THE LOCAL-GLOBAL PRINCIPLE

AARON BLUMENFELD

Abstract. The local-global principle establishes a one-to-one correspondence between solvability of quadratic forms in the rational numbers and the solvability of these forms in fields known as the p-adic numbers. In this paper, we introduce the p-adic numbers, state and prove the local-global principle, and discuss higher algebraic forms with respect to the local-global principle.

1. Introduction

Perhaps the most investigated area of number theory is whether or not an equation has diophantine solutions. Sometimes the most basic techniques of modular arithmetic and quadratic residues suffice to show that an equation has no diophantine solutions. A more difficult question is whether or not a given equation has rational solutions.

It may not be difficult to exhibit a particular rational solution if there is one; on the other hand, if one can factor the equation, for example, into linear factors and therefore find every real root, then show that no root is rational, then such an equation certainly has no rational solutions. In general, however, such questions in number theory are very difficult to approach.

In the early 20th century, Kurt Hensel introduced the p-adic numbers, motivated by ideas of Laurent series. He realized that one could extend such power series to series in powers of some prime, and the analogy is quite strong – many deep properties are shared. Specifically, a p-adic number is a number of the form $\sum_{n=-k}^{\infty} a_n p^n$ for some integer k and a fixed prime p (each a_n is a residue modulo p). The immediate question is whether such a definition makes sense – how can this series actually converge to a number if the powers of p increase without bound unless the coefficients become 0 at some point? Of course, such a series could never converge in the real numbers because the terms of the underlying sequence are increasing, but that's because of our standard of "closeness" – i.e., the Euclidean metric. If we view

this through what's known as the p-adic metric, then the higher powers of p become smaller and effectively vanish, allowing such a series to converge. One thing to realize is that this definition of the p-adic numbers is not totally rigorous. Specifically, they are what's known as the completion of the rational numbers with respect to the p-adic metric, just as the real numbers can be defined as the completion of the rational numbers with respect to the absolute value to which we're accustomed.

Once the theory of the p-adic numbers was sufficiently developed, the Hasse-Minkowski theorem, more commonly known as the local-global principle, was proved. This roughly states that a quadratic polynomial has rational solutions if and only if it has solutions in every p-adic field and in the real numbers. The rationals are the global field in this case; each p-adic field and the real numbers are the local fields. In this language, the theorem says that an equation has global solutions if and only if it has local solutions everywhere. Since the rationals are contained in every p-adic field and in the real numbers, necessity is rather obvious. That this is a sufficient condition for the existence of a rational solution is what's remarkable. An algebraic form is said to satisfy the Hasse principle (or the local-global principle) if this turns out to be true. It is true for quadratic forms; for higher forms, it is rare for a condition as strong as this one to be true, however.

In this paper, we provide an introduction to the p-adic numbers, state and prove the local-global principle for quadratic forms in three variables (for conics), and discuss the local-global principle with respect to higher algebraic forms, showing that the principle does not, in general, hold beyond quadratic forms.

2. p-adic Numbers

2.1. **p-adic Valuations and Norms.** Recall that an absolute value on $\mathbb{Q}$, the rational numbers, is a function $|\ |:\mathbb{Q}\to\mathbb{R}$ that satisfies the following three properties:
1) $|x|=0$ if and only if $x=0$
2) $|x\cdot y|=|x|\cdot|y|$ for all $x,y\in\mathbb{Q}$
3) $|x+y|\leq|x|+|y|$ for all $x,y\in\mathbb{Q}$

Additionally, an absolute value is said to be non-Archimedean if it satisfies $|x+y|\leq\max\{|x|,|y|\}$ for all $x,y\in\mathbb{Q}$. This is in fact equivalent to the statement that a norm is Archimedean if the natural numbers are unbounded in $\mathbb{Q}$ [2]. This statement of the condition, however, shows that in any (complete) non-Archimedean field (specifically, in the field of p-adic numbers), a sequence (a_n) is Cauchy (and therefore

convergent) as long as $\lim_{n\to\infty} |a_{n+1}-a_n| = 0$. Of course, this is not the case in the real numbers (just consider the partial sums of the harmonic series).

Also recall that a metric on $\mathbb{Q}$ is a function $d : \mathbb{Q} \to \mathbb{R}$ such that:
1) $d(x, y) \geq 0$ for all $x, y \in \mathbb{Q}$; furthermore, $d(x, y) = 0$ if and only if $x = y$
2) $d(x, y) = d(y, x)$ for all $x, y \in \mathbb{Q}$
3) $d(x, z) \leq d(x, y) + d(y, z)$ for all $x, y, z \in \mathbb{Q}$

It is easy to see that an absolute value naturally induces a metric d defined by $d(x, y) = |x - y|$.

The typical example of an absolute value is $|\ | : \mathbb{Q} \to \mathbb{R}$, where $|x|$ is the standard (Euclidean) absolute value on the real line. We now proceed to define the p-adic norm on the $\mathbb{Q}$. Before doing so, we define the p-adic valuation on $\mathbb{Z}$ for a fixed prime p.

Definition 2.1. We define the p-adic valuation $v_p : \mathbb{Z}\backslash\{0\} \to \mathbb{R}$ to be the unique nonnegative integer $v_p(n) = m$ such that $n = p^m \cdot n'$, where $p \nmid n'$.

This is simply the highest power of p that divides n. We also extend v_p to the rationals as follows. If $x = \frac{a}{b}$, then define $v_p(x) = v_p(a)-v_p(b)$. Note that a and b need not be relatively prime. For example, $v_7(329) = 1, v_3(18/36) = 2 - 2 = 0 = v_3(1/2)$.

Now we define the p-adic norm of any rational number:

Definition 2.2. If $x \in \mathbb{Q}$, then the p-adic norm of x is given by $|x|_p = p^{-v_p(x)}$. The convention is that $|0|_p = 0$ (sometimes $v_p(0)$ is set to be ∞ since we can always factor as many multiples of p out of 0 as we want and still get 0; this is consistent with $|0|_p = p^{-\infty} = 1/p^\infty = 1/\infty = 0$ if we think of "p^∞" in the usual way).

One of the most important properties to notice about $|\ |_p$ is that for n divisible by a large power of p, its image under the p-adic norm is small. This is important when considering p-adic numbers since they can (and usually do) have expansions with powers of p increasing without bound.

