The Local–Global Principle Using the Hasse–Minkowski Theorem

Akshatha Arunkumar

Received January 3, 2026
Accepted March 1, 2026
Electronic access March 15, 2026

The Hasse–Minkowski Theorem is a central result in number theory that connects local and global perspectives on quadratic equations. It states that a quadratic equation with rational coefficients has a non-trivial rational solution if and only if it has a solution over the real numbers and over every p-adic field. This idea shows how studying equations locally, one prime at a time, can determine whether they have a global solution. This paper offers an expository overview of the theorem and its mathematical foundation. It begins with quadratic forms and their properties, such as discriminants and isotropy, then introduces local fields and p-adic numbers, which describe completions of Q. The discussion highlights the Hilbert symbol and the Hilbert Reciprocity Law, which connect local conditions to produce the global result established by the theorem. Several examples and applications are explored, including the representation of integers as sums of squares and the classification of rational solutions. The paper concludes by showing how the local–global principle underlying this theorem continues to shape modern number theory, linking classical results with ongoing research in arithmetic geometry and algebraic structures.

Keywords: Hasse–Minkowski theorem, quadratic forms, p-adic numbers, Hilbert symbol, local–global principle, number theory

Introduction

The Hasse–Minkowski Theorem is a cornerstone in the theory of quadratic forms over number fields, offering a powerful local-global principle. It addresses the question of whether a quadratic equation, such as $ax^2 + by^2 + cz^2 = 0$, has a non-trivial solution (i.e. not all variables are zero) in rational numbers by checking its solvability in the real numbers and the p-adic numbers, which are completions of the rationals with respect to prime-based metrics[1]. Similarly, it determines when two quadratic forms are equivalent, meaning one can be transformed into the other via a linear change of variables. Historically, Hermann Minkowski proved the theorem for rational numbers, and Helmut Hasse generalized it to number fields. Its significance lies in its use of p-adic numbers, introduced by Kurt Hensel, to solve arithmetic problems, marking a significant advancement in number theory. This paper focuses on the theorem over Q, providing a clear exposition suitable for readers familiar with introductory algebra and number theory. The Hasse–Minkowski Theorem emerged from Hermann Minkowski's work on quadratic forms in the early 20th century, building on Kurt Hensel's discovery of p-adic numbers in 1897. Helmut Hasse later generalized it to number fields, formalizing the local-global principle. This theorem revolutionized number theory by providing a systematic method for solving Diophantine equations using local fields, thereby establishing it as a cornerstone for modern algebraic geometry and arithmetic.

Consider the equation

$$x^2 + y^2 = 3z^2.$$

Does it admit a non-trivial rational solution? Over R the form is indefinite, so solutions certainly exist, e.g. $(1, 1, \sqrt{2/3})$. Over Q_3, we can check for solutions by assuming $x, y, z \in Z_3$ and are not all divisible by 3 (by scaling). The equation $x^2 + y^2 = 3z^2$ modulo 3 becomes $x^2 + y^2 \equiv 0 \pmod 3$. Since the quadratic residues mod 3 are 0 and 1, this requires $x \equiv 0 \pmod 3$ and $y \equiv 0 \pmod 3$. This means x^2 and y^2 are divisible by 9. So $x^2 + y^2 = 9x_0^2 + 9y_0^2 = 3z^2$, which simplifies to $3(x_0^2 + y_0^2) = z^2$. This implies z must also be divisible by 3. Since $x, y,$ and z are all divisible by 3, this contradicts our assumption. Therefore, the only solution in Q_3 is the trivial one $(0, 0, 0)$.

Since a local obstruction appears at $p = 3$, there can be no rational solution. This illustrates the "easy" direction of Hasse–Minkowski: any rational solution must survive in every completion, so a failure in Q_3 blocks global solvability. The deep content of the Hasse–Minkowski Theorem is the converse: if a quadratic form has a non-trivial solution over R and every Q_p, then it necessarily has one over Q. This local-global principle is special to quadratic forms; for higher-degree equations (such as Selmer's cubic) local solvability does not imply global solvability.

Preliminaries and Definitions

Throughout, F denotes a field of characteristic $\neq 2$. Boldface letters $\mathbf{x}$, $\mathbf{y}$ represent column vectors.

Quadratic Forms

Definition 1 (Quadratic Form).
Let $n \geq 1$. A quadratic form in n variables over F is a homogeneous polynomial of degree 2,

$$Q(x_1, \ldots, x_n) = \sum_{i \leq j} c_{ij} x_i x_j = (x_1 \; x_2 \; \cdots \; x_n) A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

where $A = A^\top$ is an $n \times n$ symmetric matrix over F.

Isotropic vectors and hyperbolic planes

Definition 2. Let Q be a quadratic form on an F-vector space V and $\mathbf{x} \in V \setminus \{\mathbf{0}\}$.

- $\mathbf{x}$ is *isotropic* (for Q) if $Q(\mathbf{x}) = 0$.
- Q (or V) is *isotropic* if it possesses an isotropic vector; otherwise it is *anisotropic*.

Definition 3 (Bracket notation for diagonal forms).
If $a_1, \ldots, a_n \in F^\times$, we write

$$\langle a_1, \ldots, a_n \rangle$$

for the diagonal quadratic form $a_1 x_1^2 + \cdots + a_n x_n^2$. Thus, for instance, $\langle 1, -1 \rangle$ denotes the hyperbolic plane $x^2 - y^2$.

Definition 4 (Hyperbolic plane).
The binary form $H = \langle 1, -1 \rangle$ is called the *hyperbolic plane*. Equivalently, $H = \{(x,y) \in F^2 \mid Q(x,y) = x^2 - y^2\}$. It contains the isotropic vectors $(1,1)$ and $(1,-1)$, which are linearly independent.

Remark 1. Any two-dimensional isotropic subspace of a non-degenerate quadratic space over F is F-isometric to H. Hyperbolic planes will be the "building blocks" in Witt decomposition.

Example 1 (Isotropic vs. anisotropic).
Over R the form $Q_1(x,y) = x^2 - 2y^2$ is isotropic because $Q_1(1, \frac{1}{\sqrt{2}}) = 0$. In contrast, $Q_2(x,y) = x^2 + 2y^2$ is anisotropic over R (both terms are ≥ 0 and vanish simultaneously only at $(0,0)$). This distinction has a geometric interpretation as shown in Figure 1, which depicts an indefinite quadratic form whose zero set is non-trivial. The surface intersects the plane $z = 0$ along a cone, corresponding to non-zero vectors for which the quadratic form vanishes.

Over Q_3 the situation reverses: $\langle 1, 2 \rangle$ becomes isotropic because reducing the equation $x^2 + 2y^2 = 0$ modulo 3 gives

$$x^2 + 2y^2 \equiv x^2 - y^2 \equiv 0 \pmod 3,$$

since $2 \equiv -1 \pmod 3$. This congruence has non-trivial solutions, for example $x \equiv y \not\equiv 0 \pmod 3$, whereas $\langle 1, -2 \rangle$ is anisotropic.

