Local-Global Principles for Diophantine Equations

Benjamin Liam Barham

A Senior Thesis submitted in partial fullfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2020

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fullfillment of the requirements for graduation from the
Honors Program of Liberty University.

_____

Ethan C. Smith, Ph.D.
Thesis Chair

_____

Timothy Sprano, Ph.D.
Committee Member

_____

David E. Schweitzer, Ph.D.
Assistant Honors Director

_____

Date

Abstract

The real number field, denoted $\mathbb{R}$, is the most well-known extension field of $\mathbb{Q}$, the field of rational numbers, but it is not the only one. For each prime p, there exists an extension field $\mathbb{Q}_p$ of $\mathbb{Q}$, and these fields, known as the p-adic fields, have some properties substantially different from $\mathbb{R}$. In this paper, we construct the p-adic numbers from the ground up and discuss the local-global principle, which concerns connections between solutions of equations found in $\mathbb{Q}$ and in $\mathbb{Q}_p$. We state the Hasse-Minkowski theorem, which addresses a type of Diophantine equation to which the local-global principle applies, and conclude with a computation in which we apply the theorem followed by Selmer's famous counterexample for cubic curves.

Local-Global Principles for Diophantine Equations

Introduction

One of the many (though certainly countable) motivations of the field of real numbers is the need for a solution to the equation $X^2 - 2 = 0$. The integers and rational numbers are intuitive and fairly simple, but solving such equations as above necessitates a field beyond the rationals. Despite this "as needed" construction of the real numbers, many of the elements of this field extension are now familiar to any student past elementary school. Such universal application of a formerly unknown extension might reasonably prompt a question: "Are there other extensions of the rational numbers?" This is one of the questions which motivates p-adic theory.

p-adic numbers occur in many areas of mathematics, from abstract number theory to geophysical modeling applications (Oleshchko and Khrennikov, 2017), but for this paper, we address the connections between p-adic solutions and rational solutions of an equation. The idea that connections exist between p-adic solutions and rational solutions is known as the local-global principle, and it essentially states that "a theorem or property holds over $\mathbb{Q}$ if and only if it holds over $\mathbb{R}$ and $\mathbb{Q}_p$ for all p" (Conrad, n.d.-c, p. 1). In many contexts, this principle does not hold, but for some, it does. In this paper, we will study how this principle applies to certain types of Diophantine equations, which are "equations or systems of polynomial equations that must be solved in integers, rational numbers, or more generally in algebraic numbers" (Cohen, 2007, p. v). However, we must begin by understanding what p-adic numbers themselves are.

Valuations

We begin with some basic number theory. Recall that for any given prime p, we can write

each $x \in \mathbb{Z}$ as $x = np^r$ for some $n \in \mathbb{Z}, r \in \mathbb{N} \cup \{0\}$ such that $p \nmid n$. Likewise, for $y \in \mathbb{Q}$, we can write $y = p^r \frac{a}{b}$ for $a, b, r \in \mathbb{Z}$ such that $p \nmid ab$ (Salzmann, Grundhöfer, Hähl, and Löwen, 2007). Using this idea, we can define the p-adic valuation following Gouvêa (1997).

Definition 1. For $x \in \mathbb{Z}$, we define the ***p*-adic valuation** function $v_p : \mathbb{Z}\backslash\{0\} \longrightarrow \mathbb{R}$ such that $v_p(x)$ is the unique positive integer satisfying the equation

$$x = p^{v_p(x)}n, \qquad p \nmid n \in \mathbb{Z}.$$

For $y \in \mathbb{Q}^\times$ such that $y = a/b$ where $a, b \in \mathbb{Z}$ and $b \neq 0$, we extend this valuation:

$$v_p(y) = v_p(a) - v_p(b).$$

Remark. One exception not handled by this definition is the valuation of 0, so we formally let $v_p(0) = +\infty$. "The reasoning here is that we can certainly divide 0 by p, and the answer is 0, which we can divide by p, and the answer is 0, which we can divide by p..." (Gouvêa, 1997, p. 25). The idea is that 0 is infinitely divisible by p, so although our definition of valuation does not directly address the valuation of 0, defining the valuation in this way is consistent and logical.

Example. Consider the 3-adic and 5-adic valuations of 90 and $\frac{13}{625}$.

$$v_3(90) = v_3(3^2 \cdot 10) = 2$$

$$v_3\left(\frac{13}{625}\right) = v_3(13) - v_3(625) = 0 - 0 = 0$$

$$v_5(90) = v_5(5^1 \cdot 18) = 1$$

$$v_5\left(\frac{13}{625}\right) = v_5(13) - v_5(5^4) = 0 - 4 = -4.$$

From these examples, we see that the more divisible $x \in \mathbb{Q}$ is by p, the higher the p-adic valuation will be. Note that 0 is not the lowest valuation possible since rational numbers containing negative powers of p exist.

We now prove some properties that will be helpful in the next section (Gouvêa, 1997).

Lemma 2. For all $x, y \in \mathbb{Q}^\times$, the following holds:

(1) $v_p(xy) = v_p(x) + v_p(y)$.

(2) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

Proof. Let $x = p^{v_p(x)}\frac{a}{b}$ and $y = p^{v_p(y)}\frac{c}{d}$ for some $a, b, c, d \in \mathbb{Z}$ such that $p \nmid abcd$ and $bd \neq 0$.

For (1), using the definition of the p-adic valuation, we obtain

$$v_p(xy) = v_p\left(p^{v_p(x)}\frac{a}{b} \cdot p^{v_p(y)}\frac{c}{d}\right) = v_p\left(p^{v_p(x)+v_p(y)} \cdot \frac{ac}{bd}\right) = v_p(x) + v_p(y).$$

For (2), suppose without loss of generality that $v_p(x) \geq v_p(y)$. Observe:

$$\begin{aligned} v_p(x+y) = v_p\left(p^{v_p(x)}\frac{a}{b} + p^{v_p(y)}\frac{c}{d}\right) &= v_p\left(\frac{p^{v_p(x)}ad + p^{v_p(y)}bc}{bd}\right) \\ &= v_p(p^{v_p(x)}ad + p^{v_p(y)}bc) - v_p(bd) \\ &= v_p\left(p^{v_p(y)}(p^{v_p(x)-v_p(y)}ad + bc)\right) - v_p(bd) \\ &= v_p\left(p^{v_p(y)}\right) + v_p\left(p^{v_p(x)-v_p(y)}ad + bc\right) - 0 \\ &\geq v_p(y). \end{aligned}$$

□

Remark. One detail that will be useful to us later is a guarantee for equality in condition (2). If $v_p(x) > v_p(y)$, then $v_p(p^{v_p(x)-v_p(y)}ad + bc) = 0$ because $p \mid (p^{v_p(x)-v_p(y)}ad)$ while $p \nmid bc$. This implies $v_p(x+y) = v_p(y)$. Thus, if $v_p(x) \neq v_p(y)$, then $v_p(x+y) = \min\{v_p(x), v_p(y)\}$.

Absolute Values

Absolute value is a familiar concept, but the traditional absolute value is actually a function specifically defined for the real numbers. In order to discuss and eventually construct the p-adic numbers, it is necessary to first establish a proper definition of an abstract absolute value.

Definition 3. Given a ring R, an **absolute value** is a function $|\cdot| : R \longrightarrow [0, \infty)$ which satisfies:

1. $|x| = 0$ if and only if $x = 0$,
2. $|x| \cdot |y| = |x \cdot y|$,
3. $|x + y| \leq |x| + |y|$

for all $x, y \in R$. Additionally, if the condition

4. $|x + y| \leq \max\{|x|, |y|\}$

is met, then $|\cdot|$ is a **non-archimedean** absolute value (Gouvêa, 1997).

Note that the usual absolute value conforms to the above definition. However, $|1 + 1| = |2| = 2 > 1 = \max\{|1|, |1|\}$, so it is not non-archimedean.

p-adic Absolute Values

What follows is the construction of a new absolute value that makes use of our previous work with p-adic valuations (Gouvêa, 1997).