Note. From here on, we refer to the Euclidean absolute value as $|\ |_\infty$. This convention may seem dubious at first, but it is useful since we can now refer to the Euclidean absolute value as $|\ |_\infty$, and in the near future, we will be able to refer to $\mathbb{R}$ in the context of the p-adic world as $\mathbb{Q}_\infty$.

2.2. **p-adic Integers and Numbers.** We can formally define the p-adic numbers to be the completion of $\mathbb{Q}$ with respect to $|\ |_p$. Two Cauchy sequences are considered equivalent if their difference (with

respect to $|\ |_p$) tends to 0; the p-adic numbers can then be defined as the set of equivalence classes under this equivalence relation. Following through with this definition, however, would lead us too far astray from the goal of this paper, and, indeed, would not be very useful in understanding the p-adic numbers; such an excursion would only be of use for showing their existence. So we define the p-adic numbers in a more accessible (and equivalent) manner.

Definition 2.3. A p-adic integer is an infinite sum $\sum_{n=0}^{\infty} a_n p^n$, where each $a_n \in \{0, 1, 2, \ldots, p-1\}$. We denote the p-adic integers by $\mathbb{Z}_p$. We sometimes write $x \in \mathbb{Z}_p$ as $x = \ldots a_n \ldots a_2 a_1 a_0$.

We can think of this intuitively as a power series in powers of p. Note that this representation by the integers $a_0, a_1, \ldots, a_n, \ldots$ is unique – unlike in $\mathbb{R}$, where $0.99999\ldots = 1.00000\ldots$.

As mentioned before, most p-adic numbers have an infinite p-adic expansion. Which ones don't? These are simply the nonnegative integers, and their p-adic expansions are simply their expansions in base p.

Example 2.4. To compute the 11-adic expansion of 229, we divide the highest power of 11 possible into 229, find the quotient, subtract 11 times the quotient and repeat. Thus, $229 = 1 \cdot 11^2 + 9 \cdot 11^1 + 9 \cdot 11^0$. So we have found that the 11-adic expansion of 229 is $9 \cdot 11^0 + 9 \cdot 11^1 + 1 \cdot 11^2$. However, in order to emphasize the prime, it is often useful to write this as $9 + 9p + p^2$.

Now that we have the p-adic integers, it is time to define all the p-adic numbers.

Definition 2.5. A p-adic number is defined by an infinite series $\sum_{n=-k}^{\infty} a_n p^n$, where k is some nonnegative integer, possibly 0 (in fact, $-k$ is the p-adic valuation of the number). If $k > 0$, then the sum is a p-adic number, but not a p-adic integer (although we can multiply through by p^k and obtain a p-adic integer) unless, of course, $a_{-k} = a_{-k+1} = \ldots = a_{-1} = 0$. We denote the p-adic numbers by $\mathbb{Q}_p$. We sometimes write $x \in \mathbb{Q}_p$ as $x = \ldots a_n \ldots a_2 a_1 a_0 . a_{-1} \ldots a_{-k}$.

One thing to notice is that $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{Q}_p$, although $\mathbb{Q} \not\subset \mathbb{Z}_p (\frac{1}{p} \notin \mathbb{Z}_p$, for instance). One can find the expansion of a rational number (or integer) in $\mathbb{Q}_p$, or in the viewpoint of completing the rationals with

respect to the p-adic absolute value, it is clear that any rational number x is in $\mathbb{Q}_p$ by considering the constant Cauchy sequence (x).

Let us now consider a couple of more interesting examples of p-adic expansions.

Example 2.6. Here is a short proof that $\sqrt{2}$ is irrational. If

$$2 = \left(\frac{1}{5^k}a_{-k} + \ldots + \frac{1}{5}a_{-1} + a_0 + 5a_1 + 5^2a_2 + \ldots\right)^2$$

is a square of a rational number, then it is a square of a 5-adic number. Perhaps this need not be in $\mathbb{Z}_p$, but upon multiplication by 5^{2k}, we see that $2 \cdot 5^{2k}$ must be a p-adic *integer*. Then

$$2 \cdot 5^{2k} = (a_{-k} + \ldots + 5^{k-1}a_{-1} + 5^k a_0 + 5^{k+1}a_1 + 5^{k+2}a_2 + \ldots)^2.$$

Then $2 \cdot 5^{2k} \equiv 0 \equiv a_{-k}^2 \pmod 5$, so $a_{-k} \equiv 0 \pmod 5$. Since a_{-k} must be a residue modulo 5, it follows that $a_{-k} = 0$. Removing a_{-k} from the preceding equation allows us to conclude in the same way that for each a_i with $i < 0$, $a_i = 0$. Thus, 2 must be the square of a p-adic *integer*, so

$$2 = (a_0 + 5a_1 + 5^2a_2 + \ldots)^2.$$

It follows, then, that $2 \equiv a_0^2 \pmod 5$. But 2 is a quadratic non-residue modulo 5, so 2 is not a square in $\mathbb{Q}_5$, and consequently, $\sqrt{2} \notin \mathbb{Q}$. This is much more concise than the famous proof by contradiction, although it does use considerably more sophisticated results.

We now state Hensel's Lemma, as it will prove useful in several examples. We will restate it and prove it in section 2.4.

Theorem 2.7. *Suppose $f(x)$ is a polynomial with coefficients in $\mathbb{Z}_p$. If there exists $\alpha_1 \in \mathbb{Z}_p$ such that $f(\alpha_1) \equiv 0 \pmod p$ and $f'(\alpha_1) \not\equiv 0 \pmod p$, then $f(x)$ has a root in $\mathbb{Z}_p$ (in other words, we can lift α_1 to a solution modulo any power of p).*

Not only can we lift α_1 to a solution modulo any power of p, but if α_n is the solution $\pmod{p^n}$, then $\alpha_n \equiv \alpha_m \pmod{p^m}$ whenever $1 \leq m < n$. This notion of the lifted solutions being congruent to the previous solutions modulo lower powers of p defines a sequence of integers that is said to be (p-adically) *coherent*.