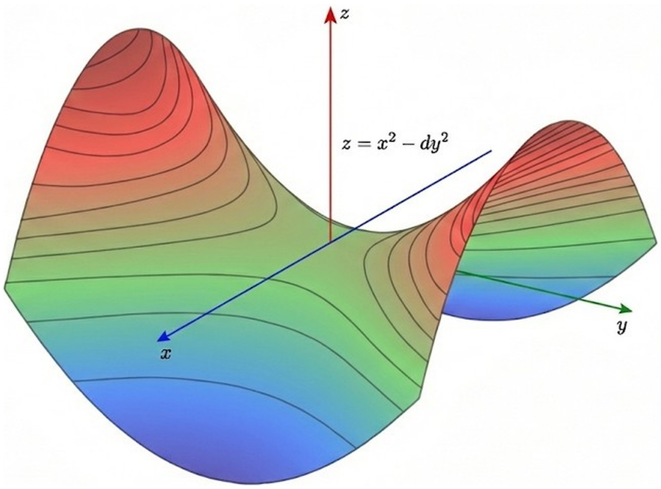

Fig. 1 The surface $z = x^2 - dy^2$ for $d > 0$, an example of an indefinite quadratic form. Its zero set is a double cone, illustrating the geometric origin of isotropic vectors.

Definition 5 (Equivalence).
Quadratic forms Q_1, Q_2 in n variables over F are *equivalent over F* if some $T \in \mathrm{GL}_n(F)$ (the group of invertible $n \times n$ matrices over F) satisfies $Q_2(\mathbf{y}) = Q_1(T\mathbf{y})$ for every $\mathbf{y} \in F^n$.

Proposition 1. Every non-degenerate quadratic form over F is equivalent to a diagonal form

$$Q(x_1, \ldots, x_n) = a_1 x_1^2 + \cdots + a_r x_r^2, \quad a_i \in F^\times,$$

where $r = \mathrm{rank}(Q)$ (see Definition 6).

Sketch. Write $Q(\mathbf{x}) = \mathbf{x}^\top A \mathbf{x}$ with A symmetric. Since $\mathrm{char}\, F \neq 2$, the element 2 is invertible in F, which allows us to complete the square. If a diagonal coefficient $a_{11} \neq 0$, then all terms involving x_1 can be grouped and rewritten by completing the square. After a suitable linear change of variables, this eliminates all cross terms involving x_1, leaving a single squared term together with a quadratic form in one fewer variable. Repeating this process inductively removes all off-diagonal terms and yields a diagonal form[2].

Example 2 (Diagonalising a binary form over Q).

$$Q(x,y) = 3x^2 + 4xy + 5y^2.$$

Its coefficient matrix is $A = \begin{pmatrix} 3 & 2 \\ 2 & 5 \end{pmatrix}$, so $\det A = 11 \neq 0$ and Q

is non-degenerate. Completing the square gives

$$Q(x,y) = 3\left(x + \tfrac{2}{3}y\right)^2 + \tfrac{11}{3}y^2.$$

Writing $u = x + \frac{2}{3}y,\ v = y$ (matrix $T = \left(\begin{smallmatrix} 1 & \frac{2}{3} \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(Q)$), we obtain the diagonal form $Q \cong \langle 3, \frac{11}{3} \rangle$.

Definition 6 (Rank).

For $Q(\mathbf{x}) = \mathbf{x}^\top A\mathbf{x}$, the *rank* of Q is $\mathrm{rank}(A)$, i.e. the dimension of the largest subspace on which Q is not identically 0.

Remark 2. After diagonalisation, $\mathrm{rank}(Q)$ is the number of non-zero diagonal coefficients.

Field extensions

Definition 7 (Field extension).

An extension K/F is a pair of fields with $F \subseteq K$. Its *degree* is $[K : F] = \dim_F K$ as an F-vector space.

Definition 8 (Finite & quadratic extensions).

An extension is *finite* if $[K : F] < \infty$. If $[K : F] = 2$ it is called *quadratic*. Every quadratic K/F has the form $K = F(\sqrt{d})$ for some $d \in F^\times \setminus F^{\times 2}$.

Definition 9 (Separable).

For characteristic 0 (in particular, $F = Q$) every algebraic extension is automatically separable: every element's minimal polynomial over F splits into distinct roots in a splitting field.

Remark 3. Finite separable extensions admit well-defined field trace $\mathrm{Tr}_{K/F}$ and norm $\mathrm{N}_{K/F}$. These appear later when we relate the Hilbert symbol to norm forms.

Example 3 (Quadratic extension of Q).

Set $K = Q(\sqrt{5})$. The minimal polynomial of $\sqrt{5}$ over Q is $x^2 - 5$, so $[K : Q] = 2$; hence K/Q is quadratic (and separable). For $\alpha = x + y\sqrt{5}$ $(x, y \in Q)$:

$$\mathrm{Tr}_{K/Q}(\alpha) = 2x, \qquad \mathrm{N}_{K/Q}(\alpha) = x^2 - 5y^2.$$

The latter gives the Pell conic $X^2 - 5Y^2 = 1$.

Fields, absolute values, and completions

Definition 10 (Absolute value).

An *absolute value* on a field K is a map $|\cdot|\colon K \to R_{\geq 0}$ such that

1. $|x| = 0 \iff x = 0$;
2. $|xy| = |x||y|$;
3. $|x + y| \leq |x| + |y|$.

It is *non-Archimedean* if $|x + y| \leq \max\{|x|, |y|\}$.

On Q there are, up to equivalence, exactly the usual absolute value $|\cdot|_\infty$ and the p-adic absolute values $|\cdot|_p$, one for each prime p[3].

Definition 11 (Completion).

Let $(K, |\cdot|)$ be a valued field. Its *completion* $\widehat{K}$ is the metric completion of K with respect to $d(x,y) = |x - y|$. We write

$$Q_\infty = R, \qquad Q_p \ (p \text{ prime})$$

for the completions of Q.

Example 4 (Real vs. p-adic magnitude).

Take $x = \dfrac{14}{75}$. The ordinary absolute value is $|x|_\infty \approx 0.187$, but factorising $x = 5^{-2} \cdot 14 \cdot 3^{-1}$ gives $v_5(x) = -2$ and $|x|_5 = 5^{-(-2)} = 25$. Thus, a "small" real can be "large" 5-adically.

Bilinear forms, discriminant, Witt decomposition

Definition 12 (Discriminant).

Let Q be a non-degenerate quadratic form in n variables over F, represented by a symmetric matrix A. Define

$$\mathrm{disc}(Q) = (-1)^{n(n-1)/2} \det A \in F^\times / F^{\times 2}.$$

That is, the discriminant is the determinant of A, corrected by a sign depending on n, taken modulo the subgroup of square elements.