Definition 4. Let p be prime. For $x \in \mathbb{Q}^\times$, we define the ***p*-adic absolute value** of x by

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

For $x = 0$, we define $|0|_p = 0$.

Before taking a closer look at this function, we will first prove that it satisfies the requirements of an absolute value.

Proposition 5. $|\cdot|_p$ is a non-archimedean absolute value on $\mathbb{Q}$.

Proof. First, note that by construction, $|x|_p > 0$ for all $x \in \mathbb{Q}^\times$, so because we defined $|0|_p = 0$, it is clear that $|x|_p = 0$ if and only if $x = 0$.

Let $x, y \in \mathbb{Q}^\times$, and let p be prime. For some $a, b, c, d \in \mathbb{Z}$ such that $p \nmid abcd$, we can write $x = p^{v_p(x)}\frac{a}{b}$ and $y = p^{v_p(y)}\frac{c}{d}$. Observe:

$$|x \cdot y|_p = \left|p^{v_p(x)}\frac{a}{b} \cdot p^{v_p(y)}\frac{c}{d}\right|_p = \left|p^{v_p(x)+v_p(y)} \cdot \frac{ac}{bd}\right|_p$$

$$= p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = \left|p^{v_p(x)}\frac{a}{b}\right|_p \cdot \left|p^{v_p(y)}\frac{c}{d}\right|_p = |x|_p \cdot |y|_p.$$

Thus, the second condition of an absolute value is satisfied. We now prove the non-archimedean condition, using Lemma 2 to justify the following inequality.

$$|x+y|_p = p^{-v_p(x+y)} \leq p^{-\min\{v_p(y),v_p(y)\}} = \max\{|x|_p, |y|_p\}.$$

Since the non-archimedean condition implies condition three, this function meets all of the conditions for a non-archimedean absolute value on $\mathbb{Q}$. □

Remark. Since $v_p(x) \neq v_p(y)$ implies $v_p(x+y) = \min\{v_p(x), v_p(y)\}$, it follows from our proof of the non-archimedean condition that $|x|_p \neq |y|_p$ guarantees that $|x+y|_p = \max\{|x|_p, |y|_p\}$.

Example. Consider the 3-adic absolute value of the following elements:

$$\left|\frac{18}{11}\right|_3 = 3^{-(v_3(18)-v_3(11))} = 3^{-2} = \frac{1}{9}$$

$$|126|_3 = 3^{-v_3(126)} = 3^{-2} = \frac{1}{9}$$

$$\left|\frac{306}{187}\right|_3 = 3^{-(v_3(306)-v_3(187))} = 3^{-2} = \frac{1}{9}$$

Note that it does not matter if the fraction is fully reduced or if the numerator and denominator share a power of p as a factor. This is necessary because absolute values must be well-defined functions. Also note that quantities which are of vastly different magnitude from the perspective of the real number absolute value can have equivalent 3-adic absolute values.

Constructing the p-adic Fields

Now we begin the work of constructing the p-adic numbers, following the approach found in Fernando Gouvea's *p-adic Numbers: An Introduction* (1997).

Incompleteness of the Rationals

First, recall that a *Cauchy sequence* is essentially a sequence of elements which are getting closer and closer together. More precisely, the sequence (x_n) is Cauchy if "for any $\varepsilon > 0$ there exists a natural number $H(\varepsilon)$ such that for all natural numbers $n, m \geq H(\varepsilon)$, the terms x_n, x_m satisfy $|x_n - x_m| < \varepsilon$" (Bartle & Sherbert, 2011, p. 85). Such sequences have many applications, but one of the most significant is in the definition of a complete field. A foundational concept in Real Analysis is that while $\mathbb{R}$ is a complete field, $\mathbb{Q}$ is not, and this is because there exists at least one Cauchy sequence in $\mathbb{Q}$ that converges to a limit ($\sqrt{2}$, for example) that is not contained in $\mathbb{Q}$.

The definition of a Cauchy sequence involves an absolute value, so what changes if we use a p-adic absolute value? To answer this, we must check whether $\mathbb{Q}$ is complete with respect to a p-adic absolute value. First, however, we need a more convenient way of checking if a sequence is Cauchy.

Lemma 6. Let $|\cdot|$ be a non-archimedean absolute value. If a sequence (x_n) of rational numbers meets the condition

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0,$$

then that sequence is Cauchy.

Proof. Let $\varepsilon > 0$. By assumption and the definition of a limit, there exists $M > 0$ such that $|x_{n+1} - x_n| < \varepsilon$ for all $n > M$. Without loss of generality, let $m = k + r > k > M$. Observe:

$$|x_m - x_k| = |x_{k+r} - x_{k+r-1} + x_{k+r-1} - x_{k+r-2} + ... + x_{k+1} - x_k|$$

$$\leq \max\{|x_{k+r} - x_{k+r-1}|, |x_{k+r-1} - x_{k+r-2}|, ..., |x_{k+1} - x_k|\} < \varepsilon$$

since $k + r > k + r - 1 > ... > k + 1 > k > M$. Thus, for any $\varepsilon > 0$, there exists M such that $|x_m - x_k| < \varepsilon$ for every $m, k > M$. Therefore, the sequence is Cauchy. □

With this result in hand, we proceed to inspect $\mathbb{Q}$. Since $\mathbb{Q}$ is not complete with respect to the usual absolute value, it is reasonable to suspect that $\mathbb{Q}$ is not complete with respect to the p-adic absolute values as well. We will now prove that this suspicion is correct.

Proposition 7. The field $\mathbb{Q}$ of rational numbers is not complete with respect to any of its p-adic absolute values.

Proof. Suppose $p > 2$ is a prime. The goal is to construct a Cauchy sequence of elements in $\mathbb{Q}$ that converges to a limit not in $\mathbb{Q}$. First consider an integer a such that

- a is not a square in $\mathbb{Q}$
- $p \nmid a$

- $X^2 \equiv a \pmod{p}$ has a solution.

As an example, if $p = 3$, we could choose $a = 7$. One way of doing this is to take a perfect square in $\mathbb{Q}$ and simply add $2p$; this will obtain the type of integer we require.

Now the goal is to construct a Cauchy sequence of rational numbers that converges to a solution to the equation $X^2 = a$. This will show that $\mathbb{Q}$ is not complete with respect to $|\cdot|_p$. Clearly, by construction of a, there exists $x_0 \in \mathbb{Q}$ such that $x_0^2 \equiv a \pmod{p}$. We will now show that given $x_{n-1} \in \mathbb{Q}$ such that $x_{n-1}^2 \equiv a \pmod{p^n}$, we can construct $x_n \in \mathbb{Q}$ so that $x_n \equiv x_{n-1} \pmod{p^n}$ and $x_n^2 \equiv a \pmod{p^n}$. This will result in the sequence we desire.

