p-ADIC NUMBERS, HASSE-MINKOWSKI THEOREM, AND ITS APPLICATIONS

XINGYU WANG

Abstract. This paper discusses the topic of finding rational and integer solutions of an equation with homogeneous polynomials of degree 2. We will introduce the notion of p-adic numbers, Legendre symbols, Hilbert symbols, and quadratic forms to build up to Hasse-Minkowski Theorem. Eventually, we apply Hasse-Minkowski Theorem to prove some important results, such as the sum of three and four squares.

Contents

1. Introduction

Historically, mathematicians such as Fermat, Euler, Gauss, and Lagrange, had been interested in finding integer solutions of equations involving quadratic polynomials. An archetypal question is "the sum of three squares" problem, "For what kind of integer n does $x^2 + y^2 + z^2 = n$ have an integer solution (x, y, z)?"

The world of math soon discovered that it is easier to find solutions in fields such as $\mathbb{Q}$ instead of integral domains such as $\mathbb{Z}$. An interesting problem that arises from finding rational solutions is finding rational points on conics, which are equations of the form $ax^2 + by^2 = c$.

Later, the introduction of p-adic numbers by Hensel, Minkowski, and Hasse shed light on equations of quadratic polynomials. They converted the problem of finding rational solutions to that of finding solutions in all p-adic number fields and the real numbers, which turn out to be easier to work on than $\mathbb{Q}$.

This paper will present answers to questions such as the sum of three and four squares through the method of p-adic numbers. We will first define the p-adic numbers and understand their structure. Then we will present the Legendre symbols,

Date: August 31, 2019.

the Hilbert symbols, and quadratic forms, which are essential elements in the statement and proof of Hasse-Minkowski Theorem, one of the most fundamental results in number theory. Finally, we will show how to use Hasse-Minkowski Theorem to show what kind of integers are the sum of three squares of integers, or even four squares. This paper attempts to give an overall picture, so we will omit the proofs of some results.

The reader may entertain themselves to think about conics after reading the paper. A conic is an equation of the form $ax^2 + by^2 = c$. Not all conics have rational points. For example, the circle $x^2 + y^2 = 1$ has rational points such as $(x, y) = (1, 0)$, but $x^2 + y^2 = 3$ does not have any rational points. The reader may find out, after reading the paper, that whether there is a rational point depends on how the coefficients a, b, and c relate to the real numbers $\mathbb{R}$ and the prime numbers.

A disclaimer before the main body is many theorems will only present results for p as an odd prime. We do not include the cases where $p = 2$, because they often yield a different result, and the proof of the theorems will take more works.

The paper assumes familiarity with linear and abstract algebra, including basic group and ring theory.

2. p-adic Numbers

There are two most common ways of defining p-adic numbers, one analytic and one algebraic. The analytic definition tells us that p-adic numbers are the completion of $\mathbb{Q}$, with respect to the p-adic metrics. The algebraic definition puts p-adic numbers as sequences. We will present the two definitions. Then, we will derive the properties of the p-adic integers and p-adic numbers mostly with the algebraic definition.

To build upon the analytic definition, let us first see the definition of p-adic distance.

Definition 2.1. (p-adic valuation) Let p be any prime number. For any rational number a, $a \neq 0$, we write

$$a = p^m \frac{u}{v} \quad (m \in \mathbb{Z}, u, v \text{ are not divisible by } p)$$

We call m the *p-adic valuation* of a, and we denote it by $m = \mathrm{ord}_p(a)$. As a convention, we take $\mathrm{ord}_p(0) = \infty$.

Definition 2.2 (p-adic absolute value)**.** If a is a rational number and p is any prime, we define the *p-adic absolute value of a* as

$$|a|_p = p^{-\mathrm{ord}_p(a)}$$

Note that $|0|_p = 0$ because $\mathrm{ord}_p(0) = \infty$.

The definition of metric follows from the definition of the p-adic absolute value naturally.

Definition 2.3 (p-adic metrics)**.** Given a prime number p, we define the p-adic metric $d_p(a, b)$ on $\mathbb{Q}$ by

$$d_p(a, b) = |a - b|_p.$$

The reader may check that the p-adic metrics give rise to $\mathbb{Q}$ as a metric space with respect to the p-adic metrics. In other words, we have defined some metrics in $\mathbb{Q}$ other than our "usual" metric.

Definition 2.4 (Analytic definition)**.** If p is a prime number, the p-adic numbers are the completion of $\mathbb{Q}$ under the p-adic metric. In other words, let S_p be the set of all Cauchy sequences in $\mathbb{Q}$ under the p-adic metric. We define the following equivalence relation on S_p: $(x_n)_{n\geq 1}$ and $(y_n)_{n\geq 1}$ are equivalent if given any ϵ, we can obtain a natural number N such that

$$\text{for all } n > N,\ |x_n - y_n|_p < \epsilon.$$

We define $\mathbb{Q}_p$ to be the set of equivalence classes.

Having defined the p-adic metrics on $\mathbb{Q}$, we now extend the sense of distance to all of $\mathbb{Q}_p$ for a given prime p.

Definition 2.5 (p-adic absolute value on $\mathbb{Q}_p$)**.** Given a prime p and $a \in \mathbb{Q}_p$, we define $\mathrm{ord}_p(a) = \infty$ if $a = 0$. If $a \neq 0$, we choose a Cauchy sequence of rational numbers (x_n) in the equivalence class of a. Then $\mathrm{ord}_p(x_n)$ is constant for sufficiently large n (the reader may check this using the properties of ord). We define $\mathrm{ord}_p(a)$ to be this constant. We let $|a|_p = 0$ if $a = 0$; $|a|_p = p^{-\mathrm{ord}_p(a)}$ otherwise.

The reader might be reminded of the construction of $\mathbb{R}$ as the completion of $\mathbb{Q}$ from the analytic definition. In fact, as a convention, we often call $\mathbb{Q}_\infty = \mathbb{R}$. One step further, the following theorem shows that the only metrics on $\mathbb{Q}$ are the standard metric and the p-adic metrics.

Theorem 2.6 (Ostrowski's Theorem)**.** *Every nontrivial norm on $\mathbb{Q}$ is equivalent to one of the norms $|\ |_p$ for some prime p or for $p = \infty$.*

We omit the proof of the above theorem, because it is irrelevant to the major topic of this paper. The reader may check Koblitz's book for the proof [4, p.3].

Given the above analytic definition of $\mathbb{Q}_p$, We define the p-adic integers as

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid \mathrm{ord}_p(a) \geq 0\}$$

The reader may check that $\mathbb{Z}_p$ under this definition is a ring.

In our algebraic definition, however, we first define the p-adic integers, and then $\mathbb{Q}_p$ by taking the field of fractions. To define the p-adic integers, we introduce the notion of inverse limit.

Definition 2.7 (Inverse Limit)**.** Given a sequence of sets X_n, $n = (1, 2, 3, \cdots)$, and a sequence of maps $f_n : X_{n+1} \to X_n$, we define the following set

$$\{(a_n)_{n\geq 1} \in \prod_{n\geq 1} X_n \mid f_n(a_{n+1}) = a_n \text{ for all } n \geq 1\}$$

as the inverse limit. We denote it by $\varprojlim_n X_n$.

