The Hasse–Minkowski Theorem

Akshatha Arunkumar

July 14, 2025

Abstract

The Hasse-Minkowski Theorem is a fundamental result in number theory that establishes a local-global principle for quadratic forms over the rational numbers. It states that a quadratic form over $\mathbb{Q}$ admits a non-trivial solution to the equation $Q(\mathbf{x}) = 0$ if and only if it does so over the real numbers $\mathbb{R}$ and every p-adic field $\mathbb{Q}_p$. Additionally, two quadratic forms are equivalent over $\mathbb{Q}$ if and only if they are equivalent over all such completions. This paper provides an expository account of the theorem, including necessary background on quadratic forms, local fields, and the Hilbert symbol, a sketch of the proof, and applications to problems such as sums of squares.

1 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.[Wan19] 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 $\mathbb{Q}$, 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.

To illustrate its power, consider the equation $x^2 + y^2 = 3z^2$. Does it have non-trivial rational solutions (i.e., $x, y, z \in \mathbb{Q}$, not all zero)? The Hasse–Minkowski Theorem answers this by checking solvability in $\mathbb{R}$ and all $\mathbb{Q}_p$. Over $\mathbb{R}$, solutions exist (e.g., $(x, y, z) = (1, 1, \sqrt{2/3})$). However, over $\mathbb{Q}_3$, setting $z = 1$ requires $x^2 + y^2 \equiv 3 \pmod 3$, which is impossible since $x^2, y^2 \equiv 0, 1 \pmod 3$. This local failure implies no rational solutions, a result we'll explore in detail later, showcasing the theorem's ability to simplify complex problems.

We begin with preliminaries on quadratic forms and local fields, followed by discussions of the Legendre and Hilbert symbols, which are crucial tools. We then state and outline the proof of the Hasse–Minkowski Theorem, concluding with applications like classifying quadratic forms and representing numbers as sums of squares.

2 Preliminaries and Definitions

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

2.1 Quadratic Forms

Definition 2.1 (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 2.2. *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 2.3 (Hyperbolic plane)**.** *The binary form $\mathbb{H} = \langle 1, -1 \rangle$ is called the* hyperbolic plane*. Equivalently, $\mathbb{H} = \{(x, y) \in F^2 \mid Q(x, y) = x^2 - y^2\}$. It contains the isotropic vectors $(1, 1)$ and $(1, -1)$, which are linearly independent.*

Remark 2.4. *Any two-dimensional isotropic subspace of a non-degenerate quadratic space over F is F-isometric to $\mathbb{H}$. Hyperbolic planes will be the "building blocks" in Witt decomposition.*

Example 2.5 (Isotropic vs. anisotropic)**.** *Over $\mathbb{R}$ 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 $\mathbb{R}$ (both terms are ≥ 0 and vanish simultaneously only at $(0,0)$). Over $\mathbb{Q}_3$ the situation reverses: $\langle 1, 2\rangle$ becomes isotropic because 2 is a square mod 3, whereas $\langle 1, -2\rangle$ is anisotropic.*

Definition 2.6 (Equivalence)**.** *Quadratic forms Q_1, Q_2 in n variables over F are* equivalent over F *if some $T \in \mathrm{GL}_n(F)$ satisfies $Q_2(\mathbf{y}) = Q_1(T\mathbf{y})$ for every $\mathbf{y} \in F^n$.*

Proposition 2.7. *Every non-degenerate quadratic form over F is equivalent to a diagonal form*

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

where $r = \mathrm{rank}(Q)$ (see Definition 2.9).