Suppose $x_{n-1} \in \mathbb{Q}$ such that $x_{n-1}^2 \equiv a \pmod{p^n}$. Then there exists $k_n \in \mathbb{Z}$ such that $x_{n-1}^2 = a + k_n p^n$. Since $p \nmid a$ and p is odd, $p \nmid 2x_{n-1}$. Clearly, p^n and $2x_{n-1}$ are coprime, and thus, $2x_{n-1}$ is invertible modulo p^n. We now let $x_n = x_{n-1} + b_n p^n$ where $0 \leq b_n < p^n$, and we let $b_n \equiv -(2x_{n-1})^{-1} k_n \pmod{p}$. This congruence implies

$$k_n + 2x_{n-1} b_n \equiv 0 \pmod{p}.$$

We multiply through by p^n to obtain

$$p^n k_n + 2x_{n-1} b_n p^n \equiv 0 \pmod{p^{n+1}}.$$

Substituting in $x_{n-1}^2 = a + k_n p^n$, we get

$$a \equiv x_{n-1}^2 + 2x_{n-1} b_n p^n \equiv x_{n-1}^2 + 2x_{n-1} b_n p^n + (b_n p^n)^2 \equiv (x_{n-1} + b_n p^n)^2 \equiv x_n^2 \pmod{p^n}.$$

By induction, we now have a sequence of elements in $\mathbb{Q}$. We now check that it is Cauchy. Note that for any x_n in the sequence, $x_n \equiv x_{n-1} \pmod{p^n}$, so $x_n = x_{n-1} + p^n b_n$ for $b_n \in \mathbb{Z}$. Thus,

$$|x_n - x_{n-1}|_p = |x_{n-1} + p^n b_n - x_{n-1}|_p = |p^n b_n|_p \leq \frac{1}{p^n}.$$

By the Squeeze Theorem, we have that $\lim_{n\to\infty} |x_n - x_{n-1}|_p = 0$. Thus, by Lemma 6, (x_n) is a Cauchy sequence. Now since $x_n^2 \equiv a \pmod{p^{n+1}}$ for any x_n, we have that $x_n^2 = a + p^{n+1}b_n$ for some $b_n \in \mathbb{Z}$. Thus,

$$|x_n^2 - a|_p = |a + p^{n+1}b_n - a|_p = |p^{n+1}b_n|_p \leq \frac{1}{p^{n+1}},$$

so we have that $\lim_{n\to\infty} |x_n^2 - a|_p = 0$. However, this implies that the limit of (x_n) is a solution to $X^2 = a$, which has no solution in $\mathbb{Q}$. Therefore, $\mathbb{Q}$ is not complete with respect to $|\cdot|_p$ for $p \geq 3$.

Now let $p = 2$. Similarly to the above, we must come up with some conditions for our initial integer and our Cauchy sequence. Let $a \in \mathbb{Z}$ satisfy the following conditions:

- a is not a cube in $\mathbb{Q}$.
- a is odd.
- $X^3 \equiv a \pmod{2}$ has a solution.

For example, $a = 29$ works.

By construction, there exists $x_0 \in \mathbb{Q}$ such that $x_0^3 \equiv a \pmod{2}$. Similarly to before, we will show that given $x_{n-1} \in \mathbb{Q}$ such that $x_{n-1}^3 \equiv a \pmod{2^n}$, we can construct $x_n \in \mathbb{Q}$ such that $x_n \equiv x_{n-1} \pmod{2^n}$ and $x_n^3 \equiv a \pmod{2^n}$.

Suppose $x_{n-1} \in \mathbb{Q}$ such that $x_{n-1}^3 \equiv a \pmod{p^n}$. Then there exists $k_n \in \mathbb{Z}$ such that $x_{n-1}^3 = a + k_n 2^n$. Since a and 3 are odd, $2 \nmid 3a$, and so $2 \nmid 3x_{n-1}$. This means that 2^n and $3x_{n-1}$ are coprime, so $3x_{n-1}$ is invertible modulo 2^n. We let $x_n = x_{n-1} + b_n 2^n$ where $0 \leq b_n < 2^n$, and we let $b_n \equiv -(3x_{n-1}^2)^{-1}k_n \pmod{2}$. This congruence yields

$$k_n + 3x_{n-1}^2 b_n \equiv 0 \pmod{2}.$$

Multiplying through by 2^n, we get

$$k_n 2^n + 3x_{n-1}^2 b_n 2^n \equiv 0 \pmod{2^{n+1}},$$

and finally, we substitute $x_{n-1}^3 = a + k_n 2^n$ to obtain

$$\begin{aligned} a \equiv x_{n-1}^3 + 3x_{n-1}^2 b_n 2^n &\equiv x_{n-1}^3 + 3x_{n-1}^2 b_n 2^n + 3x_{n-1}(b_n 2^n)^2 + (b_n 2^n)^3 \\ &\equiv (x_{n-1} + b_n 2^n)^3 \\ &\equiv x_n^3 \pmod{2^{n+1}}. \end{aligned}$$

To see that this sequence is Cauchy, see that $x_n = x_{n-1} + 2^n b_n$ for $b_n \in \mathbb{Z}$, and this implies

$$\lim_{n\to\infty} |x_n - x_{n-1}|_2 = \lim_{n\to\infty} |x_{n-1} + 2^n b_n - x_{n-1}|_2 = \lim_{n\to\infty} |2^n b_n|_2 \leq \lim_{n\to\infty} \frac{1}{2^n} = 0.$$

Now for any x_n in the sequence, $x_n^3 \equiv a \pmod{2^{n+1}}$, which implies that $x_n^3 = a + 2^{n+1} b_n$ for some $b_n \in \mathbb{Z}$. This means that we can write

$$|x_n^3 - a|_2 = |a + 2^{n+1} b_n - a|_2 = |2^{n+1} b_n|_2 \leq \frac{1}{2^{n+1}}.$$

Clearly, $\lim_{n\to\infty} |x_n^3 - a|_2 = 0$, but this implies that the limit of (x_n) is a solution to $X^3 = a$, which does not have a solution in $\mathbb{Q}$. Therefore, $\mathbb{Q}$ is not complete with respect to $|\cdot|_2$.

Combining the above, we have proven that $\mathbb{Q}$ is not complete with respect to any $|\cdot|_p$. □

The *p*-adic Numbers

Now that we have shown that $\mathbb{Q}$ is not complete, we can now begin constructing the p-adic fields. How do we begin? Well, the proof above demonstrated that $\mathbb{Q}$ is not complete because there exist "gaps" in $\mathbb{Q}$. Although a Cauchy sequence may be composed entirely of

rational numbers, it is possible that it will converge to a gap that the rational numbers do not include. The way, then, to construct a complete field is to specifically define its elements so that every rational Cauchy sequence converges to an element in the field. One way to do this is to make each element a Cauchy sequence, and this is where we will begin.

Definition 8. Let $|\cdot|_p$ be a non-archimedean absolute value on $\mathbb{Q}$. We denote by $\mathcal{C}$ the set

$$\mathcal{C} = \{(x_n) : (x_n) \text{ is a Cauchy sequence with respect to } |\cdot|_p\}.$$

This definition provides "numbers" to work with. Next, we define how they interact.

Proposition 9. Let $(x_n), (y_n) \in \mathcal{C}$. "Defining

$$(x_n) + (y_n) = (x_n + y_n)$$

$$(x_n) \cdot (y_n) = (x_n y_n)$$

makes $\mathcal{C}$ a commutative ring with unity" (Gouvêa, 1997, p. 53).

The reader is invited to check that $(x_n + y_n)$ and $(x_n y_n)$ are Cauchy sequences. Assuming this is true, we can see that the constant sequences $(0) = (0, 0, 0, ...)$ and $(1) = (1, 1, 1, ...)$ are the zero and the 1 in $\mathcal{C}$, respectively, and the rest of the ring axioms follow quite simply from properties of the rational numbers.

We now have a commutative ring. One important thing to note is that there is a "copy" of the rational numbers in $\mathcal{C}$. Let $(x) = (x, x, x, ...)$ be a constant sequence where $x \in \mathbb{Q}$. Clearly, (x) is a Cauchy sequence, so if we let $f : \mathbb{Q} \to \mathcal{C}$ be a function defined by $f(x) = (x)$, we see that f is an inclusion of $\mathbb{Q}$ in $\mathcal{C}$. This is easy to check through the addition and multiplication rules for $\mathcal{C}$.

However, $\mathcal{C}$ is vastly larger than $\mathbb{Q}$, and it is not a field because it contains zero divisors. Thus, our final step is to find a maximal ideal of $\mathcal{C}$.

Definition 10. "We define $\mathcal{N} \subset \mathcal{C}$ to be the ideal

$$\mathcal{N} = \{(x_n) : x_n \to 0\} = \{(x_n) : \lim_{n\to\infty} |x_n|_p = 0\}$$

of sequences that tend to zero with respect to the absolute value $|\cdot|_p$" (Gouvêa, 1997, p. 54).