Example 2.8. On the other hand, we can show that $\mathbb{Q}_p$ is strictly bigger than $\mathbb{Q}$. For example, $f(x) = x^2 - 2 = 0$ is solvable in $\mathbb{Q}_7$. We can solve this by considering $x^2 \equiv 2 \pmod 7$. One solution is 3, so set $a_0 = 3$ (and $f'(3) = 6 \not\equiv 0 \pmod 7$). Then $x = 3 + 7k$, so consider

$$(3+7k)^2 \equiv 9+42k \equiv 2 \pmod{49}$$
$$\Rightarrow 42k \equiv 42 \pmod{49},$$

which gives $k = 1$. Thus, $x \equiv 10 \pmod{49}$. Continuing in this way, we construct a coherent sequence $(3, 10, 108, 2166, \ldots)$. Now $10 = 3 + 1 \cdot 7, 108 = 10 + 2 \cdot 7^2, 2166 = 108 + 6 \cdot 7^3, \ldots$. So $x = 3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 = \ldots 6213$ in $\mathbb{Z}_7$. This is, in fact, a 7-adic square root of 2. If we had taken our first number to be 4 instead of 3, we would have found the other 7-adic square root of 2.

Example 2.9. Let's compute $\frac{14}{8}$ in $\mathbb{Q}_5$. We do this by considering modular equations in powers of 5. We write

$$\frac{14}{8} = a_0 + 5a_1 + 25a_2 + 125a_3 + \ldots.$$

So $\frac{14}{8} \equiv 3 \equiv a_0 \pmod{5}$. So $a_0 = 3$ since in general, any $a_i \in \{0, 1, \ldots, p-1\}$. Now $\frac{14}{8} \equiv 8 \pmod{25}$. So $8 = a_0 + a_1 p \Rightarrow a_1 = 1$.

$$\frac{14}{8} \equiv 33 \pmod{125} \Rightarrow a_0 + a_1 p + a_2 p^2 = 3 + 1 \cdot 5 + 25 \Rightarrow a_2 = 1.$$

Similarly, we can find that $a_3 = 1$, $a_4 = 1, a_5 = 1$, and so on. So in $\mathbb{Q}_5$, $\frac{14}{8} = 3 + p + p^2 + p^3 + p^4 + p^5 + \ldots$. Since clearly $8 = 3 + p$, if we multiply out the expansion of $\frac{14}{8}$ by 8, we obtain

$$\begin{aligned}
&(3 + p + p^2 + p^3 + p^4 + p^5 + \ldots)(3 + p) \\
&= 9 + 6p + 4p^2 + 4p^3 + 4p^4 + 4p^5 + \ldots \\
&= (4 + p) + 6p + 4p^2 + 4p^3 + 4p^4 + 4p^5 + \ldots \\
&= 4 + (2p + 5p) + 4p^2 + 4p^3 + 4p^4 + 4p^5 + \ldots \\
&= 4 + 2p + (5p^2 + 4p^3) + 4p^4 + 4p^5 + \ldots \\
&= 4 + 2p + (5p^3 + 4p^4) + 4p^5 + \ldots \\
&= 4 + 2p + (5p^4 + 4p^5) + \ldots \\
&= 4 + 2p + 5p^5 + \ldots \\
&= 4 + 2p + \ldots \\
&= 4 + 2p,
\end{aligned}$$

which is the 5-adic expansion of 14. Note that we were able to rearrange the terms, observing that $p = 5$, so for example $5p^3 + 4p^4 = p^4 + 4p^4 = 5p^4$.

Example 2.10. Now let's compute the p-adic expansion of -6 in $\mathbb{Q}_{11}$. We proceed as before: $-6 \equiv 5 \pmod{11}$, so $a_0 = 5$. $-6 \equiv 115 \equiv 5 + 10 \cdot 11 \pmod{121}$, so $a_1 = 10$. Similarly, $a_2 = 10, a_3 = 10, a_4 = 10, a_5 = 10$, and so on. So $-6 = 5+10p+10p^2+10p^3+10p^4+10p^5+\ldots$. We can similarly check this computation by noting that the 11-adic expansion of 6 is simply 6, so

$$\begin{aligned} & -6+6 \\ &= 11 + 10p + 10p^2 + 10p^3 + 10p^4 + \ldots \\ &= 11p + 10p^2 + 10p^3 + 10p^4 + \ldots \\ &= 11p^2 + 10p^3 + 10p^4 + \ldots \\ &= 11p^3 + 10p^4 + \ldots \\ &= 11p^4 + \ldots \\ &= \ldots \\ &= 0. \end{aligned}$$

In fact, if the p-adic expansion of x is

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \ldots,$$

then

$$-x = (p-a_0) + (p-1-a_1)p + (p-1-a_2)p^2 + \ldots + (p-1-a_n)p^n + \ldots.$$

As a corollary, this gives the p-adic expansion of -1 to be

$$(p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \ldots + (p-1)p^n + \ldots.$$

Just as in the case of the real numbers, a p-adic number is rational if and only it is (eventually) periodic.

2.3. **Arithmetic in $\mathbb{Q}_p$.** In this section, we outline the basic algorithms for p-adic arithmetic [3]. Addition, subtraction and multiplication are more or less the same: proceed from right to left (when written in the form $x = a_n a_{n-1} \ldots a_2 a_1 a_0 . a_{-1} \ldots a_{-k}$). To divide, we also proceed from right to left.

For example, in $\mathbb{Q}_7$:

$$\begin{array}{rr} \ldots 30231.46 & \ldots 6142.05 \\ +\ldots 04024.14 & -\ldots 1642.06 \\ \hline = \ldots 34255.63 & = \ldots 4166.66 \end{array}$$

$$\begin{array}{r} \ldots \quad 263 \\ \times \ldots \quad 154 \\ \hline \ldots \quad 445 \\ \ldots \quad 141 \\ \ldots 263 \\ \hline \ldots \quad 455 \end{array}$$

$$\begin{array}{r|l} & \ldots 615 \\ \hline \ldots 153 & \ldots 421 \\ & \ldots 161 \\ \hline & \ldots 230 \\ & \ldots 153 \\ \hline & \ldots 400 \\ & \ldots 4 \\ \hline & \ldots \end{array}$$

Now we cap off this section by computing a p-adic square root.

Example 2.11. One might be prone to wonder if $\mathbb{Q}_p$ is simply a distorted view of $\mathbb{R}$. We will do away with any such doubt by showing that $x^2 + 1 = 0$ is solvable in $\mathbb{Q}_5$ (in fact, in $\mathbb{Z}_5$), whereas it is clearly unsolvable in $\mathbb{R}$. To find a square root, we approach this computation using the notation of Hensel's Lemma, which we prove in the next section.