Definition 2.8 (Algebraic definition of p-adic integers)**.** Let $X_n = \mathbb{Z}/p^n\mathbb{Z}$, and let $a_n = f_n(a_{n+1}) = a_{n+1} \pmod{p^n}$. Thus, $a_n = f_n(a_{n+1}) \in \mathbb{Z}/p^n\mathbb{Z}$. We define the p-adic integers $\mathbb{Z}_p$ to be $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, i.e., the inverse limit of $\mathbb{Z}/p^n\mathbb{Z}$.

Given two elements in the inverse limit, (a_n) and (b_n), we define addition and multiplication over $\mathbb{Z}_p$ as $(a_n) + (b_n) = (a_n + b_n)$ and $(a_n) \cdot (b_n) = (a_n b_n)$. If $a_n = 0$ for all $n \in \mathbb{N}$, then we call (a_n) the additive identity; if $a_n = 1$ for all $n \in \mathbb{N}$, then (a_n) is the multiplicative identity. The reader may check that the algebraic definition with this definition of addition and multiplication gives rise to $\mathbb{Z}_p$ as a ring.

We extend the notion of absolute value to $\mathbb{Z}_p$ in the following way. For any $a = (a_n) \in \mathbb{Z}_p$, we define $\mathrm{ord}_p(a)$ to be the largest N such that $a_n = 0$ for all $n \leq N$. Then we have $|a| = p^{-\mathrm{ord}_p(a)}$.

We can now check the additional fact that $\mathbb{Z}_p$ is an integral domain.

Theorem 2.9. *$\mathbb{Z}_p$ is an integral domain.*

Proof. Take any $a, b \in \mathbb{Z}_p$. Then $|a \cdot b| = |a| \cdot |b|$. Hence, if $a \cdot b = 0$, one of $|a|$ and $|b|$ has to be 0. Thus, one of a and b has to be 0. □

Hence, in the algebraic definition, we can put $\mathbb{Q}_p$ to be the field of fractions of $\mathbb{Z}_p$.

The analytic and algebraic definitions of p-adic numbers are equivalent. One may check Kato's book [1, p.67] to understand the equivalence of the two.

Having built the definitions, we want to present a very useful tool that we will frequently use to find and build a p-adic integer. Hensel's Lemma is a p-adic version of the Newtonian method of approximation. The statement and proof of Hensel's Lemma tells us how to construct a p-adic integer a, given $a \pmod p$ and a polynomial. We will give a concrete example of how Hensel's Lemma is useful after proving it.

Lemma 2.10 (Hensel's Lemma)**.** *If $f(x) \in \mathbb{Z}_p[x]$, $c_0 \in \mathbb{Z}/p\mathbb{Z}$ is a root of $f \pmod p$, and $f'(c_0) \not\equiv 0 \pmod p$, then there exists a unique $c \in \mathbb{Z}_p$ such that $f(c) = 0$ and $c \equiv c_0 \pmod p$.*

Proof. To find a p-adic integer root means to find an inverse limit $c = (c_n)_{n\geq 1}$ such that $f(c) = 0$. Given an initial $c_0 \in \mathbb{Z}/p\mathbb{Z}$, we gradually "lift" the c_0 up to $c_1, c_2, \cdots$, where $c_i \in \mathbb{Z}/p^{i+1}\mathbb{Z}$, such that $c_i \equiv c_{i-1} \pmod p^i$. For example, $c_1 \equiv c_0 \pmod p$. This lifting process produces a p-adic integer that accords with the algebraic definition. Meanwhile, since we wish this p-adic integer c to be the root of f, we need each $f(c_n) \equiv 0 \pmod p^{n+1}$. Thus, our goal is to construct a sequence $c = (c_n)_{n\geq 0} \in \prod_{n\geq 1}(\mathbb{Z}/p^n\mathbb{Z})$ such that the following conditions hold:

(1) $f(c_n) \equiv 0 \pmod p^{n+1}$
(2) $c_n \equiv c_{n-1} \pmod p^n$

The construction is done inductively. We will omit the basic case, the construction of c_1 from c_0, because the method is exactly the same as the construction of c_n from c_{n-1}, which we will show below. Suppose we have obtained c_{n-1} that satisfies the above two conditions. To obtain c_n that satisfies condition 2, we wish to find $b_n \in \mathbb{Z}/p^{n-1}\mathbb{Z}$ such that $c_n = p^n b_n + c_{n-1}$. For such c_n to satisfy condition 1, we "Taylor expand" $f(c_n)$. Note that eventually we want $f(c_n) \equiv 0 \pmod p^n$, so we neglect the terms that are multiples of p^n.

$$f(c_n) = f(p^n b_n + c_{n-1}) \tag{1}$$

$$= f(c_{n-1}) + f'(c_{n-1}) b_n p^n \pmod p^{n+1} \tag{2}$$

We know that $f(c_{n-1})$ is a multiple of p^n, so $f(c_{n-1}) = p^n\alpha$ for some $\alpha \in \mathbb{Z}$. Since we have $c_{n-1} \equiv c_0 \pmod p$ inductively, $f'(c_0) \neq 0$ implies $f'(c_{n-1}) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Thus, $f'(c_{n-1})$ is invertible.

Now, the equation 1 becomes

$$f(c_n) = p^n\alpha + f'(c_{n-1}) b_n p^n \pmod p^{n+1}.$$

Since the inverse of $f'(c_{n-1})$ exists and is unique in $\mathbb{Z}/p\mathbb{Z}$, as long as $b_n = (p-\alpha)(f'(c_{n-1}))^{-1}$ in $\mathbb{Z}/p\mathbb{Z}$, we will have

$$\begin{aligned} f(c_n) &= p^n(\alpha + f'(c_{n-1}) \cdot (p-\alpha)(f'(c_{n-1}))^{-1}) \\ &= p^n \cdot p \\ &= 0 \pmod{p}^n \end{aligned}$$

Note that b_n is unique.

Let $c = c_0 + b_1 p + \cdots + b_n p^n + \cdots$. Then $f(c) = 0$, because $f(c) \equiv f(c_n) \equiv 0 \pmod{p}^n$ for all $n \in \mathbb{N}$. The uniqueness of c follows from the uniqueness of b_n's. □

The following is a concrete example of the application of Hensel's Lemma. This example helps us see how $\mathbb{Q}_p$ is a field containing $\mathbb{Q}$, but it is different from $\mathbb{R}$.

Example 2.11. $\sqrt{-1}$ exists in $\mathbb{Q}_5$.

Proof. Take $f(x) = x^2+1$. Then $f(2) = 4+1 \equiv 0 \pmod 5$. Hence, $f'(2) = 2\cdot 2 \equiv 4 \pmod 5$. By Hensel's Lemma, there exists a root of $f(x)$ in $\mathbb{Z}_p$, and that root is $\sqrt{-1}$. □

In the next part of this section, we will use the previous definitions and results to show some key results on the elements and structures of $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

Let's first introduce a representation of elements in $\mathbb{Z}_p$ that follows from the algebraic definition of p-adic integers. We claim that any p-adic integer a can be represented as

$$a = a_o + a_1 p + \cdots + a_n p^n + \cdots \tag{3}$$

where $a_i \in \{0, 1, \cdots, p-1\}$. Let 's check that a power series of the form 3 is an element in $\mathbb{Z}_p$. Let $x_n = a \pmod{p}^n$. Then $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ and we have $x_n = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1}$ for some $a_i \in \mathbb{Z}/p^i\mathbb{Z}$. Similarly, we have $x_{n-1} = a_0 + a_1 p + \cdots + a_{n-2}p^{n-2}$. Under this representation of x_n and x_{n-1}, $x_{n-1} \equiv x_n \pmod{p}^{n-1}$. Thus, we have checked the sequence $(x_n)_{n\geq 1}$ is indeed an inverse limit. Thus, a gives rise to an element of $\mathbb{Z}_p$.