We now have two steps left: proving that $\mathcal{N}$ is an ideal of $\mathcal{C}$ and that it is a maximal ideal. That it is an ideal is quite intuitive. Real analysis demonstrates that the limit of two convergent sequences multiplied element-wise will be the product of the limits of the sequences. Thus, if $(x_n) \in \mathcal{C}$ and $(a_n) \in \mathcal{N}$, it seems reasonable that the sequence $(x_n a_n)$ will converge to 0. The reader is invited to work out the details, but we will move on to maximality.

Theorem 11. The set $\mathcal{N}$ is a maximal ideal of the commutative ring $\mathcal{C}$.

Proof. We will use an approach from Bachman (1964). Let $(x_n) \in \mathcal{C}$ such that (x_n) does not tend to zero with respect to $|\cdot|_p$. We begin by showing there exists some $\delta > 0$ such that $|x_n|_p > \delta$ for every $n > N$ where N is a sufficiently high natural number. Suppose to a contradiction that there is no such δ. We choose $\varepsilon > 0$, and since (x_n) is Cauchy, there exists an integer $M \in \mathbb{N}$ such that $|x_n - x_m|_p < \frac{\varepsilon}{2}$ for any $n, m > M$. By assumption, there exists some $k > M$ such that $|x_k|_p < \frac{\varepsilon}{2}$. Consider for any $m > M$:

$$|x_m|_p = |x_m + x_k - x_k|_p \leq |x_m - x_k|_p + |x_k|_p < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

However, since ε is arbitrary, $|x_m|_p < \varepsilon$ for every $m > M$ then implies that (x_n) does tend to zero, which is false. Thus, there exists a constant $\delta > 0$ and $N \in \mathbb{N}$ such that $|x_n|_p > \delta$ for all $n > N$.

We choose $\varepsilon > 0$, and note the existence of $N_x \in \mathbb{N}$ such that $|x_n - x_m|_p < \varepsilon$ for all $n, m > N_x$. Now we define a new sequence (y_n) so that $y_n = 0$ for all $n \leq N_y$ and $y_n = \frac{1}{x_n}$ for all $n > N_y$. We let $N = \max\{N_x, N_y\}$ and $m, n > N$. Observe

$$|y_n - y_m|_p = \left|\frac{1}{x_n} - \frac{1}{x_m}\right|_p = \left|\frac{x_m - x_n}{x_n x_m}\right|_p = \frac{|x_m - x_n|_p}{|x_n|_p |x_m|_p} < \frac{|x_m - x_n|_p}{\delta^2} < \frac{\varepsilon}{\delta^2}.$$

Since ε is arbitrary, (y_n) is Cauchy, and we therefore have that $(x_n)(y_n)$ is also Cauchy. Note that $(x_n)(y_n) = (0, 0, ..., 0, 1, 1...) = (1) - (1, 1, ..., 1, 0, 0, ...)$.

Now suppose that I is an ideal of $\mathcal{C}$ with $\mathcal{N} \subset I$. Let $(x_n) \in I$ and $(x_n) \notin \mathcal{N}$, noting that this means that (x_n) does not tend to zero. By the above work, we know that for this (x_n) there exists a corresponding $(y_n) \in \mathcal{C}$. Since $(x_n)(y_n) = (1) - (1, 1, ..., 1, 0, 0, ...)$ and I is an ideal, $(x_n)(y_n) \in I$. However, $(1, 1, ..., 1, 0, 0, ...) \in \mathcal{N} \subset I$ because it tends to zero. Thus, if we add this sequence to $(x_n)(y_n)$, we have that $(1) \in I$. This implies that $I = \mathcal{C}$, so $\mathcal{N}$ is a maximal ideal of $\mathcal{C}$. □

Definition 12. The field of p-adic numbers is defined as the quotient of the ring $\mathcal{C}$ by its maximal ideal $\mathcal{N}$, or in other words, $\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$ (Gouvêa, 1997).

We have now constructed the p-adic fields, and the final step is to extend the p-adic absolute value to irrational elements of $\mathbb{Q}_p$.

Definition 13. If a rational sequence (x_n) converges to $x \in \mathbb{Q}_p$, then we define

$$|x|_p = \lim_{n\to\infty} |x_n|_p.$$

For example, if a sequence of integers coprime to p converges to an irrational $x \in \mathbb{Q}_p$, then $|x|_p = 1$. The reader is invited to check that the choice of sequence converging to x does not change the absolute value of x.

Hensel's Lemma

Now that we have constructed the p-adic numbers, we can advance to developing some properties. We begin by defining an important subring of our field.

Definition 14. We define the ring of p-adic integers as

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

By definition, $|0|_p = 0$ for every prime p, so 0 is clearly a p-adic integer. Note also that every nonzero integer is also a p-adic integer since for every $x \in \mathbb{Z}$, $v_p(x) \geq 0$, and thus, $|x|_p = x^{-v_p(x)} \leq p^0 = 1$. Thus, 1 is also a p-adic integer. It follows from properties of a non-archimedean absolute value that $\mathbb{Z}_p$ is closed, for if $x, y \in \mathbb{Z}_p$, then $|x-y|_p \leq \max\{|x|_p, |-y|_p\} = \max\{|x|_p, |y|_p\} \leq 1$ and $|xy|_p = |x|_p \cdot |y|_p \leq 1 \cdot 1 = 1$. The rest of the ring axioms follow from the fact that $\mathbb{Z}_p \subset \mathbb{Q}_p$, a field. Thus, $\mathbb{Z}_p$ is a ring.

Next we have a useful identity.

Proposition 15. Let $F(X) = c_0 + c_1X + ... + c_nX^n$ be a polynomial of degree n with coefficients $c_j \in \mathbb{Z}_p$. Then for $a, b \in \mathbb{Z}_p$, we can write

$$F(a+b) = \sum_{k=0}^{d} b^k \left(\frac{F^{(k)}(a)}{k!}\right)$$

where $F^{(k)}(a)$ is the (formal) k-th derivative of $F(a)$.

Proof. First note that for a p-adic polynomial F with degree n, we can write

$$F(X) = \sum_{j=0}^{n} c_j X^j.$$

Now consider that by the binomial theorem and properties of sums, we can write

$$\begin{aligned} F(a+b) = \sum_{j=0}^{n} c_j (a+b)^j &= \sum_{j=0}^{n} c_j \sum_{k=0}^{j} \binom{j}{k} a^{j-k} b^k \\ &= \sum_{k=0}^{n} \left(\sum_{j=k}^{n} c_j \binom{j}{k} a^{j-k} \right) b^k \\ &= \sum_{k=0}^{n} b^k \left(\sum_{j=k}^{n} c_j \frac{j!}{k!(j-k)!} a^{j-k} \right) \\ &= \sum_{k=0}^{n} b^k \frac{1}{k!} \left(\sum_{j=k}^{n} c_j \frac{j!}{(j-k)!} a^{j-k} \right). \end{aligned}$$

However, the inner sum above is equivalent to the k-th formal derivative of $F(a)$, and thus, we have

$$F(a+b) = \sum_{k=0}^{n} b^k \left(\frac{F^{(k)}(a)}{k!} \right).$$

□

Remark. It will shortly be important to recognize that $\frac{F^{(k)}(a)}{k!}$, as in the proof above, is a p-adic integer. This may not seem obvious at first, but observe that since $\binom{j}{k}$ is an integer, the sum $\sum_{j=k}^{n} c_j \binom{j}{k} a^{j-k}$ is an integer. Thus, it is also a p-adic integer. However, the proof above then shows that this sum is equivalent to $\frac{F^{(k)}(a)}{k!}$, and therefore, it must be that $\frac{F^{(k)}(a)}{k!} \in \mathbb{Z}_p$.

We can now state a result found in Gouvêa (1997) that is vital to solving equations in $\mathbb{Q}_p$.

Theorem 16 (Hensel's Lemma). Let $F(X) = c_0 + c_1 X + c_2 X^2 + ... + c_n X^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. Suppose there exists $\alpha_1 \in \mathbb{Z}_p$ such that

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

where $F'(X)$ is the formal derivative of $F(X)$. Then there exists $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$.