We have $f(x) = x^2 + 1, f'(x) = 2x$.

$$f(x) \equiv 0 \pmod 5 \Rightarrow x^2 \equiv 4 \pmod 5,$$

which is solvable with a solution $\alpha_1 = 2$. Note that $f'(\alpha_1) = 4 \not\equiv 0 \pmod 5$. So by Hensel's Lemma, there exists a 5-adic square root of -1. If we set

$$f(\alpha_2) \equiv f(\alpha_1) + f'(\alpha_1)\beta_1 p \equiv 5(1 + 4\beta_1) \equiv 0 \pmod{25},$$

then this means that $f(\alpha_2) \equiv 1 + 4\beta_1 \equiv 0 \pmod 5$. This gives $\beta_1 = 1$. So $\alpha_2 = 2 + 1 \cdot 5$. Similarly,

$$f(\alpha_3) \equiv 25(2 + 14\beta_2) \equiv 0 \pmod{125} \Rightarrow f(\alpha_3) \equiv 2 + 4\beta_2 \pmod 5,$$

which gives $\beta_2 = 2$;

$$\text{f}(\alpha_4) \equiv 125(26 + 114\beta_3) \pmod{625} \Rightarrow f(\alpha_4) \equiv 1 + 4\beta_3 \pmod 5,$$

so that $\beta_3 = 1$. So

$$a = \alpha_1 + \beta_1 \cdot 5 + \beta_2 \cdot 5^2 + \beta_3 \cdot 5^3 + \ldots = 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + \ldots = \ldots 1212.$$

We could have also started with $\alpha_1 = 3$ and obtained a second square root.

2.4. **Hensel's Lemma.** In this section, we restate and prove Hensel's Lemma, which formally establishes the connection between solving equations modulo powers of primes and the p-adic expansions of numbers (i.e., the roots to polynomials with p-adic integer coefficients).

Theorem 2.12. *Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$ is a polynomial with coefficients in $\mathbb{Z}_p$. Further suppose there is an $\alpha_1 \in \mathbb{Z}_p$ that satisfies both $f(\alpha_1) \equiv 0 \pmod p$ and $f'(\alpha_1) \not\equiv 0 \pmod p$. Then there is a unique p-adic integer a such that $f(a) = 0$ and $a \equiv \alpha_1 \pmod p$.*

Note. What this theorem is essentially saying is that we can lift solutions modulo all powers of p, provided that $f'(\alpha_1) \not\equiv 0 \pmod p$, as we did in example 2.8.

Remark. By $f'(x)$, we of course mean the formal derivative: $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1$.

Proof. To prove this, we construct a sequence of integers that converges to a. Specifically, we construct a sequence $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$ that satisfies the following conditions for all $n \in \mathbb{N}$:
1) $f(\alpha_n) \equiv 0 \pmod{p^n}$
2) $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$

Note. The second condition simply means that (α_n) should be a coherent sequence.

We prove the existence of α_n for all $n \in \mathbb{N}$ by induction. By assumption, α_1 exists; this is our base case. Now supposing that some α_k exists, we show that α_{k+1} exists. To find α_{k+1}, since our sequence should be coherent, $\alpha_{k+1} = \alpha_k + \beta_k p^k$, where $\beta_k \in \mathbb{Z}_p$. Thus, should it exist, we obtain

$$\begin{aligned} f(\alpha_{k+1}) &= f(\alpha_k + \beta_k p^k) \\ &= \sum_{i=0}^{n} a_i(\alpha_k + \beta_k p^k)^i \\ &= \sum_{i=0}^{n} (a_i \alpha_k^i + i a_i \alpha_k^{i-1} \beta_k p^k + p^{2k} m), m \in \mathbb{Z}_p \\ &\equiv \sum_{i=0}^{n} a_i \alpha_k^i + \beta_k p^k \sum_{i=0}^{n} i a_i \alpha_k^{i-1} \pmod{p^{k+1}} \\ &= f(\alpha_k) + f'(\alpha_k)\beta_k p^k. \end{aligned}$$

Since $f(\alpha_k) \equiv 0 \pmod{p^k}$, we write $f(\alpha_k) = p^k l, l \in \mathbb{Z}_p$. Then we have $p^k l + f'(\alpha_k)\beta_k p^k \equiv 0 \pmod{p^{k+1}}$, or equivalently, $l + f'(\alpha_k)\beta_k \equiv 0 \pmod{p}$. Since by assumption $f'(\alpha_k) \not\equiv 0 \pmod{p}$, we can invert it modulo p, so β_k does exist and is, in fact, unique. So we set $\alpha_{k+1} = \alpha_k + \beta_k p^k$.

This completes the induction. So setting

$$a = \alpha_1 + \beta_1 p + \beta_2 p^2 + \ldots + \beta_n p^n + \ldots$$

finishes the proof. □

Hensel's Lemma is considered the p-adic analogue of Newton's method from real analysis because of the strategy of iterative approximation of a root. This lemma establishes the natural correspondence between solving equations modulo powers of p and solving equations in $\mathbb{Q}_p$.

2.5. **Basic Analysis in $\mathbb{Q}_p$.** Although the p-adic numbers are significantly different from the real numbers, they do in fact bear many similarities – they are both normed fields and complete metric spaces. In fact, one deeper similarity is that the concepts from calculus can be extended to the p-adic numbers.

In this section, we discuss the basics of analysis in $\mathbb{Q}_p$. In a certain sense, limits (of sequences) are quite similar, but of course the notion of "closeness" (i.e., $\epsilon - \delta$ definitions) comes through the metric induced by the p-adic absolute value, not through the metric induced by the Euclidean absolute value. The fact that this metric is non-Archimedean implies that checking the convergence of an infinite series is equivalent to checking the convergence of the underlying sequence, so most of p-adic analysis lies in the theory of power series.

The theory of derivatives in the p-adic world is developed, but defining functions as power series is much more powerful in this context. This is because the analogues of the intermediate value theorem and the mean value theorem don't exist (technically, there is an intermediate value theorem for $\mathbb{Q}_p$, but it is far less interesting).

Integration in the p-adics is a much trickier subject and is beyond the scope of this paper. The p-adic numbers are not an ordered field and are non-Archimedean, which means that there is no concept of an interval or a curve. The theory of p-adic integration lies in the concepts of p-adic distributions, measures, and limits of Riemann sums; it even requires considering $\mathbb{C}_p$, the completion of the algebraic closure of $\mathbb{Q}_p$ (as $\mathbb{Q}_p$ is not algebraically closed, and its algebraic closure, $\bar{\mathbb{Q}}_p$, is not complete) [4].