Remark 4. If Q_1 and Q_2 are equivalent quadratic forms over F (see Definition 5), then $\mathrm{disc}(Q_1) = \mathrm{disc}(Q_2)$ in $F^\times / F^{\times 2}$. Indeed, if $Q_2(\mathbf{y}) = Q_1(T\mathbf{y})$ with $T \in \mathrm{GL}_n(F)$, then their coefficient matrices satisfy $A_2 = T^\top A_1 T$, so

$$\det(A_2) = \det(T)^2 \det(A_1).$$

Thus, the two determinants differ by a square in $F^\times$, and hence represent the same class in $F^\times / F^{\times 2}$.

Every quadratic form Q yields such a B by $B(\mathbf{x}, \mathbf{y}) = \frac{1}{2}\big(Q(\mathbf{x} + \mathbf{y}) - Q(\mathbf{x}) - Q(\mathbf{y})\big)$.

Example 5. For the diagonal ternary form $\langle 1, 1, 1 \rangle$ we have

$$\mathrm{disc}\big(\langle 1, 1, 1 \rangle\big) = (-1)^3 = -1 \quad \text{in } Q^\times / Q^{\times 2}.$$

Hence $\langle 1, 1, 1 \rangle$ is not Q-equivalent to $\langle 1, 1, -1 \rangle$, whose discriminant is $+1$.

Example 6 (Hyperbolic plane).

$H = \langle 1, -1 \rangle$ is isotropic, since $(1, 1)$ is a non-trivial zero. Any isotropic plane is F-isometric to H.

Definition 13 (Orthogonal sum).

If Q_1 and Q_2 are quadratic forms over F, their *orthogonal sum* is written $Q_1 \perp Q_2$, and defined on the direct sum of the underlying vector spaces by

$$(Q_1 \perp Q_2)(v_1, v_2) = Q_1(v_1) + Q_2(v_2).$$

More generally, $Q^{\perp r}$ denotes the orthogonal sum of r copies of Q.

Theorem 1 (Witt decomposition).

Every non-degenerate quadratic form Q over F decomposes uniquely (up to isometry) as

$$Q \cong H^{\perp r} \perp Q_{\text{an}},$$

where H is the hyperbolic plane and Q_{an} is anisotropic. The integer r is the *Witt index* of Q. See[4].

Example 7 (Witt decomposition of a quaternary form).

Let

$$Q = \langle 1, 1, -1, -1 \rangle = x^2 + y^2 - z^2 - w^2.$$

Choose isotropic vectors $\mathbf{v}_1 = (1,0,1,0)$ and $\mathbf{v}_2 = (0,1,0,1)$ with $B_Q(\mathbf{v}_1, \mathbf{v}_2) = 0$. They span a hyperbolic plane H; repeating with another pair yields

$$Q \cong H \perp H,$$

so the Witt index is 2 and the anisotropic part is 0.

Norms and traces in quadratic extensions

For $K = F(\sqrt{d})$ and $\alpha = x + y\sqrt{d}$, put

$$\mathrm{Tr}_{K/F}(\alpha) = 2x, \qquad \mathrm{N}_{K/F}(\alpha) = x^2 - dy^2.$$

The norm form $\mathrm{N}_{K/F}$ is a basic 2-variable quadratic form whose local isotropy answers norm-related questions.

Local Fields and Completions

Classical Diophantine problems over Q can often be understood one prime at a time. This idea is made precise by working in the *completions* of Q—the real field R at the infinite place and the p-adic fields Q_p at each finite place p.

Ostrowski's classification of norms on Q

Proposition 2 (Product formula). For every $x \in Q^\times$,

$$\prod_{p \le \infty} |x|_p = 1.$$

Theorem 2 (Ostrowski, 1916). Every non-trivial absolute value on Q is equivalent to either

$$|\cdot|_\infty \quad \text{(the usual Archimedean norm)} \quad \text{or} \quad |\cdot|_p \quad (p \text{ a prime}).$$

No other inequivalent norms exist.

Idea of proof. For any $x \in Q^\times$ write $x = \pm p_1^{k_1} \cdots p_r^{k_r}$. If $|\cdot|$ is non-Archimedean one shows $|x| = \rho^{k_j}$ for a single prime p_j; rescaling makes it $|\cdot|_{p_j}$. If $|\cdot|$ is Archimedean, Kronecker's lemma implies it coincides (up to equivalence) with the usual absolute value. A more detailed proof can be found at[5].

Remark 5. Ostrowski's theorem shows that, up to equivalence, the only non-trivial completions of Q are the real field R (corresponding to $|\cdot|_\infty$) and the p-adic fields Q_p for primes p. Hence, when we say a statement holds "at every completion of Q," we really mean: it holds over R and over Q_p for each prime p. Verifying local conditions at these places is therefore exhaustive in the Hasse–Minkowski theorem.

Example 8 (Product formula sanity check).

For $n = 30 = 2 \cdot 3 \cdot 5$ one has

$$|30|_\infty = 30, \quad |30|_2 = 2^{-1}, \quad |30|_3 = 3^{-1}, \quad |30|_5 = 5^{-1},$$

$$|30|_p = 1 \ (p \neq 2, 3, 5).$$

Hence $|30|_\infty \prod_p |30|_p = 30 \cdot 2^{-1} \cdot 3^{-1} \cdot 5^{-1} = 1$, illustrating the global product formula used implicitly in Ostrowski's proof.

p-adic valuation and norm

Definition 14 (p-adic valuation).

For a prime p and a non-zero rational $x \in Q^\times$, write $x = p^k a/b$ with $a, b \in Z$ not divisible by p. Set $v_p(x) = k$ and $v_p(0) = \infty$.

Definition 15 (p-adic norm).

The p-adic norm is

$$|x|_p = p^{-v_p(x)}, \quad x \in Q.$$

It satisfies the non-Archimedean inequality $|x+y|_p \le \max\{|x|_p, |y|_p\}$.

Completions and the field Q_p

Completing $(Q, |\cdot|_p)$ in the metric $d_p(x,y) = |x-y|_p$ yields the p-adic field Q_p. For the usual absolute value, we obtain $Q_\infty = R$. Elements of Q_p can be written as series $\sum_{n \ge k} a_n p^n$ with digits $a_n \in \{0, \ldots, p-1\}$.

Constructing p-adic Numbers

As mentioned above, the p-adic numbers Q_p arise as the completion of Q with respect to the p-adic norm. For example, in Q_5, the number $\frac{1}{1-5} = -\frac{1}{4}$ can be written as a 5-adic series:

$$\frac{1}{1-5} = \sum_{n=0}^{\infty} 5^n = 1 + 5 + 5^2 + \cdots.$$

This series converges in Q_5 because $|5^n|_5 = 5^{-n} \to 0$ as $n \to \infty$.

Figure 2 illustrates the hierarchical structure of the 5-adic integers Z_5, showing how residue classes modulo higher powers of 5 nest within one another.

