A LOCAL-GLOBAL PRINCIPLE FOR SUMS OF TWO SQUARES

NATALIE LEONARD

Abstract. This paper will explore a simple consequence of the Hasse-Minkowski local-global principle for p-adics, namely, the sums of two squares theorem. First, I will introduce and define the p-adic numbers and elementary operations on the p-adic numbers. Then, I will discuss and prove the sums of two squares theorem on the integers. Finally, I will extend this theorem to the p-adic integers.

Contents

1. Introduction to the p-adics

Definition 1.1. We write $x \equiv_n y$ if n divides $x - y$ or equivalently $x - y = nk$ for some $k \in \mathbb{Z}$. In this case, we also write $x - y \equiv 0 \pmod{n}$.

Remark 1.2. $x \equiv_n y$ is an equivalence relation on $\mathbb{Z}$. Note: the equivalence classes form a ring which we denote $\mathbb{Z}/n$. Additionally, we denote the field $\mathbb{Z}/p$ as $\mathbb{F}_p$, where p is a prime.

Theorem 1.3. *(Fermat's Little Theorem) For all primes p and integers a, either $a \equiv 0 \pmod{p}$ or $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. We will prove this theorem through induction on a, noting that all negative integers will follow once the statement is shown for positive integers. For the base case, if $a = 1$ then $1^{p-1} \equiv 1 \pmod{p}$, as required. Now, suppose that $a^p \equiv a \pmod{p}$ holds for all $1 \leq a \leq k$. Consider $a = k + 1$. We take the binomial expansion to see $(k+1)^p \equiv k^p + \binom{p}{1}k^{p-1} + ... + \binom{p}{p-1}k + 1 \pmod{p}$. As the coefficients of each term barring the first and last will contain a factor of p, they will therefore disappear when taken mod p. Therefore: $(k+1)^p = k^p + 1 \pmod{p}$. So, by the inductive hypothesis $(k+1)^p = k+1 \pmod{p}$, which implies $(k+1)^{p-1} \equiv 1 \pmod{p}$ and we are done. □

Theorem 1.4. *(Wilson's Theorem) A number n is prime if and only if*

$$(n-1)! \equiv -1 \pmod{n}$$

Proof. Consider the polynomial $P(x) = x^{p-1} - 1$ for $x \in \mathbb{F}_p$. By Fermat's Little Theorem, for all $x \not\equiv 0 \pmod{p}$, x is a root to $P(x)$. And as $\mathbb{F}_p$ has only $p-1$ elements, then:

$$P(x) = x^{p-1} - 1 = \prod_{k=1}^{p-1}(x-k)$$

Now, for all primes, $(-1)^{p-1} \equiv 1 \pmod{p}$, so equivalently:

$$x^{p-1} - 1 = \prod_{k=1}^{p-1}(-k-x)$$

Let $x = 0$ to reach the desired conclusion, that $-1 \equiv (p-1)! \pmod{p}$. □

We now move on to constructing the p-adic numbers.

Definition 1.5. Fix a prime $p \in \mathbb{Z}$. Define $v_p : \mathbb{Z}\backslash\{0\} \to \mathbb{Z}$, the p-adic **valuation** as follows: take some $n \in \mathbb{Z}$. Then $v_p(n)$ satisfies:

$$n = p^{v_p(n)}n' \text{ where } p \nmid n'$$

We set $v_p(0) = \infty$. In $\mathbb{Q}$, given some $x = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, then:

$$v_p(x) = v_p(a) + v_p(b)$$

Lemma 1.6. *For all $x, y \in \mathbb{Q}$:*

(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 $x = p^a x'$ where $a = v_p(x)$ and $y = p^b y'$ where $b = v_p(y)$. Then $x \cdot y = p^a x' \cdot p^b y'$ which implies $x \cdot y = p^{a+b}x'y'$. As $p \nmid x'$ and $p \nmid y'$, $p \nmid x'y'$ so $v_p(xy) = a + b = v_p(x) + v_p(y)$, as required.

For the second part, let $x =^a x'$ and $y = p^b y'$ with a and b defined as before. Suppose, without loss of generality, that $a < b$. Then $x + y = p^a x' + p^b y'$ and we can factor out p^a from both terms so, $x + y = p^a(x' + p^{b-a}y')$. Now, $x' + p^{b-a}y'$ cannot contain a factor of p or $v_p(x) \neq a$. Therefore, $v_p(x+y) \geq a = v_p(x) = \min\{v_p(x), v_p(y)\}$, as required. □

Definition 1.7. For any $x \in \mathbb{Q}$, $x \neq 0$, define the p-adic absolute value as follows:

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

We set $|0|_p = 0$. Additionally, we let $|-|_\infty$ be the usual absolute value.

