P-ADIC NUMBERS, QUADRATIC FORMS, AND THE HASSE-MINKOWSKI THEOREM

CINDY ZHANG

Abstract. In this paper, we will explore the Hasse-Minkowski theorem and the local-global principle in number theory. We will introduce the field of p-adic numbers as well as the notions of quadratic forms, local and global fields, and Hilbert symbols. We shall also cover the topics of Hensel's lemma, the approximation theorems, and the Hilbert reciprocity. Eventually, we will prove the Hasse-Minkowski theorem and discuss some of its implications.

Contents

1. Introduction 2
2. p-adic Numbers, Hensel's Lemma, and Squares in $\mathbb{Q}_p$ 2
2.1. p-adic Numbers 2
2.2. Hensel's Lemma 4
2.3. Squares in $\mathbb{Q}_p$ 5
3. The Approximation Theorems 5
4. Quadratic Forms 6
5. Classifications of Quadratic Forms over $\mathbb{F}_p$ and $\mathbb{Q}_p$ 8
5.1. Classification of Quadratic Forms over $\mathbb{F}_p$ with $p \neq 2$ 9
5.2. Classification of Quadratic Forms over $\mathbb{Q}_p$ 9
6. The Hilbert Symbol and Hilbert Reciprocity 10
6.1. Tate's Proof of the Hilbert Reciprocity 11
7. A Full Proof of the Hasse-Minkowski Theorem 14
7.1. Three Forms of the Local-Global Principle 14
7.2. Preparations 15
7.3. Proof of the Hasse-Minkowski Theorem: $n = 1, 2, 3$. 16
7.4. Proof of the Hasse-Minkowski Theorem: $n = 4$. 18
7.5. Proof of the Hasse-Minkowski Theorem: $n \geq 5$ 19
8. Some Corollaries 19
8.1. Sums of Squares 19
8.2. Representability of Rational Numbers 20
Acknowledgments 21
References 21
Appendix A. Proof of the Strong Approximation Theorem 22

Date: November 10, 2021.

1. Introduction

"One cannot blame a respectable mathematician for looking twice at the equation

$$-1 = 4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \cdots ."[7]$$

Motivated by the analogies between the number fields and the function fields, Kurt Hensel introduced a whole new number field—the p-adic numbers. Although mathematicians found this new invention interesting in a formal way, they asked: what is the point of having this new world of numbers? While Hensel himself tried to demonstrate the usefulness of his invention, it was his student Helmut Hasse who manifested the potential and power of the p-adic numbers in 1921. What Hasse showed is that, for quadratic forms, an equation has a rational solution if and only if it has a solution in $\mathbb{R}$ and a solution in the field of p-adic numbers $\mathbb{Q}_p$ for each prime p. [6] This is known as the Hasse-Minkowski theorem, and the idea of searching for solution in $\mathbb{Q}$ by piecing together solutions in all the $\mathbb{Q}_p$'s and $\mathbb{R}$ is called the local-global principle in number theory.

To explore the Hasse-Minkowski theorem, we shall first remind our readers of some basic facts about the field of p-adic numbers, including Hensel's lemma, the square classes in $\mathbb{Q}_p$, and the approximation theorems. Then, we'll define quadratic forms over a field and classify all forms over $\mathbb{F}_p$ and $\mathbb{Q}_p$ respectively. After that comes the exploration of the Hilbert symbol and the Hilbert reciprocity, which will shed light on the relations among the completions of $\mathbb{Q}$. Finally, we will give a full proof of the Hasse-Minkowski theorem and look at some of its corollaries.

2. p-adic Numbers, Hensel's Lemma, and Squares in $\mathbb{Q}_p$

2.1. ***p*-adic Numbers.** To obtain the p-adic number field $\mathbb{Q}_p$, we will first introduce the notion of the p-adic absolute value on $\mathbb{Q}$.

Definition 2.1 (The p-adic Valuation)**.** Let $p \in \mathbb{Z}$ be prime. Then, for any non-zero $x \in \mathbb{Q}$, the ***p*-adic valuation** of x, denoted by $v_p(x)$, is the unique integer which satisfies

$$x = p^{v_p(x)} \frac{a}{b} \ \ (a, b \in \mathbb{Z} \setminus \{0\}), \ \ p \nmid ab.$$

Define $v_p(0) = +\infty$.

Definition 2.2 (The p-adic Absolute Value)**.** For any non-zero $x \in \mathbb{Q}$, the ***p*-adic absolute value** of x is defined by

$$|x|_p = p^{-v_p(x)}.$$

We extend this absolute value to all of $\mathbb{Q}$ by defining $|0|_p = 0$.

Once we have an absolute value on a field, we can put a metric on the field and study its topology.

Definition 2.3 (The p-adic Metric)**.** Let $p \in \mathbb{Z}$ be prime and $|\cdot|_p$ be the p-adic absolute value. We define the p-adic distance $d_p(x, y)$ between two elements $x, y \in \mathbb{Q}$ by

$$d_p(x, y) = |x - y|_p.$$

This allows us to define the notion of equivalence of absolute values.

Definition 2.4 (Equivalence of Absolute Values)**.** Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on a field F are called equivalent if they define the same topology on F, that is, if every set that is open with respect to one is also open with respect to the other.

Recall that the "usual" absolute value $|\cdot|$ on the field of real numbers $\mathbb{R}$ is defined by

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0, \end{cases}$$

which can be applied to $\mathbb{Q}$ via the inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$. We'll denote this absolute value by $|\cdot|_\infty$ from now on.

Although we won't be able to go into the details, $|\cdot|_\infty$ and $|\cdot|_p$ with p prime give rise to very different topologies. This is due to the fact that, unlike $|\cdot|_\infty$, $|\cdot|_p$ is non-archimedean and thus gives rise to a totally disconnected topological space even on the completed field. Readers who are interested can look at [5]. While the topology the archimedean absolute value gives on $\mathbb{Q}$ is also totally disconnected, it becomes connected after completion to $\mathbb{R}$. The following theorem by Ostrowski says that we've found all the absolute values on $\mathbb{Q}$.

Theorem 2.5 (Ostrowski)**.** *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to one of the absolute values $|\cdot|_p$, where p is a prime or $p = \infty$.*

All the absolute value $|\cdot|_p$ for $p \leq \infty$ should be equally treated. As $\mathbb{Q}$ is not complete with respect to $|\cdot|_\infty$, the readers can check that $\mathbb{Q}$ is not complete with respect to $|\cdot|_p$ for any prime $p \in \mathbb{Z}$ either. While taking the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ produces $\mathbb{R}$, we can complete $\mathbb{Q}$ with respect to $|\cdot|_p$ for each prime p similarly.

Theorem 2.6. *For each prime $p \in \mathbb{Z}$, there exists a field $\mathbb{Q}_p$ with a non- archimedean absolute value $|\cdot|_p$, such that:*

(a) there exists an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, and the absolute value induced by $|\cdot|_p$ on $\mathbb{Q}$ via this inclusion is the p-adic absolute value;
(b) the image of $\mathbb{Q}$ under this inclusion is dense in $\mathbb{Q}_p$ (with respect to $|\cdot|_p$); and
(c) $\mathbb{Q}_p$ is complete with respect to the absolute value $|\cdot|_p$.

The field $\mathbb{Q}_p$ satisfying (i), (ii) and (iii) is unique up to unique isomorphism preserving the absolute values.

Proof. See [5]. □

So the p-adic valuation on $\mathbb{Q}$ extends to $\mathbb{Q}_p$. In other words,

Lemma 2.7. *For each $x \in \mathbb{Q}_p$, $x \neq 0$, there exists an integer $v_p(x)$ such that $|x|_p = p^{-v_p(x)}$. For $x = 0$, we define $v_p(0) = +\infty$.*

Definition 2.8 (p-adic Integers)**.** The ring of p-adic integers is defined to be the set

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Let's also note some useful topological facts about $\mathbb{Q}_p$ and characterizations of its elements.

Theorem 2.9. *(i) $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

(ii) Every element in $\mathbb{Z}_p$ can be written uniquely in the form

$$b_0 + b_1 p + b_2 p^2 + ...$$

with $b_i \in \{0, 1, ..., p-1\}$, and every such series $b_0 + b_1 p + b_2 p^2 + ...$ with $b_i \in \{0, 1, ..., p-1\}$ represents an element of $\mathbb{Z}_p$. In particular, $\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ for all $n \in \mathbb{N}$.

(iii) Every element in $\mathbb{Q}_p$ can be written uniquely in the form

$$b_{n_0} p^{n_0} + b_{n_0+1} p^{n_0+1} + ...$$

for some $n_0 \in \mathbb{Z}$ and $b_i \in \{0, 1, ..., p-1\}$, and every such series $b_{n_0} p^{n_0} + b_{n_0+1} p^{n_0+1} + ...$ for some $n_0 \in \mathbb{Z}$ and $b_i \in \{0, 1, ..., p-1\}$ represents an element of $\mathbb{Q}_p$.

Proof. See [1]. □

The group of ***p*-adic units** $\mathbb{Z}_p^\times$ is the collection of all invertible elements in $\mathbb{Z}_p$. For any $x \in \mathbb{Z}_p^\times$, we have $x^{-1} \in \mathbb{Z}_p^\times$, $|x|, |x|^{-1} \leq 1$, and $|x||x^{-1}| = |xx^{-1}| = 1$, which imply that $|x| = |x^{-1}| = 1$. In other words,

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\} = \{\sum_{i \geq 0} a_i p^i : a_0 \neq 0\}.$$

Note that given any $x \in \mathbb{Q}_p$, there is a unique $u \in \mathbb{Z}_p^\times$ such that $x = p^{v_p(x)} u$.

2.2. Hensel's Lemma.

Just as Newton's method provides a root-finding algorithm for a real-valued function, Hensel's lemma says that one can find the roots of a univariate polynomial in $\mathbb{Q}_p$ via successive approximation.

There are ususally two forms of Hensel's lemma, one stronger than the other.

Theorem 2.10 (Hensel's Lemma)**.** [5] *Let $F(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. Suppose that there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that*

$$F(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p},$$

and

$$F'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

where $F'(X)$ is the formal derivative of $F(X)$. Then there exists a unique p-adic integer $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$ and $F(\alpha) = 0$.

It turns out that if we weaken the conditions $F(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p}$ and $F(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p}$, we can obtain a more general Hensel's lemma, which is stated as follows.

