Two Applications of the Hasse-Minkowski Theorem

An Elementary Introduction

Shuhang Xue and Horace Fusco

Alex Barrios
Elementary Theory of Numbers
Carleton College
6/07/20

Abstract

We wish to use the Hasse-Minkowski Theorem to prove two results in elementary number theory, Fermat's Two Square Theorem and Lagrange's Four Squares Theorem. The proof of Fermat's Sum of Two Squares Theorem will be covered in detail, while the proof of the four squares Theorem will be roughly sketched at the end of this paper. The aim of this paper is to give undergraduate readers a taste of how to use the Hasse-Minkowski Theorem to find solutions to quadratic forms. We demonstrate that using this theorem, one can break down the complicated problem of solving a quadratic form into two simpler ones: finding a solution in $\mathbb{R}$ and a solution over a small number of p-adic fields.

To make this material accessible, we firstly introduce the necessary languages to phrase the powerful Hasse-Minkowski Theorem in the first two sections. Those definitions including: quadratic form, compatible system of congruences, compatible family of solutions, and p-adic numbers. To motivate our readers, we prove the equivalence of solving rational solutions for two-variable equation and integer solutions for a three-variable quadratic form.

After making our audience familiar with the necessary language, we gently introduce the Hasse-Minkowski Theorem in three versions. The reason behind providing different versions of the Hasse-Minkowski Theorem is to firstly give readers a intuitive interpretation, and then dive into the modern language of this powerful theorem in algebraic number theory. Finally, in the rest of our paper, we will rely on the third version, finding solutions in certain p-adic fields, such that $p = 2$.

We further simplify the relatively complicated problem of finding solutions in every p-adic field, into finding one congruence for $p = 2$ and each prime p diving n in $q(X, Y, Z) = X^2 + Y^2 - nZ^2$. To make readers understand this simplification, in the fourth section, we discussed polynomial congruences and present a method to generate a compatible system of solutions.

Then, we move on to the proof of Fermat's Sum of Two Squares Theorem. By lemma 3.1, we reduce n to be square-free and odd. Moreover, we prove two important lemmas to tackle Fermat's puzzle into two different cases: $p = 2$ and p is prime dividing n. First, we prove the Sum of Squares Theorem with rational solutions. Finally, we showed that the rational solutions imply integer solutions to complete the proof.

In the last section, we roughly sketched the proof of Lagrange's Theorem on the sum of four squares. Similar to the thought process of proving Sum of Two Square Theorems, we firstly guarantee the existence of solution over $\mathbb{Q}_2$ for all $n \in \mathbb{N}$. Then, we simplify the proof of Sum of Lagrange's Four Squares Theorem into showing the existence of solution over $\mathbb{Q}_p$, where p is prime dividing n, for all $n \in \mathbb{N}$.

1 The Power of Hasse-Minkowski

The Hasse-Minkowski Theorem describes the circumstances where a quadratic form is guaranteed to have integer solutions.

Definition 1.1. *A quadratic form is a homogeneous polynomial,* $Q(X_1, ..., X_n)$ *of degree 2 with* $n \geq 2$ *variables.* $Q(X_1, ..., X_n) = a_{1,1}{X_1}^2 + a_{1,2}X_1X_2 + ... + a_{n,n}{X_n}^2$ *with* $a_{1,1}, a_{1,2}, ..., a_{n,n} \in \mathbb{Z}$

To make full use of this incredibly powerful theorem, we need to be able to apply it in situations that don't explicitly contain a quadratic form. The following two theorems, which will be the focus of this paper, are applications where a quadratic form can be constructed in order to use the Hasse-Minkowski theorem after a little bit of manipulation.

Theorem 1.1 (Fermat's sum of sq)**.** *An odd prime,* p *is the sum of two integer squares if and only if* $p \equiv 1 \pmod 4$.

Theorem 1.2 (Lagrange's four sq)**.** *For every* $x \in \mathbb{N}$*,* x *can be expressed as the sum of four squares.* $x = a^2 + b^2 + c^2 + d^2$ *for some* $a, b, c, d \in \mathbb{Z}$.

The barrier to applying the Hasse-Minkowski theorem directly to either of these two theorems is that although they both involve quadratic equations, Hasse-Minkowski is concerned with quadratic forms. So, we must understand the connection between quadratic forms and quadratic equations in order to use the heavy weapon at our disposal.

The way we will make use of the relationship between quadratic forms and quadratic equations is by constructing a quadratic form in terms of a given quadratic equation. Let f be a quadratic equation with integer coefficients, define quadratic form Q as follows.

$$f(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$$

$$Q(X, Y, Z) = Z^2 f(\tfrac{X}{Z}, \tfrac{Y}{Z}) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2$$

We need a few definitions about the solutions of Q. We say an integral solution , $Q(b_1, b_2, ..., b_n) = 0$ with $b_1, b_2, ..., b_n \in \mathbb{Z}$ is *non trivial* if there is some $b_n \neq 0$, and we say it is a *primitive solution* if $\gcd(b_1, b_2, ..., b_n) = 1$. We will remark that any non trivial integral solution implies a primitive solution, as we encourage the reader to verify.