Figure 3 illustrates how the partial sums converge 5-adically even though their absolute size grows in the real numbers.

Such series make Q_p a complete field, enabling tools like Hensel's lemma for solving equations.

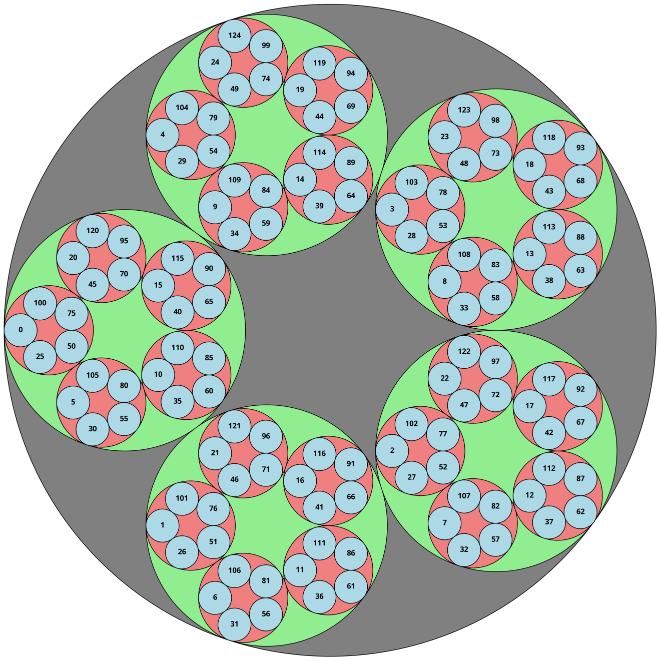

Fig. 2 A visualization of the 5-adic integers Z_5, showing the nested structure of residue classes modulo 5 and their further refinement modulo 25, 125, and so on.

Topology of Q_p

Each Q_p is locally compact (meaning every point has a compact neighborhood) and totally disconnected (meaning the only connected subsets are single points). The compact open unit group $Z_p^\times$ (the p-adic integers with no factor of p) is procyclic for $p \neq 2$ (it is the limit of cyclic groups).

Strong approximation

The strong approximation theorem states that for any finite set S of primes, the diagonal embedding $Q \hookrightarrow \prod_{v \in S} Q_v$ is dense. This means any set of p-adic numbers in these fields can be simultaneously approximated by a single rational number. This property is key, as it lets us patch local solutions into a global one once obstructions vanish.

Why bother with completions?

- **Analytic control.** Limits exist in a completion, so Newton iteration and Hensel's lemma can lift solutions of congruences to genuine p-adic (hence rational) solutions.
- **Local–global philosophy.** Many arithmetic statements are true over Q exactly when they hold in every completion; Hasse–Minkowski for quadratic forms is the prime example.

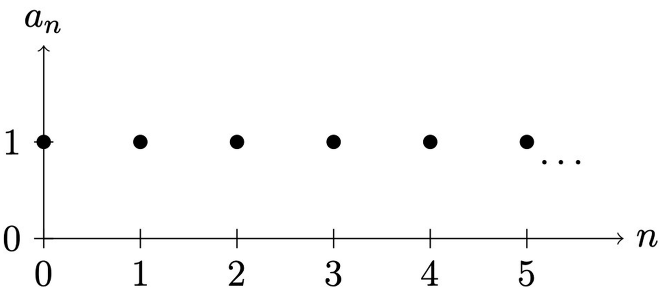

Fig. 3 5-adic expansion of $-\frac{1}{4} = 1 + 5 + 5^2 + \cdots$ in Q_5. Each dot represents $a_n = 1$.

Hensel's Lemma

Lemma 1 (Hensel's Lemma, simple form).
Let p be a prime and $f(x) \in Z_p[x]$. Assume there exists $a_0 \in Z_p$ such that

$$f(a_0) \equiv 0 \pmod{p} \quad \text{and} \quad f'(a_0) \not\equiv 0 \pmod{p}.$$

Then there is a unique $\tilde{a} \in Z_p$ satisfying

$$f(\tilde{a}) = 0 \quad \text{and} \quad \tilde{a} \equiv a_0 \pmod{p}.$$

Equivalently, any root modulo p with non-vanishing derivative lifts to a unique root in the entire p-adic field Q_p.

Example (lifting a square root of 2 from F_7 to Q_7)

We illustrate Hensel's lemma with the congruence $x^2 \equiv 2 \pmod{7}$.

1. In F_7, $3^2 = 9 \equiv 2$, so $x_0 = 3$ is a root modulo 7.
2. Let $f(x) = x^2 - 2$. Because $f'(x_0) = 2x_0 = 6 \not\equiv 0 \pmod{7}$, Hensel's lemma applies.
3. One Newton–Hensel step (working mod 49):
$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)} = 3 - \frac{9-2}{6} = 3 - \frac{7}{6}.$$
We need $6^{-1} \pmod{49}$. Since $6 \cdot 41 = 246 = 49 \cdot 5 + 1$, we have $6^{-1} \equiv 41 \pmod{49}$. Hence
$$\frac{7}{6} \equiv 7 \cdot 41 = 287 \equiv 42 \pmod{49}, \quad \text{so} \quad x_1 \equiv 3 - 42 \equiv -39 \equiv 10 \pmod{49}.$$
4. Verification: $10^2 = 100 = 49 \cdot 2 + 2 \equiv 2 \pmod{49}$. Thus $x_1 = 10$ is a root modulo 49. Repeating the process (or invoking Hensel directly) yields a unique $\tilde{x} \in Z_7$ with $\tilde{x} \equiv 10 \pmod{49}$ and $\tilde{x}^2 = 2$.

Remark 6. The condition $f'(\tilde{x}) \not\equiv 0 \pmod{p}$ is essential for Hensel's lemma: it ensures the lift exists and is unique.

Isotropy over local fields: quick examples

We record three illustrative calculations that foreshadow the local analysis in the Hasse–Minkowski theorem.

Example 9 (A binary form anisotropic over R but isotropic over Q_3).

Take $B = \langle 1, 2\rangle = x^2 + 2y^2$.

- Over R both terms are non-negative and vanish simultaneously only at $(0,0)$; B is anisotropic.
- In F_3 we have $2 \equiv -1$, and $x^2 - y^2 = 0$ has solutions $(1,1)$, $(1,2)$. Hensel's lemma lifts either to a 3-adic isotropic vector, so B is isotropic over Q_3.

Example 10 (Hyperbolic plane everywhere locally).

The form $H = \langle 1, -1\rangle$ is isotropic over R (obvious) and over every Q_p, since $x^2 \equiv y^2 \pmod{p}$ always has non-trivial solutions.

These computations illustrate that local isotropy can vary wildly with the place v, highlighting the necessity of checking all completions in the Hasse–Minkowski criterion.

Legendre Symbol and Quadratic Residues

Basic definitions

Definition 16 (Quadratic residue modulo p).