Theorem 2.11 (The Stronger Form of Hensel's Lemma)**.** [5] *Let $F(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. Suppose that there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that*

$$|F(\alpha_1)|_p < |F'(\alpha_1)|_p^2.$$

Then, there exists a unique p-adic integer $\alpha \in \mathbb{Z}_p$ such that $|\alpha - \alpha_1|_p < |F'(\alpha_1)|_p$ and $F(\alpha) = 0$.

The second form is stronger in a sense that it recovers the first form as a special case and applies to some situations where the first does not. For example, if we take $p = 2$ and consider the polynomial $F(X) = X^2 - 17$, then the first form of Hensel's lemma will never apply because $F'(X) = 2X \equiv 0 \pmod{2\mathbb{Z}_2}$. However, if we take $\alpha_1 = 1$, we see that

$$|F(\alpha_1)|_2 = |-16|_2 = 2^{-4} < 2^{-1}|F'(\alpha_1)|_p^2.$$

So the second form implies that $F(X)$ has a root in $\mathbb{Q}_2$ indeed. [5]

2.3. **Squares in $\mathbb{Q}_p$.** These two forms of Hensel's lemma allow us to determine the squares in $\mathbb{Q}_p$. In particular, when p is an odd prime, we can first find all the squares in $\mathbb{Z}_p^\times$ and then extend our result to all of $\mathbb{Q}_p$ using the weaker form of Hensel's lemma (Theorem 2.10). When $p = 2$, we can apply the stronger form of Hensel's lemma and find all squares in $\mathbb{Q}_2$ similarly. It turns out that [5]:

Proposition 2.12. *Let $p \neq 2$ be a prime, and let $b \in \mathbb{Z}_p^\times$ be a p-adic unit. Then, b is the square of an element of $\mathbb{Z}_p^\times$ iff there exists an $\alpha_1 \in \mathbb{Z}_p$ such that $\alpha_1^2 \equiv b \pmod{p\mathbb{Z}_p}$.*

Proof. Apply the weak form of Hensel's lemma (Theorem 2.10) to $X^2 - b$. □

Theorem 2.13 (Squares in $\mathbb{Q}_p$ with $p \neq 2$)**.** *Let $p \neq 2$ be a prime. An element $x \in \mathbb{Q}_p$ is a square if and only if it can be written as $x = p^{2n}y^2$ with $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^\times$ a p-adic unit. The quotient group $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ has order four. If $c \in \mathbb{Z}_p^\times$ is any element whose reduction modulo p is not a quadratic residue, then the set $\{1, p, c, cp\}$ is a complete set of coset representatives.*

For the case when $p = 2$, we get a slightly different result. The condition for an element in $\mathbb{Z}_2^\times$ to be a square is different.

Proposition 2.14. *$b \in \mathbb{Z}_2^\times$ is a square in $\mathbb{Z}_2$ iff $b \equiv 1 \pmod{8\mathbb{Z}_2}$.*

The quotient $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ also turns out to have a slightly different structure.

Theorem 2.15 (Squares in $\mathbb{Q}_2$)**.** *An element $x \in \mathbb{Q}_2^\times$ is a square if and only if it can be written as $x = p^{2n}x'$ with $n \in \mathbb{Z}$ and $x' \equiv 1 \bmod 8$ a p-adic unit. The group $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ has order 8, and is generated by the classes of $-1, 5$, and 2, so that a complete set of coset representatives is $\{1, -1, 5, -5, 2, -2, 10, -10\}$.*

3. The Approximation Theorems

The approximation theorems are essential ingredients for our proof of the Hasse-Minkowski theorem in section 7. We will call either a prime of $\mathbb{Z}$ or the formal symbol ∞ a **place** of $\mathbb{Q}$.

Before we state the approximation theorems, let's first note the following proposition, which says that an element in any completion $\mathbb{Q}_\nu$ sufficiently close to 1 is guaranteed to be a square in $\mathbb{Q}_\nu$.

Proposition 3.1. *Let ν be a place of $\mathbb{Q}$. Then, there is an $\epsilon > 0$ such that if an $x \in \mathbb{Q}_\nu$ satisfies $|1 - x| < \epsilon$, then $x = y^2$ for some $y \in \mathbb{Q}_\nu^\times$.*

The approximation theorems are about how one can go from the local places ν's to obtain information in the global field $\mathbb{Q}$.

Theorem 3.2 (Rational Form of the Weak Approximation Theorem)**.** *If S is a finite set of places of $\mathbb{Q}$ and we are given $x_\nu \in \mathbb{Q}_\nu$ and $\epsilon_\nu \in \mathbb{R}_{>0}$ for all $\nu \in S$, then there is an $x \in \mathbb{Q}$ such that $|x - x_\nu| < \epsilon_\nu$ for all $p \in S$.*

Proof. Use the Chinese remainder theorem to find an $x \in \mathbb{Q}$ such that $|x - x_\nu| < \epsilon_\nu$ for all $p \in S \smallsetminus \{\infty\}$ first. Then, adjust x so that $|x - x_\infty| < \epsilon_\infty$. □

In other words, the inclusion $\mathbb{Q} \hookrightarrow \prod_{\nu \in S} \mathbb{Q}_p$, where S is finite, is always dense.

While theorem 3.2 will apply to a finite set of places including ∞, we can have the following variant of weak approximation to obtain a rational number with "stronger properties" assuming Dirichlet's theorem on primes in arithmetic progressions.

Theorem 3.3 (Dirichlet's Theorem)**.** *Let $a, d \in \mathbb{N}$ be such that* $\gcd(a, d) = 1$. *Then, there exist infinitely many primes p such that $p \equiv a \pmod{d}$.*

This stronger approximation theorem will allow us to have more control on the absolute value $|x|_\nu$ for all but finitely many places, while the trade-off is that the $x \in \mathbb{Q}$ we find will be close to all places $\nu \in S$ but ∞.

Theorem 3.4 (The Strong Approximation Theorem)**.** *If S is a finite set of places of $\mathbb{Q}$ containing ∞ and we are given $x_\nu \in \mathbb{Q}_\nu^\times$ for all $\nu \in S$ and $\epsilon_\nu \in \mathbb{R}_{>0}$ for all $\nu \in S \smallsetminus \infty$, then there is a prime $p_0 \notin S$ and an $x \in \mathbb{Q}^\times$ such that:*

(1) $|x - x_\nu| < \epsilon_\nu$ for all $p \in S \smallsetminus \infty$;
(2) x has the same sign as x_∞;
(3) $|x|_p = 1$ for all $p \notin S \cup \{p_0\}$.

Proof. See a proof of this in Appendix A. □

4. Quadratic Forms

From now on, a field will always mean a field with characteristic not 2.

Definition 4.1 (Quadratic Forms and Quadratic Space)**.** Let V be a vector space over a field F. A **quadratic form** on V is a function $q : V \to F$ such that

(1) $q(ax) = a^2 q(x)$ for any $a \in F$ and $x \in V$, and
(2) the function $V \times V \to F$ defined by
$$(x, y) \mapsto q(x + y) - q(x) - q(y)$$
is a bilinear form.

The pair (V, q) is called a **quadratic space**, and the dimension of q is defined by $\dim(q) = \dim(V)$.

We say the quadratic form q is **isomorphic** to q', written $q \cong q'$, if $q(x) = q'(Cx)$ for some invertible matrix C.

Note that the function defined in (2) above always maps (x, y) and (y, x) to the same element in F. A bilinear function with this property is called a **symmetric bilinear form**.

Definition 4.2 (Symmetric Bilinear Form)**.** A **symmetric bilinear form** on a vector space V is a bilinear function $B : V \times V \to F$ such that

(1) B is bilinear, and
(2) $B(v, w) = B(w, v)$ for all $v, w \in V$.

Given a quadratic space (V, q), we define an associated symmetric bilinear form $h_q : V \times V \to F$:
$$(x, y) \mapsto \frac{1}{2}[q(x + y) - q(x) - q(y)].$$

Two quadratic spaces (V, q) and (V', q') are **isometric** if there exists an invertible linear map $L : V \to V'$ such that $h_{q'}(Lx, Ly) = h_q(x, y)$. Moreover, we have the following fundamental result of Witt.

Theorem 4.3 (Witt's Cancellation Theorem)**.** *Let U_1, U_2, V_1, V_2 be quadratic spaces, with V_1 and V_2 isometric. If $U_1 \bigoplus V_1 \cong U_2 \bigoplus V_2$, then $U_1 \cong U_2$.*

The matching of q and h_q defines a bijection

$$\{\text{quadratic forms } V \to F\} \Longleftrightarrow \{\text{sysmetric bilinear forms } V \times V \to F\}.$$

For any quadratic form q and any choice of basis $\{e_i\}_{1 \le i \le n}$, we can define an associated symmetric matrix $A_q = [a_{ij}]_{1 \le i,j \le n}$ by

$$a_{ij} := h_q(e_i, e_j).$$

This matrix A_q does depend on our choice of basis by construction. Given a different choice of basis, the associated matrix will become $X^T A_q X$, where X is the corresponding change of basis matrix. In particular, $\det(X^T A_q X) = \det(A_q) \cdot \det(X)^2$, which suggests that the determinant of an associated matrix of q is defined up to a square in $F^\times$. [3]

Definition 4.4. Given a quadratic space (V, q), the **discriminant** of q is defined by

$$\operatorname{disc}(q) := [\det(A_q)] \in F/(F^\times)^2,$$

where $[\det(A_q)]$ is the image of $\det A_q$ in the quotient.

We say that q is **nondegenerate** (or **non-singular**, **regular**), or an **inner product**, if $\det(A_q) \neq 0$. In this case, (V, q) is called an **inner product space**.

h_q also allows us to introduce the notion of orthogonality.

Definition 4.5. $v, w \in (V, q)$ are called orthogonal if and only if $h_q(v, w) = 0$. Given a subspace W of V, the set of elements perpendicular to W is defined by

$$W^\perp := \{v \in V : h_q(v, w) = 0, \forall w \in W\}.$$

Theorem 4.6. *Every quadratic space has an orthogonal basis, i.e. any form can be diagonalized as*

$$q \cong a_1 X_1^2 + \cdots + a_1 X_1^2,$$

and then we shall write

$$q \cong \langle a_1, ..., a_n \rangle = \langle a_1 \rangle + \cdots + \langle a_n \rangle,$$

where $\langle a_i \rangle$ denotes the one-dimensional form $q(X_i) = a_i X_i^2$.