Now we get to the crux of the relationship between f and Q. There is a bijection between primitive integral solutions of Q, (x, y, z) with $z \neq 0$ and rational solutions of f.

$$Q(x, y, z) = 0 \to f(\tfrac{x}{z}, \tfrac{y}{z}) = 0$$

$$f(\tfrac{a}{b}, \tfrac{c}{d}) = 0 \to Q(\tfrac{an}{b}, \tfrac{cn}{d}, n) = 0$$

with $n = \operatorname{lcm}(b, d)$.

Plugging in and solving will verify these relationships. We note here that we have established a bijection between integral solutions of a quadratic form and rational solutions of a quadratic equation, so even though the Hasse Minkowski theorem might guarantee integer solutions to the quadratic form, if we are concerned with integer solutions to a quadratic equation, we must still show later that the existence of rational solutions to a quadratic equation implies the existence of integer solutions.

Now that we have a bijection between solutions of a quadratic equation and a quadratic form, we state an instrumental fact.

Lemma 1.3. *Considering a quadratic function, f with integer coefficients.* $f(x,y) = ax^2 + bxy + cy^2 + dx + ey + f$

And a quadratic form

$Q(X,Y,Z) = Z^2 f(\frac{X}{Z}, \frac{Y}{Z})$

Provided $b^2 - 4ac$ is not a rational square, the following two statements are equivalent.

- *Q has a non trivial integral solution.*
- *f has a rational solution.*

Proof. What we are really trying to show here is that a solution (u,v,w) to Q will have $w \neq 0$, because this is what will allow our bijection to work. We will show that if $b^2 - 4ac$ is not a square, then every integral solution (u,v,w) of Q will have $w \neq 0$. Towards a contradiction, suppose (u,v,w) is a solution of Q with $w = 0$.

$$0 = Q(u,v,0) = au^2 + buv + cv^2$$

We know $b^2 - 4ac$ is not a square so a and c are non-zero. Then $au^2 + buv + cv^2 = 0$ implies:

$u = \frac{-bv \pm \sqrt{b^2v^2 - 4acv^2}}{2a} = (\frac{-b \pm \sqrt{b^2 - 4ac}}{2a})v$

So it follows that $\pm\sqrt{b^2 - 4ac} = 2au/v + b$, thus $b^2 - 4ac = (2au/v + b)^2$, a rational square, contradicting our assumption. Therefore if (u,v,w) is a an integral solution of Q, then $w \neq 0$. ■

Note that we have let f be a quadratic equation in two variables, but the bijection we have established can be generalized for more variables, as we will need it to in order to apply it to Lagrange's four squares theorem. We will also have to show that any solution (x,y,z,w,a) to $L(X,Y,Z,W,A) = X^2 + Y^2 + Z^2 + W^2 - nA^2 = 0$ has $a \neq 0$ in order for $(\frac{x}{a}, \frac{y}{a}, \frac{z}{a}, \frac{w}{a})$ to be a solution to $f(x,y,z,w) = x^2 + y^2 + z^2 + w^2 - n = 0$. But this is not hard to show at all because a sum of squares will always be positive, so any solution clearly will not have $a = 0$. The same argument can be applied for the solutions to the quadratic form relevant to the two square theorem. We have presented general information to show how the Hasse-Minkowski theorem might be applied in other scenarios, but for our purposes or our purposes 1.3 is overkill.

2 The Hasse-Minkowski Theorem

Before diving into the statement of Hasse Minkowski Theorem, let's introduce the necessary languages pertaining to the theorem: a compatible system of congruences, a compatible family of solutions, and p-Adic numbers.

2.1 A Compatible System of Congruences

Definition 2.1. *Let $\{m_k\}_{k\geq 1}$ be a sequence of positive integers. We say that $S = \{a_k \mod m_k\}_{k\geq 1}$ forms a compatible (or coherent) family of congruence classes if the following condition is satisfied: if $gcd(m_j, m_k) = d$, then $a_k \equiv aj \mod d$. Equivalently, S is compatible if every system of finitely many linear congruences in S has an integer solution.*

The best way to interpret this language, is to think about the solution given by *the Chinese Remainder Theorem*. Firstly, let's consider an example of a compatible system of congruences.

Example 2.1. *Let $a_1, a_2, ..., a_r \in \mathbb{N}$ be pairwise relatively prime, and let $k_1, k_2, ..., k_r \in \mathbb{Z}$. Then, the following is a compatible system of congruences.*

$$\begin{cases} k_1 \equiv r \pmod{a_1}, \\ k_2 \equiv r \pmod{a_2}, \\ \vdots \\ k_r \equiv r \pmod{a_r}. \end{cases} \tag{1}$$

Moreover, the solution to this system is $s \equiv s_0 \pmod{m}$, where $m = a_1 \cdot a_2 \cdot ... a_r$.

With the knowledge of the general version of *the Chinese Remainder Theorem*, we know that there is nothing special about relatively primes. From the constructive proof of *the Chinese Remainder Theorem*, whether there is a compatible system of congruences (a solution to the congruences class) depends on whether Diophantine equations have solutions.

Example 2.2. *Consider the set of congruence classes*

$$S = \{2 \mod 3, 3 \mod 5, 4 \mod 7, 8 \mod 15, 18 \mod 35\}$$

S is a compatible system of congruence, since it satisfies the following condition:

If $gcd(m, s) = d$, a mod n and b mod m, then $a \equiv b \mod d$.

