can assume there exists $y \in \mathbb{Z}^n, z \in \mathbb{Q}^n$ such that

$$\frac{x}{t} = y + z$$

and $f(z) < 1$. If $f(z) = 0$, it must be that $z = 0$, implying $x/t = y$ and $t = 1$ by minimality. Assume that $f(z) = 0$, and write

$$a = f(y) - nb = 2(nt - f(x+y) - f(x) - f(y))t' = at + bx' = ax + by.$$

It can be calculated that $f(x') = t'^2 n$, and $t' < t$, contradicting the minimality of $t$. □

This theorem applies to sums of two and three squares. Let $f(x_1, x_2, x_3) = \sum_{i=1}^n x_i^2$, $n < 4$. Then there exists $\mathbf{y} \in \mathbb{Q}$ such that $x_i - y_i \leq \frac{1}{2}$, so $f(\mathbf{x}-\mathbf{y}) = \sum_{i=1}^n (x_i - y_i)^2 \leq \sum_{i=1}^n \left(\frac{1}{2}\right)^2 = \frac{n}{4} < 1$. Now we can prove our desired sums of squares theorems.

**Theorem 5.2** (Fermat)**.** *Let $n \in \mathbb{N}$. Then $n$ is a sum of two squares if and only if $v_p(n)$ is even for every prime $p$ such that $p \equiv 3 \pmod 4$.*

*Proof.* By the Hasse–Minkowski Theorem and Theorem 5.1, we only need to prove that $x^2 + y^2 - nz^2$ is isotropic over all $\mathbb{Q}_v$, or that $(-1, n)_v = 1$ for all $v$. If $v = \infty$, this is obvious. So assume $v = p$ is prime.

If $p$ is an odd prime, write $n = p^{v_p(n)}n'$. Then Theorem 3.3 shows that

$$(-1, n)_p = \left(\frac{-1}{p}\right)^{v_p(n)}.$$

If $p \equiv 1 \pmod 4$, $\left(\frac{-1}{p}\right) = 1$, so $(-1, n)_p = 1$ unconditionally. If $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ so $(1, n)_p = 1$ if and only if $v_p(n)$ is even.

If $p = 2$, write $n = 2^{v_2(n)}n'$ Then Theorem 3.3 shows that

$$(-1, n)_p = (-1)^{\frac{n'-1}{2}}.$$

$n'$ is $1 \pmod 4$ exactly when $v_p(n)$ is even for every prime $p$ such that $p \equiv 3 \pmod 4$.

Applying Theorem 5.1 and the Hasse–Minkowski Theorem proves the desired result. □

Sums of three squares are a bit more difficult.

**Theorem 5.3** (Legendre)**.** *Let $n \in \mathbb{N}$. Then $n$ is a sum of three squares if and only if $n \neq 4^a(8b - 1)$ for some $a, b$.*

*Proof.* We first reduce to the case $a = 0$. The only squares modulo 4 are $0, 1$. So if $x^2 + y^2 + z^2 = n$ is divisible by 4, $x^2 \equiv y^2 \equiv z^2 \equiv 0 \pmod 4$, so all of $x, y, z$ are even, and we can factor out 4 from $n$. The squares modulo 8 are $0, 1, 4$, so three squares cannot add up to $-1 \pmod 8$.

Assume that $4 \nmid n$, and $n \not\equiv 7 \pmod 8$. We need to prove $x^2+y^2+z^2-nw^2$ is isotropic over $\mathbb{Q}_v$ for all $v$. It clearly is isotropic over $\mathbb{R}$. If $p$ is an odd prime, $x^2+y^2+z^2$ is isotropic over $\mathbb{Q}_p$ by Theorem 2.10, so $x^2+y^2+z^2-nw^2$ is as well.

Now consider $p = 2$. Notice that since $n \not\equiv 7 \pmod 8$, there exist $y, z$ such that

$$1^2 + y^2 + z^2 - n \equiv 0 \pmod 8.$$

Since

$$\frac{\partial f}{\partial x} = 2x$$

is $2 \pmod 4$ at $x = 1$, Hensel's Lemma allows us to lift to a solution in $\mathbb{Q}_2$.

Applying Theorem 5.1 and the Hasse–Minkowski Theorem proves the desired result. □

## 6. Further Reading

More about the theory of rational quadratic forms can be found in [7]. Many question we have not dealt with are solved, such as the classification of forms in $\mathbb{Q}_p$ up to equivalence. (There are surprisingly few!) Minkowski only proved the Hasse–Minkowski Theorem for $\mathbb{Q}$, but Hasse extended it

to number fields. To learn about this version of the theorem, see Lam [4]. Another direction Theorem 2.1 could have been generalized in is the Grunwald–Wang Theorem, which deals with $n$th powers.

**Theorem 6.1** (Grunwald–Wang)**.** *A rational number $a$ is a $n$th power in $\mathbb{Q}_p$ for almost every prime $p$ if and only if $a$ is a perfect $n$th power in $\mathbb{Q}$, or $8 \mid n$ and $a = 2^{\frac{n}{2}} b^n$ for $b \in \mathbb{Q}$.*

That is, $2^4 = 16$ is the only real exception. 16 is an exception due to the factorization $x^8 - 16 = (x^2 - 2)(x^2 + 2)(x^2 - 2x + 2)(x^2 + 2x + 2)$ Like the Hasse–Minkowski Theorem, this theorem generalizes to fields other than $\mathbb{Q}$. For a proof of the general version of this theorem, see Neukirch.[6]

## References


[1] Tom M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. New York, NY: Springer, 1976. ISBN: 978-0-387-90163-3. DOI: 10.1007/978-1-4757-5579-4.

[2] J. W. S. Cassels. *Rational quadratic forms*. English. Vol. 13. Lond. Math. Soc. Monogr. Academic Press, London, 1978.

[3] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction*. 3rd ed. Universitext. Cham: Springer, 2020. ISBN: 978-3-030-47295-5. DOI: 10.1007/978-3-030-47295-5.

[4] T. Y. Lam. *Introduction to Quadratic Forms over Fields*. Vol. 67. Graduate Studies in Mathematics. Providence, RI: American Mathematical Society, 2005. ISBN: 978-1-4704-8017-2.

[5] Hermann Minkowski. *Geometrie der Zahlen*. Leipzig: B. G. Teubner, 1910.

[6] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. 2nd ed. Vol. 323. Grundlehren der mathematischen Wissenschaften. Berlin: Springer, 2008. ISBN: 978-3-540-37888-4. DOI: 10.1007/978-3-540-37889-1.

[7] Jean-Pierre Serre. *A course in arithmetic. Translation of "Cours d'arithmetique". 2nd corr. print*. English. Vol. 7. Grad. Texts Math. Springer, Cham, 1978.



Euler Circle
*Email address*: stephenzh99@gmail.com