We shall also check that any element in $\mathbb{Z}_p$ can be represented in terms of 3. Given any $x \in \mathbb{Z}_p$. Then by the algebraic definition of $\mathbb{Z}_p$, $x = (x_n)_{n\geq 1}$ where $x_{n+1} \equiv x_n \pmod{p}^n$. We define a sequence $(a_n)_{n\geq 0}$ in the following way. Let $a_0 = x_1$ and $a_n = \frac{x_{n+1}-x_n}{p^n}$. Then $a_n \in \mathbb{Z}/p\mathbb{Z}$ because $x_{n+1} \equiv x_n \pmod{p}^n$. Hence, we can represent x in terms of 3 where each coefficient in front of p^i is in $\mathbb{Z}/p\mathbb{Z}$.

We call the 3 *the power series representation of an element in* $\mathbb{Z}_p$. We will use this representation of p-adic integers in later theorems.

Theorem 2.12 (Elements in $\mathbb{Z}_p^\times$)**.** *Suppose $a \in \mathbb{Z}_p$ and $a = a_0 + a_1 p + \cdots + a_n p^n + \cdots$, where $a_i \in \{0, 1, \cdots, p-1\}$. Then $a \in \mathbb{Z}_p^\times$ if and only if $a_0 \neq 0$.*

Proof. If a is a unit, there exists some $b \in \mathbb{Z}_p$ such that $a \cdot b = 1$. Thus,

$$ab \bmod p \equiv 1$$

and so,

$$(a \bmod p)(b \bmod p) \equiv 1.$$

This is equivalent to

$$a_0 \cdot b_0 = 1 \text{ in } \mathbb{Z}/p\mathbb{Z}$$

where $b = b_0 + b_1 p + \cdots + b_n p^n + \cdots$. Hence, $a_0 \neq 0$.

If $a_0 \neq 0$, then $a \neq 0$, because $a \not\equiv 0 \pmod{p}$. By Hensel's Lemma, the polynomial $f(x) = ax - 1$ has a unique root in $\mathbb{Z}_p$. This root is the inverse of a, and so $a \in \mathbb{Z}_p^\times$. □

After showing the power series representation of a p-adic integer, we now show the power series representation of a p-adic number. The following theorem uses the algebraic definition of the p-adic numbers.

Theorem 2.13. *For any $x \in \mathbb{Q}_p$, x can be uniquely written as*

$$x = \sum_{i=-m}^{\infty} p^i a_i$$

for some $m \in \mathbb{Z}^{\geq 0}$ and $a_i \in \{1, 2, \cdots, p-1\}$.

Proof. Since $\mathbb{Q}_p^\times$ is the field of fraction of $\mathbb{Z}_p$, for any $x \in \mathbb{Q}_p$, $x = \frac{a}{b}$, where $a, b \in \mathbb{Z}_p$ and $b \neq 0$. By Theorem 2.12, we write a and b as

$$a = a_0 + a_1 p + a_2 p^2 + \cdots$$
$$b = b_m p^m + b_{m+1} p^{m+1} + \cdots$$

where $a_i, b_j \in \{0, 1, \cdots, p-1\}$, and $b_m \neq 0$. In other words, we write b by eliminating all terms with coefficients 0 and start with the m-th term with nonzero coefficient. Collecting the p^m, we have

$$\begin{aligned} b &= p_m(b_m + b_{m+1} p + b_{m+1} p^2 + \cdots) \\ &= p_m \cdot u \end{aligned}$$

where $u \in \mathbb{Z}_p^\times$ because $b_m \neq 0$. Hence,

$$\begin{aligned} \frac{a}{b} &= \frac{a}{p^m \cdot u} \\ &= \frac{1}{p^m} \cdot \frac{a}{u} \end{aligned}$$

But since u has a multiplicative inverse in $\mathbb{Z}_p$, $\frac{a}{u} \in \mathbb{Z}_p$. Thus, by Theorem 2.12, $\frac{a}{u} = \sum_{i=0}^{\infty} c_i p^i$ for some $c_i \in \{0, 1, \cdots, p-1\}$. But then,

$$\begin{aligned} \frac{a}{b} &= \frac{1}{p^m} \cdot \frac{a}{u} \\ &= \frac{1}{p^m} \cdot \sum_{i=0}^{\infty} c_i p^i \\ &= \sum_{i=-m}^{\infty} c_{i+m} p^i \end{aligned}$$

Renaming the coefficients, we get $x = \sum_{i=-m}^{\infty} p^i a_i$ for some $m \in \mathbb{Z}^{\geq 0}$ and $a_i \in \{0, 1, \cdots, p-1\}$. □

The above theorem shows any p-adic number can be expressed as a power series in p, and only finitely many terms have negative powers of p.

The following theorem determines the structure of $\mathbb{Q}_p^\times$. We want to understand the structure of $\mathbb{Q}_p$ in terms of rings that we are more familiar with.

Theorem 2.14. *For $p \neq 2$, $(\mathbb{Q}_p^\times, \cdot) \cong (\mathbb{Z}, +) \times (\mu_{p-1}, \cdot) \times (\mathbb{Z}_p, +)$, where μ_{p-1} is the set of the $(p-1)$-th root of unity and the isomorphism is a group isomorphism.*

Proof. We divide the proof into a few steps.

Step 1. Show that $(\mathbb{Q}_p^\times, \cdot) \cong (\mathbb{Z}, +) \times (\mathbb{Z}_p^\times, \cdot)$.

Since $\mathbb{Q}_p^\times = \mathbb{Q}_p - \{0\}$, by Theorem 2.13, any $a \in \mathbb{Q}_p^\times$ can be written uniquely as $a = p^n a'$ for some $n \in \mathbb{Z}$ and $a \in \mathbb{Z}_p^\times$. Note that if $a, b \in \mathbb{Q}^\times$, $a = p^n a'$ and $b = p^m b'$, where $n, m \in \mathbb{Z}$ and $a', b' \in \mathbb{Z}_p^\times$. Hence, $a \cdot b = p^{m+n} a'b'$, where $a'b' \in \mathbb{Z}_p$. Thus, the group isomorphism holds.

Step 2. Show that $(\mathbb{Z}_p^\times, \cdot) \cong (\mu_{p-1}, \cdot) \times (1 + p\mathbb{Z}_p, \cdot)$.

Take any $x \in \mathbb{Z}_p^\times$. Then we take $a = x(\pmod p)$, and $b = a^{-1}x$. Then $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $b \equiv 1 \pmod p$.

Consider the group homomorphism f from $\mathbb{Z}_p^\times$ to $(\mathbb{Z}/p\mathbb{Z})^\times$ defined by $x \mapsto x(\pmod p)$. We can think of the map this way: for some $x \in \mathbb{Z}_p$, we write it in the power series form $x = x_0 + x_1 p + \cdots x_n p^n + \cdots$. Thus, f maps x to x_0. By Thm 2.12, $x_0 \neq 0$ since x is a unit. The kernel of f is all elements in $\mathbb{Z}_p^\times$ that map to $1 \in (\mathbb{Z}/p\mathbb{Z})^\times$. Hence they are all of the form $1 + px$ for some $x \in \mathbb{Z}_p$. On the other hand, any $1+px \in 1+p\mathbb{Z}_p$ satisfies $1+px \equiv 1 \pmod p$. Hence, $\mathrm{Ker}(f) = (1+p\mathbb{Z}_p)$.