Since any form can be decomposed into $q \cong \langle a_1, ..., a_r \rangle + \langle 0, ..., 0 \rangle$ with $a_i \in F^\times$, we will be interested in the nondegenerate quadratic spaces from now on.

Another crucial question to ask is: when is there a nonzero vector $v \in V$ such that $h_q(v, v) = q(v) = 0$? This leads to the following definition.

Definition 4.7. An element $x \in (V, q)$ is called **isotropic** if $h_q(x, x) = q(x) = 0$. Otherwise, we say x is **anisotropic**.

A quadratic space is **anisotropic** iff every nonzero vector is anisotropic. Otherwise, we call it an isotropic space.

The prototype of an isotropic space is the **hyperbolic plane**, which is a 2-dimensional quadratic space defined by

$$Q(X,Y) = X^2 - Y^2.$$

We will use H_2 to denote (V,Q). Moreover, we have the following useful fact.

Proposition 4.8. *Let (V,q) be a nondegenerate quadratic space which contains an isotropic vector. Then V contains a hyperbolic plane.*

Proof. See [3] for a constructive proof. □

A quadratic space of dimension $2r$ that is isomorphic to r copies of H_2 is called a **hyperbolic space**.

The following theorem of Witt says that a nondegenernate quadratic space can always be split into a hyperbolic part (i.e. an isotropic part) and an anisotropic part.

Theorem 4.9 (Witt's Decomposition Theorem)**.** *Let (V,q) be a nondegenerate quadratic space. Then, $q \cong H_2^{\oplus r} \oplus q_0$, where q_0 is anisotropic. Moreover, such a decomposition is unique up to isomorphism.*

Proof. The existence is not hard to prove by induction using orthogonal decomposition and Proposition 4.8. The uniqueness follows from Proposition 4.8 and Theorem 4.3. □

In particular, Witt's decomposition theorem says that the isotropic parts of the quadratic spaces really look the "same"; it is the anisotropic part that characterizes a quadratic space. This motivates the following definitions which describe the structure of quadratic forms over a particular field.

Definition 4.10 (u-invariant of a Field)**.** The u**-invariant** $u(F)$ of a field F is the largest dimension of an anisotropic quadratic space over F, or ∞ if this does not exist.

Definition 4.11 (Witt Ring)**.** [9] Let q and q' be quadratic forms. We say $q \sim q'$ (Witt equivalent) if their anisotropic parts are isometric $q_0 \cong q_0'$. Let $W(F)$ denote the set of all equivalence classes of forms over the field F with respect to this equivalence relation $\sim$. Define an addition on $W(k)$ by

$$[q_1] + [q_2] = [q_1 \oplus q_2]$$

and a product

$$[q_1] \cdot [q_2] = [q_1 \otimes q_2].$$

Then these operations are well-defined, and $W(F)$ is a commutative ring with identity given by $[\langle 1 \rangle]$, $0 = [H_2]$, and additive inverse of $[\langle a_1, ..., a_n \rangle]$ given by $[\langle -a_1, ..., -a_n \rangle]$. $W(F)$ is called the **Witt ring** of F.

5. Classifications of Quadratic Forms over $\mathbb{F}_p$ and $\mathbb{Q}_p$

We'll see that the Hasse-Minkowski theorem reduces questions over $\mathbb{Q}$ about quadratic forms with rational coefficients to the corresponding questions over $\mathbb{Q}_p$ for $p \in \{\text{all primes}\} \cup \{\infty\}$. It is thus essential for us to understand quadratic forms over $\mathbb{Q}_p$, which closely relates to the classification of forms over $\mathbb{F}_p$, the finite field with p elements.

5.1. Classification of Quadratic Forms over $\mathbb{F}_p$ with $p \neq 2$.

Proposition 5.1. *Let p be an odd prime. Then, any quadratic form in greater than or equal to 3 variables over $\mathbb{F}_p$ is isotropic.*

Proof. Let $\mathrm{char}(\mathbb{F}_p) \neq 2$. By theorem 4.6, any quadratic form over $\mathbb{F}_p$ can be written in the form $Q(X,Y,Z) = aX^2 + bY^2 + cZ^2$, with $a,b,c \in \mathbb{F}_p^\times$. We will show that $Q(X,Y,Z) = 0$ always has a nontrivial solution over $\mathbb{F}_p$.

Indeed, take $Z = 1$ and set $Q(X,Y,1) = 0$. Then, we'll have

$$aX^2 = -bY^2 - c. \tag{5.2}$$

Since the LHS of equation (5.2) depends only on X and the RHS of equation (5.2) depends only on Y, let's make a counting argument. Both the set $\{aX^2 : X \in \mathbb{F}_p\}$ and $\{-bY^2 - c : Y \in \mathbb{F}_p\}$ have size $\frac{p+1}{2}$, while $\mathbb{F}_p$ has p elements. By the pigeonhole principle, there must be some $x, y \in \mathbb{F}_p$ such that

$$ax^2 = -by^2 - c,$$

and $(x,y,1)$ is a nontrivial solution to $Q(X,Y,Z) = 0$. □

Theorem 5.3. *Let $\mathbb{F}_p$ be the finite field with p elements ($p \neq 2$, prime). Then, $u(\mathbb{F}_p) = 2$.*

Proof. Let $v \in \mathbb{F}_p/(\mathbb{F}_p^\times)^2$. Then, the 2-dimensional form $Q(X,Y) = X^2 - vY^2$ has no non-trivial zero and is thus anisotropic. So $u(\mathbb{F}_p) \geq 2$. Since proposition 5.1 implies that $u(\mathbb{F}_p) \leq 2$, $u(\mathbb{F}_p) = 2$. □

5.2. Classification of Quadratic Forms over $\mathbb{Q}_p$.

The classification of quadratic forms over $\mathbb{Q}_p$ with p prime is closely related to that for $\mathbb{F}_p$.

Theorem 5.4 (Classification of Quadratic Forms over $\mathbb{Q}_p$, $p \neq 2$)**.** *Suppose that p is an odd prime. Then, $W(\mathbb{Q}_p) \cong W(\mathbb{F}_p) \bigoplus W(\mathbb{F}_p)$, where $\mathbb{F}_p$ is the field of p elements. In particular, any form f over $\mathbb{Q}_p$ can be written in the form*

$$f \cong \langle u_1, \cdots, u_r \rangle \oplus \langle pv_1, \cdots, pv_s \rangle,$$

with $u_i, v_j \in \mathbb{Z}_p^\times$.

Proof. See p.63-64 in [2]. □

Corollary 5.5. *Let p be an odd prime. Then, $u(\mathbb{Q}_p) = 4$.*

Proof. Suppose $q(X_1, ..., X_n)$ is a quadratic form over $\mathbb{Q}_p$ with $n \geq 5$. Then, by theorem 5.4,

$$q(X_1, ..., X_n) \cong \langle u_1, \cdots, u_r \rangle \oplus \langle pv_1, \cdots, pv_s \rangle,$$

with $u_i, v_j \in \mathbb{Z}_p^\times$ and $r + s = n$. In particular, either $r \geq 3$ or $s \geq 3$, which implies that either $\langle u_1, \cdots, u_r \rangle$ or $\langle pv_1, \cdots, pv_s \rangle$ must be isotropic by theorem 5.3. So there must be a nontrivial tuple $(\alpha_1, ..., \alpha_n) \in \mathbb{F}_p^n$ such that $q(\alpha_1, ..., \alpha_n) = 0$. Without loss of generality, suppose $\alpha_1 \neq 0 \bmod p$ and fix all the α_i with $2 \leq i \leq n$. Then, $x_1 = \alpha_1$ is such that

$$F(x_1, \alpha_2, ..., \alpha_n) \equiv 0 \pmod{p\mathbb{Z}_p} \text{ and } F'(x_1, \alpha_2, ..., \alpha_n) = u_1 x_1 \not\equiv 0 \pmod{p\mathbb{Z}_p}.$$

So by Theorem 2.10 (i.e. the weaker form of Hensel's lemma), $x_1 = \alpha_1$ can be lifted to a unique root of $q(X_1, \alpha_2, ..., \alpha_n)$ over $\mathbb{Q}_p$. Hence, $q(X_1, ..., X_n)$ is isotropic over $\mathbb{Q}_p$. □

The structure of quadratic forms over $\mathbb{Q}_2$ needs to be handled separately again due to the different structure of squares in $\mathbb{Q}_2$.

Theorem 5.6 (Classification of Quadratic Forms over $\mathbb{Q}_2$)**.** [2]

$$W(\mathbb{Q}_2) \cong \mathbb{Z}/8\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}.$$

However, it turns out that, for $\mathbb{Q}_2$, every 5-dimensional form is isotropic as well, and there is a unique anisotropic 4-dimensional form $\langle 1, -5, 2, -10\rangle$ up to isomorphism. (See p.36 in [11] and [4].) Thus, in fact,

Theorem 5.7. *$u(\mathbb{Q}_p) = 4$ for all primes p.*

6. The Hilbert Symbol and Hilbert Reciprocity

We shall introduce the Hilbert Symbol in this section and eventually prove the Hilbert reciprocity, which will be another essential ingredient for the proof of the Hasse-Minkowski theorem.

Definition 6.1. Let E be a local field. Given $a, b \in E^\times$, the **Hilbert Symbol** $(a, b)_E$ is defined as

$$(a,b)_E = \begin{cases} 1 & \text{if } \langle a, b, -1\rangle \text{ is isotropic over } E, \\ -1 & \text{otherwise.} \end{cases}$$

Theorem 6.2 (Hilbert Reciprocity)**.** *Let $a, b \in \mathbb{Q}$. Then,*

$$(a,b)_{\mathbb{R}} \prod_{p,\ prime} (a,b)_{\mathbb{Q}_p} = \prod_{\nu} (a,b)_{\mathbb{Q}_\nu} = +1,$$

where the place ν ranges over all primes and ∞. In particular, the number of places ν in which the equation $aX^2 + bY^2 - Z^2 = 0$ does not have a nontrivial solution is finite and even.

One can derive Hilbert reciprocity from Quadratic reciprocity. We will refer the readers to [2] or [11] for such an approach, while presenting a different proof here, which relies on the more general notion of a symbol (or a Steinberg symbol) and the calculation of the K_2 group of $\mathbb{Q}$, which will be defined now.