2.2 A Compatible Family of Solutions

Definition 2.2. *Let q be a quadratic form in n variables. A sequence of solutions $\{a_{1,m}, ..., a_{n,m} \pmod m\}_{m\geq 1}$ of $q \equiv 0 \mod m$, for each $m \geq 1$, forms a compatible family of solutions if each coordinate forms a compatible system of congruences; i.e. $\{a_{i,m} \mod m\}_{k\geq 1}$ forms a compatible family of congruences,*

for each i = 1,...,n.
Note that $a_{i,j}$ means the i-th coordinate in the j-th modulus.

We say that a compatible family of solutions is non-trivial if there is some $m \geq 2$ such that the solution $(a_{1,m}, ..., a_{n,m}) \mod m$ is not congruent to $(0, ..., 0) \mod m$.

To better understand this notion, it would be helpful to consider a numerical example.

Example 2.3. *$X^2 + Y^2 \equiv 3Z^2 \mod m$ has no non-trivial compatible system of solutions.*

Consider the cases of $m = 2$ and $m = 4$. When $m = 2$, the only non-trivial solutions of $Q(X, Y, Z) = X^2 + Y^2 - 3Z^2 = 0$ are $(1, 1, 0), (1, 0, 1)$, and$(0, 1, 1)$. When $m = 4$, the only non-trivial solutions of $Q = 0$ are $(2, 0, 0), (0, 2, 0), (2, 0, 2)$, and$(0, 2, 2)$. Then, for the non-trivial (nonzero) coordinate, we get a congruence class $\{1 \pmod 2, 2 \pmod 4\}$. Because 1 is not congruent to 2 modulo $2 = gcd(2, 4)$, then this is not a compatible system of congruences. Thus, there is no compatible solutions for $X^2 + Y^2 \equiv 3Z^2 \mod m$.

2.3 The First Version of Hasse-Minkowski Theorem

Equipped with all necessary languages, we can finally present the Hasse-Minkowski Theorem, which was originally proved by Hermann Minkowski and generalized by Helmut Hasse. Also known as local-global principle, this theorem has profound influence in algebraic number theory, since it breaks down the complicated problem of checking whether a quadratic form over real number, into checking the existence of solutions in smaller fields (specifically p-Adic fields, which I am going to define later in this section). This bridge turns out to be crucial to prove many famous results, including the one we are going to show is this paper — *Fermat's Sum of Square Theorem.*

Theorem 2.1. *(Hasse-Minkowski Theorem). Let $q(X_1, ..., X_n)$ be a regular quadratic form defined over $\mathbb{Q}$. Then, $q = 0$ has a non-trivial integral solution (i.e., not all coordinates are zero) if and only if there is a non-trivial solution over $\mathbb{R}$and the congruences $q \equiv 0 \mod m$, for all $m > 1$, have a non-trivial compatible system of solutions.*

Here is a example for readers to have a quick taste of the power of Hasse-Minkowski Theroem in solving the real solutions of quadratic equations.

Example 2.4. *Let n be a natural number. By the Hasse-Minkowski Theorem, $X^2 + Y^2 = nZ^2$ has a nontrivial integral solution if and only if $X^2 + Y^2 = nZ^2$ has a non-trivial solution over $\mathbb{R}$(which turns out to be very easy to show) and the congruences $X^2 + Y^2 \equiv 3Z^2 \mod m$, for all $m > 1$ have a non-trivial compatible system of congruences.*

This example indeed is the equivalent form of Fermat's Last Theorem in quadratic form with three variables. Thus, over goal right now is to show the existence of a non-trivial compatible system of congruences for all m¿1. However, this result is quiet hard to show directly. Let's go ahead and introduce the version Hasse-Minkowski Theorem in the language of p-Adic numbers.

2.4 Hasse-Minkowski Theorem Stated in The Language of P-Adic Numbers

Before introducing the Hasse Minkowski Theorem in the language of p-adic number, we first state another equivalent version of this theorem about modulo prime p to all $k > 1$ orders.

Theorem 2.2. *(Hasse-Minkowski Theorem, prime version). Let $q(X_1, ..., X_n)$ be a regular quadratic form defined over $\mathbb{Q}$. Then, $q = 0$ has a non-trivial integral solution if and only if there is a non-trivial solution over $\mathbb{R}$ and, for each prime $p > 1$,there is a non-trivial compatible system of solutions of $q \equiv 0 \mod p^k$, for all $k \geq 1$; i.e., $\{x_{i,p^k} \mod p^k\}_{k\geq 1}$ forms a compatible family of congruences, for each i = 1,...,n, with every fixed odd prime p.*

Essentially, with this definition, we can further breaking down the relatively hard question of a large compatible system of solutions to several compatible system of solutions with all odd primes. To systematically phrase this version of Hasse Minkowski Theorem, the notion of p-adic numbers is naturally tied in to the conversation.

We can simply understand a p-adic as a set of compatible system of congruences modulo p^k, for all $k \geq 1$. Let's formally introduce the definition of p-adic numbers.

Definition 2.3. *The p-adic integers, denoted by $\mathbb{Z}_p$, are defined as follows:*

$$\mathbb{Z}_p = \{(a_1.a_2, ...) : a_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ such that } a_{n+1} \equiv a_n \mod p^n\}.$$

To understand this abstract definition, let's consider the number 200 as a 3-adic number. More generally, any number a $\in \mathbb{N}$ is contained in a p-adic ring.