Theorem 1.8. *(Ostrowski) For all $x \in \mathbb{Q}^\times$:*

$$\prod_{p \leq \infty} |x|_p = 1$$

Proof. Let x be some positive integer with a unique prime factorization $x = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$. We break the above product into cases:

(1) Take $q \neq p_i$ for all $1 \leq i \leq n$ such that $q \neq \infty$. Then x will not have a factor of q so $v_1(x) = 0$ and $|x|_q = 1$.

(2) Take $q = p_i$ for some i. Then $v_q(x) = v_{p_i}(x) = a_i$ and $|x|_q = p_i^{-a_i}$.

(3) Now consider $|x|_\infty$. This will simply be the "normal" absolute value so $|x|_\infty = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$ as x is positive.

Taking all three cases, $\prod_{p \leq \infty} |x|_p = p_1^{-a_1} p_2^{-a_2} ... p_n^{-a_n} \cdot (p_1^{a_1} p_2^{a_2} ... p_n^{a_n}) = 1$. A similar argument can be made for negative non-integral x. □

We now turn to defining $\mathbb{Q}_p$ and $\mathbb{Z}_p$. $\mathbb{Q}_p$ is created through "completions" via Cauchy sequences. First, we define Cauchy sequences in the usual sense:

Definition 1.9. A sequence (x_n) is Cauchy if for every $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $n, m > N$ we have:

$$|x_n - x_m| < \epsilon$$

Definition 1.10. Let $\mathcal{C} = \mathcal{C}_p(\mathbb{Q}) := \{(x_n) : (x_n) \text{ is Cauchy}\}$.

Definition 1.11. Let $\mathcal{N} := \{(x_n) : \lim_{n \to \infty} |x_n|_p = 0\} = \{(x_n) : x_n \to 0\}$.

Proposition 1.12. *$\mathcal{N}$ is a maximal ideal of $\mathcal{C}$.*

Proof. First, $\mathcal{N}$ is an ideal: for an arbitrary Cauchy sequence (x_n), we can find an upper bound, and, given a sequence (y_n) that tends to zero, then $(x_n y_n)$ tends to zero, so $(x_n y_n) \in \mathcal{N}$.

To show that $\mathcal{N}$ is maximal, the goal is to show that the unit element (i.e. (1)) is contained in any ideal I generated by some sequence $(x_n) \notin \mathcal{C}$ where $(x_n) \in \mathcal{N}$. This works: if (1) is contained in I, then I must be the entire ring. Our strategy is to take (x_n) and define a sequence (y_n) such that $(x_n y_n) \in \mathcal{N}$. Now, as (x_n) does not tend to 0, there exists some $N \in \mathbb{N}$ and some $c > 0$ such that for all $n \geq N$, $|x_n| \geq c$. Define (y_n) by letting $y_i = 0$ for all $i < N$ and $y_i = \frac{1}{x_i}$ for all $i \geq N$. It is immediate that (y_n) is Cauchy and therefore contained in $\mathcal{C}$. And, for all $n \geq N$, $x_n y_n = 1$. So, $1 - x_n y_n$ tends to 0 as n tends to infinity, and therefore $(x_n y_n) \in \mathcal{N}$. As (1) can be generated by (x_n) and $\mathcal{N}$, $\mathcal{N}$ is a maximal ideal.

What does this mean? A maximal ideal is maximal if there are no other ideals "in between." In this case, this means that there are no ideals of $\mathcal{C}$ larger than $\mathcal{N}$ that are not all of $\mathcal{C}$. □

Definition 1.13. Define the field of p-adic numbers $\mathbb{Q}_p$ to be $\mathbb{Q}_p := \mathcal{C}/\mathcal{N}$.

Definition 1.14. Denote $\mathbb{Z}_p$ as follows:

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

Note: while this definition works on a technical level, it doesn't provide much insight into what p-adic integers actually look like. So, more functionally, a p-adic integer is a series of the form:

$$a_1p + a_2p^2 + a_3p^3 + ...$$

where p is a prime and each a_i is an integer (usually between 1 and $p-1$). This second definition is analogous to the first, as the p-adic absolute value tells us whether a p-adic number has factors of p in the numerator or denominator. The closed unit ball, described in Definition 1.14, simply denotes all p-adic numbers with a non-negative number of factors of p.

We now introduce Hensel's Lemma, a powerful tool for solving equations in $\mathbb{Q}_p$.

Theorem 1.15. *(Hensel's Lemma) Take some prime $p \geq 3$. Let $F(X) = a_0 + a_1X + ... + a_nX^n$ be a polynomial where each $a_i \in \mathbb{Z}_p$, such that $F(\alpha_1) \equiv 0 \pmod{p}$ and $F'(\alpha_1) \not\equiv 0 \pmod{p}$ for some $\alpha_1 \in \mathbb{Z}_p$. Then there exists a unique p-adic integer, $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_1 \pmod{p}$ and $F(\alpha) = 0$.*

Proof. Our aim in proving this important theorem is to construct a Cauchy sequence that converges to an α that satisfies the above statement. So, we will find a sequence of integers $\alpha_1, ..., \alpha_n$ such that for all $n \geq 1$ we have $F(\alpha_n) \equiv 0 \pmod{p^n}$ and $\alpha_n \equiv \alpha_{n+1} \pmod{p^n}$. Now, α_1 exists from the givens. We proceed with induction. Assume that α_n exists such that $F(\alpha_n) \equiv 0 \pmod{p^n}$ and $\alpha_n \equiv \alpha_{n+1} \pmod{p^n}$ and moreover that $F'(\alpha_n) \not\equiv 0 \pmod{p^n}$. Let $\alpha_{n+1} = \alpha_n + b_np^n$ for some $b_n \in \mathbb{Z}_p$.