2.5.1. *Sequences and Series.* As mentioned above, a sequence (x_n) in $\mathbb{Q}_p$ is Cauchy (i.e., convergent since we're working in a complete metric space) if and only if $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$. This is simply because the p-adic numbers are non-Archimedean, so it suffices to check the limit of the underlying sequence to check the convergence of a series.

Recalling that the metric we're working with is $d(x, y) = |x - y|_p = 1/p^{v_p(x-y)}$, high powers of p are "small" and small powers of p are "large." With this in mind, it follows that $\lim_{n\to\infty} n! = \lim_{n\to\infty} p^n = 0$, while $\lim_{n\to\infty} n$ and $\lim_{n\to\infty} 1/n$ diverge.

The condition for convergence of a series also gives a nice bound on the actual sum: $\left|\sum_{n=0}^{\infty} x_n\right| \leq \sup\{|x_0|, |x_1|, \ldots, |x_n|, \ldots\}$.

Most basic results about convergence of series in $\mathbb{R}$ also apply to the p-adic case. The difference with p-adic series is the *extra* non-Archimedean property, giving us another angle from which to attack sequences and series.

One more surprising result about p-adic series is that, unlike in the real case, convergence implies unconditional convergence.

2.5.2. *Derivatives.* Just as when working with sequences in $\mathbb{Q}_p$, definitions of continuity and derivatives remain unchanged except that the notion of "closeness" is determined by the p-adic metric. In this light, derivatives are similar to their real-valued analogues. So we can still apply the power rule, the chain rule, and so on.

There are two problems to address, however. In differential calculus, the two main theorems are the intermediate value theorem and the mean value theorem.

The intermediate value theorem is proved more generally than in the real numbers by considering the image of a connected set under a continuous function. The problem with this in $\mathbb{Q}_p$ is that the p-adic numbers are totally disconnected – the connected components of $\mathbb{Q}_p$ are the one-element subsets. So while the intermediate value theorem is still true, it doesn't give us any useful or interesting information.

When considering a p-adic version of the mean value theorem, we again run into the trouble that $\mathbb{Q}_p$ is not an ordered field, so there is no meaning to the statement "$a < b$." In fact, just because two p-adic functions have the same derivative does not mean that they differ by a constant, as the case is in the real numbers. For this reason, when considering analysis in the p-adic numbers, it is much nicer to work with power series.

2.5.3. *Power Series.* One reason to define functions by power series in $\mathbb{Q}_p$ is that it is possible to prove a p-adic mean value theorem. Indeed, if two functions defined by power series have the same derivative, then they do differ by a constant. Thus, it is plain that working with power series in the p-adic world solves a number of issues.

Much of the theory of power series is a natural transition from $\mathbb{R}$. For example, consider a power series

$$f(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Most of the same methods in finding the region of convergence work just as in the Archimedean case, but one thing that is rather surprising is that in order to check the boundary cases, we only have to check

one case, as this gives us information about every boundary case. In other words, if the radius of convergence is denoted by r, then whenever $|x|_p < r$, the series converges, and whenever $|x|_p > r$, it diverges. To deal with the boundary cases, suppose there is some $\alpha \in \mathbb{Q}_p$ so that $|\alpha|_p = r$. Then $\sum_{n=0}^{\infty} a_n \alpha^n$ converges if and only if $\sum_{n=0}^{\infty} a_n \beta^n$ for all $\beta \in \mathbb{Q}_p$ with $|\beta|_p = r$.

One other anomaly is that if a function defined by a power series is periodic, then it must be a constant function. This is quite different from real analysis, in which the basic trigonometric functions are periodic (and clearly not constant).

Many other familiar results from the Archimedean case of the real numbers do, however, carry over. We can add, subtract, multiply, divide, and differentiate series just as usual (with the same radius of convergence).

We conclude our treatment of analysis in $\mathbb{Q}_p$ with a discussion of two critical functions defined by power series, the p-adic logarithm and exponential.

The p-adic logarithm and exponential, denoted $\log_p(x)$ and $\exp_p(x)$, respectively, are defined by

$$\log_p(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}(x-1)^n}{n}, \exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

The logarithm converges for $|x-1|_p < 1$ and the exponential converges for $|x|_p < p^{-1/(p-1)}$. This is quite different from the real case, where the exponential converges for all $x \in \mathbb{R}$. This is because as n tends to infinity, so, too, does $n!$ (in the reals), so $x^n/n!$ tends to 0 for any real number x. But in the p-adic case, as we saw before, $n!$ gets quite small, so $x^n/n!$ grows quite large.

As is to be anticipated, the p-adic logarithm and exponential behave as they should:

$$\begin{aligned}
&\log_p(xy) = \log_p(x) + \log_p(y),\\
&\exp_p(x+y) = \exp_p(x)\exp_p(y),\\
&\log_p(\exp_p(x)) = x,\\
&\exp_p(\log_p(1+x)) = 1+x.
\end{aligned}$$

It should be noted, however, that these identities only hold when x and y are in the regions of convergence of the p-adic logarithm and

exponential functions. For example, if $p = 2$, $x = -2$, then $\log_2(-1) = 0$, but $\exp_2(0) = 1 \neq -1$.

3. The Local-Global Principle

Given Hensel's Lemma, it is easy enough to see when we can find a solution to some quadratic equation in $\mathbb{Q}_p$ for some p. Now we focus on finding solutions to such equations in $\mathbb{Q}$. Clearly since $\mathbb{Q} \subset \mathbb{Q}_p$ for all $p \leq \infty$, if we can find any field of p-adic numbers (or the real numbers) with no solution, then there is no rational solution. This means that if there is a "global" solution (in $\mathbb{Q}$), then there is a "local" solution (in $\mathbb{Q}_p$) everywhere (for all $p \leq \infty$).

The idea of the local-global principle is that if there is a rational solution, then we can construct it by considering all of the local fields (every $\mathbb{Q}_p$). In fact, Hasse-Minkowski's theorem, better known as the local-global principle, states that if $f(x_1, x_2, \ldots, x_n)$ is a homogeneous polynomial of degree 2 in n variables with rational coefficients, then $f(x_1, x_2, \ldots, x_n) = 0$ has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{Q}_p$ for every $p \leq \infty$.

This proof of this theorem is the subject of the first half of Serre's *A Course in Arithmetic*[2]; in this section, we prove it for quadratic forms in 3 variables.