Definition 6.3. Let F be a field and A be an abelian group (written multiplicatively). A **symbol** or a **Steinberg symbol** on F with values in A is a function

$$\varphi : F^\times \times F^\times \to A$$

such that

(a) (Bimultiplicativity in the 1st slot) $\varphi(ab, c) = \varphi(a, c)\varphi(b, c)$;
(b) (Bimultiplicativity in the 2nd slot) $\varphi(a, bc) = \varphi(a, b)\varphi(a, c)$;
(c) (Steinberg Relation) $\varphi(a, b) = 1$ if $a + b = 1$, $a, b \in \mathbb{F}^\times$.

Example 6.4. On $\mathbb{Q}_\nu$, the Hilbert Symbol $(\cdot,\cdot)_{\mathbb{Q}_\nu}$ is a symbol with values in $\{\pm 1\}$.

Remark 6.5. If $f : F \to E$ is a field homomorphism and φ is a symbol on E, then $\varphi \circ f$ is a symbol on F.

For example, $(\cdot,\cdot)_{\mathbb{Q}_v}$ restricts to a symbol on $\mathbb{Q}$.

Definition 6.6 (The Tame Symbol)**.** For a prime p, there exists a **tame symbol** on $\mathbb{Q}$ defined by

$$(a,b)_p = (-1)^{v_p(a)v_p(b)} \cdot \overline{a^{v_p(b)}/b^{v_p(a)}} \in \mathbb{F}_p^\times,$$

where the reduction $\overline{a^{v_p(b)}/b^{v_p(a)}} = a^{v_p(b)}/b^{v_p(a)} \pmod p$ is well defined because $v_p(a^{v_p(b)}/b^{v_p(a)}) = 0$. In particular, this symbol is trivial when $p = 2$. Moreover,

$$(a,b)_p = \begin{cases} a \bmod p, & \text{if } \gcd(a,p) = 1 \text{ and } b = p, \\ 1, & \text{if } \gcd(a,p) = \gcd(b,p) = 1. \end{cases}$$

Now comes the definition of the K_2 group of a field F, denoted by $K_2(F)$, and the universal symbol on F.

Definition 6.7. Set A to be the free abelian group (with group operation written multiplicatively) on the set $F^\times \times F^\times$ modulo the subgroup generated by

$$(ab,c)(a,c)^{-1}(b,c)^{-1}$$
$$(a,bc)(a,b)^{-1}(a,c)^{-1}$$
$$(a,b) \text{ if } a+b=1.$$

This A is denoted by $K_2(F)$.

There exists a **universal symbol** on F with values in $K_2(F)$ defined by

$$(a,b) \mapsto \{a,b\} := \text{the image of } (a,b) \text{ in } K_2(F).$$

In particular, there is a bijection

$$\{\text{Symbols on } F \text{ with values in } A\} \to \{\text{Homomorphisms } K_2(F) \to A\}.$$

6.1. **Tate's Proof of the Hilbert Reciprocity.** Before we present the full proof, here is the underlying idea of the proof: first, we will find the group structure of $K_2(\mathbb{Q})$; then, we will use this information to deduce that certain relation must hold among the Hilbert symbols on all $\mathbb{Q}_v$'s. This proof can be found in [8], and the way it will be presented here is based on [4].

6.1.1. *Step 1: Find the Group Structure of $K_2(\mathbb{Q})$.*

Theorem 6.8.

$$K_2(\mathbb{Q}) \cong A_2 \bigoplus A_3 \bigoplus A_5 + \cdots,$$

where $A_2 = \mathbb{Z}/2\mathbb{Z}$ and $A_p = (\mathbb{Z}/p\mathbb{Z})^\times$. In particular, the isomorphism is given by

$$(a,b) \mapsto ((a,b)_{\mathbb{Q}_2}, (a,b)_3, (a,b)_5, \cdots).$$

Remark 6.9. Note that the first entry of the image is the value of the Hilbert symbol in $\mathbb{Q}_2$, while each of the rest is the value of a tame symbol.

Proof. Let's first show that this map is well-defined. In particular, since the map goes from $K_2(\mathbb{Q})$ to $\prod_{p \text{ prime}} A_p$, let's show that the image actually lands in $\bigoplus_{p \text{ prime}} A_p$. Indeed, the tame symbol (x,y) is trivial if there is no p in x or y.

For $n \geq 1$, define subgroup $L_n \subseteq K_2(\mathbb{Q})$ as the subgroup generated by the symbols $\{x,y\}$, where $x,y \in \mathbb{Z}$ and $|x|_\infty, |y|_\infty \leq n$. So we obtain a chain of subgroups:

$$\{1\} \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq K_2(\mathbb{Q}).$$

Notice that this filtration is exhaustive, i.e. $\bigcup_n L_n = K_2(\mathbb{Q})$. Indeed, given any symbol $\varphi(\frac{a}{b}, \frac{c}{d})$ with $a,b,c,d \in \mathbb{Z}$ and $b,d \neq 0$, we can write

$$\varphi(b, \frac{c}{d})\varphi(b,d) = \varphi(b,c) \in L_{\max(|b|,|c|)} \subseteq K_2(\mathbb{Q})$$

and so $\varphi(b, \frac{c}{d}) \in K_2(\mathbb{Q})$. Then, we can write

$$\varphi(\frac{a}{b}, \frac{c}{d})\varphi(b, \frac{c}{d})\varphi(a, d) = \varphi(a, c) \in L_{\max(|a|,|c|)} \subseteq K_2(\mathbb{Q}),$$

which implies that $\varphi(\frac{a}{b}, \frac{c}{d}) \in K_2(\mathbb{Q})$.

Also, notice that L_1 is generated by $\{1,1\}, \{-1,1\}, \{1,-1\}$ and $\{-1,-1\}$. In particular, it follows from the bimultiplicativity of a symbol that $\{1,1\}, \{-1,1\}, \{1,-1\}$ are all trivial. To show that $\{x,y\}$ is nontrivial, we only need to show that there exists a symbol φ on which $\varphi(x,y) \neq 1$. Indeed, if we take the real Hilbert symbol $(\cdot,\cdot)_{\mathbb{R}}$ and restrict it to $\mathbb{Q}$, we'll get $(-1,-1)_{\mathbb{R}} = -1$, since the form $\langle 1,1,1,1\rangle$ is anisotropic over $\mathbb{R}$. So $\{-1,-1\}$ is nontrivial. Thus, L_1 is generated by $\{-1,-1\}$ and is a cyclic group of order 2.

Another observation is that, if n is not prime, then $L_{n-1} = L_n$. Indeed, let $\{x,y\} \in L_n$. Then, we have $|x|,|y| \leq n$. Since n is not prime, we can write $n = ab$ with $a, b \in \mathbb{Z}$ and $1 < a, b \leq n-1$. So using bimultiplicativity, we can show that $\{x,y\} \in L_{n-1}$.

Let $\varphi_p : K_2(\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$ be defined by $\varphi_p(x,y) = (x,y)_p$. Then, for any $\{x,y\} \in L_{p-1}$, $\varphi_p(x,y) = (x,y)_p = 1 \in (\mathbb{Z}/p\mathbb{Z})^\times$, because $\gcd(x,p) = \gcd(x,p) = 1$. Thus, we have a map $\varphi_p : L_p/L_{p-1} \to (\mathbb{Z}/p\mathbb{Z})^\times$.

Lemma 6.10. *The map $\varphi_p : L_p/L_{p-1} \to (\mathbb{Z}/p\mathbb{Z})^\times$ defined by*

$$\varphi_p(x,y) = (x,y)_p \in (\mathbb{Z}/p\mathbb{Z})^\times$$

is an isomorphism for all prime p.

Assume for now this lemma. We'll prove by induction that, for $n \geq 2$, the map $L_n \to \bigoplus_{p\leq n} A_p$ induced by the $\mathbb{Q}_2$ Hilbert symbol on the 2th factor and tame symbol on the p-th factor is an isomorphism. If this holds, then Tate's theorem follows.

Base case: When $n = 2$, we want to show that $\varphi_2 : L_n \to A_2 = \mathbb{Z}/2\mathbb{Z}$ is an isomorphism. Indeed, by lemma 6.10, when $p = 2$, $\varphi_2 : L_2/L_1 \to (\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ is an isomorphism. So $L_2 = L_1$, which is cyclic of order 2 generated by $\{-1,-1\}$. Moreover, $\varphi_2(-1,-1) = -1 \in A_2$. So it follows that $L_n \cong A_2$.

Inductive Step: Assume that, for $n-1$, the map $L_{n-1} \to \bigoplus_{p\leq n-1} A_p$ induced by the $\mathbb{Q}_2$ Hilbert symbol on the 2th factor and tame symbol on the p-th factor is an isomorphism.

Suppose n is not prime, then we have $L_{n-1} = L_n$ and $\bigoplus_{p\leq n-1} A_p = \bigoplus_{p\leq n} A_p$. So it follows immediately from the inductive hypothesis that $L_n \cong \bigoplus_{p\leq n} A_p$.

Suppose n is prime, then we have a short exact sequence

$$0 \to L_{n-1} \to L_n \to L_n/L_{n-1} \to 0.$$

On the other hand, we can build another short exact sequence

$$0 \to \bigoplus_{p\leq n-1} A_p \to \bigoplus_{p\leq n} A_p \to A_p \to 0.$$

Since $L_{n-1} \cong \bigoplus_{p\leq n-1} A_p$ and $L_p/L_{p-1} \cong (\mathbb{Z}/p\mathbb{Z})^\times$, we have $L_n \cong \bigoplus_{p\leq n} A_p$ by the snake lemma.

Now let's prove the lemma we assumed in the proof.

Proof of Lemma 6.10. Let's first argue the surjectivity. Any element in $(\mathbb{Z}/p\mathbb{Z})^\times$ is represented by an integer $0 < x < p$. We claim that $\varphi_p(x,p) = \{x,p\} = [x] \in (\mathbb{Z}/p\mathbb{Z})^\times$. Indeed, since $\gcd(x,p) = 1$, we have $(x,p) = x \bmod p$.

Then, we'll show that the $\{x,p\}$'s give all of the classes in L_p/L_{p-1}. We will show this in two steps:

(a) Let's show that the $\{x,p\}$'s form a subgroup of L_p/L_{p-1}.

Take $0 < x < p$ and $0 < y < p$. Let z be the least positive residue of $xy \bmod p$. Then, we have

$$z = xy + p \cdot q$$

for some $q \in \mathbb{N}$. Divide by xy on both sides, we get

$$1 = \frac{z}{xy} + \frac{pq}{xy},$$

and it follows from the Steinberg relation that

$$\{\frac{z}{xy}, \frac{pq}{xy}\} = 1.$$

Since

$$q = \frac{xy - z}{p} < \frac{xy}{p} < \frac{p^2}{p} = p,$$

we have $|q| < p$ and so $\{\frac{z}{xy}, p\} \equiv \{\frac{z}{xy}, \frac{pq}{xy}\} = 1$.