Proof. Let $F(X) = c_0 + c_1X + c_2X^2 + ... + c_nX^n$. We proceed with a strategy derivative of approaches from Robert (2000) and Cassels (1986).

Since $\mathbb{Z}_p$ is a ring, the fact that all coefficients of $F(X)$ as well as α_1 are in $\mathbb{Z}_p$ implies that $F^{(n)}(\alpha_1) \in \mathbb{Z}_p$ for all n. Thus, $|F^{(n)}(\alpha_1)|_p \leq 1$. Combining this with our assumption, we obtain

$$|F(\alpha_1)|_p < |F'(\alpha_1)|_p^2 \leq |F'(\alpha_1)|_p \leq 1.$$

Now we define $b_1 = -\frac{F(\alpha_1)}{F'(\alpha_1)}$, noting that by our assumption, $F(\alpha_1)$ is more than twice as divisible by p as $F'(\alpha_1)$. Therefore, $|b_1|_p < 1$, and $b_1 \in \mathbb{Z}_p$. With this b_1, we have that $F(\alpha_1) + b_1F'(\alpha_1) = 0$.

Now consider $F(\alpha_1 + b_1)$. By Proposition 15, we can write

$$F(\alpha_1 + b_1) = F(\alpha_1) + F'(\alpha_1)b_1 + \frac{F''(\alpha_1)}{2!}b_1^2 + ... + \frac{F^{(n)}(\alpha_1)}{n!}b_1^n.$$

The first two terms sum to 0, and $\frac{F^{(j)}(\alpha_1)}{j!} \in \mathbb{Z}_p$. The non-archimedean property yields

$$|F(\alpha_1 + b_1)|_p \leq \max_{j\geq 2} \left|\frac{F^{(j)}(\alpha_1)}{j!}b_1^j\right|_p \leq \max_{j\geq 2} \left|b_1^j\right|_p.$$

Since $|b_1|_p < 1$, $|b_1^j|_p < |b_1^2|_p$ for all $j > 2$. Thus, $|b_1^2|_p \geq \max_{j\geq 2} \left|\frac{F^{(j)}(\alpha_1)}{j!}b_1^j\right|_p$, and we write

$$|F(\alpha_1 + b_1)|_p \leq |b_1^2|_p = \left|\frac{F(\alpha_1)^2}{F'(\alpha_1)^2}\right|_p = \frac{|F(\alpha_1)|_p^2}{|F'(\alpha_1)|_p^2} < \frac{|F(\alpha_1)|_p^2}{|F(\alpha_1)|_p} = |F(\alpha_1)|_p.$$

Similarly, we have

$$|F'(\alpha_1 + b_1) - F'(\alpha_1)|_p \leq |b_1|_p < \frac{|F'(\alpha_1)|_p^2}{|F'(\alpha_1)|_p} = |F'(\alpha_1)|_p. \tag{1}$$

Recall that for a non-archimedean absolute value, $|x|_p \neq |y|_p$ implies $|x + y|_p = \max\{|x|_p, |y|_p\}$. By (1), we have that

$$|F'(\alpha_1 + b_1)|_p = |F'(\alpha_1 + b_1) - F'(\alpha_1) + F'(\alpha_1)|_p = |F'(\alpha_1)|_p.$$

So we have that α_1 and b_1 satisfy $|F(\alpha_1 + b_1)|_p < |F(\alpha_1)|_p$ and $|F'(\alpha_1 + b_1)|_p = |F'(\alpha_1)|_p$.

Now we define $\alpha_{n+1} = \alpha_n + b_n$, where $b_n = -\frac{F(\alpha_n)}{F'(\alpha_n)}$, and we suppose that $|F(\alpha_n)|_p < |F'(\alpha_n)|_p^2$. By similar calculations to the above, we have that

$$\begin{aligned} |F'(\alpha_n + b_n) - F'(\alpha_n)|_p &= |F'(\alpha_n) - F'(\alpha_n) + F''(\alpha_n)b_n + \ldots|_p \\ &\leq \max_{j\geq 2} \left| \frac{F^{(j)}(\alpha_n)}{(j-1)!} b_n^{j-1} \right|_p \\ &= |b_n|_p \\ &< |F'(\alpha_n)|_p, \end{aligned}$$

and therefore, $|F'(\alpha_n + b_n)|_p = |F'(\alpha_n)|_p$. In addition, since $F(\alpha_n) + b_n F'(\alpha_n) = 0$, we can write

$$|F(\alpha_n + b_n)|_p \leq \max_{j\geq 2} \left| \frac{F^{(j)}(\alpha_n)}{j!} b_n^j \right|_p \leq |b_n^2|_p = \frac{|F(\alpha_n)|_p^2}{|F'(\alpha_n)|_p^2} < |F(\alpha_n)|.$$

By induction, we now have a sequence of elements (α_n) such that for every α_n, $|F'(\alpha_n)|_p = |F'(\alpha_1)|_p$ and $|F(\alpha_{n+1})|_p < |F(\alpha_n)|_p$. Note that this second condition implies

$$|F(\alpha_n)|_p \leq \frac{1}{p}|F(\alpha_{n-1})|_p \leq \frac{1}{p^2}|F(\alpha_{n-2})|_p \leq \ldots \leq \frac{1}{p^{n-1}}|F(\alpha_1)|_p \leq \frac{1}{p^n}.$$

If we choose $\varepsilon > 0$, it is clear that there exists $n \in \mathbb{N}$ such that $\frac{1}{p^n} < \varepsilon$. Thus, for this same n, $|F(\alpha_n) - 0|_p < \varepsilon$, so by the limit definition, $\lim_{n\to\infty} F(\alpha_n) = 0$.

Now observe

$$|\alpha_{n+1} - \alpha_n|_p = |b_n|_p = \left| \frac{F(\alpha_n)}{F'(\alpha_n)} \right|_p = \frac{|F(\alpha_n)|_p}{|F'(\alpha_1)|_p}.$$

Since $|F'(\alpha_1)|_p$ is a constant, our above work with $F(\alpha_n)$ yields $\lim_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p = 0$. By Lemma 6, (α_n) is a Cauchy sequence, and a limit $\alpha \in \mathbb{Z}_p$ exists. Therefore, we have found $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$. □

Remark. Note carefully that $|F(\alpha_n)|_p$ and $\frac{1}{p^n}$ are real numbers in this context whereas $F(\alpha_n)$ is a p-adic number. The limit definition still applies to p-adic numbers, but when we speak of the limit of $F(\alpha_n)$, we speak of the p-adic limit as opposed to the real limit of $|\alpha_{n+1} - \alpha_n|_p$. This is an important distinction, for while the real limit of the sequence $(\frac{1}{p^n})$ is 0, the p-adic limit of $(\frac{1}{p^n})$ does not exist.

This form of Hensel's Lemma will be necessary later in this paper, but Gouvêa lists a weaker version which is easier to apply in certain contexts (1997). We state this version below.

Corollary 17 (Weak Hensel's Lemma). Let $F(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. Suppose that there exists $\alpha_1 \in \mathbb{Z}_p$ such that

$$F(\alpha_1) \equiv 0 \pmod{p} \qquad \text{and} \qquad F'(\alpha_1) \not\equiv 0 \pmod{p},$$

where $F'(X)$ is the formal derivative of $F(X)$. Then there exists $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$.

Proof. Observe:

$$F'(\alpha) \not\equiv 0 \pmod{p} \Leftrightarrow v_p(F'(\alpha)) \leq 0 \Leftrightarrow -v_p(F'(\alpha)) \geq 0 \Leftrightarrow |F'(\alpha)|_p \geq 1$$

and

$$F(\alpha) \equiv 0 \pmod{p} \Leftrightarrow v_p(F(\alpha)) > 0 \Leftrightarrow |F(\alpha)|_p < 1.$$

Thus, $|F(\alpha)|_p < |F'(\alpha)|_p^2$, and by Theorem 16, there exists $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$. □

Remark. For brevity's sake, we will henceforth use the term "Hensel's Lemma" for these two results interchangeably unless the context requires clarification.