Sketch. Write $Q(\mathbf{x}) = \mathbf{x}^\top A \mathbf{x}$ with A symmetric. Because $\mathrm{char}\, F \neq 2$, repeatedly complete the square to kill off-diagonal entries, obtaining a diagonal matrix congruent to A. [Mar09]

Example 2.8 (Diagonalising a binary form over $\mathbb{Q}$)**.** *Consider the form*

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

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

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

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

□

Definition 2.9 (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 2.10. *After diagonalisation,* $\mathrm{rank}(Q)$ *is the number of non-zero diagonal coefficients.*

2.2 Field extensions

Definition 2.11 (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 2.12 (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 2.13 (Separable)**.** *For characteristic* 0 *(in particular,* $F = \mathbb{Q}$*) every algebraic extension is automatically* separable*: every element's minimal polynomial over* F *splits into distinct roots in a splitting field.*

Remark 2.14. *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 2.15 (Quadratic extension of $\mathbb{Q}$)**.** *Set* $K = \mathbb{Q}(\sqrt{5})$*. The minimal polynomial of* $\sqrt{5}$ *over* $\mathbb{Q}$ *is* $x^2 - 5$*, so* $[K:\mathbb{Q}] = 2$*; hence* $K/\mathbb{Q}$ *is quadratic (and separable). For* $\alpha = x + y\sqrt{5}$ $(x, y \in \mathbb{Q})$*:*

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

the latter giving the Pell conic $X^2 - 5Y^2 = 1$*.*

2.3 Fields, absolute values, and completions

Definition 2.16 (Absolute value)**.** *An* absolute value *on a field* K *is a map* $|\cdot| \colon K \to \mathbb{R}_{\geq 0}$ *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 $\mathbb{Q}$ 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 [Ser73].

Definition 2.17 (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*

$$\mathbb{Q}_\infty = \mathbb{R}, \qquad \mathbb{Q}_p \ (p \text{ prime})$$

for the completions of $\mathbb{Q}$*.*

Example 2.18 (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.*

2.4 Bilinear forms, discriminant, Witt decomposition

Definition 2.19 (Symmetric bilinear form)**.** *A symmetric bilinear form on an F-vector space V is $B\colon V \times V \to F$ with $B(\mathbf{x},\mathbf{y}) = B(\mathbf{y},\mathbf{x})$ and linear in each argument.*

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

Definition 2.20 (Discriminant)**.** *For Q represented by A, set*

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

Example 2.21. *For the diagonal ternary form $\langle 1,1,1\rangle$ we have*

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

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

Example 2.22 (Hyperbolic plane)**.** $\mathbb{H} = \langle 1,-1\rangle$ *is* isotropic*, since $(1,1)$ is a non-trivial zero. Any isotropic plane is F-isometric to $\mathbb{H}$.*

Theorem 2.23 (Witt decomposition)**.** *Every non-degenerate quadratic form Q over F decomposes uniquely (up to isometry) as*

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

where $\mathbb{H}$ is the hyperbolic plane and Q_{an} is anisotropic. The integer r is the Witt index *of Q. See [O'M71].*

Example 2.24 (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 $\mathbb{H}$; repeating with another pair yields

$$Q \cong \mathbb{H} \perp \mathbb{H},$$

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

2.5 Norms and trace in quadratic extensions

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

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

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

3 Local Fields and Completions

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

3.1 Ostrowski's classification of norms on $\mathbb{Q}$

Proposition 3.1 (Product formula)**.** *For every $x \in \mathbb{Q}^\times$, $\prod_{p \le \infty} |x|_p = 1$.*

Theorem 3.2 (Ostrowski, 1916)**.** *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to* either

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

No other inequivalent norms exist.

Idea of proof. For any $x \in \mathbb{Q}^\times$ 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 [Rui22].

□

Remark 3.3. *Ostrowski's theorem shows that, up to equivalence, the* only *non-trivial completions of $\mathbb{Q}$ are the real field $\mathbb{R}$ (corresponding to $|\cdot|_\infty$) and the p-adic fields $\mathbb{Q}_p$ for primes p. Hence, whenever we say a statement holds "at every completion of $\mathbb{Q}$," we really mean: it holds over $\mathbb{R}$ and over $\mathbb{Q}_p$ for each prime p—no further places need be considered.*

Remark 3.4. *Consequently the only completions of $\mathbb{Q}$ are $\mathbb{R}$ and the p-adic fields $\mathbb{Q}_p$. Verifying local conditions at those places is therefore exhaustive in the Hasse–Minkowski theorem.*