(b) Let's show that the $\{x,p\}$'s generate L_p/L_{p-1}.

Indeed, this is the case, since L_{p-1} is generated by $\{a,b\}$ with $0 < a, b \leq p-1$ and L_p is generated by $0 < a, b \leq p$.

□

So the proof of theorem 7.11 is now complete. □

6.1.2. *Step 2: Deduce the relation among the $(a,b)_{\mathbb{Q}_\nu}$s.* Rephrasing $K_2(\mathbb{Q}) \cong \bigoplus_p A_p$ as follows: For every symbol $\varphi : F^\times \times F^\times \to A$, there exists a unique homomorphism $f_p : A_p \to A$ for all p such that

$$\varphi(x,y) = f_2((x,y)_{\mathbb{Q}_2}) \prod_{p>2} f_p((x,y)_p).$$

Let's apply this to the real Hilbert symbol $\varphi(x,y) = (x,y)_{\mathbb{R}} \in \{\pm 1\}$. Since $\{\pm 1\}$ has order 2 and the Hilbert symbol $\mathbb{Q}^\times \times \mathbb{Q}^\times \to \{\pm 1\}$ factors through $(\mathbb{Z}/p\mathbb{Z})^\times$ via the Legendre symbol, there exists $\epsilon_p \in \{0,1\}$ for all p such that, for all $x, y \in \mathbb{Q}^\times$,

$$(x,y)_{\mathbb{R}} = \prod_p (x,y)_{\mathbb{Q}_p}^{\epsilon_p}$$

Thus, to prove Hilbert reciprocity, we only need to show that $\epsilon_p = 1$ for all p. To show this, let's plug in $x = y = -1$. Then, we have

$$(-1,-1)_{\mathbb{R}} = -1 = (-1,-1)_{\mathbb{Q}_2}^{\epsilon_2} = (-1)^{\epsilon_2},$$

and so $\epsilon_2 = 1$.

Let $p \equiv 3 \bmod 4$. Then, we have

$$(-1,p)_{\mathbb{R}} = 1 = (-1)^{\frac{p-1}{2}} \cdot (-1,p)_p^{\epsilon_p} = (-1) \cdot (-1)^{\epsilon_p},$$

and so $\epsilon_p = 1$.

Let $p \equiv 5 \bmod 8$. Then, we have

$$(2,p)_{\mathbb{R}} = 1 = 1 \cdot (2,p)_p^{\epsilon_p} = 1 \cdot 1^{\epsilon_p},$$

and so $\epsilon_p = 1$.

So we are left with the case when $p \equiv 1 \bmod 8$. In this case, we need to apply the following lemma, which is not quite easy to prove.

Lemma 6.11. *If $p \equiv 1 \bmod 8$, then there exists a prime q such that the Legendre symbol $\left(\dfrac{p}{q}\right) = -1$.*

Proof. See proof in [8] pp.104–106. □

Taking this lemma for granted and applying it to (p, q), one can use induction to show that $\epsilon_p = 1$.

Remark 6.12. It's not hard to deduce Quadratic reciprocity from Hilbert reciprocity. Hence, the Hilbert reciprocity on $\mathbb{Q}$ is equivalent to Quadratic reciprocity.

7. A Full Proof of the Hasse-Minkowski Theorem

In this section, we will consider a quadratic form q over the rationals $\mathbb{Q}$, i.e a degree-2 homogeneous polynomial with rational coefficients. For every place ν, with $\nu = p$ a prime or ∞, q gives a quadratic form q_ν, where we take exactly the same polynomial but allowing the variables to live in the completion of $\mathbb{Q}$. The Hasse-Minkowski theorem encapsulates the idea of the local-global principle. In particular, the knowledge of q_ν for all local places ν, i.e. all possible completions of $\mathbb{Q}$, can give us knowledge of q over the global field $\mathbb{Q}$.

7.1. Three Forms of the Local-Global Principle.

There are three forms of the Hasse-Minkowski theorem, which are stated as follows. [4]

Theorem 7.1 (Form 1)**.** *If the quadratic form q_ν over $\mathbb{Q}_\nu$ is isotropic for all ν, then q is isotropic over $\mathbb{Q}$.*

Theorem 7.2 (Form 2)**.** *Let $a \in \mathbb{Q}$. If the quadratic form q_ν over $\mathbb{Q}_\nu$ represents a for all ν, then q over $\mathbb{Q}$ represents a.*

Theorem 7.3 (Form 3)**.** *Let q, f be two quadratic forms over $\mathbb{Q}$. If $q_\nu \cong f_\nu$ over $\mathbb{Q}_\nu$ for all ν, then $q \cong f$ over $\mathbb{Q}$.*

Let's first observe that, in fact, "Form 1" implies "Form 2" and "Form 3".

"Form 1" $\implies$ "Form 2": Recall that for any quadratic form q over any field F (with char$(F) \neq 2$), q represents an element $a \in F$ if and only if the form $q + \langle -a \rangle$ is isotropic. Thus, if q_ν over $\mathbb{Q}_\nu$ is isotropic for all ν, then the form $q + \langle -a \rangle$ is isotropic for all $a \in \mathbb{Q}_\nu$ for all ν, and if q is isotropic over $\mathbb{Q}$, then q over $\mathbb{Q}$ represents a.

"Form 1" $\implies$ "Form 3": Suppose that q over $\mathbb{Q}$ represents some $a \neq 0 \in \mathbb{Q}$. Then, $q + \langle -a \rangle$ is isotropic and so must contains a hyperbolic plane. That is, we can write

$$q + \langle -a \rangle \cong H_2 + q'.$$

Since q is isotropic over $\mathbb{Q}_\nu$ and $q_\nu \cong f_\nu$ over $\mathbb{Q}_\nu$ for all ν, $f + \langle -a \rangle \cong q + \langle -a \rangle$ must also be isotropic. Thus, it follows from "Form 1" that $f + \langle -a \rangle$ is isotropic over $\mathbb{Q}$. So we can also write

$$f + \langle -a \rangle \cong H_2 + f'.$$

Now, let's use induction on the number of variables.

Notice that q' has one variable less than q and f' has one variable less than f. Since $q_\nu \cong f_\nu$ over $\mathbb{Q}_\nu$ for all ν, we have

$$q_\nu + \langle -a \rangle \cong f_\nu + \langle -a \rangle \implies H_2 + q'_\nu \cong H_2 + f'_\nu$$

over $\mathbb{Q}_\nu$ for all ν. By Witt's cancellation theorem, $q'_\nu \cong f'_\nu$ for all ν, and therefore $q' \cong f'$ over $\mathbb{Q}$ by the inductive hypothesis. Hence,

$$g + \langle -a \rangle \cong H_2 + q' \cong H_2 + f' \cong f + \langle -a \rangle$$

over $\mathbb{Q}$, and it follows from Witt's cancellation theorem again that $q \cong f$ over $\mathbb{Q}$.

Remark 7.4. Hasse-Minkowski theorem is special to degree-2 equations. A famous example of the failure of the local-global principle is Selmer's example:

$$3X^3 + 4Y^3 + 5Z^3 = 0,$$

which has a nontrivial solution in $\mathbb{Q}_\nu$ for all ν, but no nontrivial solution in $\mathbb{Q}$.[10]

Remark 7.5. The proof of Hasse-Minkowski theorem relies on two big theorems: Hilbert reciprocity and Dirichlet's theorem on primes in arithmetic progressions. The proof will be by induction on the number of variables and based on [4].

7.2. **Preparations.**

Before diving into the actual proof, let's first collect several useful lemmas which will be helpful for us in the course of the proof.

Lemma 7.6. *Let ν be a place of $\mathbb{Q}$ and $a, b, c \in \mathbb{Q}_\nu^\times$. Then, $aX^2 + bY^2$ represents c over $\mathbb{Q}$ if and only if $(a,b)_{\mathbb{Q}_\nu} = (c, -ab)_{\mathbb{Q}_\nu}$.*

Proof. Given that $a, b, c \in \mathbb{Q}_\nu^\times$, $aX^2 + bY^2$ represents c over $\mathbb{Q}$ if and only if $\frac{a}{c}X^2 + \frac{b}{c}Y^2$ represents 1, which is the case if and only if the form $\frac{a}{c}X^2 + \frac{b}{c}Y^2 - z^2$ is isotropic over $\mathbb{Q}$. By definition, this is equivalent to that $(\frac{a}{c}, \frac{b}{c})_{\mathbb{Q}} = 1$, which implies that $(\frac{a}{c}, \frac{b}{c})_{\mathbb{Q}_\nu} = 1$ for all ν.

Now, let's expand out this equation using the bimultiplicativity of the Hilbert symbol. Since

$$\begin{aligned} 1 = (\frac{a}{c}, \frac{b}{c})_{\mathbb{Q}_\nu} &= (ac, bc)_{\mathbb{Q}_\nu} = (a,b)_{\mathbb{Q}_\nu}(c,b)_{\mathbb{Q}_\nu}(a,c)_{\mathbb{Q}_\nu}(c,c)_{\mathbb{Q}_\nu} \\ &= (c, ab)_{\mathbb{Q}_\nu}(a,b)_{\mathbb{Q}_\nu}(c,-1)_{\mathbb{Q}_\nu} = (c,-ab)_{\mathbb{Q}_\nu}(a,b)_{\mathbb{Q}_\nu}, \end{aligned}$$

we must have $(c, -ab)_{\mathbb{Q}_\nu} = (a,b)_{\mathbb{Q}_\nu}$. □

Lemma 7.7. *Let K be a field and $a, b \in K^\times$. Then, the form $aX^2 + bY^2 - Z^2$ is isotropic if and only if $a \in N_{K(\sqrt{b})}(K(\sqrt{b})^\times)$. Moreover, $N_{K(\sqrt{b})}(K(\sqrt{b})^\times) \subseteq K^\times$ is closed under multiplication.*

Proof. If $b \in K^\times$ is a square, then $K(\sqrt{b}) = K$ and so the statement is trivial.

Suppose that $b \in K^\times$ is not a square. Then, $K(\sqrt{b})$ is a quadratic extension of K. Suppose $aX^2 + bY^2 - Z^2$ is isotropic. Then there exists tuple (x_0, y_0, z_0) with at least one nonzero entry such that $ax_0^2 + by_0^2 - z_0^2 = 0$.