Example. For which p is $\frac{1}{2}$ a p-adic integer? We can determine this by applying Hensel's Lemma to the polynomial $F(X) = 2X - 1$. Note that we cannot apply Hensel's Lemma to this function if $p = 2$ because $2x - 1 \equiv -1 \not\equiv 0 \pmod 2$. Consider, then, $p \neq 2$. Then $p + 1$ is an even number, and therefore, $\frac{p+1}{2} \in \mathbb{Z}_p$. Observe

$$F\left(\frac{p+1}{2}\right) = 2\left(\frac{p+1}{2}\right) - 1 = p + 1 - 1 \equiv 0 \pmod p.$$

Further, $F'(\frac{p+1}{2}) = 2 \not\equiv 0 \pmod p$. Therefore, by Hensel's Lemma, there exists a p-adic integer which solves this equation, and this implies that $\frac{1}{2}$ is a p-adic integer for all $p \neq 2$. Of course, we already know this since for $p \neq 2$ we have $|\frac{1}{2}|_p = p^{-[v_p(1)-v_p(2)]} = p^0 = 1$, and in this way, we can also find that $|\frac{1}{2}|_2 = 2^1 = 2 \geq 1$, implying that 2 is not a 2-adic integer. However, this example demonstrates the power of Hensel's Lemma as a computational tool.

This result provides an effective method of determining whether or not *any* polynomial has a root in a given $\mathbb{Z}_p$, an ability essential to making use of the local-global principle.

The Local-Global Principle and Applications

The reason that Hensel's lemma is such a valuable tool with regards to the local-global principle is that there are situations where the local-global principle does hold. This section details some examples of situations in which the local-global principle either applies or fails. We will begin with the former.

Hasse-Minkowski

The Hasse-Minkowski Theorem is perhaps the best example of a circumstance in which the local-global principle reliably applies. Although its application is restricted to one type of equation, it still has quite a bit of power. A similar version of the following statement of the

theorem can be found in Gouvêa (1997).

Theorem 18 (Hasse-Minkowski). Let $F(X_1, X_2, ..., X_n) \in \mathbb{Q}[X_1, X_2, ..., X_n]$ be a quadratic form (a homogeneous polynomial of degree 2 in n variables). The equation

$$F(X_1, X_2, ..., X_n) = 0$$

has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{R}$ and $\mathbb{Q}_p$ for each p.

Note that the forward direction of this theorem is immediate: because of the inclusion of $\mathbb{Q}$ into $\mathbb{Q}_p$, a rational solution implies a solution in every $\mathbb{Q}_p$ and in $\mathbb{R}$. The proof of the other direction is beyond the scope of this paper, but its application is much simpler to grasp. In order to discover whether or not a rational solution exists, we must determine whether or not solutions exist in $\mathbb{Q}_p$, and we have already seen these types of problems in specific $\mathbb{Q}_p$. However, in order to tackle an application of Hasse-Minkowski, we need two lemmas from Gouvêa (1997).

Lemma 19. For any $n \in \mathbb{Z}$ such that $0 \leq n < p-1$, the following holds:

$$\sum_{x=0}^{p-1} x^n \equiv 0 \pmod{p}.$$

Proof. Note first that for $n = 0$, we obtain $1 + 1 + ... + 1 = p \equiv 0 \pmod{p}$. Also note that this takes care of the case $p = 2$ since we require that $n < p - 1$.

Now let $1 \leq n < p - 1$. We first recall Lagrange's Theorem, which states that a polynomial of degree n has at most n solutions modulo p for p a prime (Hardy & Wright, 1979). Since $n < p - 1$, there exist at most $p - 2$ incongruent solutions to the congruence $x^n - 1 \equiv 0 \pmod{p}$, and therefore, at least two elements of $\mathbb{Z}/p\mathbb{Z}$ are not solutions. We will choose $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that a is one of these non-solutions.

Now recall that $\mathbb{Z}/p\mathbb{Z}$ under addition is a cyclic group, and note that p and a are relatively prime. In addition, since $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, which is a cyclic group under multiplication, $a^n \in (\mathbb{Z}/p\mathbb{Z})^\times$. Accordingly, $\sigma_a : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ defined by $\sigma_a(x) = ax$ for all $x \in \mathbb{Z}/p\mathbb{Z}$ is an automorphism (Dummit & Foote, 2004). Therefore, since $0, 1, ..., p-1$ are all distinct modulo p, we have that $a(0), a(1), ..., a(p-1)$ are also all distinct modulo p, and this means that

$$\sum_{x=0}^{p-1} x^n \equiv \sum_{x=0}^{p-1} (ax)^n \pmod{p}.$$

Observe

$$(a^n - 1)\sum_{x=0}^{p-1} x^n = \sum_{x=0}^{p-1} (ax)^n - \sum_{x=0}^{p-1} x^n \equiv 0 \pmod{p}.$$

Now since we chose a such that $a^n - 1 \not\equiv 0 \pmod{p}$, we must have

$$\sum_{x=0}^{p-1} x^n \equiv 0 \pmod{p}.$$

□

Lemma 20. Let $p \neq 2$ be prime, and let $a, b, c \in \mathbb{Z}$ be relatively prime with $p \nmid abc$. Then there exist $x_0, y_0, z_0 \in \mathbb{Z}$, not all divisible by p, such that

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{p}.$$

Proof. Since we are working modulo p, we have p^3 options for (x_0, y_0, z_0). We will attempt to count how many of these p^3 options are solutions to the congruence. Recall Fermat's Little theorem, which states that for any prime p, $k^{p-1} \equiv 1 \pmod{p}$ for all $k \in \mathbb{Z}$ (Dummit & Foote, 2004). With this result, for any 3-tuple (x_0, y_0, z_0) we can write

$$(ax_0^2 + by_0^2 + cz_0^2)^{p-1} \equiv \begin{cases} 1 \pmod{p} & (x_0, y_0, z_0) \text{ not a solution} \\ 0 \pmod{p} & (x_0, y_0, z_0) \text{ a solution.} \end{cases}$$

This means that we can write the number N of non-solutions as

$$N \equiv \sum_{(x,y,z)} (ax^2 + by^2 + cz^2)^{p-1} \pmod{p}$$

where $\sum_{(x,y,z)}$ means that there are exactly p^3 summands, one for each (x_0, y_0, z_0). Expanding this expression using the multinomial theorem, we obtain

$$N \equiv \sum_{(x,y,z)} \left(\sum_{k_1+k_2+k_3=p-1} \binom{p-1}{k_1, k_2, k_3} x^{2k_1} y^{2k_2} z^{2k_3} \right) \pmod{p},$$

which we can rewrite as

$$N \equiv \sum_{k_1+k_2+k_3=p-1} \binom{p-1}{k_1, k_2, k_3} \left(\sum_{(x,y,z)} x^{2k_1} y^{2k_2} z^{2k_3} \right) \pmod{p}.$$

Since $k_1 + k_2 + k_3 = p - 1$, it must be true for every $\sum_{(x,y,z)} x^{2k_1} y^{2k_2} z^{2k_3}$ that $2k_t < p - 1$ for some $t \in \{1, 2, 3\}$. Otherwise $2(k_1 + k_2 + k_3) \geq 3(p - 1)$, which is a contradiction. We can therefore split up the above sum as $N \equiv \sum_1 + \sum_2 + \sum_3 \pmod{p}$, where $\sum_1$ sums only terms for which $2k_1 < p - 1$, $\sum_2$ sums terms where $2k_1 \geq p - 1$ and $2k_2 < p - 1$, and $\sum_3$ sums the remaining terms for which only $2k_3 < p - 1$.