Example 3.5 (Product formula sanity check)**.** *For $n = 30 = 2 \cdot 3 \cdot 5$ one has*

$$|30|_\infty = 30, \quad |30|_2 = 2^{-1}, \quad |30|_3 = 3^{-1}, \quad |30|_5 = 5^{-1}, \quad |30|_p = 1 \ (p \neq 2, 3, 5).$$

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

3.2 p-adic valuation and norm

Definition 3.6 (p-adic valuation)**.** *For a prime p and a non-zero rational $x \in \mathbb{Q}^\times$, write $x = p^k \, a/b$ with $a, b \in \mathbb{Z}$ not divisible by p. Set $v_p(x) = k$ and $v_p(0) = \infty$.*

Definition 3.7 (p-adic norm)**.** *The* p-adic norm *is*

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

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

3.3 Completions and the field $\mathbb{Q}_p$

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

3.4 Constructing p-adic Numbers

As mentioned above, the p-adic numbers $\mathbb{Q}_p$ arise as the completion of $\mathbb{Q}$ with respect to the p-adic norm. For example, in $\mathbb{Q}_5$, 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 $\mathbb{Q}_5$ because $|5^n|_5 = 5^{-n} \to 0$ as $n \to \infty$. The following diagram illustrates the 5-adic expansion of $-\frac{1}{4}$. Such series make $\mathbb{Q}_p$ a complete field, enabling tools

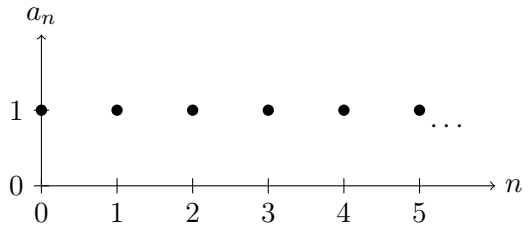

Figure 1: 5-adic expansion of $-\frac{1}{4} = 1 + 5 + 5^2 + \cdots$ in $\mathbb{Q}_5$. Each dot represents $a_n = 1$.

like Hensel's lemma for solving equations.

3.5 Topology of $\mathbb{Q}_p$

Each $\mathbb{Q}_p$ is locally compact and totally disconnected. The compact open unit group $\mathbb{Z}_p^\times$ is pro-cyclic for $p \neq 2$.

3.6 Strong approximation

For any finite set S of primes, the diagonal embedding $\mathbb{Q} \hookrightarrow \prod_{v \in S} \mathbb{Q}_v$ is dense. This lets us patch local solutions into a global one once obstructions vanish.

3.7 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 $\mathbb{Q}$ exactly when they hold in every completion; Hasse–Minkowski for quadratic forms is the prime example.

3.8 Hensel's Lemma

Lemma 3.8 (Hensel's Lemma, simple form)**.** *Let p be a prime and $f(x) \in \mathbb{Z}_p[x]$. Assume there exists $a_0 \in \mathbb{Z}_p$ such that*

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

Then there is a unique $\tilde{a} \in \mathbb{Z}_p$ satisfying

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

Equivalently, any root modulo p with non-vanishing derivative lifts to a unique root in the entire p-adic field $\mathbb{Q}_p$.

3.9 Example: lifting a square root of 2 from $\mathbb{F}_7$ to $\mathbb{Q}_7$

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

1. In $\mathbb{F}_7$, $3^2 = 9 \equiv 2$, 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

$$\frac{7}{6} \equiv 7 \cdot 41 = 287 \equiv 42 \pmod{49}, \qquad \text{so } x_1 \equiv 3 - 42 \equiv -39 \equiv 10 \pmod{49}.$$

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 $\tilde{x} \in \mathbb{Z}_7$ with $\tilde{x} \equiv 10 \pmod{49}$ and $\tilde{x}^2 = 2$.

Remark 3.9. *The condition $f'(\tilde{x}) \not\equiv 0 \pmod{p}$ is essential for Hensel's lemma: it ensures the lift exists and is unique.*

3.10 Isotropy over local fields: quick examples

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

Example 3.10 (A form isotropic over $\mathbb{R}$ but anisotropic over $\mathbb{Q}_5$)**.** *Consider* $Q = \langle 1, 1, -3\rangle = x^2 + y^2 - 3z^2$.