Take any element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, and let $f(x) = x^{p-1} - 1$. Then $f(a) = a^{p-1} \equiv 1 \pmod p$ by Fermat's Little Theorem. Furthermore, $f'(a) = (p-1)a^{p-2} \not\equiv 0 \pmod p$ because $a^{p-2} \equiv a^{-1} \pmod p$. Hence, by Hensel's Lemma, there exists a unique root $x \in \mathbb{Z}_p$ such that $x^{p-1} = 1$ and $x \equiv a \pmod p$.

Hence the map is a bijection.

Step 3. Show that $(1 + p\mathbb{Z}_p, \cdot) \cong (p\mathbb{Z}_p, +)$, and so the theorem holds.

Recall the Taylor expansion of log and exp functions,

$$\log(t) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(t-1)^n \quad \text{and} \quad \exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

We claim that log and exp functions are inverses of each other, and so their domains are isomorphic.

First, we will need the following result from Kato's book [1, p.71] without proving it: If $c \in \mathbb{R}$ and $c > \frac{1}{p-1}$, then for any $n \geq 1$ we have

$$nc - \mathrm{ord}_p(n!) \geq c. \tag{4}$$

Next, take any $x \in (p\mathbb{Z}_p, +)$. Let $c = 1$. Then since $p \neq 2$,

$$c > \frac{1}{p-1}.$$

By 4, for all $n \geq 1$,

$$n - \mathrm{ord}_p(n!) \geq 1.$$

For each term in $\exp(x)$, since $\mathrm{ord}_p(x) \geq 1$, $\mathrm{ord}_p(x^n) \geq n$ if $n \geq 1$. Then

$$\mathrm{ord}_p(\frac{x^n}{n!}) \geq n - \mathrm{ord}_p(n!) \geq 1.$$

Thus, except when $n = 0$, all terms in the exponential function is divisible by p. Thus, $\exp(x) \in 1 + p\mathbb{Z}_p$. Similarly, take $t \in (1 + p\mathbb{Z}_p, *)$. We have

$$\mathrm{ord}_p((-1)^{n-1}\frac{(t-1)^n}{n}) \geq 1$$

for $n \geq 1$. Thus, $\log(x) \in p\mathbb{Z}_p$. Then exp and log are inverses of each other by similar proof when defining exp and log in $\mathbb{R}$. Thus,

Since $(\mathbb{Z}_p, +) \cong (p\mathbb{Z}_p, +)$ by $x \mapsto px$ and $px \mapsto x$, we have $(1 + p\mathbb{Z}_p, \cdot) \cong (p\mathbb{Z}_p, +) \cong (\mathbb{Z}_p, +)$. Together with the first two steps, we obtain the theorem. □

Lastly, we present the structure of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$. The theorem tells us about the squares in $\mathbb{Q}_p$.

Theorem 2.15. *If $p \neq 2$, $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

Proof. By Theorem 2.14, $(\mathbb{Q}_p^\times, \cdot) \cong (\mathbb{Z}, +) \times (\mu_{p-1}, \cdot) \times (\mathbb{Z}_p, +)$. We can write

$$(\mathbb{Q}_p^\times, \cdot) \cong (\mathbb{Z}, +) \times (\mathbb{Z}/(p-1)\mathbb{Z}, +) \times (\mathbb{Z}_p, +) \tag{5}$$

because $(\mathbb{Z}/(p-1)\mathbb{Z}, +) \cong (\mu_{p-1}, \cdot)$. Therefore,

$$\mathbb{Q}_p^{\times 2} \cong (\mathbb{Z}, +)^2 \times (\mathbb{Z}/(p-1)\mathbb{Z}, +)^2 \times (\mathbb{Z}_p, +)^2. \tag{6}$$

Since the operations of the groups on the right-hand side are addition, we have To obtain the quotient $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, we quotient each term on the right-hand side of equations 5 and 6. Then

$$(\mathbb{Z}, +)/(\mathbb{Z}, +)^2 \cong (\mathbb{Z}, +)/(2\mathbb{Z}, +) \cong \mathbb{Z}/2\mathbb{Z}.$$

Since p is even, $p - 1$ is odd, so

$$(\mathbb{Z}/(p-1)\mathbb{Z}, +)/(\mathbb{Z}/(p-1)\mathbb{Z}, +)^2 \cong \mathbb{Z}/2\mathbb{Z}.$$

Note that $\mathbb{Z}_p/(\mathbb{Z}_p)^2 \cong \mathbb{Z}_p/2\mathbb{Z}_p$ is the trivial group. Since 2 is a unit in $\mathbb{Z}_p$, the ideal generated by 2 in $\mathbb{Z}_p$ is precisely $\mathbb{Z}_p$.

Therefore, for $p \neq 2$,

$$\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

□

3. Legendre Symbols and Quadratic Reciprocity Law

At the end of the last section, we have started to investigate squares in $\mathbb{Q}_p^\times$. In this section, we will introduce Legendre symbols, which represent if an element is a square in $\mathbb{Z}/p\mathbb{Z}$. We will also present Quadratic Reciprocity Law of the Legendre symbols. This is a foundational step towards the definition of Hilbert symbols and the Hasse-Minkowski Theorem. We refer mostly to Kato's book [1] in this section.

Definition 3.1 (Legendre symbol)**.** For any prime number p and an integer a coprime to p, we define the Legendre symbol $\left(\frac{a}{p}\right)$ in the following way:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{Z}/p\mathbb{Z} \\ -1 & \text{if } a \text{ is not a square in } \mathbb{Z}/p\mathbb{Z} \end{cases}$$

Here is a simple example of the Legendre symbols.

Example 3.2. In $\mathbb{Z}/5\mathbb{Z}$, we have $1 \equiv 1^2 \pmod 5$ and $4 \equiv 2^2 \pmod 5$. However, 2 or 3 is not the square of any element in $\mathbb{Z}/5\mathbb{Z}$. Hence, $\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1$, but $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$.

The following basic property follows from the definition of the Legendre symbol:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

We will now present the Quadratic Reciprocity Law, which is the key theorem of Legendre symbols. It contains one main statement and two supplementary laws.

Theorem 3.3 (Quadratic Reciprocity Law)**.** *Let p be an odd prime number.*

(1) (Quadratic Reciprocity Law) If q is an odd prime number other than p, we have

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

(2) (First supplementary law)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

(3) (Second supplementary law)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \end{cases}$$

Proof. The proof is not easy, and for this paper, we only need the statement of the theorem. The curious readers may check [2, p.7-9] for the proof. □

4. Hilbert Symbols and Hilbert Reciprocity Law

Hilbert symbols, like Legendre symbols, only take values in $\{\pm 1\}$. It determines if an equation of homogeneous quadratic polynomials has a solution in the p-adic fields. The symbols will be used extensively in the discussion of Hasse-Minkowski Theorem. The Hilbert symbols can be represented in terms of the Legendre symbols. The Hilbert Reciprocity Law, which is equivalent to the Quadratic Reciprocity Law, is a beautiful theorem in itself, because it tells us how all the prime numbers reciprocate with one another.