Example 2.5. *The number 200 in $\mathbb{Z}_3$ is given by*

$$200 = (2, 2, 11, 38, 200, 200, 200, 200, 200, ...).$$

Note that all the congruences after mod 2^5 becomes 200, since $200 < p^k$, for $k \geq 5$; and this system is compatible since, $m \equiv m \mod p^k$, for all $k \geq 1$.

After understanding the definition of p-adic numbers, observe that in the prime version of Hasse Minkowski Theorem, every compatible system of congruences is indeed a p-adic number.

Theorem 2.3. *(Hasse-Minkowski Theorem,* p*-adic version). Let $q(X_1, ..., X_n)$ be a regular qua-dratic form defined over $\mathbb{Q}$. Then, $q = 0$ has a non-trivial integral solution if and only if there is a non-trivial solution over $\mathbb{R}$ and over $\mathbb{Q}_p$ for each prime p.*

Note that $\mathbb{Q}_p$ means the p-adic field, such that $\mathbb{Z}$ sits inside $\mathbb{Q}_p$ by Example 2.4. Under the language of p-adic number, the statement of Hasse Minkowski Theorem is very concise. Coming back to our goal of proving Fermat's Sum of Squares Theorem, we can then translate the problem into finding non-trivial solutions in each $\mathbb{Q}_p$.

Example 2.6. *Let n be a natural number. By the Theorem 2.3, $X^2+Y^2 = nZ^2$ has a nontrivial integral solution if and only if $X^2+Y^2 = nZ^2$ has a non-trivial solution over $\mathbb{R}$ and over $\mathbb{Q}_p$, for each prime p.*

Indeed, we can further narrow down p into 2 and all the odd primes that divides n. Thus we only have finitely many primes to consider.

Example 2.7. *Let n be a natural number. By the Theorem 2.3, $X^2+Y^2 = nZ^2$ has a nontrivial integral solution if and only if $X^2+Y^2 = nZ^2$ has a non-trivial solution over $\mathbb{R}$ and over $\mathbb{Q}_p$, for $p = 2$ and each prime p dividing n.*

This last version of Hasse-Minkowski Theorem is exactly what I will use to prove Fermat's Sum of Squares Theorem. By only considering 2-adic and p-adic fields such that p divides n, the puzzle left by Fermat can be finally solved.

3 Solving The Solution Over $\mathbb{Q}_p$

3.1 Reducing n

Aiming to add a few constraints to n, we are looking at the most representative value of n. Reducing n to odd and square-free case gives us more conditions to work with the proof of the Sum of Squares Theorem.

Lemma 3.1. *Let $n > 1$. The following statements are equivalent:*

i The number n is a sum of two (rational) squares.

ii The number $2^k n$ is a sum of two (rational) squares, for every $k \geq 1$.

iii The number nt^2 is a sum of two (rational) squares, for any $t \in \mathbb{Z}$.

Proof. (1) Show i and ii are equivalent. ($\Longrightarrow$) By induction, let S(k) be for $k \in \mathbb{N}$, $2^k n$ is a sum of squares. Assume that n is a sum of two squares, let $n = a^2 + b^2$, where $a, b \in \mathbb{N}$. Claim that S(1) holds true. Since $2n = 2(a^2 + b^2) = (a + b)^2 + (a - b)^2$, 2n is a sum of squares. Suppose that s(k-1) is true. Then, relabel a, b if necessary, $2^{k-1} = a^2 + b^2$. By the same token, $2^k = 2(a^2 + b^2) = (a + b)^2 + (a - b)^2$, which suggests that S(k) holds true. ($\Longleftarrow$) By induction, similar to the if direction, assume that $2n = a^2 + b^2$. Then,

$n = (a^2 + b^2)/2 = [(a+b)/2]^2 + [(a-b)/2]^2$, which shows that 2n/2 is a sum of squares. Therefore, i and ii are equivalent.
(2) Show i and iii are equivalent. ($\Longrightarrow$) Suppose $n = a^2 + b^2$, then $nt^2 = a^2t^2 + b^2t^2 = at^2 + bt^2$, which implies that nt^2 is a sum of squares.
($\Longleftarrow$) Assume $nt^2 = a^2 + b^2$, then divide both sides by t^2. Then, $n = \frac{a^2}{t^2} + \frac{a^2}{t^2} = (\frac{a}{t})^2 + (\frac{b}{t})^2$. Therefore, nt^2 being a sum of squares implies that n is a sum of squares.
In conclusion, i, ii, and iii are equivalent. ■

The lemma 3.1 provides a powerful tool for us to reduce n to be odd and square-free. All of collections of integers that can be written as a sum squares can be derived from a smaller subset that only contains odd and square-free numbers. Later on, readers will see the crucial role of those two conditions.

3.2 Solving The Solution Over $\mathbb{Q}_p$

In the second section, we finally simplify the puzzle of proving Fermat's Sum of Squares Theorem into solving p-adic numbers over $\mathbb{Q}_p$ for $p = 2$ and each prime p diving n. In this section, I will present a powerful Lemma that can further breaking down systems of compatible solutions into solving individual congruence.
The following Lemma is introduced here to motivate the proof, but will be proved in details relied on the investigation of polynomial congruences, specifically whether there is an integer solution to $f(x) \equiv 0 \mod p^k$, decided by $f'(x)$ and the divisibility of $f(x)$

Lemma 3.2. *Let c be an integer not divisible by a prime p. Then:*

(1) The quadratic form $q = x^2 - c = 0$ has solution over $\mathbb{Q}_2$ if and only if $c \equiv 1 \mod 8$.