- *Real place:* Q *is indefinite, hence isotropic (e.g.* $(1, 1, \sqrt{2/3})$*).*
- 5*-adic place: write* $-3 \equiv 2 \pmod 5$*. Completing squares shows that any non-trivial* 5*-adic zero would imply* 2 *is a square* $\bmod 5$*, which it is not; thus* Q *is anisotropic in* $\mathbb{Q}_5$.

Example 3.11 (A binary form anisotropic over $\mathbb{R}$ but isotropic over $\mathbb{Q}_3$)**.** *Take* $B = \langle 1, 2\rangle = x^2 + 2y^2$.

- *Over* $\mathbb{R}$ *both terms are non-negative and vanish simultaneously only at* $(0, 0)$*;* B *is anisotropic.*
- *In* $\mathbb{F}_3$ *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* $\mathbb{Q}_3$.

Example 3.12 (Hyperbolic plane everywhere locally)**.** *The form* $\mathbb{H} = \langle 1, -1\rangle$ *is isotropic over* $\mathbb{R}$ *(obvious) and over every* $\mathbb{Q}_p$*, 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.

4 Legendre Symbol and Quadratic Residues

4.1 Basic definitions

Definition 4.1 (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 $x \in \mathbb{Z}$*. Otherwise* a *is a* quadratic non-residue.

Definition 4.2 (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 $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{-1, 0, 1\}$ *descends to a group homomorphism* $\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}$.

Example 4.3 (Computing a Legendre symbol)**.** *Compute*

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

Method 1: Euler's Criterion. *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* $\left(\tfrac{7}{19}\right) = +1$*. Thus* 7 *is a quadratic residue modulo* 19*.*

Method 2: Quadratic Reciprocity. *Write* $7 = 19 - 12 \equiv -12 \equiv 7 \bmod 19$ *(already reduced). Since* $7 \equiv 3 \pmod 4$ *and* $19 \equiv 3 \pmod 4$*, Quadratic Reciprocity gives*

$$\left(\tfrac{7}{19}\right) \;=\; (-1)^{\frac{7-1}{2}\cdot\frac{19-1}{2}}\left(\tfrac{19}{7}\right) \;=\; (-1)^{3\cdot 9}\left(\tfrac{5}{7}\right) \;=\; -\left(\tfrac{5}{7}\right).$$

Now $5 \equiv 5 \pmod 7$*, and* $5^3 = 125 \equiv -1 \pmod 7$*, so* $\left(\tfrac{5}{7}\right) = -1$ *by Euler's criterion; therefore* $\left(\tfrac{7}{19}\right) = (-1)\cdot(-1) = +1$*, agreeing with Method 1 [Con11a].*

4.2 Quadratic Reciprocity

Theorem 4.4 (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 $\left(\tfrac{-1}{p}\right) = (-1)^{(p-1)/2}$ *and* $\left(\tfrac{2}{p}\right) = (-1)^{(p^2-1)/8}$*, this completely determines all Legendre symbols.*

Example 4.5. *Compute* $\left(\tfrac{7}{19}\right)$*. 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* $\left(\tfrac{5}{7}\right) = -1$*, hence* $\left(\tfrac{7}{19}\right) = +1$*.*

4.3 Example: deciding local solvability with $\left(\frac{\cdot}{p}\right)$

Determine whether

$$x^2 \equiv 5 \pmod{11}$$

has a solution.

$$\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{11-1}{2}} \qquad \text{(Quadratic Reciprocity)}$$
$$= \left(\frac{1}{5}\right)(-1)^{2\cdot 5} = 1.$$

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

Remark 4.6. *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.*

5 Hilbert Symbol and Local Quadratic Forms

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

Definition 5.1 (Hilbert Symbol)**.** *For a local field K (e.g., $\mathbb{Q}_p$ or $\mathbb{R}$) and $a, b \in K^\times$, the* Hilbert symbol $(a,b)_K$ *is defined as:*

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

Example 5.2. *In $\mathbb{Q}_7$, both 5 and 6 are 7-adic units. The explicit formula for odd p gives $(5,6)_7 = 1$, so $x^2 - 5y^2 - 6z^2 = 0$ has a non-trivial 7-adic solution.*