Definition 4.1 (Hilbert Symbols)**.** For any $a, b \in \mathbb{Q}_p^\times$, where p is any prime or ∞, we have

$$(a,b)_p = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a solution } (z,x,y) \neq (0,0,0) \text{ in } \mathbb{Q}_p. \\ -1 & \text{otherwise.} \end{cases}$$

We call $(a,b)_p$ the Hilbert symbol of a and b relative to $\mathbb{Q}_p$. Note that $\mathbb{Q}_\infty = \mathbb{R}$, and $(a,b)_\infty$ denotes the Hilbert symbol of a and b relative to $\mathbb{R}$.

In the above definition, the Hilbert symbol indicates if the equation $z^2 - ax^2 - by^2 = 0$ has a solution in a given field. We will now show a more computation-friendly representation of Hilbert symbol in the following theorem in terms of the Legendre symbols.

Theorem 4.2 (Hilbert Symbols in terms of Legendre Symbols)**.** *In $\mathbb{Q}_p$ for a given prime p, if we write $a = p^\alpha u$ and $b = p^\beta v$, where u and v are p-adic units, then*

$$(a,b)_p = \begin{cases} (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha & \text{if } p \neq 2 \\ (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} & \text{if } p = 2. \end{cases} \tag{7}$$

where $\epsilon(u) = \frac{u-1}{2}$ and $\omega(u) = \frac{u^2-1}{8}$.

Note that by our definition of Hilbert symbols, if $p = \infty$, $(a,b)_\infty = 1$ if $a > 0$ or $b > 0$; $(a,b)_\infty = -1$ if $a < 0$ and $b < 0$.

Proof. See [2, p.20-22]. □

The Hilbert symbols in $\mathbb{Q}^\times$ satisfy the following properties. (We quote directly from [1, p.54-55]).

Proposition 4.3 (Properties of Hilbert symbols)**.** *Let v be any prime number or ∞. Suppose $a, b \in \mathbb{Q}^\times$. Then we have the following.*

(1) $(a,b)_v = (b,a)_v$
(2) $(a,bc)_v = (a,b)_v(a,c)_v$
(3) $(a,-a)_v = 1$. *If* $a \neq 1$, *then* $(a,1-a)_v = 1$.
(4) If p is an odd prime and $a, b \in \mathbb{Z}_{(p)}^\times$, where

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \text{ is not divisible by } p\},$$

then we have the following,
(a) $(a,b)_p = 1$.
(b) $(a,pb)_p = (\frac{a \pmod p}{p})$.
(5) If $a, b \in \mathbb{Z}_{(2)}^\times$, then
(a)
$$(a,b)_2 = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 4 \text{ or } b \equiv 1 \pmod 4 \\ -1 & \text{if } a \equiv b \equiv -1 \pmod 4. \end{cases}$$
(b) $(a,pb)_p = (\frac{a \pmod p}{p})$.

Proof. The proof is not difficult. The reader may check the properties using Theorem 4.2. □

The following result, Hilbert Reciprocity Law, is a statement that involves the behavior of all $\mathbb{Q}_p$, for all prime p's. It tells us that $\mathbb{Q}_p$'s behave much simpler than we think: only finitely many $\mathbb{Q}_p$'s give different result. It shows how the prime numbers reciprocate with one another with limited irregularity.

Theorem 4.4 (Hilbert Reciprocity Law)**.** *Let $a, b \in \mathbb{Q}^\times$. Then $(a,b)_v$ is equal to 1 except for finitely many v's, and we have*

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

where v runs through all the primes and ∞.

Proof. By (2) of Proposition 4.3, to prove the theorem we only need to consider cases where a or b is prime or -1. By (1) of Proposition 4.3, the order of a and b does not affect the value of $(a,b)_v$. Thus, we only need to prove the theorem for the following four cases:

(1) $a = -1$ and $b = -1$ or 2
(2) $a = 2$ and $b = 2$
(3) a is an odd prime, and $b = -1$ or 2
(4) a and b are both odd primes.

Case 1 By the second half of (3) of Proposition 4.3, $(2,-1)_v = (2,1-2)_v = 1$ for all v. Hence,

$$\prod_v (2,-1)_v = 1.$$

Also, by (5-1) of Proposition 4.3, $(-1,-1)_2 = -1$ and $(-1,-1)_v = 1$ by (4-1) for all odd prime v, and $(-1,-1)_\infty = -1$ because $z^2 + x^2 + y^2 = 0$ has no non-trivial

solution. Hence,

$$\prod_v (-1,-1)_v = 1.$$

Case 2 By (2) of Proposition 4.3,

$$(2,2)_v = (2,-1)_v(2,-2)_v.$$

By (3) of Proposition 4.3, $(2,-2)_v = 1$, and so $(2,2)_v = (2,-1)_v$. Together with the result from **Case 1**, we know that $(2,2)_v = (2,-1)_v = 1$ for all v.

For the following two cases, we quote the results directly from Kato [1,p.56]. The proof involves simple manipulation of Proposition 4.3 and Theorem 4.2.

Case 3

$$(a,-1)_v = \begin{cases} \left(\frac{-1}{a}\right) & \text{if } v = a \\ (-1)^{\frac{a-1}{2}} & \text{if } v = 2 \\ 1 & \text{for other } v. \end{cases}$$

$$(a,2)_v = \begin{cases} \left(\frac{2}{a}\right) & \text{if } v = a \\ (-1)^{\frac{a^2-1}{8}} & \text{if } v = 2 \\ 1 & \text{for other } v. \end{cases}$$

Case 4

$$(a,b)_v = \begin{cases} \left(\frac{b}{a}\right) & \text{if } v = a \\ \left(\frac{a}{b}\right) & \text{if } v = b \\ (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}} & \text{if } v = 2 \\ 1 & \text{for other } v \end{cases}$$

□

The relationship between Hilbert Reciprocity Law and Quadratic Reciprocity Law is even stronger. The two are, in fact, equivalent. We have proven Hilbert Reciprocity Law, assuming Quadratic Reciprocity Law. We shall now show the reverse direction.

Theorem 4.5. *Hilbert Reciprocity Law implies Quadratic Reciprocity Law.*

Proof. The proof involves some quite simple calculations, so we will only show the full proof of the main statement of Quadratic Reciprocity Law. We will mention the ideas of how to prove the first and second supplementary laws.

(1) Recall the main statement of Quadratic Reciprocity Law: if q is an odd prime number other than p, we have

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

We let $a = p$ and $b = q$ in the statement of the Hilbert Reciprocity Law. Then we know

$$\prod_{v \text{ prime}} (p,q)_v = 1.$$

If $v = 2$, then by Theorem 4.2, $p = 2^0 \cdot p$ and $q = 2^0 \cdot q$. Hence, $(p,q)_2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

If $v = p$, then also by Theorem 4.2, $p = p^1 \cdot 1$ and $q = p^0 \cdot q$. Hence, $(p,q)_p = \left(\frac{q}{p}\right)$.

If $v = q$, then similarly $(p,q)_q = \left(\frac{p}{q}\right)$.
If $v \neq 2, p$ or q, then $(p,q)_v = 1$.
Hence,

$$\begin{aligned}\prod_{v \text{ prime}} (p,q)_v &= (p,q)_2 \cdot (p,q)_p \cdot (p,q)_q \cdot \prod_{v \neq 2,p,q} (p,q)_v \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) \cdot 1 \\ &= 1.\end{aligned}$$

By the last two lines,

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

The proof of the first and second supplementary laws is similar. We apply Hilbert Reciprocity Law to $\prod_v (-1,p)_v$ and $\prod_v (2,p)_v$. Then for the first supplementary law, we examine $(-1,p)_v$ for $v = 2$, $v = p$ and all the other v's. For the second supplementary law, we examine $(2,p)_v$ for $v = 2$, $v = p$ and all other primes v. Then we obtain the result.