(2) The quadratic form $q = x^2 - c = 0$ has solution over $\mathbb{Q}_p$, where $p > 2$, if and only if $x^2 \equiv c \mod p$ has a solution.

With the help of Lemma 3.2, instead of solving every congruence and then prove this system is compatible, we can simply prove two congruence: (1) $c \equiv 1 \mod 8$, and (2) $x^2 \equiv c \mod p$. So far, we have all the languages and Lemma that are necessary to prove When Fermat's Sum of Square Theorem has rational solutions.

4 Polynomial Congruences

To prove lemma 3.2 we will take a brief detour into the world of polynomial congruence. We will give a general way of building up a compatible system of solutions to a polynomial in $\mathbb{Z}/p^k\mathbb{Z}$ for $k \geq 1$. Note that this is equivalent to finding a solution to the polynomial over $\mathbb{Q}_p$.

We begin with a general statement about polynomial congruences

Lemma 4.1. *For a prime p and an polynomial $f(x)$ with integer coefficients, we have the following congruence for any integer t.*

$$f(x+p^k t) \equiv f(x) + f'(x)p^k t \pmod{p^{k+1}\mathbb{Z}[x]}$$

Which is to say, there exists a polynomial $h(x)$ such that $(f(x+p^k t)-(f(x)+f'(x)p^k t)$ is divisible by $p^{k+1}h(x)$ for all t.

Proof. We will proceed by induction on the degree of f. If the degree of f is 0 then f is a constant function, and the result holds. Now we will assume the result is true for polynomials of degree n and show that it must be true for polynomials of degree $n+1$. Let $f(x)$ be a polynomial of degree $n+1$. For some integer a we can write $f(x) = a + xg(x)$ for a polynomial g of degree n. Using the product rule we have $f'(x) = g(x)+xg'(x)$. We know the lemma is true for g so we will simply perform algebraic manipulations to produce the desired result.

$$\begin{aligned}
&f(x+p^k t) \equiv a + (x+p^k t)g(x+p^k t) \equiv a + (x+p^k t)(g(x) + g'(x)p^k t) \\
&\equiv a + xg(x) + (xg'(x) + g(x))p^k t + g'(x)t^2 p^{2k} \\
&\equiv a + xg(x) + (xg'(x) + g(x))p^k t \\
&\equiv f(x) + f'(x)p^k t \pmod{p^{k+1}\mathbb{Z}[x]}
\end{aligned}$$

By the principle of mathematical induction, this result is true for polynomials of all degrees. ■

Now we have the tool we need to consider when and how we can construct a p-adic solution to a polynomial. There are general results on this topic that are readily accessible, but here we will limit ourselves to what is useful in proving Lemma 3.2.

Lemma 4.2. *If there exists a solution s_k to $f(x) \equiv 0 \pmod{p^k}$, and $f'(s_k)$ is not divisible by p, then there is a solution s_{k+1} to $f(x) \equiv 0 \pmod{p^{k+1}}$ with $s_{k+1} \equiv s_k \pmod{p^k}$ given by:*

$$s_{k+1} \equiv s_k - f(s_k)(f'(s_k))^{-1} \pmod{p^{k+1}}$$

Where $(f'(s_k))^{-1}$ is the multiplicative inverse of $f'(s_k)$ in $\mathbb{Z}/p^{k+1}\mathbb{Z}$, which we know exists because $f'(s_k)$ and p are relatively prime by assumption.

Proof. Because $s_{k+1} \equiv s_k \pmod{p^k}$, we have $s_{k+1} = s_k + p^k t$ for some integer t. By 4.1 we have $f(s_{k+1}) \equiv f(s_k + p^k t) \equiv f(s_k) + f'(s_k)p^k t \pmod{p^{k+1}}$. We want s_k and s_{k+1} to be solutions, so $f(s_k) \equiv 0 \pmod{p^k}$ and $f(s_{k+1}) \equiv 0 \pmod{p^{k+1}}$, so by the former equivalence we know $\frac{f(s_k)}{p^k}$ is an integer, and by the latter we know $f(s_k) + f'(s_k)p^k t \equiv 0 \pmod{p^{k+1}}$. Rearranging, we have $f'(s_k)t \equiv \frac{-f(s_k)}{p^k} \pmod{p}$. And because we know $p \nmid f'(s_k)$, there must be a unique solution for t, specifically, $t \equiv \frac{-(f'(s_k))^{-1}f(s_k)}{p^k} \pmod{p}$. Giving us:
$s_{k+1} \equiv s_k + p^k t \equiv s_k - f(s_k)(f'(s_k))^{-1} \pmod{p^{k+1}}$

■

This allows us to recursively generate a p-adic solution to $f(x)$ provided there is a solution to $f(x) \equiv 0 \pmod{p}$ (as we can then generate compatible solutions $\pmod{p^2}$, $\pmod{p^3}$ and so on). But there is a catch: p cannot be 2. In our proof of 4.2, we relied on the assumption that $p \nmid f'(s_k)$, and in our consideration of the quadratic equations $f(x) = x^2 - c$, we have $f'(s_k) = 2s_k$. If $p > 2$ non trivial solutions will definitionally be relatively prime to p, but as we can see, if $p = 2$ we have a problem, so we will consider the 2-adic case separately.