Example 5.3 (Computing Hilbert Symbols)**.**

Over $\mathbb{Q}_5$, compute $(2,3)_5$. Since 2 and 3 are 5-adic units, we use the formula $(a,b)_p = (-1)^{\epsilon(a)\epsilon(b)}\left(\frac{a}{p}\right)^{\epsilon(b)}\left(\frac{b}{p}\right)^{\epsilon(a)}$, where $\epsilon(x) = \frac{x-[x]_p}{p}$ is the p-adic valuation residue. Here, $\epsilon(2) = \epsilon(3) = 0$ since $2, 3 \in \mathbb{Z}_5^\times$. Thus, $(2,3)_5 = \left(\frac{2}{5}\right)\left(\frac{3}{5}\right)$. Since $2^2 \equiv 4 \pmod 5$ and $3^2 \equiv 4 \pmod 5$, both are non-squares, so $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$, giving $(2,3)_5 = (-1)\cdot(-1) = 1$. Thus, $z^2 = 2x^2 + 3y^2$ has a non-trivial solution in $\mathbb{Q}_5$.

Over $\mathbb{R}$, compute $(-1,-1)_\infty$. Since both $a = -1$ and $b = -1$ are negative, the form $z^2 = (-1)x^2 + (-1)y^2 = -x^2 - y^2$ is negative definite and only zero at $(0,0)$. Thus, $(-1,-1)_\infty = -1$, indicating anisotropy.

Proposition 5.4 (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 $K \neq \mathbb{C}$).*

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 $Q_{ab,c}(x,y,z) = x^2 - ab\,y^2 - cz^2$ 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. [Con11b] □

Example 5.5 (Bilinearity check)**.** *Over $\mathbb{Q}_3$: $(30,7)_3 = (6\cdot 5,7)_3 = (6,7)_3(5,7)_3$, matching Proposition 5.4. Explicit calculation confirms each factor.*

Theorem 5.6 (Hilbert Reciprocity)**.** *For $a, b \in \mathbb{Q}^\times$ one has*

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

where the product ranges over all places $v\colon \mathbb{Q} \hookrightarrow \mathbb{R}$ or $\mathbb{Q}_p$.

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

$$(a,b)_v = 1 \iff b \text{ is a norm from } K \otimes_{\mathbb{Q}} \mathbb{Q}_v.$$

Class field theory (or the product formula for global Hilbert symbols) asserts that an element of $\mathbb{Q}^\times$ 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 $n \in \mathbb{Q}^\times$ chosen so that $(a,n)_v = (a,b)_v$ except at one place, one deduces $\prod_v (a,b)_v = 1$. See *Cassels–Fröhlich, §VI.1* for a full, elementary proof.

□

Example 5.7. *Take $a = 3$, $b = 5$. Direct computation shows*

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

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

For $\mathbb{R}$, $(a,b)_R = -1$ if and only if $a < 0$ and $b < 0$. For $\mathbb{Q}_p$, 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 $a, b \in \mathbb{Q}^\times$, $\prod_v (a,b)_v = 1$, where v runs over all places.

6 Hasse-Minkowski Theorem and Proof

Theorem 6.1 (Hasse-Minkowski Theorem)**.** *Let Q be a quadratic form over $\mathbb{Q}$. Then $Q(\mathbf{x}) = 0$ has a non-trivial solution over $\mathbb{Q}$ if and only if it has a non-trivial solution over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime p. Moreover, two quadratic forms over $\mathbb{Q}$ are equivalent if and only if they are equivalent over $\mathbb{R}$ and every $\mathbb{Q}_p$.*

Proof. We prove first the *isotropy* statement and then the *equivalence* statement, following the classical dimension–4–induction route.

Step 1. Local invariants. For a local field F of characteristic $\neq 2$ and a non-degenerate quadratic form $Q \cong \langle a_1, \dots, a_n \rangle$ define

$$\dim Q = n, \qquad d_F(Q) = (-1)^{n(n-1)/2} \det(Q) \in F^\times / F^{\times 2},$$

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

where $(\cdot,\cdot)_F$ is the Hilbert symbol (Definition 5.1). Cassels–Fröhlich (VI.2) shows that the triple $(\dim, d_F, \epsilon_F)$ *classifies* quadratic forms over F: two forms are F-isometric iff their triples coincide. We shall use this fact tacitly whenever we pass from global to local data and back.