Let p be an odd prime. An integer a is a *quadratic residue* modulo p if the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution $x \in Z$. Otherwise, a is a *quadratic non-residue*.

Definition 17 (Legendre symbol).

For an odd prime p and any integer a, define

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue } (\bmod p), \\ -1 & \text{if } a \text{ is a quadratic non-residue } (\bmod p). \end{cases}$$

The map $\left(\frac{\cdot}{p}\right) : Z \to \{-1, 0, 1\}$ descends to a group homomorphism $\left(\frac{\cdot}{p}\right) : (Z/pZ)^\times \longrightarrow \{\pm 1\}$.

Example 11 (Computing a Legendre symbol).

Compute $\left(\frac{7}{19}\right)$. Because 19 is prime,

$$\left(\tfrac{7}{19}\right) = 7^{(19-1)/2} \bmod 19 = 7^9 \bmod 19.$$

Fast exponentiation:

$$7^2 = 49 \equiv 11, \quad 7^4 \equiv 11^2 = 121 \equiv 7, \quad 7^8 \equiv 7^2 = 11.$$

Hence $7^9 = 7^8 \cdot 7 \equiv 11 \cdot 7 = 77 \equiv 1 \pmod{19}$, so $\left(\frac{7}{19}\right) = +1$. Thus 7 is a quadratic residue modulo 19.

Quadratic Reciprocity

Theorem 3 (Quadratic Reciprocity Law).

For distinct odd primes p and q,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Equivalently,

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\dfrac{p}{q}\right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4}, \\ -\left(\dfrac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

Together with the supplementary laws $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ and $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, this completely determines all Legendre symbols.

Example 12. Compute $\left(\frac{7}{19}\right)$. Since $7 \equiv 3 \pmod{4}$ and $19 \equiv 3 \pmod{4}$,

$$\left(\tfrac{7}{19}\right) = -\left(\tfrac{19}{7}\right) = -\left(\tfrac{5}{7}\right).$$

Because $5^3 = 125 \equiv -1 \pmod{7}$ we have $\left(\frac{5}{7}\right) = -1$, hence $\left(\frac{7}{19}\right) = +1$.

Example: deciding local solvability with $(\cdot/p)$

Determine whether $x^2 \equiv 5 \pmod{11}$ has a solution.

$$\begin{aligned} \left(\frac{5}{11}\right) &= \left(\frac{11}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{11-1}{2}} \quad \text{(Quadratic Reciprocity)} \\ &= \left(\frac{1}{5}\right)(-1)^{2\cdot 5} = 1. \end{aligned}$$

Hence 5 is a quadratic residue mod 11, so the congruence is solvable. Indeed $x \equiv 4$ or $x \equiv 7$ works.

Remark 7. Legendre symbols (and their higher-power generalisation, the Jacobi symbol) give a quick local test at each prime. In later sections, we will combine these local conditions with Hensel's lemma and completions to analyse global solvability of quadratic forms.

Hilbert Symbol and Local Quadratic Forms

The Hilbert symbol is a key invariant for classifying quadratic forms over local fields.

Definition 18 (Hilbert Symbol).

For a local field K (e.g., Q_p or R) and $a, b \in K^\times$, the Hilbert symbol $(a,b)_K$ is defined as:

$$(a,b)_K = \begin{cases} 1 & \text{if } x^2 - ay^2 - bz^2 = 0 \text{ has a non-trivial solution in } K, \\ -1 & \text{otherwise.} \end{cases} \tag{1}$$

Proposition 3 (Explicit formula for p odd).

Let p be an odd prime. Write $a = p^{\alpha}u$, $b = p^{\beta}v$ with $\alpha, \beta \in Z$ and $u, v \in Z_p^{\times}$. Then

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

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. In particular, if pab then $(a,b)_p = 1$ unless both $\left(\frac{u}{p}\right) = \left(\frac{v}{p}\right) = -1$.

Remark 8 (Real place).

Over R one has $(a,b)_{\infty} = -1$ iff $a < 0$ and $b < 0$, otherwise $+1$.

Example 13 (Computing $(2,3)_5$).

Over Q_5, $2 = 5^0 \cdot 2$, $3 = 5^0 \cdot 3$, so $\alpha = \beta = 0$. By Proposition 3,

$$(2,3)_5 = (-1)^0\left(\tfrac{2}{5}\right)^0\left(\tfrac{3}{5}\right)^0 = 1.$$

Thus $z^2 = 2x^2 + 3y^2$ has a nontrivial 5-adic solution.

Proposition 4 (Basic properties of the Hilbert symbol).

Let K be a local field with $\operatorname{char} K \neq 2$ and $a, b, c \in K^{\times}$. Then

1. Symmetry: $(a,b)_K = (b,a)_K$.
2. Bilinearity in the first slot: $(ab,c)_K = (a,c)_K(b,c)_K$ (and hence also in the second by (1)).
3. $(a,-a)_K = 1$.
4. If $a \neq 1$ then $(a,1-a)_K = 1$.
5. $(a,b)_K = 1$ for every b iff a is a square in K (for $K \neq C$).

Proof. Write $Q_{a,b}(x,y,z) = x^2 - ay^2 - bz^2$. (1) follows because $Q_{a,b}$ and $Q_{b,a}$ are isometric via $(x,y,z) \mapsto (x,z,y)$. For (2) observe $Q_{ab,c}(x,y,z) = x^2 - aby^2 - cz^2$ splits into the direct orthogonal sum of $Q_{a,c}$ and $Q_{b,c}$ on suitable 2-planes, so the symbol multiplies. Property (3) is immediate from $x^2 - ay^2 + az^2 = 0$ with $(x,y,z) = (\sqrt{a},1,1)$. For (4) note $x^2 - ay^2 - (1-a)z^2 = 0$ has the rational solution $(1,a,1)$. Finally, (5) is a restatement of the fact that the 1-dimensional quadratic form $\langle a \rangle$ is isotropic over K exactly when a is a square[6].

Example 14 (Bilinearity check).

Over Q_3: $(30,7)_3 = (6 \cdot 5,7)_3 = (6,7)_3(5,7)_3$, matching Proposition 4. Explicit calculation confirms each factor.

Theorem 4 (Hilbert Reciprocity).

For $a, b \in Q^{\times}$ one has

$$\prod_v (a,b)_v = 1,$$

where the product ranges over all places v: $Q \hookrightarrow R$ or Q_p.

Sketch of proof. Let $K = Q(\sqrt{a})$ and write $\mathrm{N}_{K/Q}(\cdot)$ for the norm. A classical argument shows

$$(a,b)_v = 1 \Longleftrightarrow b \text{ is a norm from } K \otimes_Q Q_v.$$

Class field theory (or the product formula for global Hilbert symbols) asserts that an element of $Q^{\times}$ is a global norm iff it is a local norm everywhere and the product of all local Hilbert symbols equals 1. Applying this to both b and an auxiliary $n \in Q^{\times}$ chosen so that $(a,n)_v = (a,b)_v$ except at one place, one deduces $\prod_v (a,b)_v = 1$. See[7].