Suppose $z_0 \neq 0$. Then, $a(\frac{x_0}{z_0})^2 + b(\frac{y_0}{z_0})^2 = 1$ and so we have

$$a = (\frac{z_0}{x_0})^2 \cdot (1 - b(\frac{y_0}{z_0})^2) = (\frac{z_0}{x_0})^2 - b(\frac{x_0}{y_0})^2 = (\frac{z_0}{x_0} - \sqrt{b}\frac{x_0}{y_0})(\frac{z_0}{x_0} + \sqrt{b}\frac{x_0}{y_0}),$$

i.e. $a = N(\frac{z_0}{x_0} + \sqrt{b}\frac{x_0}{y_0}) \in N_{K(\sqrt{b})}(K(\sqrt{b})^\times)$.

Suppose $z_0 = 0$. Then we must have $x_0, y_0 \neq 0$. Moreover, $ax_0^2 = -by_0^2$ and so

$$a = -b(\frac{y_0}{x_0})^2 = (\sqrt{b}\frac{y_0}{x_0})(-\sqrt{b}\frac{y_0}{x_0}) = N(\sqrt{b}\frac{y_0}{x_0}) \in N_{K(\sqrt{b})}(K(\sqrt{b})^\times).$$

Conversely, suppose $a \in N_{K(\sqrt{b})}(K(\sqrt{b})^\times)$. Then, there must be some $y, z \in K$ with not both zero such that

$$a = (z + \sqrt{b}y)(z - \sqrt{b}y) = z^2 - by^2.$$

So $(1, y, z)$ is a nontrivial solution to $aX^2 + bY^2 - Z^2 = 0$, i.e. the form $aX^2 + bY^2 - Z^2$ is isotropic over K. □

Lemma 7.8. *Let $f = aX^2 + bY^2 - Z^2$ be an isotropic quadratic form over $\mathbb{Q}_\mu$ for all μ (i.e. all primes p and ∞), where $a, b \in \mathbb{Z} \setminus \{0\}$ are square-free and $|a| + |b| \geq 3$. Then, a is a square mod b.*

Proof. By the Chinese remainder theorem, to show that a is a square mod b, it suffices to show that a is a square mod p for all $p \mid b$.

Since $f = aX^2 + bY^2 - Z^2 = 0$ has nontrivial solution over $\mathbb{Q}_p$ for all p and f is homogeneous, we can clear denominator and find a nontrivial solution in $\mathbb{Z}_p$ for all p. Moreover, we can make $v_p(X) = 0$, $v_p(Y) = 0$, or $v_p(Z) = 0$ by multiplication by powers of p.

Since $p \mid b$ and $aX^2 + bY^2 - Z^2 = 0$, we have $p \mid aX^2 - Z^2$, i.e. $aX^2 \equiv Z^2 \pmod{p}$. I claim that $X \pmod{p}$ is a unit. Indeed, suppose for a contradiction that $p \mid X$. Then $p \mid Z$ as well. So we can further divide $f = 0$ through by p, contradicting the primitivity, i.e. $v_p(X) = 0$, $v_p(Y) = 0$, or $v_p(Z) = 0$.

So $X \bmod p$ is invertible, and thus we have $a \equiv \frac{Z^2}{X^2} \pmod{p}$. Since this is true for all $p \mid b$, a is a square mod b. □

7.3. Proof of the Hasse-Minkowski Theorem: $n = 1, 2, 3$.

Proof. Let f be a quadratic form over $\mathbb{Q}$. Then, after diagonalization, we can write

$$f(X_1, ..., X_n) = a_1X_1^2 + \cdots + a_nX_n^2, a_i \in \mathbb{Q}^\times.$$

Since f has a nontrivial zero if and only if $a_1^{-1}f$ has a nontrivial zero, we can assume that f is monic. Moreover, since we can always modify a_i by a square and clear denominator, it suffices for us to consider the form

$$f(X_1, ..., X_n) = X_1^2 + a_2X_2^2 \cdots + a_nX_n^2,$$

where $a_i \in \mathbb{Z} \setminus \{0\}$ and a_i is square-free for all $2 \leq i \leq n$.

Now, let's induct on the dimension of the form n.

1. **n=1:** The form $f = X_1^2$ does not have a nontrivial zero and is always anisotropic. So there is no 1-dimensional form satisfying the hypothesis.
2. **n=2:** Consider the form $f = X_1^2 + a_2X_2^2$, where $a_2 \in \mathbb{Z} \setminus \{0\}$ is square-free. If f is isotropic over $\mathbb{Q}_\nu$ for all ν, then the equation $X_1^2 + a_2X_2^2 = 0$ has a nontrivial solution (so X_1, X_2 are both nonzero). So $-a_2 \in (\mathbb{Q}_\nu^\times)^2$ for all places ν. In particular,

$$-a_2 \in (\mathbb{Q}_\infty^\times)^2 \implies -a_2 > 0 \implies a_2 < 0,$$

$$-a_2 \in (\mathbb{Q}_p^\times)^2, \forall p \implies v_p(-a_2) \text{ is even for all } p.$$

Since a_2 is square-free, it must be that $a_2 = -1$. So $f = X_1^2 - X_2^2 \cong H_2$, which is isotropic over $\mathbb{Q}$.

3. **n=3:** Consider the form $f = X_1^2 + a_2X_2^2 + a_3X_3^2$, where $a_2 \in \mathbb{Z} \smallsetminus \{0\}$ is square-free. Let's multiply through by -1, rename the variables, and consider instead

$$f = -X_1^2 - a_2X_2^2 - a_3X_3^2 = aX^2 + bY^2 - Z^2,$$

where a, b are square-free integers. We will prove the desired statement by induction on $|a| + |b|$.

Base case: When $|a| + |b| = 2$, $a, b \in \{\pm 1\}$. The only time when f does not have a nontrivial solution in $\mathbb{Q}$ is when $a = b = -1$. However, this is also the only time when f does not have a nontrivial zero over $\mathbb{Q}_\nu$ for all ν, since it does not have a nontrivial zero over $\mathbb{R}$. So f is isotropic over $\mathbb{Q}_\nu$ for all ν implies that f is isotropic over $\mathbb{Q}$ for the base case.

Inductive Step: Suppose that f is isotropic over $\mathbb{Q}_\nu$ for all ν implies that f is isotropic over $\mathbb{Q}$ for $3 \leq |a| + |b| \leq m$.

We shall assume $|a| \leq |b|$ (otherwise just interchange a and b.) When $|a| + |b| \geq 3$, by lemma 7.8, a is square mod b. That is, we have $a = t^2 \pmod b$ for some $t \in \mathbb{Z} \smallsetminus \{0\}$, i.e.

$$t^2 - a = (t + \sqrt{a})(t - \sqrt{a}) = bb' \tag{7.9}$$

for some $b' \in \mathbb{Z}$. In particular, we shall choose t so that $|t| \leq |b|/2$ and notice that $bb' \in N_{\mathbb{Q}_\nu}(\mathbb{Q}_\nu(\sqrt{a})^\times)$. Since $N_{\mathbb{Q}_\nu}(\mathbb{Q}_\nu(\sqrt{a})^\times)$ is a group, we have $b \in N_{\mathbb{Q}_\nu}(\mathbb{Q}_\nu(\sqrt{a})^\times)$ if and only if $b' \in N_{\mathbb{Q}_\nu}(\mathbb{Q}_\nu(\sqrt{a})^\times)$. Thus, by lemma 7.7, the form $bU^2 + aV^2 - W^2$ is isotropic over $\mathbb{Q}_\nu$ if and only if the form $b'U^2 + aV^2 - W^2$ is isotropic over $\mathbb{Q}_\nu$.

Now, I claim that $|b'| < |b|$. Indeed, it follows from equation 7.9 that

$$|b'| = |\frac{t^2 - a}{b}| = \frac{|t^2 - a|}{|b|} \leq \frac{|t^2| + |a|}{|b|} \leq \frac{|b|^2/4 + |b|}{|b|} = \frac{|b|}{4} + 1. \tag{7.10}$$

Suppose for a contradiction that $\frac{|b|}{4} + 1 \geq |b|$, then

$$\frac{3}{4}|b| \leq 1 \implies |b| \leq \frac{4}{3},$$

which means that $b \in \{\pm 1\}$, contradicting our assumption that $|a| \leq |b|$ and $|a| + |b| \geq 3$. So we must have

$$|b'| \leq \frac{|b|}{4} + 1 < |b|,$$

which means that $|a| + |b'| < |a| + |b|$. So by the inductive hypothesis, the form

$$b'U^2 + aV^2 - W^2 = 0$$

is isotropic over $\mathbb{Q}_\nu$ for all ν implies that f is isotropic over $\mathbb{Q}$. Hence, the form $bU^2 + aV^2 - W^2$ is isotropic over $\mathbb{Q}_\nu$ implies that the form $bU^2 + aV^2 - W^2$ is isotropic over $\mathbb{Q}$. This completes the proof of the $n = 3$ case. □

7.4. **Proof of the Hasse-Minkowski Theorem:** $n = 4$.

Proof. Consider the diagonal form

$$f = aX^2 + bY^2 - cZ^2 - dW^2,$$

with $a, b, c, d \in \mathbb{Q}^\times$. Since f is isotropic for all ν by assumption, f represents 0 for all ν. So there exists $t_\nu \in \mathbb{Q}_\nu^\times$ such that

$$aX^2 + bY^2 = t_\nu = cZ^2 + dW^2. \tag{7.11}$$

(We can assume that $t_\nu \in \mathbb{Q}_\nu^\times$, because if $t_\nu = 0$, then both $aX^2 + bY^2$ and $cZ^2 + dW^2$ are isomorphic to the hyperbolic plane H_2 and thus represents any element in $\mathbb{Q}_\nu$.) By lemma 7.6, equation 7.11 is true if and only if $(t_\nu, -ab)_{\mathbb{Q}_\nu} = (a, b)_{\mathbb{Q}_\nu}$ and $(t_\nu, -cd)_{\mathbb{Q}_\nu} = (c, d)_{\mathbb{Q}_\nu}$.