Step 2. A four-variable core lemma. Let $Q = \langle a, b, c, d \rangle$ with $abcd \in \mathbb{Q}^{\times 2}$. Form the quaternion algebra

$$(a,b) \;=\; \mathbb{Q}\langle i, j \mid i^2 = a,\ j^2 = b,\ ij = -ji \rangle.$$

Its norm form is precisely $N_{(a,b)}(x) = x_1^2 - a x_2^2 - b x_3^2 + ab x_4^2 = Q$. Hence

$$Q \text{ is isotropic over a field } F \iff (a,b) \text{ is split over } F,$$

because a non-trivial zero of N is a zero-divisor in the algebra. By the Albert–Brauer–Hasse–Noether theorem (or, equivalently, Hilbert-symbol reciprocity) a quaternion algebra over $\mathbb{Q}$ splits globally iff it splits at every completion. Therefore

a diagonal 4-fold with square total product is isotropic over $\mathbb{Q}$ precisely when it is isotropic in $\mathbb{R}$ and in every $\mathbb{Q}_p$.

Step 3. Local ⇒ global isotropy (all n). We proceed by induction on $n = \dim Q$.

Base $n = 1, 2$. A binary form $ax^2 + by^2$ that is anisotropic over $\mathbb{Q}$ must have a, b of the same square-class in every completion, contradicting local isotropy; hence a locally isotropic binary form has a rational zero.

$n = 3$. A ternary form isotropic everywhere must be isotropic at some finite prime p. Choose an integral p-adic zero, then use the Chinese Remainder Theorem and weak approximation to lift it to $\mathbb{Q}$; details appear in [Ser73].

$n = 4$. Reduce to the diagonal case with square total product and invoke the core lemma of Step 2.

Induction $n \geq 5$. Let Q be locally isotropic. Because $\mathbb{Q}$ is dense in each $\mathbb{Q}_v$, choose $\mathbf{v} \in \mathbb{Q}^n$ such that $\alpha := Q(\mathbf{v}) \neq 0$ but α is *v-adically small* for some place where Q already has an isotropic vector. Since B_Q is non-degenerate, pick $\mathbf{w} \in \mathbb{Q}^n$ with $B_Q(\mathbf{v}, \mathbf{w}) = 1$. Then $H = \operatorname{span}\{\mathbf{v}, \mathbf{w}\}$ is a hyperbolic plane, and $Q \cong H \perp Q_0$ with $\dim Q_0 = n - 2$. Local isotropy of Q forces local isotropy of Q_0; by the induction hypothesis Q_0 is isotropic over $\mathbb{Q}$, whence so is Q.

Thus the "local ⇒ global" direction for isotropy holds for every dimension, completing part (i) of the theorem.

Step 4. Local ⇒ global equivalence. Assume Q and Q' are isometric in $\mathbb{R}$ and in each $\mathbb{Q}_p$. Then $\dim Q = \dim Q'$, $d_{\mathbb{Q}}(Q) = d_{\mathbb{Q}}(Q')$, because these invariants already agree everywhere locally and lie in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. For the Hasse invariant note $\epsilon_v(Q) = \epsilon_v(Q')$ $(\forall v)$. Taking the product over all v and invoking Hilbert reciprocity (Theorem 5.6) gives $1 = \prod_v \epsilon_v(Q) = \prod_v \epsilon_v(Q')$, so the common value of $\epsilon_v(Q) = \epsilon_v(Q')$ is $+1$ at all but (possibly) one place, hence at *every* place by the local coincidence already observed. Consequently, the global triples $(\dim, d, \epsilon)$ of Q and Q' coincide.

Finally, any two rational forms with identical global triples are isometric over $\mathbb{Q}$: adjoin hyperbolic planes until the difference of the two diagonalisations becomes a multiple of a split 2-plane, then cancel iteratively.