Example 15. Take $a = 3$, $b = 5$. Direct computation shows

$$(3,5)_{\infty} = 1, \quad (3,5)_2 = 1, \quad (3,5)_3 = -1, \quad (3,5)_5 = -1,$$

and $(3,5)_p = 1$ for all other p, so $\prod_v (3,5)_v = 1$ as predicted by reciprocity.

For R, $(a,b)_R = -1$ if and only if $a < 0$ and $b < 0$. For Q_p, the Hilbert symbol can be computed using the Legendre symbol and local invariants. The Hasse invariant of a quadratic form, defined using Hilbert symbols, helps classify forms over local fields. Hilbert reciprocity states that for $a, b \in Q^{\times}$, $\prod_v (a,b)_v = 1$, where v runs over all places.

Hasse–Minkowski Theorem and Proof

Theorem 5 (Hasse–Minkowski Theorem).

Let Q be a quadratic form over Q. Then $Q(\mathbf{x}) = 0$ has a non-trivial solution over Q if and only if it has a non-trivial solution over R and over Q_p for every prime p. Moreover, two quadratic forms over Q are equivalent if and only if they are equivalent over R and every Q_p.

Let $Q = \langle a_1, \ldots, a_n \rangle$ be a non-degenerate quadratic form over Q. The goal is to show:

$$Q(\mathbf{x}) = 0 \text{ has nontrivial } \mathbf{x} \in Q^n \Leftrightarrow Q \text{ is isotropic over}$$

R and all Q_p $\forall p$,

$$Q \sim Q' \text{ over } Q \Leftrightarrow Q \sim Q' \text{ over } R \text{ and } Q_p \ \forall p.$$

For any local field F, the local invariants are: dimension, discriminant $d_F(Q) = (-1)^{n(n-1)/2}\det(Q) \in F^{\times}/F^{\times 2}$, and Hasse invariant

$$\varepsilon_F(Q) = \prod_{1 \le i < j \le n} (a_i, a_j)_F,$$

where $(a,b)_F$ is the Hilbert symbol. Quadratic forms over F are equivalent iff these three invariants agree.

Necessity: Immediate: a rational solution persists in all completions.

Sufficiency: Diagonalize Q over Q, $Q = \langle a_1, \ldots, a_n \rangle$, so $Q(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i^2$. Assume Q is isotropic in all Q_p and R.

Consider cases by n:

Case $n = 1$: $Q(x) = a_1x^2$. The only nontrivial solution in Q requires $a_1 = 0$, which is ruled out for non-degeneracy.

Case $n = 2$: Let $Q(x,y) = a_1x^2 + a_2y^2$. Then Q is isotropic over a field F if and only if $-a_1/a_2$ is a square in F. Thus, isotropy over R and over every Q_p implies that $-a_1/a_2$ is a square in all completions of Q. By the local–global principle for squares[8], an element of $Q^\times$ that is a square in R and in every Q_p is already a square in Q. Hence Q is isotropic over Q.

Case $n = 3$ (Proof sketch): Let $Q(x,y,z) = ax^2 + by^2 + cz^2$. After scaling, assume $c = 1$. Then Q is isotropic over a field F if and only if the Hilbert symbol $(a,b)_F = 1$. Hence, isotropy at every completion Q_v is equivalent to $(a,b)_v = 1$ for all places v. By Hilbert reciprocity,

$$\prod_v (a,b)_v = 1,$$

and the condition $(a,b)_v = 1$ for all v is equivalent to b being a norm from the quadratic extension $Q(\sqrt{a})/Q$[9]. Thus there exist $u,w \in Q$ with

$$b = u^2 - aw^2,$$

and substituting $(x,y,z) = (w,0,u)$ gives a nontrivial rational zero of Q.

Case $n = 4$ (Proof sketch): Let $Q = \langle a,b,c,d \rangle$ and scale so that $abcd \in Q^{\times 2}$. In dimension 4, isotropy of Q over a field F is equivalent to the splitting of an associated quaternion algebra $(a,b)_F$, and local isotropy at a place v is therefore equivalent to the splitting of $(a,b)_{Q_v}$. By the global reciprocity law for quaternion algebras, a quaternion algebra over Q splits if and only if it splits at every completion. Hence if Q is isotropic over R and over every Q_p, the associated quaternion algebra splits globally, and therefore Q is isotropic over Q[10].

Case $n \geq 5$ (Proof sketch): In dimension at least 5, a nondegenerate quadratic form over a number field that is isotropic over every completion is isotropic over the field itself. This follows from the structure theory of quadratic forms and the local–global principle for isotropy in sufficiently large dimension[9]. Hence, since Q is isotropic over R and over every Q_p, it is isotropic over Q. Equivalently, Q splits off a hyperbolic plane,

$$Q \cong H \perp Q',$$

and we conclude by induction on the dimension. While this principle guarantees existence, the quantitative problem of bounding the size of nontrivial isotropic vectors is more subtle; Dietmann[11] gives explicit bounds for small solutions of quadratic Diophantine equations.

Equivalence: Suppose Q, Q' are quadratic forms of the same dimension, equivalent at every completion. Then $d_Q(Q) = d_Q(Q')$ and $\varepsilon_v(Q) = \varepsilon_v(Q')$ for all v. By the product formula for Hilbert symbols and Hasse invariants (Hilbert reciprocity), and the matching local invariants everywhere, the forms must also be equivalent over Q. Indeed, patch local isometries at each place to get a global isometry, as quadratic form equivalence over global fields is determined by the aggregate of local invariants.

Applications

We highlight three classical consequences of the Hasse–Minkowski theorem and sketch the underlying proofs.

Sums of squares

Theorem 6 (Lagrange, 1770).

Every nonnegative integer is the sum of four integer squares.

Let $n \in N$. We seek $x_1,x_2,x_3,x_4 \in Z$ such that $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Step 1: Consider the difference form

$$Q_n(x_1,x_2,x_3,x_4,z) = x_1^2 + x_2^2 + x_3^2 + x_4^2 - nz^2,$$

which is a quadratic form over Q in five variables. By the local-global principle, Q_n is isotropic over Q if and only if it is isotropic over R and every Q_p. Over R, Q_n is isotropic because there are both positive and negative coefficients. Over each Q_p, it is a classical fact that any $u \in Q_p^\times$ is a sum of four squares for $p \neq 2$. For $p = 2$, one checks explicitly or uses Hensel's lemma to lift solutions from F_2. So, by Hasse–Minkowski, there exist $x_1,x_2,x_3,x_4,z \in Q$, $z \neq 0$, so that

$$n = \frac{x_1^2 + x_2^2 + x_3^2 + x_4^2}{z^2}$$

and thus n is a sum of four rational squares.