Theorem 3.1. *A quadratic form $f(x_1, x_2, x_3)$ with rational coefficients has a non-trivial solution in $\mathbb{Q}$ if and only if it has a non-trivial solution in $\mathbb{Q}_p$ for every prime $p \leq \infty$.*

We follow the proof given by Cassels in *Lectures on Elliptic Curves* [1].

As mentioned above, it is obvious that if there is a rational solution, then there is a real solution and a p-adic solution for every p.

Now we can't necessarily write the quadratic form as

$$f_1 x_1^2 + f_2 x_2^2 + f_3 x_3^2 = 0.$$

However, by appropriately transforming the quadratic form, we can work with an equation in that form. It is plain that such a transformation carries rational points to rational points, as does its inverse. Thus, we assume that we have such a form to begin with.

We can assume that $f_1, f_2, f_3 \neq 0$ since if any is equal to 0, then we can set the two variables to 0 and the variable with 0 coefficient to anything. We can also assume that $f_1, f_2, f_3 \in \mathbb{Z}$ since we can multiply through to clear the denominators. Further, we may assume that f_1, f_2 and f_3 are square-free since for example, if $f_1 = ab^2$, then $f_1 x_1^2 =$

$ab^2x_1^2 = a(bx_1)^2$, so in this case, we replace x_1 with bx_1. Furthermore, if $\gcd(f_1, f_2, f_3) > 1$, then we can divide out any common prime factors. If for example, $p \mid \gcd(f_1, f_2)$, but $p \nmid f_3$, then we replace x_3 by px_3, then we divide the whole equation by p. In any case, we end up with $f_1f_2f_3$ being square-free.

Thus, we need only prove the theorem for

$$f(x_1, x_2, x_3) = f_1x_1^2 + f_2x_2^2 + f_3x_3^2 = 0,$$

where f_1, f_2, f_3, and $f_1f_2f_3$ are all square-free.

In order to prove the theorem, we require the following two lemmas.

Lemma 3.2. *Let $m > 0$ be an integer and let $\mathcal{S} \subset \mathbb{R}^n$ with volume $V(\mathcal{S}) > m$. Then there are $m + 1$ distinct points $\boldsymbol{s}_0, \ldots, \boldsymbol{s}_m$ of $\mathcal{S}$ such that $\boldsymbol{s}_i - \boldsymbol{s}_j \in \mathbb{Z}^n$ $(0 \leq i, j \leq m)$.*

Proof. Let $\mathcal{W} \subset \mathbb{R}^n$ be the unit cube of points $\mathbf{w}$ with $0 \leq w_j < 1$ $(1 \leq j \leq n)$. Thus, every $\mathbf{x} \in \mathbb{R}^n = \mathbf{w} + \mathbf{z}$ for some $\mathbf{z} \in \mathbb{Z}^n$. Let $\chi(\mathbf{x})$ be the characteristic function of $\mathcal{S}$. Then we have that

$$\begin{aligned} m < V(\mathcal{S}) &= \int_{\mathbb{R}^n} \chi(\mathbf{x}) d\mathbf{x} \\ &= \int_{\mathcal{W}} \left(\sum_{\mathbf{z} \in \mathbb{Z}^n} \chi(\mathbf{w} + \mathbf{z}) \right) d\mathbf{w}. \end{aligned}$$

We know that $V(\mathcal{W}) = 1$, so there is a $\mathbf{w}_0 \in \mathcal{W}$ so that

$$\sum_{\mathbf{z} \in \mathbb{Z}^n} \chi(\mathbf{w}_0 + \mathbf{z}) > m,$$

or equivalently,

$$\sum_{\mathbf{z} \in \mathbb{Z}^n} \chi(\mathbf{w}_0 + \mathbf{z}) \geq m + 1.$$

So we set $\mathbf{s}_j = \mathbf{w}_0 + \mathbf{z}$, where $\mathbf{w}_0$ is the real n-tuple that satisfies the preceding statement. □

Lemma 3.3. *Let Λ be a subgroup of $\mathbb{Z}^n$ of index m. Let $\mathcal{C} \subset \mathbb{R}^n$ be a symmetric convex set of volume $V(\mathcal{C}) > 2^n m$. Then $\mathcal{C}$ and Λ have an intersection point aside from $\boldsymbol{0} = (0, \ldots, 0)$.*

Proof. Let $\mathcal{S} = \{\frac{\mathbf{c}}{2} : \mathbf{c} \in \mathcal{C}\}$. Then $V(\mathcal{S}) > m$, so by lemma 3.2, there are $m + 1$ distinct points $\mathbf{c}_0, \ldots, \mathbf{c}_m \in \mathcal{C}$ such that $\frac{1}{2}\mathbf{c}_i - \frac{1}{2}\mathbf{c}_j \in \mathbb{Z}^n$, where $0 \leq i, j \leq m$. There are also $m + 1$ points $\frac{1}{2}\mathbf{c}_i - \frac{1}{2}\mathbf{c}_0$, where $0 \leq i \leq m$ and m cosets of $\mathbb{Z}^n$ modulo Λ. So at least two of them have

to be in the same coset (by the pigeonhole principle); i.e., there exist i, j $(i \neq j)$ so that $\frac{1}{2}\mathbf{c}_i - \frac{1}{2}\mathbf{c}_j \in \Lambda$. To finish the proof, we note that $\mathcal{C}$ is symmetric, so $-\mathbf{c}_j \in \mathcal{C}$; thus, $\frac{1}{2}\mathbf{c}_i - \frac{1}{2}\mathbf{c}_j = \frac{1}{2}\mathbf{c}_i + \frac{1}{2}(-\mathbf{c}_j) \in \mathcal{C}$ since $\mathcal{C}$ is convex. □

Now that we have our two lemmas, we are ready to prove the local-global principle.

Proof. We will divide the proof into three cases and define a subgroup Λ of $\mathbb{Z}^3$ by certain conditions based on the three cases we consider. The idea is to define Λ so that it is of order $m = 4|f_1 f_2 f_3|_\infty$ with $f(\mathbf{x}) \equiv 0 \pmod{m}$ for any $\mathbf{x} \in \Lambda$. Then we can apply the two previous lemmas to conclude that $f(\mathbf{x}) = 0$ for some non-trivial vector $\mathbf{x}$, showing the existence of a rational point.