Lemma 4.3. *There is a 2-adic solution to $x^2 = c$ if and only if $c \equiv 1 \pmod{8}$.*

Proof. We must have $c \equiv 1 \pmod{2}$, and the squares of all odd numbers $(2n+1)^2 \equiv 4n(n+1) + 1 \equiv 1 \pmod{8}$, so if $c \not\equiv 1 \pmod{8}$, there can be no 2-adic solution to $x^2 = c$. Now we assume $c \equiv 1 \pmod{8}$. Of the residues in $\mathbb{Z}/2^k\mathbb{Z}$, there are 2^{k-3} multiples of 8, so there are 2^{k-3} residues $\equiv 1 \pmod{8}$. Because all odd squares are $\equiv 1 \pmod{8}$, it is sufficient to show that there exist 2^{k-3} squares of odd numbers that are distinct modulo 2^k to show that there is a solution to $x^2 \equiv c \pmod{2^k}$.
To achieve a contradiction, we will consider the set S containing the first 2^{k-3} odd numbers (which are all less than 2^{k-2}). Suppose $a, b \in S$ with $a^2 \equiv b^2 \pmod{2^k}$ and $a > b$. We have $2^k \mid (a-b)(a+b)$. Since a and b are odd, either $(a-b)$ or $(a+b)$ is $\equiv 2 \pmod{4}$. Thus, one is divisible by two and not four, making the other divisible by 2^{k-1}. but we have $1 \leq b < a \leq 2^{k-2} < 2^{k-1}$, so neither $(a-b)$ nor $(a+b)$ can be divisible by 2^{k-1}. We have a contradiction, so we know every $c \equiv 1 \pmod{8}$ is equivalent modulo 2^k to the square of some odd number.
And furthermore, if we have found solutions to $x^2 \equiv c \pmod{2^k}$ to for two consecutive values of k, $s_k^2 \equiv c \pmod{2^k}$ and $s_{k-1}^2 \equiv c \pmod{2^{k-1}}$, we know $s_k^2 \equiv c \pmod{2^{k-1}}$ so $s_k^2 \equiv s_{k-1}^2 \pmod{2^{k-1}}$, but for any solution s_k we can always have $-s_k$ is also a solution, so we can choose that $s_k \equiv s_{k-1} \pmod{2^{k-1}}$, giving us a 2-adic solution. ∎

Wee are now ready to proceed to the proof of Fermat's sum of two squares theorem.

5 Proof of Fermat's Sum of Squares Theorem

Let us remind you how we are going to tackle Fermat's Sum of Two Squares Theorem using Hasse-Minkowski Theorem. In the first section, we know that the rational numbers that can be written in a form of sum of two squares corresponds to the points on the curve $x^2 + y^2 = n$. Moreover, the associated form is given by $(\frac{X}{Z})^2 + (\frac{X}{Z})^2 = n \iff X^2 + Y^2 + nZ^2 = 0$. Applying Hasse-Minkowski Theorem, it suffices to find solutions over $\mathbb{R}$ and $\mathbb{Q}_p$, such that $p = 2$ and each p dividing n.
Moreover, based on the discussion of Polynomial Congruences, from the third section, we reduce n to be odd and square-free. More importantly, to solve the quadratic form over $\mathbb{Q}_p$, it's equivalent to solve a single congruence for each p.

5.1 Lemmas Towards Fermat's Sum of Squares Theorem

The first Lemma corresponds to the first case in Lemma 3.2.

Lemma 5.1. *Let n be an odd integer. Then, the quadratic form $q(X,Y,Z) = X^2 + Y^2 - nZ^2 = 0$ has a solution over $\mathbb{Q}_2$ if and only if $n \equiv 1 \mod 4$.*

Proof. ($\Longrightarrow$) If $n \equiv 1 \pmod 4$ then $n \equiv 1 \pmod 8$ or $n \equiv 5 \pmod 8$. If $n \equiv 1 \pmod 8$, we know by 4.3 that $x^2 = n$ has a 2-adic solution, S, so $(S, 0, 1)$ is a solution to q over $\mathbb{Q}_2$. If $n \equiv 5 \pmod 8$, we can construct a similar solution $(V, 2, 1)$, so we have $V^2 = n - 4$, where $n - 4 \equiv 1 \pmod 8$, so we can let V be the 2-adic solution guaranteed by 4.3.

($\Longleftarrow$) To show that when $n \equiv 3 \mod 4$, there is no solution over $\mathbb{Q}_p$, it's equivalent to show there is no nontrivial compatible system of congruences mod 2 and mod 4. From Example 2.3, we know that when $n = 3$, there is no compatible solution. We can generalize this result to all $n \equiv 3 \pmod 4$. Similar to Example 2.3, we can always reduce the solution of $X^2 + Y^2 - nZ^2 \equiv 0 \mod 2$ to $(0,0,0) \mod 4$, which implies that it would be impossible to have a nontrivial solution over $\mathbb{Q}_2$. ■

The next Lemma corresponds to the case that p is an odd prime in Lemma 3.2. With lemma 3.1, we constrain n to be square free to get our desired result.