Consider $\sum_1$. By Lemma 19 and the fact that $2k_1 < p - 1$, we can observe that

$$\begin{aligned}
\sum\nolimits_1 &\equiv \sum_{k_1+k_2+k_3=p-1} \binom{p-1}{k_1, k_2, k_3} \left(\sum_{(x,y,z)} x^{2k_1} y^{2k_2} z^{2k_3} \right) \\
&\equiv \sum_{k_1+k_2+k_3=p-1} \binom{p-1}{k_1, k_2, k_3} \left(\sum_{(y,z)} y^{2k_2} z^{2k_3} \left(\sum_{x=1}^{p-1} x^{2k_1} \right) \right) \\
&\equiv \sum_{k_1+k_2+k_3=p-1} \binom{p-1}{k_1, k_2, k_3} \left(\sum_{(y,z)} y^{2k_2} z^{2k_3} (0) \right) \equiv 0 \pmod{p}.
\end{aligned}$$

Thus, $\sum_1 \equiv 0 \pmod{p}$. However, a similar inspection of $\sum_2$ and $\sum_3$ show the same result. Thus, we have that $N \equiv 0 \pmod{p}$, or in other words, N is divisible by p.

Now since the number of non-solutions is divisible by p, it must be that the number S of solutions is divisible by p as well since these two numbers sum to p^3. However, consider that one of the p^3 options for (x_0, y_0, z_0) is $(0,0,0)$, which is certainly a solution. Thus, $S > 0$, and the fact that $p \mid S$ then implies that $S > 1$ since 1 is not prime. Therefore, there is a solution other than $(0,0,0)$, and that solution must be non-trivial. □

This result is powerful in our context. Hensel's Lemma requires only that the equation has a solution modulo p, so Lemma 20 enables us to prove the existence of solutions for infinitely many p-adic fields, requiring us only to check $\mathbb{Q}_p$ for p dividing a coefficient of the equation. We will now demonstrate this idea through an example, found in Hatley (2009), of the Hasse-Minkowski Theorem in action.

Example. Does the equation $5X^2 + 7Y^2 - 13Z^2 = 0$ have any non-trivial rational solutions?

Note that $(\sqrt{5 \cdot 7}, 12, \sqrt{13 \cdot 7})$ is a real solution, so we now only have to deal with $\mathbb{Q}_p$. We will take the cases $p = 2, 5, 7, 13$ individually from all other p.

Let $p \nmid 2 \cdot 5 \cdot 7 \cdot 13$. Since the coefficients of this equation are distinct primes, Lemma 20 gives us that there exists $x_0, y_0, z_0 \in \mathbb{Z}$ such that $5x_0^2 + 7y_0^2 - 13z_0^2 \equiv 0 \pmod{p}$. In addition, we know that at least one of these integers is not divisible by p. It is no loss of generality to assume that $p \nmid x_0$, and accordingly, we let $F(X) = 5X^2 + 7y_0^2 - 13z_0^2$ and observe that $F(x_0) \equiv 0 \pmod{p}$. In addition, since $p \nmid 2 \cdot 5 \cdot x_0$, we have that $F'(x_0) = 10x_0 \not\equiv 0 \pmod{p}$. Thus, by Hensel's Lemma, a solution x_0 exists for $F(X)$, and since p was any prime not equal to $2, 5, 7$, or 13, we now have only four primes left to check.

Let $p = 2$. If $Y = 0$ and $Z = 1$, then we have $F(X) = 5X^2 - 13$ and $F'(X) = 10X$. Testing

$X = 1$, we obtain

$$|5(1^2) - 13|_2 = |-8|_2 = \frac{1}{8} < \frac{1}{4} = |10(1)|_2.$$

Thus, Hensel's Lemma tells us that a 2-adic solution exists for $F(X)$.

Let $p = 5$. If $X = 0$ and $Z = 1$, then we have $F(Y) = 7Y^2 - 13$ and $F'(Y) = 14Y$. If we let $Y = 7$, then we obtain

$$F(7) = 330 \equiv 0 \pmod 5 \qquad \text{and} \qquad F'(7) = 98 \not\equiv 0 \pmod 5.$$

Hensel's Lemma then gives a solution for $F(Y)$, and thus, a 5-adic solution exists.

Let $p = 7$. If $Y = 0$ and $Z = 1$, then we have $F(X) = 5X^2 - 13$ and $F'(X) = 10X$. Letting $X = 2$, we get

$$F(2) = 7 \equiv 0 \pmod 7 \qquad \text{and} \qquad F'(2) = 20 \not\equiv 0 \pmod 7.$$

By Hensel's Lemma, there is a 7-adic solution.

Let $p = 13$. If $X = 5$ and $Z = 0$, then $F(Y) = 45 + 7Y^2$ and $F'(Y) = 14Y$. $Y = 1$ gives us

$$F(1) = 52 \equiv 0 \pmod{13} \qquad \text{and} \qquad F'(1) = 14 \not\equiv 0 \pmod{13},$$

so Hensel's Lemma yields a 13-adic solution.

We have found a solution for all p-adic fields and the real numbers, and thus, by the Hasse-Minkowski Theorem, we know that a rational solution to this quadratic form exists.

Selmer's Counterexample

Since the local-global principle applies to any quadratic form, it is natural to then ask whether it applies to higher order equations. The following counterexample from mathematician

Ernst Selmer (as cited in Conrad, n.d.-c) demonstrates that the local-global principle does not work so nicely with other types of polynomials.

Theorem 21. The equation $3X^3 + 4Y^3 + 5Z^3 = 0$ has only the zero solution over $\mathbb{Q}$, but there is a nonzero solution over every completion $\mathbb{Q}_p$ and over $\mathbb{R}$.

Proof. Note first that $(\sqrt[3]{3}, \sqrt[3]{4}, -\sqrt[3]{5})$ is a solution to the equation in $\mathbb{R}$. We now address $\mathbb{Q}_p$, using a method of proof from Keith Conrad's *The Local-Global Principle* (n.d.-c).

First, we will look at the requirements for an element of $\mathbb{Z}_p$ to be a cube. The original form of Hensel's Lemma gives us that for $F(X) = X^3 - \alpha$, the existence of $\beta \in \mathbb{Z}_p$ such that $|\beta^3 - \alpha|_p < |3\beta^2|_p \leq |3|_p^2$ will imply that a solution exists for $F(X)$, and thus, that α is a cube in $\mathbb{Z}_p$.

Now let $p = 2$. If $X = 1$ and $Y = 0$, then the equation becomes $Z^3 = -\frac{3}{5}$. Then $\beta = 1$ yields $|1^3 + \frac{3}{5}|_2 = |\frac{8}{5}|_2 = \frac{1}{8} < 1 = |3|_2^2$. Thus, by Hensel's Lemma, there exists a cubic root of $-\frac{3}{5}$, and we have a nontrivial 2-adic solution.

Let $p = 3$. If $X = 0$ and $Y = 1$, then $Z^3 = -\frac{4}{5}$. Setting $\beta = 4$, we get $|4^3 + \frac{4}{5}|_3 = |\frac{324}{5}|_3 = \frac{1}{81} < \frac{1}{9} = |3|_3^2$. Hensel's Lemma tells us the cube root of $-\frac{4}{5}$ exists, and therefore, a 3-adic solution exists.

For $p = 5$, if $Z = 0$ and $X = 1$, we have $Y^3 = -\frac{3}{4}$. Letting $\beta = 7$, we obtain $|7^3 + \frac{3}{4}|_5 = |\frac{1375}{4}|_5 = \frac{1}{125} < 1 = |3|_5^2$. Thus, by Hensel's Lemma, the cubic root of $-\frac{3}{4}$ exists, and we have a 5-adic solution.

Now let $p \geq 7$ be prime, noting that this means 3 and 5 are not congruent to 0 modulo p. Recall that the group $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) - \{0\}$ is a multiplicative cyclic group of order $p - 1$. We will inspect how many cubes exist in this group by observing the endomorphism

$\Phi_3 : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ defined by $\Phi_3(a) = a^3$ for $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.