□

5. Quadratic Forms

This paper discusses homogeneous polynomials of degree 2. Such polynomials are called quadratic forms. For example, $x^2 - y^2$ and $x^2 + 2xy - y^2$ are quadratic forms. The theory of quadratic forms can simplify many degree 2 polynomials to simpler forms. It categorizes quadratic forms to equivalence classes, and provides invariants to each equivalence class. We will see in the proof of Hasse-Minkowski Theorem how this simplification saves us much trouble.

There are few definitions of quadratic forms. The following is the most intuitive and conventional one:

Definition 5.1 (Quadratic form)**.** A quadratic form in n variables over a field k is a function f of the form

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

where $a_{ij} \in k$ for all $i, j \in \{1, \cdots, n\}$, and $a_{ij} = a_{ji}$.

Let (a_{ij}) be a matrix called A. Then A is symmetric and we say that A is the corresponding matrix of the quadratic form f. We call a quadratic form f non-degenerate if $\det(A) \neq 0$. In this definition, we consider f as an element of the polynomial ring.

Another definition of quadratic forms relates to symmetric bilinear forms.

Definition 5.2. Let V be a vector space over a field k, where $\mathrm{char}(k) \neq 2$. A function $Q : V \to k$ is called a quadratic form on V if:
(1) $Q(ax) = a^2 Q(x)$ for $a \in k$ and $x \in V$
(2) The function $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form.

We denote

$$x.y = \frac{1}{2}(Q(x+y) - Q(x) - Q(y))$$

.

Definition 5.2 is equivalent to 5.1. We will omit the formal proof of this fact. The reader may check [8] for the equivalence of several definitions of quadratic forms. We want to introduce Definition 5.2 because we can talk about the dimension of a quadratic form from this fact. Hereafter, we will use the two definitions interchangeably.

Definition 5.3 (Rank of a quadratic form)**.** The rank of a quadratic form is the rank of its corresponding matrix A.

Quadratic forms can be divided into equivalence classes. In fact, we shall soon use this fact to convert all quadratic forms to the simpler ones of the form $f(x_1, \cdots, x_n) = \sum_{i=1}^{n} a_i x_n^2$. It will be an important step in the proof of Hasse-Minkowski Theorem.

Definition 5.4 (Equivalence of two quadratic forms)**.** Suppose f and g are two quadratic forms over n variables. Let A and A' be the corresponding matrices of f and g, respectively. We say that $f \sim g$ if there exists an invertible matrix X such that

$$A' = X \cdot A \cdot X^t$$

From the above definition, we have

$$\det(A') = (\det(X))^2 \det(A)$$

where $\det(X) \in k^*$. Thus, for each equivalence class of quadratic forms, we can associate a coset in $k^*/(k^*)^2$. We call it the determinant of f, $d(f)$ (and also, the determinant of g, $d(g)$). It turns out that the determinant is an invariant of the equivalence class of f, i.e., for all $g \sim f$, $d(g) = d(f)$.

Any quadratic form is equivalent to a much "nicer" quadratic form, a diagonal quadratic form. A diagonal quadratic form is a quadratic form with formula like $f(x_1, \cdots, x_n) = \sum_{i=1}^{n} a_i x_i^2$, where $a_i \in k$. We put it formally into a theorem.

Theorem 5.5. *Every quadratic form is equivalent to a diagonal quadratic form.*

Proof. See Serre's book [2, p.34]. □

The notion of "represents" is essential to this paper. A quadratic form $f : V \to F$ represents $a \in F$ if there exists at least one non-trivial solution $x \in V$ such that $f(x) = a$.

We have mentioned two invariants of an equivalence class of quadratic forms, the rank (we call it $n(f)$) and the determinant, $d(f)$. There is a third one that particularly relates to the p-adic fields, $\mathbb{Q}_p$. For any quadratic form f over $\mathbb{Q}_p$, we take a diagonal quadratic form that f is equivalent to,

$$a_1 x_1^2 + \cdots + a_n x_n^2$$

where $a_j \in \mathbb{Q}_p^\times$. Then we let $c_p(f) = c(f) = \prod_{i<j}^{n} (a_i, a_j)_p$. Note that $(a_i, a_j)_p$ is the Hilbert symbol. We call $c(f)$ the Hasse-Minkowski invariant.

The three invariants, $n(f)$, $d(f)$, and $c(f)$ do not depend on the choice of representatives in the equivalence class of quadratic forms. Furthermore, there is a theorem that shows that these three invariants are sufficient to identify a particular equivalence class.

Theorem 5.6. *Suppose $p \neq \infty$. Then $n(f), d(f), c(f)$ is a complete set of invariants of the equivalence class of f.*

Proof. See [3, p.56-63]. □

The above three invariants are especially helpful in determining if a quadratic form f represents some element in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ for some p-adic field $\mathbb{Q}_p$. Thus, we present the following theorem.

Theorem 5.7. *Let $a \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$. Then f represents a if and only if:*
(1) $n = 1$ and $a = d$,
(2) $n = 2$ and $(a, -d) = \epsilon$,
(3) $n = 3$ and either $a \neq -d$ or $a = -d$ and $(-1, -d)_p = c$.
(4) $n \geq 4$.
Note that n denotes the rank of f, d the determinant, and c the Hasse-Minkowski invariant. The theorem holds not only for the field $\mathbb{Q}_p$, but also any fields if we define their Hilbert symbols.

Proof. See Serre's book [2, p.36-37]. □

We will use the result of Theorem 5.7 in the proof of sum of three squares.

6. Hasse-Minkowski Theorem

Having built the background, we are ready to see the essential theorem in the paper, Hasse-Minkowski Theorem. It is important because it helps convert problems in $\mathbb{Q}$ into problems in $\mathbb{R}$ and $\mathbb{Q}_p$. Such conversion is often called "Local-Global Principle". The principle applies widely to number theory and geometry. Instead of analyzing a quadratic form in $\mathbb{Q}$, the global field, we can analyze it in the local fields, at each $\mathbb{Q}_p$ and $\mathbb{R}$. As we will soon see in the next section - the Application of Hasse-Minkowski Theorem, the conversion from global to local property is helpful because over the local fields, we only need to examine finitely many local fields, $\mathbb{Q}_p$. These local fields are easier to study than $\mathbb{Q}$. The reader may refer to Keith Conrad's notes [5] to understand the philosophy of the local-global principle.

Theorem 6.1 (Hasse-Minkowski Theorem)**.** *Let f be a quadratic form over $\mathbb{Q}$. Then f represents 0 if and only if for all $v \in V$, the form f_v represents 0.*

Proof. Note that by the definition of "represents," this statement simply means: $f = 0$ has a non-trivial solution in $\mathbb{Q}$ if and only if $f = 0$ has a non-trivial solution over all $\mathbb{Q}_p$ and $\mathbb{R}$.

The forward direction is easy. Since $\mathbb{Q} \subset \mathbb{Q}_p$ for all primes p and $p = \infty$, finding a rational solution means finding a solution in all $\mathbb{Q}_p$ and $\mathbb{R}$.