Step 5. The "global ⇒ local" direction. The forward implications in both parts of the theorem are immediate: a rational isotropic vector or an $\mathbb{Q}$-isometry remains so after embedding $\mathbb{Q} \hookrightarrow \mathbb{R}, \mathbb{Q}_p$.

Together, Steps 3–5 establish both assertions of the Hasse–Minkowski Theorem. □

7 Applications

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

7.1 Sums of squares

Theorem 7.1 (Lagrange, 1770)**.** *Every positive integer is a sum of four squares.*

Sketch via Hasse–Minkowski. Fix $n \in \mathbb{N}$. Consider the *difference form*

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

A non-trivial rational zero with $z \neq 0$ gives n as a sum of four squares after scaling. Hence, it suffices to show Q_n is isotropic over $\mathbb{Q}$.

Local check. Over $\mathbb{R}$, the form is clearly isotropic because it has positive and negative coefficients. Over each $\mathbb{Q}_p$, write $n = p^k u$ with $u \in \mathbb{Z}_p^\times$. If $p \neq 2$ then u is a sum of three squares in $\mathbb{F}_p$, so Hensel's lemma lifts to a p-adic zero with $z \equiv 1$. For $p = 2$, an explicit check shows Q_n is isotropic in $\mathbb{Q}_2$ as well [Cas78].

Global step. Since Q_n is isotropic in $\mathbb{R}$ and every $\mathbb{Q}_p$, Hasse–Minkowski (Theorem 6.1) implies Q_n is isotropic over $\mathbb{Q}$, completing the proof. □

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

7.2 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.

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.

7.3 Classification of quadratic forms over $\mathbb{Q}$

Theorem 7.2. *Two non-degenerate quadratic forms Q, Q' over $\mathbb{Q}$ are equivalent over $\mathbb{Q}$ if and only if*

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

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

Idea. Over each completion $\mathbb{Q}_v$, the triple $(\dim, \operatorname{disc}, \epsilon_v)$ with $\epsilon_v(Q) = \prod_{i<j}(a_i, a_j)_v$ classifies quadratic forms [Cas78]. If the three data agree globally, then $Q \cong Q'$ locally everywhere. The second part of Theorem 6.1 (equivalence) then upgrades these local isometries to a rational isometry. □

Algorithmic test for $\mathbb{Q}$-equivalence

A practical version of Theorem 7.2 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 $\mathbb{Q}$-equivalent.

1. **Diagonalise.** Use Proposition 2.7 to write $Q \cong \langle a_1, \dots, a_n\rangle$ and $Q' \cong \langle a'_1, \dots, a'_n\rangle$.
2. **Match discriminants.** If $\operatorname{disc}(Q) \neq \operatorname{disc}(Q') \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ return No.
3. **Compute local symbols.** For each finite set of primes dividing $2\operatorname{disc}(Q)\operatorname{disc}(Q')$ 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 $T \in \mathrm{GL}_n(\mathbb{Q})$ by CRT-patching the local isometries; see [Cas78].
5. **Return.** Output T (or Yes) if the gluing succeeds, otherwise No.

Example 7.3 (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: $\operatorname{disc}(Q) = \operatorname{disc}(Q') = +1$. 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 $T = \operatorname{diag}(1, 1, 1, \frac{1}{2}) \in \mathrm{GL}_4(\mathbb{Q})$ 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.

7.4 Rational points on conics

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

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

has a $\mathbb{Q}$-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 $p \mid 2ab$.

Proof sketch. 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 $\mathbb{R}$. Condition (b) is equivalent to isotropy over each $\mathbb{Q}_p$ by Definition 5.1. Applying Theorem 6.1 yields the desired equivalence. □

Remark 7.4. *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

Hasse–Minkowski is sharp: for degree >2 local solvability need *not* imply a rational solution.

Proposition 7.5 (Selmer, 1951)**.** *The homogeneous cubic*

$$S(x, y, z) = 3x^3 + 4y^3 + 5z^3 = 0$$

has a non-trivial zero in $\mathbb{R}$ and in every $\mathbb{Q}_p$, yet no non-trivial solution in $\mathbb{Q}$.

Local solvability.