First suppose that $p \not\equiv 1 \pmod 3$. By Lagrange's Theorem from group theory, the order of each element must divide the order of $(\mathbb{Z}/p\mathbb{Z})^\times$ (Dummit & Foote, 2004), which is $p-1$, so because 3 does not divide $p-1$, there exist no elements of order 3. This implies that $\ker \Phi_3 = \{a \in (\mathbb{Z}/p\mathbb{Z})^\times : |a| = 1\} = \{1\}$. By the First Isomorphism Theorem,

$$\mathrm{Im}(\Phi_3) \cong (\mathbb{Z}/p\mathbb{Z})^\times / \{1\} = (\mathbb{Z}/p\mathbb{Z})^\times,$$

and thus, every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cube. Now clearly 3 has an inverse $\frac{1}{3}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, and since every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cube, we have that $\frac{1}{3}$ is a cube. This means that $X^3 - \frac{1}{3} \equiv 0 \pmod p$ has a solution, and by Hensel's Lemma, there exists $x \in \mathbb{Z}_p$ such that $x^3 = \frac{1}{3}$. Therefore, $(x, 1, -1)$ is a solution to $3X^3 + 4Y^3 + 5Z^3 = 0$.

Now suppose that $p \equiv 1 \pmod 3$. Note that if there exists $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $k^3 = 3$, then $(k^{-1})^3 = \frac{1}{3}$. Thus, $\frac{1}{3}$ is a cube, and by the above work there exists a solution to Selmer's equation. Assume then that 3 is not a cube. It is quite clear that the image $\mathrm{Im}(\Phi_3)$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$, and furthermore, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is abelian, $\mathrm{Im}(\Phi_3)$ is a normal subgroup. Again, the First Isomorphism Theorem provides that $\mathrm{Im}(\Phi_3) \cong (\mathbb{Z}/p\mathbb{Z})^\times / \ker \Phi_3$, and we can then write $|\mathrm{Im}(\Phi_3)| = |(\mathbb{Z}/p\mathbb{Z})^\times / \ker \Phi_3| = \frac{|(\mathbb{Z}/p\mathbb{Z})^\times|}{|\ker \Phi_3|}$ by Lagrange's Theorem (Dummit & Foote, 2004). Rewriting the equation and again applying Lagrange obtains $|(\mathbb{Z}/p\mathbb{Z})^\times / \mathrm{Im}(\Phi_3)| = |\ker \Phi_3|$. Now $\ker \Phi_3 = \{a \in (\mathbb{Z}/p\mathbb{Z})^\times : |a| = 1, 3\}$, which clearly contains 1. Because 3 is prime and divides $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$, Cauchy's Theorem provides that there is at least one element of order 3 in $(\mathbb{Z}/p\mathbb{Z})^\times$ as well (Dummit & Foote, 2004). However, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, which implies that $(\mathbb{Z}/p\mathbb{Z})^\times$ has $\varphi(3) = 2$ elements of order 3 (Dummit & Foote, 2004), and thus,

$|\ker \Phi_3| = |(\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{Im}(\Phi_3)| = 3$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, $(\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{Im}\Phi_3$ is a cyclic group of order 3 with coset representatives $\{1, 3, 9\}$. Thus, for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have that $a \equiv b^3 \pmod p$, $a \equiv 3b^3 \pmod p$, or $a \equiv 9b^3 \pmod p$. We will now consider $a = 5$.

First, suppose $5 \equiv b^3 \pmod p$ for some $b \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then by Hensel's Lemma, 5 is a cube, so taking $y \in \mathbb{Z}_p$ such that $y^3 = 5$, we have that $(y, -y, 1)$ is a solution to Selmer's equation.

Next, suppose $5 \equiv 3b^3 \pmod p$ for some $b \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then by Hensel's Lemma, $\frac{5}{3}$ is a cube, so taking $y \in \mathbb{Z}_p$ such that $y^3 = \frac{5}{3}$, we have that $(y, 0, -1)$ solves Selmer's equation.

Finally, suppose $5 \equiv 9b^3 \pmod p$ for some $b \in (\mathbb{Z}/p\mathbb{Z})^\times$. Multiplying both sides of the congruence by 3, we find by Hensel's Lemma that 15 is a cube in $\mathbb{Z}_p$. Letting $y \in \mathbb{Z}_p$ such that $y^3 = 15$, we have that $(3y, 5, -7)$ solves Selmer's equation.

Combining the above, we have that for any prime p there exists a solution in $\mathbb{Q}_p$ as well as in $\mathbb{R}$ for the equation $3X^3 + 4Y^3 + 5Z^3 = 0$. However, although it is beyond the scope of this paper, it can be proven that $(0, 0, 0)$ is the only rational solution to this equation. Thus, we have that the restriction of the Hasse-Minkowski Theorem to quadratic forms is necessary, for the theorem does not apply to cubic forms in general. □

Conclusion

Clearly, the local-global principle is not universal, but this prompts a more interesting question. Why is it that Hasse-Minkowski works with homogeneous second-order diophantine equations? Given that the local-global principle does not apply to cubic equations or to integer solutions of equations, it is fascinating that a situation exists in which the principle applies consistently. The very existence of Hasse-Minkowski merits further research into potential applications of the local-global principle in other contexts.

References

Aitken, W., & Lemmermeyer, F. (n.d.). Counterexamples to the Hasse principle: An elementary introduction [PDF]. Retrieved from https://public.csusm.edu/aitken_html/m372/diophantine.pdf.

Bachman, G. (1964). *Introduction to p-adic numbers and valuation theory*. New York-London: Academic Press.

Bartle, R. G., & Sherbert, D. R. (2011). *Introduction to real analysis* (4th ed.). Hoboken, NJ: John Wiley & Sons, Inc.

Carlitz, L. (1952). Primitive roots in a finite field. *Transactions of the American Mathematical Society*, *73*, 373–382. doi:10.2307/1990797

Cassels, J. W. S. (1986). *Local fields*. Cambridge, UK: Cambridge University Press.

Cohen, H. (2007). *Number theory. vol. i. tools and Diophantine equations*. New York, NY: Springer.

Conrad, K. (n.d.-a). Counterexample to the local-global principle [PDF]. Retrieved from https://pdfs.semanticscholar.org/0845/647bdc32652b79367eb8e752b62f734d9dad.pdf.

Conrad, K. (n.d.-b). Hensel's lemma [PDF]. Retrieved from http://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf.

Conrad, K. (n.d.-c). The local global principle [PDF]. Retrieved from http://kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf.

Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (3rd ed.). Hoboken, NJ: John Wiley & Sons, Inc.

Gamzon, A. (2006). The Hasse-Minkowski theorem [PDF]. Retrieved from https://opencommons.uconn.edu/cgi/viewcontent.cgi?article=1017context&=srhonors_theses.

Gouvêa, F. Q. (1997). *p-adic numbers: An introduction* (2nd ed.). Berlin: Springer-Verlag.

Hardy, G. H., & Wright, E. M. (1979). *An introduction to the theory of numbers* (5th ed.). New York, NY: Oxford University Press.

Hatley, J. (2009). Hasse-Minkowski and the local-to-global principle [PDF]. Retrieved from http://www.math.union.edu/~hatleyj/Capstone.pdf.

Koblitz, N. (1980). *p-adic analysis: A short course on recent work*. Cambridge, UK: Cambridge University Press.

Oleshchko, K., & Khrennikov, A. Y. (2017). On applications of *p*-adics to geophysics: Linear and quasilinear diffusion of a water-oil emulsion. *Teoreticheskaya i Matematicheskaya Fizika*, *190*(1), 179–190. doi:10.4213/tmf9142

Ralph, C. C., & Simanca, S. R. (2012). *Arithmetic differential operators over the p-adic integers*. Cambridge, UK: Cambridge University Press.

Robert, A. M. (2000). *A course in p-adic analysis*. New York, NY: Springer-Verlag.

Salzmann, H., Grundhöfer, T., Hähl, H., & Löwen, R. (2007). *The classical fields: Structural features of the real and rational numbers*. Cambridge, UK: Cambridge University Press.

Serre, J.-P. (1973). *A course in arithmetic*. New York-Heidelberg: Springer-Verlag.