The backwards direction needs quite some work. Let's first simplify the quadratic forms. By Theorem 5.5, all quadratic forms are equivalent to some diagonal quadratic forms. Thus, we only need to consider quadratic forms of the form $f = a_1x_1^2 + \cdots + a_nx_n^2$. As the hypothesis of the theorem, suppose f represents 0 over all $\mathbb{Q}_p$ and $\mathbb{R}$.

(The entire proof consists of four cases, namely $n = 2, 3, 4$ and $n \geq 5$. We will only show the case of $n = 3$ due to time and space constraints. For the entire proof of all numbers of variables, we recommend the reader to check [2,p.41-43] or [3, p.78-85]. They provide two different proofs.)

If n=3, f is of the form $f = z^2 - ax^2 - by^2$, where $a, b, c \in \mathbb{Q}$. (The coefficient in front of z does not affect if f represents 0 or not, so we can just take it as 1.) The proof is divided into a few steps.

Step 1 Arrange f so that a and b are square-free integers (integers that are not squares of some integers).

We want to create a new quadratic form $f' = z^2 - ax^2 - by^2$, where a' and b' are square-free integers, so that f' represents 0 in $\mathbb{Q}$ is equivalent to f represents 0 in $\mathbb{Q}$. First, f represents 0 is equivalent to kf represents 0 for some $k \in \mathbb{Z}$. Thus, we can convert f to some f' with integer coefficients. If any one of the integer coefficients contains a square, we can extract the square-free part of the integer, and incorporate the square part to the integer. More specifically, if $a = a'\alpha^2$ for some a' not a square, and $a', \alpha \in \mathbb{Z}$,

$$ax^2 + by^2 + cz^2 = a'(\alpha x)^2 + by^2 + cz^2.$$

If the quadratic form on the left-hand side represents 0, then so does the right-hand side; vice versa. We can do the same manipulation to all three coefficients, and so eventually, it is sufficient for us to consider $f = z^2 - ax^2 - by^2$ for square-free integers a and b.

Step 2 Apply strong induction to the integer $m = |a| + |b|$. Without loss of generality, assume that $|a| \leq |b|$.

Step 2-1 Let's examine the base case of induction. If $m = 0$, then $0 \cdot x^2 + 0 \cdot y^2 = 1$ has no real solution, so the hypothesis fails. If $m = 1$, then $a = 0, b = 1$. Thus, we have solutions $(x, y, z) = (\pm 1, \pm 1, 0)$.

If $m = 2$, there are three cases corresponding to the following solution:

$$-x^2 - y^2 + z^2 = 0 \text{ has a solution } (x, y, z) = (0, 1, 1)$$

$$-x^2 + y^2 + z^2 = 0 \text{ has a solution } (x, y, z) = (1, 1, 0)$$

$x^2 + y^2 + z^2 = 0$ does not have any solution in $\mathbb{R}$, so the hypothesis fails.

For $m = 1, 2$, or 2, all quadratic forms where the hypothesis holds have rational solutions, so the base case works.

Step 2-2 Suppose the theorem holds for all quadratic formd f up to $m - 1$. We want to show that the theorem holds for a quadratic form f with $|a| + |b| = m$.

Since b is a square free integer, $b = \pm p_1 \cdots p_n$ for distinct prime numbers $p_1, \cdots, p_n$.

Step 2-2-1 We want to show that a is a square modulo b. By Chinese Remainder Theorem, it suffices to show that a is a square modulo p_i for each p_i.

If $a \equiv 0 \pmod{p)_i}$, then a is a square of 0. Since a is an integer, $a \in \mathbb{Z}_p$. Thus, if $a \not\equiv 0 \pmod{p)_i}$, a is a unit in $\mathbb{Z}_p$ (Theorem 2.12). We now introduce the following result without proving it (the reader may refer to [2, p.14] for the proof):

Let $f^{(i)} \in \mathbb{Z}_p[x_1, \cdots, x_n]$ be homogeneous polynomials with p-adic integer coefficients. Then $f^{(i)}$ have a non-trivial common zero in $(\mathbb{Q}_p)^m$ if and only if they have a common primitive zero in $(\mathbb{Z}_p)^m$. (A point $x = (x_1, \cdots, x_m) \in (\mathbb{Z}_p)^m$ is called **primitive** if one of the x_i is a unit.)

By our hypothesis of the theorem, $z^2 - ax^2 - by^2 = 0$ has a solution in $(\mathbb{Q}_{p_i})^3$. Thus, by the above result, it has a primitive solution (x, y, z) in $(\mathbb{Z}_p)^3$, with one of $x, y, z \neq 0$.

Since $p_i \mid b$, $p_i \mid z^2 - ax^2$. If $p_i \mid x$, then $p_i \mid z$, so $p_i^2 \mid by^2$. Hence $p_i \mid y$. But then p_i divides all of x, y, z. This contradicts with the fact that x, y, z are primitive.

Thus, $p_i \nmid x$. Thus, x is invertible in $\mathbb{Z}/p_i\mathbb{Z}$, and so is x^2. Thus, $a \equiv z^2(x^{-1})^2 \pmod{p}_i$, and so a is a square modulo p_i. Hence, a is a square in $\mathbb{Z}/b\mathbb{Z}$.

Step 2-2-2 By the above result, there exists some $t \in \mathbb{Z}$ such that $t^2 = a + bb'$ for some $b' \in \mathbb{Z}$. Since a is the square of t in $\mathbb{Z}/b\mathbb{Z}$, $t \in \mathbb{Z}/b\mathbb{Z}$. Thus, $|t| \leq \frac{|b|}{2}$.

If $b' = 0$, then $a = t^2$, so $a(\frac{1}{t})^2 + b \cdot 0^2 = z^2$. There exists a solution in $\mathbb{Q}$.

If $b' \neq 0$, then

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

The last step is because $m > 2$ and $|a| \leq |b|$, so $|b| \geq 2$.

Step 3 $ax^2+by^2 = z^2$ has non-trivial rational solutions if and only if $ax^2+b'y^2 = z^2$ has non-trivial rational solutions.

This is due to the fact that we can find a bijection between the set of rational solutions of $ax^2 + by^2 = z^2$ and that of $ax^2 + b'y^2 = z^2$. One may refer to Kato's book [1,77] to see such bijection.

Step 4 By the result of **Step 3**, we only need to consider $ax^2 + b'y^2 = z^2$. If $|a| < |b|$, since we assumed by the induction hypothesis that the theorem holds for smaller m, $ax^2 + b'y^2 = z^2$ has rational solutions. Thus, $ax^2 + by^2 = z^2$ also has rational solutions.

If $|a| = |b|$, then $|b'| < |a|$. This case is also of the form "$|a| < |b|$". Thus, the theorem holds again. □

We extend Hasse-Minkowski to f represents a for some $a \in \mathbb{Q}$ that might not be 0.

Corollary 6.2. *Let $a \in \mathbb{Q}^\times$. Then f represents a in $\mathbb{Q}$ if and only if it does so in all $\mathbb{Q}_p$ and $\mathbb{R}$.*

Proof. We can apply Hasse-Minkowski Theorem to the quadratic form $az^2 - f$ and obtain the result. □

7. The Applications of Hasse-Minkowski Theorem

In this section, we will present and prove the motivating problem mentioned at the beginning of the paper. "What integers are the sums of three/four squares?" Having built the definitions of quadratic forms, we can state the question in terms of quadratic forms, "Which integer n can be represented by the quadratic form, $x^2 + y^2 + z^2$, for $x, y, z \in \mathbb{Z}$?"