Step 2 (Descent from rationals to integers): Suppose n admits a rational representation

$$n = \left(\frac{a_1}{m}\right)^2 + \left(\frac{a_2}{m}\right)^2 + \left(\frac{a_3}{m}\right)^2 + \left(\frac{a_4}{m}\right)^2, \quad a_i, m \in Z,\ m > 0.$$

Clearing denominators gives

$$nm^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

We show by descent on m that one can reach $m = 1$. Choose integers a_i, m with $\gcd(a_1,\dots,a_4,m) = 1$ such that $nm^2 = \sum a_i^2$ and m minimal. If $m = 1$ we are done. Let p be a prime dividing m. Reduce the congruence $\sum a_i^2 \equiv 0 \pmod{p}$. Since not all a_i vanish mod p (minimality of m), this gives a nontrivial quadruple mod p satisfying $\sum x_i^2 \equiv 0 \pmod{p}$. It is a classical fact that every prime p divides a sum of four squares, so there exist integers r_1,r_2,r_3,r_4 with $r_1^2 + r_2^2 + r_3^2 + r_4^2 = p^2$ and at least one r_i divisible by p. Using Euler's identity

$$\begin{aligned}&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\ &= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + \cdots + (x_4y_1 + x_3y_2 - x_2y_3 + x_1y_4)^2,\end{aligned}$$

multiply the two representations

$$(a_1^2 + \cdots + a_4^2)(r_1^2 + \cdots + r_4^2) = (nm^2)(p^2).$$

Because one r_i is divisible by p, all new coordinates produced by Euler's formula are divisible by p; dividing by p^2 yields another representation

$$n(m')^2 = b_1^2 + b_2^2 + b_3^2 + b_4^2$$

with $m' = m/p < m$. This contradicts the minimality of m unless $m = 1$.

By repeated application of this reduction for each prime dividing m, we eventually reach $m = 1$, producing integers x_i with $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Hence, any rational representation can be converted into an integer one.

Alternatively, Gauss's reduction algorithm applied to the lattice of quadruples representing n guarantees one can always find integer solutions. This yields Lagrange's integer result from the Hasse–Minkowski rational step combined with integrality tools.

More generally, modern work has extended this perspective to classify which quadratic forms represent all positive integers. Most notably, the 290-Theorem of Bhargava and Hanke[12] shows that a positive-definite integral quadratic form is universal if and only if it represents each integer in a specific finite test set contained among the integers up to 290. Related classification results for forms representing all odd integers were established by Rouse[13].

The same reasoning with the ternary difference form $x^2 + y^2 + z^2 - nw^2$ recovers Legendre's three-square criterion $n \not\equiv 0, 4, 7 \pmod 8$.

Application to Sums of Three Squares

Legendre's three-square theorem states that a positive integer n can be represented as a sum of three squares if and only if it is not of the form $4^k(8m+7)$. Using Hasse–Minkowski, we check local conditions at infinity (real positive definite fails for negative, but difference form is indefinite) and at $p = 2$ (anisotropic for forbidden forms mod 8). This local failure at $p = 2$ or infinity explains the criterion.

Table 1 shows that the integers 1, 2, 3, and 9 can be written as sums of three squares, but 7 cannot. This illustrates the exceptional case identified by Legendre's three-square theorem and demonstrates how a local obstruction leads to global non-representability.

n	Representation
1	$1^2 + 0^2 + 0^2$
2	$1^2 + 1^2 + 0^2$
3	$1^2 + 1^2 + 1^2$
7	No Representation
9	$3^2 + 0^2 + 0^2$

Table 1 First few positives and three-square representations.

Classification of quadratic forms over Q

Theorem 7. Two non-degenerate quadratic forms Q, Q' over Q are equivalent over Q if and only if

$$\dim Q = \dim Q', \quad \mathrm{disc}(Q) = \mathrm{disc}(Q') \in Q^\times / Q^{\times 2}, \quad (a_i, a_j)_v = (a'_i, a'_j)_v \text{ for all } v,$$

i.e. they have the same dimension, the same discriminant, and matching Hilbert invariants at every place.

Idea. Over each completion Q_v, the triple $(\dim, \mathrm{disc}, \varepsilon_v)$ with $\varepsilon_v(Q) = \prod_{i<j}(a_i, a_j)_v$ classifies quadratic forms[14]. If the three data agree globally, then $Q \cong Q'$ locally everywhere. The second part of Theorem 5 (equivalence) then upgrades these local isometries to a rational isometry.

Algorithmic test for Q-equivalence

A practical version of Theorem 7 is the Cassels–Ehrlich algorithm. Given two non-degenerate forms Q, Q' in the same number of variables, it decides (in polynomial time for fixed dimension) whether they are Q-equivalent.

1. **Diagonalise.** Use Proposition 1 to write $Q \cong \langle a_1, \ldots, a_n \rangle$ and $Q' \cong \langle a'_1, \ldots, a'_n \rangle$.

2. **Match discriminants.** If $\mathrm{disc}(Q) \neq \mathrm{disc}(Q') \in Q^\times / Q^{\times 2}$, return No.

3. **Compute local symbols.** For each finite set of primes dividing $2\,\mathrm{disc}(Q)\,\mathrm{disc}(Q')$ and for $v = \infty$: evaluate $(a_i, a_j)_v$ and $(a'_i, a'_j)_v$. If any place disagrees, return No.

4. **Solve a gluing problem.** Having identical local invariants, construct an explicit isometry matrix $T \in \mathrm{GL}_n(Q)$ by CRT-patching the local isometries; see[14].

5. **Return.** Output T (or Yes) if the gluing succeeds, otherwise No.

While the Cassels–Ehrlich algorithm handles equivalence, determining specific small solutions or enumerating representations requires more specialized techniques. Simon[15] and Kirschmer and Voight[16] have developed advanced algorithms for solving quadratic equations in dimension 4 and higher, optimizing the computational complexity of finding explicit solutions.

Example 16 (Two equivalent quaternary forms).

Let $Q = \langle 1, 1, 1, -1 \rangle$, $Q' = \langle 2, 2, 2, -2 \rangle$.

Step 1: already diagonal.

Step 2: $\mathrm{disc}(Q) = \mathrm{disc}(Q') = +1$.

Step 3: for every place v, $(1,1)_v = (2,2)_v = 1$ and the mixed symbols coincide, so local data match.

Step 4: a CRT construction gives $T = \mathrm{diag}(1, 1, 1, \frac{1}{2}) \in \mathrm{GL}_4(Q)$ with $Q'(x) = Q(Tx)$. Hence, the algorithm outputs Yes.

This result may be viewed as the global analogue of Witt's local classification and is a template for more sophisticated adelic invariants in higher-degree forms.

Rational points on conics

Let $a, b \in Q^{\times}$. The projective conic

$$C_{a,b}\colon ax^2 + by^2 = z^2$$

has a Q-rational point $[x : y : z] \neq [0 : 0 : 0]$ if and only if the following local conditions hold:

1. **Real place:** a and b are not both negative.
2. **p-adic places:** $(a,b)_p = 1$ for every prime $p \mid 2ab$.