Let $S = \{\infty, 2\} \cup \{p : p \text{ is prime and } p \mid abcd\}$. Since, by proposition 3.1, given any place ν of $\mathbb{Q}$, there is an $\delta_\nu > 0$ such that if $x \in \mathbb{Q}_\nu$ satisfies $|1 - x| < \delta_\nu$, then $x = y^2$ for some $y \in \mathbb{Q}_\nu^\times$, we shall choose ϵ_ν's so that $\frac{\epsilon_\nu}{|t_\nu|} < \delta_\nu$ for all ν. By the Strong Approximation theorem (i.e. theorem 3.4), there is some $t \in \mathbb{Q}^\times$ such that t and t_∞ have the same sign and for all $\nu \neq \infty \in S$, $|t - t_\nu| < \epsilon_\nu$, (i.e. $|\frac{t}{t_\nu} - 1| < \frac{\epsilon_\nu}{|t_\nu|} < \delta_\nu$). So $\frac{t}{t_\nu} \in \mathbb{Q}_\nu^{\times 2}$ for all $\nu \in S$. Therefore,

$$(t, -ab)_{\mathbb{Q}_\nu} = (t_\nu, -ab)_{\mathbb{Q}_\nu} = (a, b)_{\mathbb{Q}_\nu},$$
$$(t, -cd)_{\mathbb{Q}_\nu} = (t_\nu, -cd)_{\mathbb{Q}_\nu} = (c, d)_{\mathbb{Q}_\nu},$$

which implies that t is represented by both $aX^2 + bY^2$ and $cZ^2 + dW^2$ in $\mathbb{Q}_\nu$ for all $\nu \in S$ by lemma 7.11.

Additionally, we can guarantee that $|t|_p = 1$ and $t \in \mathbb{Z}_p^\times$ for all $p \notin S \cup \{p_0\}$, where p_0 is a special prime that is not in S. Since p must be odd and $p \nmid ab$, $t, -ab \in \mathbb{Z}_p^\times$. So it follows from Hensel's lemma that, for all $p \notin S \cup \{p_0\}$, we have

$$(t, -ab)_{\mathbb{Q}_p} = 1 = (a, b)_{\mathbb{Q}_p},$$
$$(t, -cd)_{\mathbb{Q}_p} = 1 = (c, d)_{\mathbb{Q}_p}.$$

So t is represented by both $aX^2 + bY^2$ and $cZ^2 + dW^2$ in $\mathbb{Q}_p$ for all $p \notin S \cup \{p_0\}$ by lemma 7.11.

Now, by Hilbert's product formula, we must have

$$(t, -ab)_\infty \prod_{p \text{ prime}} (t, -ab)_{\mathbb{Q}_p} = 1 = (a, b)_\infty \prod_{p \text{ prime}} (a, b)_{\mathbb{Q}_p},$$
$$(t, -cd)_\infty \prod_{p \text{ prime}} (t, -cd)_{\mathbb{Q}_p} = 1 = (c, d)_\infty \prod_{p \text{ prime}} (c, d)_{\mathbb{Q}_p},$$

which implies that we must have

$$(t, -ab)_{\mathbb{Q}_{p_0}} = (a, b)_{\mathbb{Q}_{p_0}},$$
$$(t, -cd)_{\mathbb{Q}_{p_0}} = 1 = (c, d)_{\mathbb{Q}_{p_0}}.$$

So t is represented by both $aX^2 + bY^2$ and $cZ^2 + dW^2$ in $\mathbb{Q}_{p_0}$ as well.

Hence, t is represented by both $aX^2 + bY^2$ and $cZ^2 + dW^2$ in $\mathbb{Q}_\nu$ for all places ν. This is the case iff. the forms $\langle a, b, -t\rangle$ and $\langle c, d, -t\rangle$ are isotropic over $\mathbb{Q}_\nu$ for all ν. So it follows from the case $n = 3$ that $\langle a, b, -t\rangle$ and $\langle c, d, -t\rangle$ are isotropic over $\mathbb{Q}$. So t is represented by $\langle a, b, -t\rangle$ and $\langle c, d, -t\rangle$ in $\mathbb{Q}$, i.e. there exist $x, y, z, w \in \mathbb{Q}$ such that

$$ax^2 + by^2 = t = cz^2 + dw^2.$$

In particular, the tuple $(x,y,z,w) \in \mathbb{Q}^{\oplus 4}$ is a non-trivial solution to

$$f = aX^2 + bY^2 - cZ^2 - dW^2.$$

So f is isotropic over $\mathbb{Q}$. □

7.5. Proof of the Hasse-Minkowski Theorem: $n \geq 5$.

Proof. For $n \geq 5$, consider the form

$$f = aX_1^2 + bX_2^2 - c_3X_3^2 - c_4X_4^2 - \cdots - c_nX_n^2$$

and let

$$S = \{\nu : \langle c_3, c_4, \cdots, c_n\rangle \text{ is not isotropic in } \mathbb{Q}_\nu\}.$$

Observe that, for $p \nmid 2c_3c_4\cdots c_n$,

$$g = c_3X_3^2 + c_4X_4^2 + \cdots + c_nX_n^2 = 0$$

has a nontrivial solution $(x_3, x_4, \cdots, x_n)$ over $\mathbb{F}_p$, since $u(\mathbb{F}_p) = 2$ and $n-2 \geq 3$. Moreover, without loss of generality, suppose that $x_3 \neq 0 \in \mathbb{F}_p$, we can fix x_i for all $4 \leq i \leq n$ and get

$$g'_{X_3} = 2a_1x_3 \neq 0 \pmod{p}.$$

So by Hensel's lemma, $\langle c_3, c_4, \cdots, c_n\rangle$ is isotropic over $\mathbb{Q}$. Since there are only finitely many $p \mid 2c_3c_4\cdots c_n$, S is finite.

For each $\nu \in S$, choose some $t_\nu \in \mathbb{Q}_\nu^\times$ represented by both $aX_1^2 + bX_2^2$ and g, i.e.

$$c_3z_{3(\nu)}^2 + c_4z_{4(\nu)}^2 + \cdots + c_nz_{n(\nu)}^2 = t_\nu = ax_\nu^2 + by_\nu^2 \text{ for some } x_\nu, y_\nu, z_{i(\nu)} \in \mathbb{Q}_\nu.$$

By the Weak Approximation theorem (i.e. theorem 3.2), there exist $x, y \in \mathbb{Q}$ such that $|\frac{x}{x_\nu} - 1| < \epsilon_\nu$ and $|\frac{y}{y_\nu} - 1| < \epsilon_\nu$ for any $\epsilon_\nu \in \mathbb{R}_{>0}$ and $\nu \in S$. By lemma 3.1, $x_\nu, y_\nu \in \mathbb{Q}_\nu$ can be chosen so that $x \in x_\nu(\mathbb{Q}_\nu^\times)^2$ and $y \in y_\nu(\mathbb{Q}_\nu^\times)^2$. So by continuity, for all $\nu \in S$, we can choose $|\frac{t}{t_\nu} - 1| < \epsilon_\nu$ for any $\epsilon_\nu \in \mathbb{R}_{>0}$ so that $t \in t_\nu(\mathbb{Q}_\nu^\times)^2$.

Since t and t_ν differ by a square, $\langle -t, c_3, c_4, \cdots, c_n\rangle$ is isotropic for all $\nu \in S$ as well. However, it is also isotropic for all $\nu \notin S$, because we said that $\langle c_3, c_4, \cdots, c_n\rangle$ is isotropic for all $\nu \notin S$. Thus, it follows from our inductive hypothesis that $\langle -t, c_3, c_4, \cdots, c_n\rangle$ is isotropic over $\mathbb{Q}$, i.e. g represents t over $\mathbb{Q}$. Thus, there exist $x, y, z_i \in \mathbb{Q}$ such that

$$ax^2 + by^2 = t = c_3z_3^2 + c_4z_4^2 + \cdots + c_nz_n^2.$$

So f is isotropic over $\mathbb{Q}$. □

8. Some Corollaries

We'll end this paper with some corollaries of the Hasse-Minkowski theorem.

8.1. Sums of Squares.

One can use the Hasse-Minkowski theorem to prove the famous theorem on sums of three squares and four squares.

We say that a positive integer m is a sum of n squares if m is representable over $\mathbb{Z}$ by the quadratic form $X_1^2 + \cdots + X_n^2$.

Theorem 8.1 (Gauss)**.** [11] *A positive integer is a sum of three squares if and only if it is not of the form $4^a(8b-1)$ with $a, b \in \mathbb{Z}$.*

Proof. See page 45-47 in [11]. □

Corollary 8.2 (Lagrange)**.** *Every positive integer is a sum of four squares.*

Proof. If $n \in \mathbb{Z}_{>0}$ is not of the form $4^a(8b-1)$ with $a, b \in \mathbb{Z}$, then it is a sum of 3 squares by theorem 8.1 and hence a sum of 4 squares (just take the 4th variable to be 0). Otherwise, $n-1$ is not of the form $4^a(8b-1)$ and so n can be expressed as the sum of three squares of $n-1$ and 1. [11]. □

8.2. **Representability of Rational Numbers.**

Corollary 8.3 (Meyer)**.** [11] *A quadratic form of dimension* ≥ 5 *represents 0 if and only if it represents 0 in* $\mathbb{R}$.

Proof. Indeed, by Corollary 5.7, such a form represents 0 in $\mathbb{Q}_p$ for all prime p. □

Remark 8.4. The Hasse-Minkowski theorem actually gives a *finite* procedure for deciding the representability of 0 (and thus any rational numbers) by a quadratic form.

Let q be a quadratic form with rational coefficients. There is finite procedure for deciding whether q represents 0 (and thus any $\gamma \in \mathbb{Q}$) in each $\mathbb{Q}_p$. See Theorem 6 on page 36 in [11] for reference. Moreover, there is a finite number of places one need to check.

(a) If $\dim(q) = 1$, then $q = aX_1^2$ is always anisotropic.
(b) If $\dim(q) = 2$, then $q = aX_1^2 + bX_2^2$ represents 0 exactly when $-\frac{b}{a} \in \mathbb{Q}^{\times 2}$.
(c) If $\dim(q) = 3$ (resp. 4), then $q = aX_1^2+bX_2^2+cX_3^2$ (resp. $q = aX_1^2+bX_2^2+cX_3^2+dX_4^2$) represents 0 in all $\mathbb{Q}_p$ with $p \nmid 2abc$ (resp. $p \nmid 2abcd$) by Theorem 5.3 and Hensel's lemma. So we only need to check for the representability of 0 in $\mathbb{R}$ and $\mathbb{Q}_p$ such that $p \mid 2abc$ (resp. $p \mid 2abcd$).
(d) If $\dim(q) \geq 5$, then we only need to check for $\mathbb{R}$ by Corollary 8.3.