Lemma 5.2. *Let n be an integer, and let p be a prime divisor of n, such that p^2 is not a divisor of n (in other words, n is square-free). Then, the quadratic form $q(X,Y,Z) = X^2 + Y^2 - nZ^2 = 0$ has a solution over $\mathbb{Q}_p$ if and only if $p \equiv 1 \mod 4$.*

Proof. ($\Longrightarrow$)To start, notice that $X^2 + Y^2 - nZ^2 \equiv X^2 + Y^2 \pmod p$ because $p \mid n$, so any solution (x, y, z) can have z be any non-zero integer. If we know $p \equiv 1 \pmod 4$ then we know -1 is a quadratic residue modulo p. This means $x^2 = -1 \pmod p$ has a solution s, which means $(s, 1, t)$ for any $t \neq 0$ is a solution to $q \equiv 0 \pmod p$ and by 4.2 we have that because $q = 0$ has a solution, q has a solution over $\mathbb{Q}_p$.

($\Longleftarrow$) Towards a contradiction, we assume $p \equiv 3 \mod 4$ and the quadratic form $X^2 + Y^2 - nZ^2 = 0$ has a nontrivial solution over $\mathbb{Q}_p$. Since by assumption, p is a divisor of n, $nZ^2 \pmod p$ is always 0, then there exists a solution $(a_1, b_1, c_1) \in \mathbb{Z}^3$, such that $a_1^2 + b_2^2 \equiv 0$.
We claim that a_1 and b_1 are both 0 modulo p. Firstly, we show that one of them has to be 0. Towards a contradiction, if a_1 and b_1 are all reduced residues modulo p. Then, $b_1 {b_1}^{-1} \equiv 1 \mod p$. Therefore, $(a{b_1}^{-1})^2 \equiv -1 \mod p$, which contradicts the Euler's identity that when $p \equiv 3 \mod 4$, -1 is not a quadratic residue modulo p. Moreover, if only one of a_1 and b_1 is zero modulo p, then it contradicts the assumption that $a_1^2 + b_2^2 \equiv 0 \mod p$. Therefore, both of them are 0 modulo p.

Since we assume the quadratic form has a nontrivial solution over $\mathbb{Q}_p$, thus c_1 must be nonzero. We aims to find a contradiction that c_1 is zero. Consider

another solution of congruence $a_2^2+b_2^2 \equiv 0 \mod p^2$. Since the those the solution in modulo p and modulo p^2 form a p-adic number, it must be the case that those two solutions are compatible. In other words, $(a_1, b_1, c_1) \equiv (a_2, b_2, c_3) \mod p^2$. Thus, $b_2 \equiv b_1 \equiv a_1 \equiv a_2 \pmod p$. And moreover, $c_1 \equiv c_2 \mod p$.
Then, $a_2^2 + b_2^2 \equiv nc_2^2 \equiv 0 \mod p^2$. Since by assumption n is not divisible by p^2, then it must be the case that c_2^2 is congruent to zero modulo p^2. It follows that $c_1 \equiv c_2 \pmod p$, which is our desired contradiction. ■

5.2 Proof of Fermat's Sum of Squares Theorem with Rational Solutions

Now we have all the building blocks for our proof of Fermat's Sum of Squares theorem. We will begin by making a statement about when there are rational solutions (x, y) to the equation $x^2 + y^2 = n$ for an integer n.

Theorem 5.3. *There is a rational x and y solving the equation $x^2 + y^2 = n$ for $n \in \mathbb{Z}$ if and only if every prime factor p of n appears with an even power in the prime factorization of n.*

Proof. $f(x, y) = x^2+y^2-n = 0$ has a rational solution if and only if $Q(X, Y, Z) = X^2 + Y^2 - nZ^2 = 0$ has a non-trivial integral solution.
By 5.1 and 5.2 we know Q has a solution over $\mathbb{Q}_p$ for $p = 2$ and $p \mid n$ if and only if $p \equiv 1 \pmod 4$ (which implies $n \equiv 1 \pmod 4$, the necessary condition for $\mathbb{Q}_2$). Q clearly has solutions over the real numbers, so by the Hasse-Minkowski theorem, Q has integer solutions if and only if $p \equiv 1 \pmod 4$ for all $p \mid n$.

This means there is a rational solution to $x^x + y^2 = n$ if and only if $p \equiv 1 \pmod 4$ for all $p \mid n$. And we have established that a solution to a square free n implies a solution to $x^x + y^2 = ns^2$ for any $s \in \mathbb{N}$, so finally we have a solution to $x^2 + y^2 = n$ for $n \in \mathbb{Z}$ if and only if every prime factor p of n appears with an even power in the prime factorization of n. ■

5.3 The Integral Solutions of Fermat's Sum of Squares Theorem

We showed the existence of rational solutions for Fermat's Sum of Two Squares Theorem. Equivalently, we answered the following question: *Let $n > 1$ be a fixed natural number. Are there rational solutions to the quadratic form $x^2 + y^2 = n$?*

But Fermat's Sum of Two Squares is about the integral solutions. Thus, it's natural to solve the following question:
Let $n > 1$ be a fixed natural number. Are there rational solutions to the quadratic form $x^2 + y^2 = n$? By the following proposition, we know those two questions are essentially equivalent:
"The quadratic equation $x^2 + y^2 = n$ has an integral solution if an only if it has rational solution."