Write the associated ternary quadratic form $Q_{a,b}(x,y,z) = ax^2 + by^2 - z^2$. A rational point on $C_{a,b}$ corresponds to an isotropic vector for $Q_{a,b}$. Condition (a) is exactly isotropy over R. Condition (b) is equivalent to isotropy over each Q_p by Definition 18. Applying Theorem 5 yields the desired equivalence.

Remark 9. Once a single rational point is known, one obtains all rational solutions by a standard line-through-a-point parameterisation.

A cubic counter-example: Selmer's form

The Hasse–Minkowski theorem is special to quadratic forms. For higher-degree equations, local solvability need not imply global solvability.

A classical counterexample is Selmer's[17] cubic equation

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

This equation has nontrivial solutions over R and over Q_p for every prime p, but no nontrivial solution over Q. Thus, it is locally solvable everywhere but not globally solvable, showing that the local–global principle fails for cubic equations.

$S(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$ is locally solvable everywhere, yet has no nontrivial rational solution.

(1) Local solvability:

- *Over R:* We have $S(1,1,0) = 7 > 0$ and $S(1,-1,0) = -1 < 0$. By the Intermediate Value Theorem[18], there exists $(x,y,0) \in R^3$ with $S = 0$.
- *Reformulation as an elliptic curve.* To study solutions over Q_p, it is convenient to pass to an equivalent projective model. After a projective change of variables, one obtains
$$E: \quad X^3 + Y^3 + 60Z^3 = 0,$$
an elliptic curve over Q. The coefficient 60 arises from Selmer's normalization, which concentrates the arithmetic difficulty at the primes $2,3,5$ and makes the 3-descent computation tractable[17].
- *Over Q_p:* For primes $p \neq 2,3,5$, the curve has good reduction. By the Hasse bound, $E(F_p)$ has nonsingular points, which lift via Hensel's lemma to points in $E(Q_p)$. Local solvability at $p = 2,3,5$ was established by Selmer. Thus, solutions exist over every Q_p.

Therefore, the equation $S(x,y,z) = 0$ is locally solvable at every place of Q.

(2) Global failure: Selmer proved using 3-descent that $E(Q)$ has no nontrivial rational points[17]. Here $E(Q)$ denotes the set of rational points on the elliptic curve E, and 3-descent is a standard method for proving the nonexistence of such points; see[19].

Thus, the "if and only if" statement of Hasse–Minkowski fails in degree 3: although $S = 0$ has real and p-adic solutions for every prime p, it has no rational solution.

Remark 10. Selmer's cubic marks the first explicit failure of the Hasse principle. Modern language interprets the obstruction via the non-trivial element of the Tate–Shafarevich group of the associated elliptic curve.

Beyond cubic curves, the failure of the Hasse principle is a major area of study in arithmetic geometry. Colliot-Thélène and Xu[20] and Poonen and Voloch[21] have explored these failures using the Brauer–Manin obstruction, while Hassett and Várilly-Alvarado[22] have extended these inquiries to K3 surfaces, showing that the local-global failure is not unique to simple cubic equations.

Conclusion

The Hasse–Minkowski Theorem demonstrates that quadratic forms over Q satisfy a local–global principle: questions of rational solvability and equivalence can be resolved entirely by examining the real completion and the p-adic fields. By developing the theory of quadratic forms alongside local fields, Hilbert symbols, and reciprocity laws, this paper showed how local invariants combine to determine global behavior. The applications discussed illustrate the power of this principle, from classical results on sums of squares and rational points on conics to the classification of quadratic forms and algorithmic equivalence tests. At the same time, the contrast with higher-degree equations such as Selmer's cubic highlights the exceptional nature of quadratic forms, for which local information is sufficient to guarantee global conclusions.

Overall, the Hasse–Minkowski Theorem provides a unifying framework that connects local arithmetic data with global structure. Its influence extends beyond classical number theory, continuing to inform modern research in arithmetic geometry and algorithmic classification problems.

References

1 X. Wang, *An Introduction to p-adic Numbers and the Hasse Principle*, 2019, University of Chicago REU Paper. Retrieved from https://math.uchicago.edu/~may/REU2019/REUPapers/Wang,Xingyu.pdf. Accessed 13 Jul 2025.

2 K. Martin, *Number Theory II: Chapter 7 — Quadratic Forms in n Variables*, 2009, University of Oklahoma Lecture Notes. Retrieved from http://www2.math.ou.edu/~kmartin/ntii/chap7.pdf. Accessed 13 Jul 2025.

3 J.-P. Serre, *A Course in Arithmetic*, Springer, 1973, vol. 7.

4 O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, 1971.

5 J. Ruiter, *A Proof of Ostrowski's Theorem*, 2022, Michigan State University. Retrieved from https://users.math.msu.edu/users/ruiterj2/math/Documents/Notes%20and%20talks/Ostrowski%27s%20Theorem.pdf. Accessed 13 Jul 2025.

6 K. Conrad, *Notes from Jack Thorne's Course on Quadratic Forms*, 2011, University of Connecticut. Retrieved from https://kconrad.math.uconn.edu/math5020f11/jackthornenotes.pdf. Accessed 13 Jul 2025.

7 J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.

8 T. Y. Lam, *Introduction to Quadratic Forms over Fields*, American Mathematical Society, 2005, vol. 67.

9 R. Elman, N. Karpenko and A. Merkurjev, *The Algebraic and Geometric Theory of Quadratic Forms*, American Mathematical Society, 2015.

10 J. Voight, *Recent Advances in Algebra*, Springer, 2021.

11 R. Dietmann, *Proceedings of the London Mathematical Society*, 2015, **110**, 579–601.

12 M. Bhargava and J. Hanke, *Inventiones Mathematicae*, 2014, **197**, 427–463.

13 J. Rouse, *American Journal of Mathematics*, 2014, **136**, 1693–1745.

14 J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, 1978, vol. 13.

15 D. Simon, *Journal de Théorie des Nombres de Bordeaux*, 2005, **17**, 909–923.

16 M. Kirschmer and J. Voight, *SIAM Journal on Computing*, 2010, **39**, 1714–1747.

17 E. S. Selmer, *Acta Mathematica*, 1951, **85**, 203–362.

18 W. Just, *Lecture Notes on the Intermediate Value Theorem*, 2021, Ohio University MATH4/530.

19 J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2nd edn, 2009, vol. 106.

20 J.-L. Colliot-Thélène and F. Xu, *Compositio Mathematica*, 2009, **145**, 309–363.

21 B. Poonen and J. F. Voloch, *Annals of Mathematics*, 2010, **171**, 511–532.

22 B. Hassett and A. Várilly-Alvarado, *Journal of Algebraic Geometry*, 2010, **19**, 601–611.