- **Real.** Take $(x, y, z) = (-1, 1, 0)$: $S = -3 + 4 = 1 > 0$ and by continuity a nearby point makes $S = 0$.
- $p \neq 2, 3, 5$**.** By Hensel, there is always a solution to $S \equiv 0 \pmod p$: choose $x \equiv 1,\ y \equiv -1,\ z \equiv 0$.
- $p = 2, 3, 5$**.** An explicit check shows a solution modulo p^2 which then lifts p-adically.

Global failure is proved by a 3-descent on the elliptic curve $X^3 + Y^3 + 60Z^3 = 0$ obtained after clearing a common factor; see [Cas78]. One finds that any rational point would force 60 to be a cube in $\mathbb{Q}^\times/\mathbb{Q}^{\times 3}$, which is false. Hence, $S = 0$ has no non-trivial rational solution. □

Remark 7.6. *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.*

7.5 Quadratic Forms in Cryptography

Quadratic forms play a crucial role in modern cryptography, particularly in lattice-based cryptography, where the Hasse-Minkowski Theorem facilitates the analysis of Diophantine equations underlying secure systems. Consider a quadratic form $Q(x_1, \ldots, x_n) = \sum a_{ij} x_i x_j$ over $\mathbb{Z}$, used to define a lattice $L = \{\mathbf{x} \in \mathbb{Z}^n : Q(\mathbf{x}) = m\}$ for some integer m. The security of lattice-based cryptosystems, such as NTRU, relies on the difficulty of finding short vectors in such lattices, which can be formulated as solving $Q(\mathbf{x}) = 0$ over $\mathbb{Q}$.

The Hasse-Minkowski Theorem helps by ensuring that if Q is isotropic over $\mathbb{Q}$ (i.e., has a non-trivial rational solution), it must be isotropic over $\mathbb{R}$ and all $\mathbb{Q}_p$. For example, in designing cryptographic protocols, one might need to verify whether a form like $x^2 + y^2 - pz^2 = 0$ (for a prime p) has rational solutions, which could weaken the lattice's security if solutions exist. By checking local isotropy (e.g., using Hilbert symbols), cryptographers can ensure the form is anisotropic over $\mathbb{Q}$, strengthening the system. This application highlights the theorem's relevance beyond pure mathematics, connecting number theory to real-world security challenges.

Acknowledgments

The author would like to thank their mentors and peers for guidance.

References

[Cas78] J. W. S. Cassels. *Rational Quadratic Forms*. Academic Press, 1978. London Mathematical Society Monographs 13.

[Cla12] Pete Clark. Local–global principles in number theory: Course notes. http://www.math.miami.edu/~armstrong/685fa12/pete%20clark.pdf, 2012. Course handout, University of Miami, accessed 13 Jul 2025.

[Con11a] Keith Conrad. Notes from jack thorne's course on quadratic forms. https://kconrad.math.uconn.edu/math5020f11/jackthornenotes.pdf, 2011. Graduate notes, accessed 13 Jul 2025.

[Con11b] Keith Conrad. Notes from jack thorne's course on quadratic forms. https://kconrad.math.uconn.edu/math5020f11/jackthornenotes.pdf, 2011. Duplicate copy at alternate path, accessed 13 Jul 2025.

[Mar09] Kimball Martin. Number theory ii: Chapter 7 — quadratic forms in n variables. http://www2.math.ou.edu/~kmartin/ntii/chap7.pdf, 2009. Lecture notes, University of Oklahoma, accessed 13 Jul 2025.

[O'M71] O. Timothy O'Meara. *Introduction to Quadratic Forms*. Springer, 1971.

[Rui22] Jack Ruiter. A proof of ostrowski's theorem. https://users.math.msu.edu/users/ruiterj2/math/Documents/Notes%20and%20talks/Ostrowski's%20Theorem.pdf, 2022. Expository notes, Michigan State University, accessed 13 Jul 2025.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer, 1973.

[Wan19] Xingyu Wang. An introduction to p-adic numbers and the hasse principle. https://math.uchicago.edu/~may/REU2019/REUPapers/Wang,Xingyu.pdf, 2019. University of Chicago REU paper, accessed 13 Jul 2025.