If there is a (non-trivial) solution in $\mathbb{Q}_p$, then there is a vector $\mathbf{a} = (a_1, a_2, a_3) \neq \mathbf{0}$ such that each $a_i \in \mathbb{Q}_p$ and $f(\mathbf{a}) = 0$. If necessary, we multiply $\mathbf{a}$ by some p-adic integer so that $\max\{|a_1|_p, |a_2|_p, |a_3|_p\} = 1$ (if $\mathbf{a}$ is a solution, then so is any multiple of $\mathbf{a}$). Now we divide the proof into three cases.

Case 1: $p \neq 2, p \mid f_1 f_2 f_3$. Without loss of generality, we may assume that $p \mid f_1$; thus, since f_1, f_2, f_3 are pairwise relatively prime, we have that $p \nmid f_2$ and $p \nmid f_3$. This means that $|f_1 a_1^2|_p < 1$. Now if $|a_2|_p < 1$, then

$$\begin{aligned} &|f_3 a_3^2|_p = |f_1 a_1^2 + f_2 a_2^2|_p < 1, \\ &|a_3|_p < 1. \end{aligned}$$

Also,

$$|f_1 a_1^2|_p = |f_2 a_2^2 + f_3 a_3^2|_p \leq \frac{1}{p^2}.$$

Now since f_1 is square-free, it follows that $|a_1|_p < 1$. This contradicts that $\max\{|a_1|_p, |a_2|_p, |a_3|_p\} = 1$, so $|a_2|_p = |a_3|_p = 1$. But since $|f_2 a_2^2 + f_3 a_3^2|_p < 1$, we divide by a_2, and there is an $r_p \in \mathbb{Z}$, with $f_2 + r_p^2 f_3 \equiv 0 \pmod{p}$.

So we set $x_3 \equiv r_p x_2 \pmod{p}$, which implies that

$$\begin{aligned} f(\mathbf{x}) &= f_1 x_1^2 + f_2 x_2^2 + f_3 x_3^2 \\ &\equiv (f_2 + r_p^2 f_3) x_2^2 \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Case 2: $p = 2, 2 \nmid f_1 f_2 f_3$. Without loss of generality, we know that a_2 and a_3 are units. The only squares modulo 4 are 0 and 1, so it follows that $f_2 + f_3 \equiv 0 \pmod 4$.

So we impose the following conditions:

$$\begin{aligned} x_1 &\equiv 0 \pmod 2 \\ x_2 &\equiv x_3 \pmod 2 \end{aligned}$$

This means that $f_1 x_1^2 \equiv 0 \pmod 4$ since x_1 is either 0 or 2 modulo 4. Note that $f_3 \equiv -f_2 \pmod 2$ since $2 \mid 4$. Thus,

$$\begin{aligned} f(\mathbf{x}) &\equiv f_2 x_2^2 + f_3 x_3^2 \\ &\equiv f_2 x_2^2 - f_2 x_2^2 \equiv 0 \pmod 4. \end{aligned}$$

Case 3: $p = 2, 2 \mid f_1 f_2 f_3$. Suppose without loss of generality that $2 \mid f_1$. Then $|a_2|_2 = |a_3|_2 = 1$. Now any odd integer squared gives 1 modulo 8, so if $|a_1|_2 < 1$, then

$$f_2 + f_3 \equiv 0 \pmod 8;$$

if $|a_1|_2 = 1$, then

$$f_1 + f_2 + f_3 \equiv 0 \pmod 8.$$

Now we impose the following conditions:

$$\begin{aligned} x_2 &\equiv x_3 \pmod 4 \\ x_1 &\equiv s^* x_3 \pmod 2, \end{aligned}$$

where $s^* = 0$ if $f_2 + f_3 \equiv 0 \pmod 8$, $s^* = 1$ otherwise. Then we have that

$$f(\mathbf{x}) \equiv f_2 x_2^2 + f_3 x_2^2 \equiv x_2^2 (f_2 + f_3) \equiv 0 \pmod 8$$

or

$$f(\mathbf{x}) \equiv f_1 x_3^2 + f_2 x_2^2 + f_3 x_2^2 \equiv f_1 x_2^2 + f_2 x_2^2 + f_3 x_2^2 \equiv x_2^2 (f_1 + f_2 + f_3) \equiv 0 \pmod 8.$$

Hence, $f(\mathbf{x}) \equiv 0 \pmod 8$.

Now the subgroup Λ is of index $m = 4|f_1 f_2 f_3|_\infty$ in $\mathbb{Z}^3$; $f(\mathbf{x}) \equiv 0 \pmod{4|f_1 f_2 f_3|_\infty}$ for any $\mathbf{x} \in \Lambda$. So we apply lemma 3.3 to Λ and the convex symmetric set

$$\mathcal{C} : |f_1|_\infty x_1^2 + |f_2|_\infty x_2^2 + |f_3|_\infty x_3^2 < 4|f_1 f_2 f_3|_\infty.$$

Now the volume of this is

$$\begin{aligned} V(\mathcal{C}) &= \frac{\pi}{3} \cdot 2^3 \cdot |4f_1 f_2 f_3|_\infty \\ &> 2^3 |4f_1 f_2 f_3|_\infty \\ &= 2^3 m. \end{aligned}$$

So $(\Lambda \cap \mathcal{C}) \backslash \{\mathbf{0}\}$ is nonempty by lemma 3.3. For any $\mathbf{x}$ in this set,

$$f(\mathbf{x}) \equiv 0 \pmod{4|f_1 f_2 f_3|_\infty}.$$

Furthermore,

$$|f(\mathbf{x})|_\infty \leq |f_1|_\infty x_1^2 + |f_2|_\infty x_2^2 + |f_3|_\infty x_3^2 < 4|f_1 f_2 f_3|_\infty,$$

thus implying that $f(\mathbf{x}) = 0$, which proves the theorem.

□

Note. Nowhere in this proof was solvability in $\mathbb{R} = \mathbb{Q}_\infty$ used. This means that we have an even stronger condition for conics: if a quadratic form is solvable in $\mathbb{Q}_p$ for every $p < \infty$, then it is solvable in $\mathbb{Q}$, and thus solvable in $\mathbb{R}$. This is, in fact, connected with quadratic reciprocity. The connection is the Hilbert Product Formula. The Hilbert symbol, $(a, b)_p$, with $a, b \in \mathbb{Q}_p$, is defined by

$$(a,b)_p = \begin{cases} 1, & \text{if } z^2 = ax^2 + by^2 \text{ has a non-trivial solution in } \mathbb{Q}_p, \\ -1, & \text{if } z^2 = ax^2 + by^2 \text{ has no non-trivial solution in } \mathbb{Q}_p. \end{cases}$$

The Hilbert Product Formula says that $\prod_{p \leq \infty} (a, b)_p = 1$, so if $(a, b)_p = 1$ whenever $p < \infty$, this implies that $(a, b)_\infty = 1$. This is Hilbert's Reciprocity Law, which is, in fact, equivalent to quadratic reciprocity.