Tentatively, we want to apply Hasse-Minkowski Theorem, so that as long as we find some n that can be represented by $x^2 + y^2 + z^2$ over all $\mathbb{Q}_p$ and $\mathbb{R}$, then n can be represented over the integers. But Hasse-Minkowski can only tell us that n is represented over the rationals. Thus, we shall show a theorem about finding integer solutions to quadratic forms given the rational solutions.

Theorem 7.1 (Davenport-Cassels)**.** *Suppose a quadratic form $f(x_1, \cdots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ satisfies the following conditions:*

(1) The range of f is positive.

(2) a_{ij}'s are integers and the corresponding matrix is symmetric.

(3) For any $x = (x_1, \cdots, x_n) \in \mathbb{Q}_p$, there exists some $y \in \mathbb{Z}_p$ such that $f(x-y) < 1$.

Then if f represents n in $\mathbb{Q}_p$, f represents n in $\mathbb{Z}_p$.

Proof. Assume that $f = n$ has rational solutions. Take $t > 0$ to be the smallest integer such that $f = t^2 n$ has integer solution $x \in \mathbb{Z}_p$. Since we want to show that f itself has integer solutions, we hope to show that $t = 1$.

By property of the quadratic forms, since $f(x) = t^2 n$, $f(\frac{x}{t}) = n$. Thus, $\frac{x}{t}$ is a rational solution to $f = n$. By condition (3), there exists $y \in \mathbb{Z}_p$ such that $f(\frac{x}{t} - y) < 1$. Let $z = \frac{x}{t} - y$.

There are two possibilities of z. If $z = 0$, then $\frac{x}{t} = y$ is an integer. Thus, we have found the integer solution $\frac{x}{t}$ to $f = n$. Hence, $t = 1$.

If $z \neq 0$, we shall yield a contradiction. We will omit the technical detail of the proof, but the idea is that we can find some $x' \in \mathbb{Z}_p$ such that $f(x') = t'^2 n$ for some $0 < t' < t$. This contradicts our assumption that t is the minimal integer. One may refer to Serre's book [2, p.46] for how to design such x' and t'. □

Hence, we have shown from the above theorem that for some quadratic forms with certain properties, having a rational solution is equivalent to having an integer solution. We are now ready to present the most important applications of Hasse-Minkowski Theorem.

Theorem 7.2 (Gauss sum of three squares)**.** *An integer n is the sum of three squares of integers if and only if $n > 0$ and n is not of the form $4^a(8b + 7)$, with $a, b \in \mathbb{Z}$.*

Proof. Let f be the quadratic form $x^2 + y^2 + z^2$. The statement of the theorem is equivalent to finding integer solutions to $f = n$ for some integers n. We want to apply Theorem 7.1 to the problem, so that as long as there is some rational solution, there is integer solutions to $f = n$. Indeed, f satisfies the three conditions listed in Theorem 7.1. The range of f is positive and the matrix is symmetric. If we have some $(x, y, z) \in \mathbb{Q}^3$ with $f(x, y, z) = n$, we let x', y', z' to be the closest integers to x, y, z respectively. Hence, $|x - x'| \leq \frac{1}{2}$, $|y - y'| \leq \frac{1}{2}$, and $|z - z'| \leq \frac{1}{2}$. Thus, $|f(x', y', z') - f(x, y, z)| \leq \frac{3}{4} < 1$.

To determine if $x^2 + y^2 + z^2$ represents n for some $n \in \mathbb{Q}$, we can appeal to Hasse-Minkowski Theorem. For the quadratic form to represent n in $\mathbb{R}$, we must have $n \geq 0$, since $x^2, y^2, z^2 \geq 0$ for all $x, y, z \in R$. Since we are not looking for the trivial solution, $n > 0$.

Since we are considering quadratic forms of three variables, we shall apply the third case of Theorem 5.7. The determinant of $f = x^2 + y^2 + z^2$ is $d(f) = 1$. By definition of the invariant c_p, $c_p(f) = \prod_{i<j}^{n} (1, 1)_p = 1$ for all p. Hence, for f to represent n, we will need that either $a \neq -1$ or $a = -1$ and $(-1, -1)_p = 1$. Note that for n to be 1 in $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$, it means that n needs to be a square in $\mathbb{Q}_p$.

If $p \neq 2$, $(-1, -1)_p = 1$. Also, n is not a square in $\mathbb{Q}_p$. Thus, f represents n for all positive n.

If $p = 2$, $(-1, -1)_2 = -1$. Thus, we have to have $a \neq -1 \in \mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2}$. Thus, $-n$ cannot be a square in $\mathbb{Q}_2$. We quote the following result to complete the proof. (The reader may refer to [2,p.18] for the proof of this result.)

For an element $x = p^n u$ of $\mathbb{Q}_2^\times$ to be a square, it is necessary and sufficient that n is even and $u \equiv 1 \pmod 8$.

Thus, $-n$ is not a square if and only if $n \neq 4^a(8b - 1)$ for some $a, b \in \mathbb{Z}$. □

Theorem 7.3 (Lagrange sum of four squares)**.** *Every positive integer is the sum of four squares.*

Proof. For any positive integer n, if n is not of the form $4^a(8b-1)$, then n is the sum of three squares. If we take the fourth variable to be 0, we will find a representation of n in terms of four squares.

If $n = 4^a(8b-1)$ for some $a, b \in \mathbb{Z}$, then $n-1$ is not of the form $4^a(8b-1)$. Hence, n can be represented by the three squares of $n-1$ and the square of 1. □

Acknowledgements

Many people have contributed to me writing this paper, and due to space limitation, I can only mention a few. I would like to first thank my mentor Karl Schaefer for taking time to meet consistently and reviewing my paper carefully during the eight-week REU program at the University of Chicago. I am also thankful to Tung Tho Nguyen, who introduced me to the study of p-adic number through the Directed Reading Program at the University of Chicago and who also helped revise my paper. I am grateful to my family and friends for their constant support to my academic pursuit, and Professor Mark Reeder for leading me to major in mathematics and supporting me both in academics and in life. I also want to thank Akhil Mathew's lectures on number theory during the REU program at UChicago. Lastly, I want to thank Professor Peter May for his insistent effort to run the REU program. It has been a very informative experience.

References

[1] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito. Number Theory 1: Fermat's Dream (Translations of Mathematical Monographs Vol 1). American Mathematical Society. 2000.
[2] Jean-Pierre Serre. A Course in Arithmetic. Springer. 1973.
[3] J.W.S. Cassels. Rational Quadratic Forms. Academic Press. 1978.
[4] Neal Koblitz. p-adic Numbers, p-adic Analysis, and Zeta-Functions (Graduate Texts in Mathematics 58. Springer. 1984.
[5] Keith Conrad. Local-Global Principle. https://kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf
[6] Richard Shadrach. 2014 Fall - Math 365 - p-adic numbers. https://math.rice.edu/ rs53/Math365Fa14/Hasse-Minkowski.pdf
[7] Adam Gamzon. "The Hasse-Minkowski Theorem" (2006). Honors Scholar Theses. 17.
[8] http://www.math.miami.edu/ armstrong/685fa12/pete_clark.pdf