Let's look at an example to see how one can solves problems using the Hasse-Minkowski theorem.

Example 8.5. Consider the quadratic form $q(X,Y,Z) = 3X^2+5Y^2-17Z^2$. Suppose we want to know if the equation $q(X,Y,Z) = 0$ has a non-trivial solution in $\mathbb{Q}^3$.

We first observe that $q(X,Y,Z) = 0$ has the non-trivial solution $(1, 0, \sqrt{\frac{3}{17}})$ in $\mathbb{R}^3$.

Then, let p be a prime with $p \neq 2, 3, 5, 17$. Then, the number of variables of $q(X,Y,Z)$ is $3 \pmod p$ because $p \neq 3, 5, 17$, which means that $q(X,Y,Z) \equiv 0 \pmod p$ has a non-trivial solution (x_0, y_0, z_0) in $\mathbb{F}_p$. Without loss of generality, assume x_0 is the non-zero value in (x_0, y_0, z_0), i.e. $x_0 \not\equiv 0 \pmod p$. If we let $f(x) = 3X^2 + 5y_0^2 - 17z_0^2$, then $f(x_0) \equiv 0 \pmod p$. Moreover, $f(x_0) \not\equiv 0 \pmod p$ because $f(x_0) = 2 \cdot 3 \cdot x_0$ and $p \nmid 2 \cdot 3 \cdot x_0$. By Hensel's Lemma (Theorem 2.10), we can lift the solution (x_0, y_0, z_0) to a solution (x_0, y_0, z_0) in $\mathbb{Q}_p^3$ for all such primes p.

In the cases that $p = 2, 3, 5, 17$, one can find that $(1, 0, 1)$ is a non-trivial solution $\pmod 2$, $(0, 2, 1)$ is a non-trivial solution $\pmod 3$, $(2, 0, 1)$ is a non-trivial solution $\pmod 5$, and $(2, 1, 0)$ is a non-trivial solution $\pmod{17}$.

Performing the same process as when $p \neq 2, 3, 5, 17$, we can use Hensel's Lemma to lift these solutions to $\mathbb{Q}_p^3$ for all primes p. Namely, we just need to define a single variable polynomial f for each solution and check that $f \neq 0$ at the point in question. Since q represents 0 in $\mathbb{R}^3$ and $\mathbb{Q}_p^3$ for all primes p, by the Hasse-Minkowski Theorem, q represents 0 in $\mathbb{Q}^3$.

Acknowledgments

Firstly, I would like to thank Professor Akhil Mathew for working with me this summer, guiding me through readings on p-adic numbers, quadratic forms, and the Hasse-Minkowski theorem, and presenting to me the depth and beauty of the subjects. I would also like to thank my mentor Thomas Hameister for being so patient and supportive, meeting with me consistently, and giving me lots of help and encouragement in math and beyond along the way. My thanks as well to the PCMI program for the lecture series on quadratic forms, Milnor K-theory, and arithmetic. Thank you to my advisor Professor Fernando Q. Gouvea for leading me to major in mathematics, sparking my interest in number theory, and inspiring me in both academics and life. Finally, thank you to Professor Peter May for organizing this REU program, along with all the professors, graduate students, and organizers who made this program possible in these uncertain times.

References

[1] Bell, R. (2021). Strange new landscape: an exploration of the p-adic numbers and modular forms. lecture.

[2] Cassels, J. W. S. (1978). Rational quadratic forms. London.

[3] Chan, C. (2021). Quadratic forms and the local global-principle. lecture.

[4] Clausen, D., amp; Mathew, A. The 30th Annual PCMI Summer Session. Quadratic forms, Milnor K-theory, and arithmetic. Lecture presented at the The 30th Annual PCMI Summer Session. https://www.ias.edu/pcmi/programs/pcmi-2021-undergraduate-summer-school. Accessed 14 August 2021.

[5] Gouvêa, F. Q. (2020). P-Adic numbers: An introduction. Cham: Springer Nature Switzerland AG.

[6] Kurt Hensel-Biography. Maths History.
https://mathshistory.st-andrews.ac.uk/Biographies/Hensel/. Accessed 15 August 2021.

[7] MacDuffee, C. C. (1938). The p-adic numbers Of hensel. The American Mathematical Monthly, 45(8), 500. doi:10.2307/2303739 .

[8] Milnor, John. Introduction to algebraic K-theory. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971. Annals of Mathematics Studies, No. 72.

[9] Scharlau, W. Algebraic theory of quadratic forms: Generic methods and Pfister forms. CORE. https://core.ac.uk/reader/11543260. Accessed 15 August 2021.

[10] Schinck, A. (2001). The local-global principle in number theory (thesis).

[11] Serre, Jean-Pierre. (1985). A Course in Arithmetic. Springer.

Appendix A. Proof of the Strong Approximation Theorem

Theorem A.1 (The Strong Approximation Theorem)**.** *If S is a finite set of places of $\mathbb{Q}$ containing ∞ and we are given $x_\nu \in \mathbb{Q}_\nu^\times$ for all $\nu \in S$ and $\epsilon_\nu \in \mathbb{R}_{>0}$ for all $\nu \in S \setminus \infty$, then there is a prime $p_0 \notin S$ and an $x \in \mathbb{Q}^\times$ such that:*

(1) $|x - x_\nu| < \epsilon_\nu$ for all $p \in S \setminus \infty$;
(2) x has the same sign as x_∞;
(3) $|x|_p = 1$ for all $p \notin S \cup \{p_0\}$.

Proof. Let $S = \{\nu_1, \cdots, \nu_n\} \cup \{\infty\}$ be a finite set of places of $\mathbb{Q}$, $x_i \in \mathbb{Q}_{\nu_i}$, and $\epsilon_i \in \mathbb{R}_{>0}$ for $1 \le i \le n$.

Let's first consider the case when $x_\infty > 0$.

For each i, write each $x_i = p^{v_{p_i}(x_i)} \cdot x_i'$ with $x_i' \in \mathbb{Z}_{p_i}^\times$. Let $k_i \in \mathbb{Z}$ be such that $p^{-k_i} < \epsilon_i$ and $-v_{p_i}(x_i) + k_i \in \mathbb{Z}_{>0}$. Set $M = \prod_{i=1}^n p_i^{-v_{p_i}(x_i)}$ and $k_i' = -v_{p_i}(x_i) + k_i$. Then, for each i, we have

$$Mx_i = \prod_{j\neq i, j\in\{1,\ldots,n\}} p_j^{-v_{p_j}(x_j)} \cdot p^{-v_{p_i}(x_i)} \cdot x_i = \prod_{j\neq i, j\in\{1,\ldots,n\}} p_j^{-v_{p_j}(x_j)} \cdot x_i' \in \mathbb{Z}_{p_i}^\times.$$

Choose an integer $\alpha_i \in \mathbb{Z}$ for each i such that

$$\alpha_i \equiv Mx_i \pmod{p_i^{k_i'}\mathbb{Z}_{p_i}}. \tag{A.2}$$

Since the $p_i' s$ are clearly coprime, by the Chinese remainder theorem, there exists $x \in \mathbb{Z}$ such that

$$x \equiv \alpha_i \pmod{p_i^{k_i'}} \tag{A.3}$$

for $1 \le i \le n$. In particular, define

$$b_i = \frac{\prod_{j\in\{1,\ldots,n\}} p_j^{k_j'}}{p_i^{k_i'}} = \prod_{j\neq i\in\{1,\ldots,n\}} p_j^{k_j'},$$

and let $b_i' \equiv b_i^{-1} \bmod p_i^{k_i'}$. Then,

$$x \equiv \sum_i \alpha_i \cdot b_i \cdot b_i' \pmod{\prod_i p_i^{k_i'}}. \tag{A.4}$$

Notice that equation (A.3) and (A.4) together implies that, for each i,

$$\alpha_i \equiv \sum_i \alpha_i \cdot b_i \cdot b_i' \pmod{p_i^{k_i'}}. \tag{A.5}$$

Since $Mx_i \in \mathbb{Z}_{p_i}^\times$, it follows from equation (A.2) that we have

$$\sum_i \alpha_i b_i b_i' \pmod{p_i} \equiv \alpha_i \pmod{p_i} \neq 0.$$

So $\gcd(\sum_i \alpha_i b_i b_i', \prod_j p_i^{k_i'}) = 1$. Thus, by Dirichlet's theorem, there exists infinitely many primes q such that

$$q \equiv \sum_i \alpha_i b_i b_i' \pmod{\prod_i p_i^{k_i'}}.$$

Take one such $q \in \mathbb{N}$ and let $p_0 = q$. Set $x = \frac{p_0}{M}$. Then, one can check that x has the desired properties:

(1) Since we have equation (A.5) and $p_0 = q \equiv \sum_i \alpha_i b_i b_i' \pmod{\prod_i p_i^{k_i'}}$, $p_0 \in \mathbb{N}$ is such that
$$|p_0 - \alpha_i|_{p_i} = |q - \alpha_i|_{p_i} \leq p_i^{-k_i'}$$
for all p_i with $\nu_i \in S$. Moreover,
$$\begin{aligned} |p_0 - \alpha_i|_{p_i} \leq p_i^{-k_i'} &\iff |\frac{1}{M}(p_0 - Mx_i)|_{p_i} = |\frac{p_0}{M} - x_i|_{p_i} \leq p_i^{-k_i} \\ &\implies |\frac{p_0}{M} - x_i|_{p_i} < \epsilon_i. \end{aligned}$$
So $x = \frac{p_0}{M} \in \mathbb{Q}$ is such that $|x - x_i|_{p_i} < \epsilon_i$ for all places $\nu_i \in S$, provided that $\nu_i \neq \infty$.

(2) $x = \frac{p_0}{M} > 0$, and we required $x_\infty > 0$.

(3) Let $p \notin S \cup \{p_0\}$. Then, since $p \nmid p_0$ and $p \nmid M$, we have $v_p(x) = v_p(\frac{p_0}{M}) = 0$ and so $|x|_p = 1$.

Now, for the case when $x_\infty < 0$, we can set
$$M = -\prod_{i=1}^{n} p_i^{-v_{p_i}(-x_i)}$$
instead and run through exactly the same argument again. The corresponding $x = \frac{p_0}{M} < 0 \in \mathbb{Q}$ will satisfy property (1) and (3). □