In "Number Theory and Geometry", the author proved it constructively on page 322. We would not directly proved it here, since the proof uses a smart trick to construct integer solutions by the known rational solutions. But I will guide you through the thought process here. To prove this preposition, it suffices to show the square-free part n' of n is also a sum of two integers; i.e., if $n = n's^2$ and $n' = x^2 + y^2$, then $n = (xs)^2 + (ys)^2$. By Lemma 3.1, $x^2 + y^2 = n$ has rational solutions if and only if $x^2 + y^2 = n'$ has rational solutions. Then we assume the rational solutions of $x^2 + y^2 = n'$ to be $(\frac{a}{c}, \frac{b}{d})$. By bring cd to the other side, we get $n'(cd)^2 = (ad)^2 + (bc)^2$. We may assume ad and bc are relatively prime, because we can divide both sides by gcd to make them relatively prime. Relabel cd with μ, ad with α, and bc with β. Using the trick to construct integer solutions, we can show n' is a sum of two squares of integers. Thus, we conclude that n has integral solutions implied by rational solutions.

Finally, we proved Fermat's Sum of Two Squares Theorem with a small detour by considering rational solutions. Through out the proof, the Hasse-Minkowski Theorem plays a big rule in breaking down the problem into solutions over p-adic fields, which are in a smaller scale to work with. There are many other powerful theorems that can be simplified by Hasse-Minkowski Theorem, like Lagrange's Sum of Four Squares in the next section. We have no space to show other applications of Hasse-Minkowski Theorem in other contexts. But at least, readers can have a taste of how to use Hasse-Minkowski Theorem to solve problems from this paper.

6 Sketch of a Proof For Lagrange's Theorem

An argument similar to the one we used to prove Fermat's theorem can be used to prove Lagrange's Four Squares theorem. Again, we must show for the quadratic form $L(X, Y, Z, W, A) = X^2+Y^2+Z^2+W^2-nA^2$, the equation $L = 0$ has solutions over $\mathbb{Q}_p$ for $p = 2$ and $p \mid n$. Once we have done that, we use the same bijection to deduce a rational solution (x, y, z, w) to $x^2 + y^2 + z^2 + w^2 = n$ for any integer n. Then one can show that a rational solution implies an integer solution. We will use similar versions of the lemmas we have proved already.

Lemma 6.1. *The quadratic form $L(X, Y, Z, W, A) = X^2+Y^2+Z^2+W^2-nA^2$ has a solution for $L = 0$ over $\mathbb{Q}_2$.*

Proof. We know by 4.3 that $x^2 = c$ has a 2-adic solution if $c \equiv 1 \pmod 8$, so if $n \equiv 1 \pmod 8$ then $(S_1, 0, 0, 0, 1)$ is a solution to L over $\mathbb{Q}_2$ were S_1 is the solution to $x^2 = n$ over $\mathbb{Q}_2$. By carefully choosing values, we can manipulate the expression so the left hand side is always a square, and the right hand side is always 1 modulo 8, giving us a solution.

- If $n \equiv 2 \pmod 8$, we can construct a similar solution $(S_2, 1, 0, 0, 1)$, so we have $S_2^2 = n - 1$, where $n - 1 \equiv 1 \pmod 8$, so we can let S_2 be the 2-

adic solution guaranteed by 4.3. We can proceed similarly by constructing solutions for each residue modulo 8.

- If $n \equiv 3 \pmod 8$ we have a solution $(S_3, 1, 1, 0, 1)$ with $S_3^2 = n - 2$.
- If $n \equiv 4 \pmod 8$ we have a solution $(S_4, 1, 1, 1, 1)$ with $S_4^2 = n - 3$.
- If $n \equiv 5 \pmod 8$ we have a solution $(S_5, 2, 0, 0, 1)$ with $S_5^2 = n - 4$.
- If $n \equiv 6 \pmod 8$ we have a solution $(S_6, 2, 1, 0, 1)$ with $S_6^2 = n - 5$.
- If $n \equiv 7 \pmod 8$ we have a solution $(S_7, 2, 1, 1, 1)$ with $S_7^2 = n - 6$.
- If $n \equiv 0 \pmod 8$ we can divide n by 4 until it isn't, and compensate by multiplying the solution by the appropriate number of 2's.

We have addressed every possibility for n, so the result is shown. ■

In order to guarantee a p-adic solution for every prime that divides n, by 4.2, we only need to show that there is a solution to the congruence $L \equiv 0 \pmod p$ for an arbitrary p, dividing n. Which amounts to showing $X^2+Y^2+Z^2+W^2 \equiv 0 \pmod p$ has a solution for an arbitrary $p > 2$. If $p \equiv 1 \pmod 4$ we obtain a solution using the quadratic character of -1 as before. If $p \equiv 3 \pmod 8$ we can use the quadratic character of -2. But if $p \equiv -1 \pmod 8$, there is more sophisticated work to do, which is beyond the scope of this paper.

7 Works Cited

We have followed closely the arguments presented in:

A. Lozano-Robledo, *Number Theory and Geometry: An Introduction to Arithmetic Geometry*, American Mathematical Society, 2019.