4. Using Local Information to Investigate Higher Algebraic Forms

Given the proof of the local-global principle for conics, the natural question to ask is if there is some way to extend the principle to higher algebraic forms – cubic forms, biquadratic forms, and so on. The answer is simply no. We show this with the following two examples.

Example 4.1. The equation $(x^2-2)(x^2-17)(x^2-34)=0$ has a root in $\mathbb{Q}_p$ for all $p \leq \infty$, but has no roots in $\mathbb{Q}$.

First consider $p=2$. 17 is a quadratic residue modulo 2. In fact, 17 is a square modulo every power of 2. This means that we can patch together square roots of 17 modulo various powers of 2 to compute a 2-adic square root of 17. So this equation is soluble in $\mathbb{Q}_2$.

Now consider $p=17$. We have $f(x)=x^2-2$, $f'(x)=2x$. Now $6^2-2 \equiv 0 \pmod{17}$, but clearly $2 \cdot 6 \equiv 12 \not\equiv 0 \pmod{17}$. Thus, by Hensel's Lemma, there is a 17-adic square root of 2, and thus a 17-adic root of this equation.

Now suppose $p \neq 2, 17$. If either 2 or 17 is a square in $\mathbb{Q}_p$, then the equation has a solution in $\mathbb{Q}_p$. If, however, neither 2 nor 17 is a square in $\mathbb{Q}_p$, then by basic quadratic residue theory (the product of two non-residues is a residue), their product, 34, is a square modulo p, and we can thus use Hensel's Lemma to find a root of the equation.

For $p=\infty$, this equation is factored, so the roots are $\pm\sqrt{2}, \pm\sqrt{17}$, and $\pm\sqrt{34}$. Clearly none of these is rational.

So this is an example that would violate any attempt to extend the local-global principle.

Example 4.2. The equation $x^4-17=2y^2$ is locally solvable everywhere, but is not solvable in $\mathbb{Q}$.

By theorems on elliptic curves, it can be determined that over any finite field with $p \geq 5$, a curve of genus 1 has a point. This point can then be lifted to a solution in $\mathbb{Z}_p$. Thus, there are solutions for any $\mathbb{Q}_p$. The only special cases to consider, then, are $\mathbb{Q}_2, \mathbb{Q}_3$, and $\mathbb{Q}_{17}$. Of course, setting $x=3, y=4\sqrt{2}$ gives a real solution.

Now we show there are no rational solutions. Suppose to the contrary that (x,y) is a solution. Set $x=\frac{a}{c}$ with a, c coprime. Then

$$\begin{aligned} &x^4-17=2y^2=(a/c)^4-17=2y^2 \\ &=a^4/c^4-17=2y^2 \\ &\Rightarrow a^4-17c^4=2y^2c^4=2(yc^2)^2 \end{aligned}$$

So we have $a^4-17c^4=2b^2$, with a, b, c pairwise relatively prime. Now set $A=a^2, C=c^2$, so that $A^2-17C^2=2b^2$. This equation is solvable everywhere locally, and hence globally; in particular, $5^2-17\cdot 1^2=2\cdot 2^2$ is a solution.

Now

$$(5A+17C+4b)(5A+17C-4b)=17(A+5C)^2.$$

If there is a common prime factor $p > 2$ that divides both factors on the left side, then it divides $5A + 17C$ and $A + 5C$, implying that it divides both $8A$ and $8C$, so it divides A and C since the only prime divisor of 8 is 2. So p divides both a and c, a contradiction (they are relatively prime). Now both factors on the left-hand side of the equation must be positive, so for integers u and v, there are two cases:

Case 1: We have

$$\begin{aligned} 5a^2 + 17c^2 \pm 4b &= 17u^2, \\ 5a^2 + 17c^2 \mp 4b &= v^2, \\ a^2 + 5c^2 &= uv. \end{aligned}$$

This implies that (upon adding the first two equations),

$$\begin{aligned} 10a^2 + 34c^2 &= 17u^2 + v^2, \\ a^2 + 5c^2 &= uv. \end{aligned}$$

Let's consider this modulo 17. 10 is a quadratic non-residue modulo 17, so $10a^2 \equiv v^2 \pmod{17}$ has no solution; this is a contradiction.

Case 2: We have that

$$\begin{aligned} 5a^2 + 17c^2 \pm 4b &= 34u^2, \\ 5a^2 + 17c^2 \mp 4b &= 2v^2, \\ a^2 + 5c^2 &= 2uv. \end{aligned}$$

This shows that

$$\begin{aligned} 10a^2 + 34c^2 &= 34u^2 + 2v^2 \\ \Rightarrow 5a^2 + 17c^2 &= 17u^2 + v^2. \end{aligned}$$

Now 5 is also a quadratic non-residue modulo 17; hence, $5a^2 \equiv v^2 \pmod{17}$ has no solution, so both cases lead to a contradiction.

Thus, these contradictions in $\mathbb{Z}/17\mathbb{Z}$ show that (x, y) cannot possibly be a rational point.

These two examples illustrate that the local-global principle is not true for higher forms. Nevertheless, the *principle* that investigating local solutions to an equation may be of use in investigating global solutions holds. On the other hand, if one can show that there is any local field over which an equation is unsolvable, then that of course does show the nonexistence of global solutions.

One of the most famous unsolved problems in mathematics is the Birch and Swinnerton-Dyer Conjecture, which roughly states that the number of global solutions is entirely determined by local information. This is not exactly a direct extension of the local-global principle, but it does emphasize the importance of patching together a global solution out of local information. While nothing as strong as the local-global principle holds for higher forms, what remains clear is that the idea of gathering information from local fields is useful in constructing global solutions.

References

[1] Cassels, J.W.S., *Lectures on Elliptic Curves*, Cambridge University Press, NY, 1991.
[2] Gouvéa, Fernando Q., *p-adic Numbers: An Introduction*, Springer-Verlag, Berlin, 2nd Ed., 2003.
[3] Katok, Svetlana, *p-adic Analysis Compared with Real*, American Mathematical Society, RI, 2007.
[4] Koblitz, Neal, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, NY, 2nd Ed., 1984.