Therefore:

$$\begin{aligned} F(\alpha_{n+1}) &= F(\alpha_n + b_np^n) \\ &\equiv F(\alpha_n) + F'(\alpha_n)b_np^n \pmod{p^{n+1}} \end{aligned}$$

The above holds if and only if there exists b_n such that $F(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}}$ is satisfied. So, it is necessary and sufficient to show:

$$F(\alpha_n) + F'(\alpha_n)b_np^n \equiv 0 \pmod{p^{n+1}}$$

Now, $F(\alpha_n) \equiv 0 \pmod{p^n}$, so for some x, $F(\alpha_1) = p^nx$.

$$p^nx + F'(\alpha_n)b_np^n \equiv 0 \pmod{p^{n+1}}$$

Divide through by p^n to find:

$$x + F'(\alpha_n)b_n \equiv 0 \pmod{p}$$

As $F'(\alpha_n) \not\equiv 0 \pmod{p^n}$, $F'(\alpha_n) \not\equiv 0 \pmod{p}$ which implies that $F'(\alpha_n)$ is invertible:

$$\implies b_n \equiv -x(F'(\alpha_n))^{-1} \pmod{p}$$

As we have found b_n satisfying the requirement that $\alpha_2 = \alpha_1 + b_np$, we can conclude that the sequence exists, that it converges to α and that $F(\alpha) = 0$, as required.

□

Remark 1.16. The above version of Hensel's Lemma notably excludes the $p = 2$ case. This is because often polynomials will fail to satisfy the second criteria: a non-zero derivative at the root. Consider the following example:

Example 1.17. Let $f(x) = x^2 - \alpha$ for any $\alpha \in \mathbb{Z}$. We want to find whether α is a square in $\mathbb{Z}_p$ for $p = 2$. We would like to use Hensel's Lemma to approach this problem; however, even though 1 or 2 will be a solution in $\mathbb{Z}_2$ (depending on the evenness or oddness of α), $f'(1) \equiv 2(1) \equiv 0 \pmod 2$ and $f'(2) \equiv 2(2) \equiv 0 \pmod 2$. So, we are unable to determine whether α is a root, because the derivative is always 0.

Because of this problem we introduce a weaker version of Hensel's Lemma that works for the $p = 2$ case.

Theorem 1.18. *Take some prime p. Let $F(X) = a_0 + a_1X + ... + a_nX^n$ be a polynomial with each $a_i \in \mathbb{Z}_p$ where for some $\alpha \in \mathbb{Z}_p$, $|f(\alpha_1)| < |f'(\alpha_1)|^2$. Then there is a unique $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$ and $|\alpha - \alpha_1| < |f'(\alpha_1)|$.*

2. Euler's sums of two squares theorem for integers

With the tools from the previous section, this paper will prove a specific case of the Hasse-Minkowski Local Global Principle. The Hasse-Minkowski Theorem is an application of the Local-Global Principle, stated below, to quadratic forms.

(The Local Global Principle) *A theorem holds over $\mathbb{Q}$ if and only if it holds over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes p.*

Notice that the above statement is not a theorem but a principle: it outlines a strategy for approaching challenging problems in $\mathbb{Q}$, by instead evaluating solutions in $\mathbb{Q}_p$ for all p. This paper will deal with the sums of two squares theorem: namely, that an integer can be written as a sum of two squares in $\mathbb{Z}$ if and only if it can be written as a sum of two squares locally at every prime p and in $\mathbb{R}$. To start, we introduce and prove the two-square theorem for the integers.

Theorem 2.1. *(Euler) A positive integer m can be written as the sum of two squares if and only if for each prime $p \mid m$ with $p \equiv 3 \pmod 4$, p has even multiplicity as a factor of m.*

This proof will build upon a few lemmas presented below:

Lemma 2.2. *(Thue's Lemma) Let p be prime. For all a such that $p \nmid a$ there exist $x, y \in \{1, 2, ..., \lfloor\sqrt{p}\rfloor\}$ such that $ax \equiv y \pmod p$ or $ax \equiv -y \pmod p$.*

Proof. Consider the set of coordinate points in $\{1, 2, ..., \lfloor\sqrt{p}\rfloor\} \times \{1, 2, ..., \lfloor\sqrt{p}\rfloor\}$. As this set clearly contains $(1 + \lfloor\sqrt{p}\rfloor)^2$ elements, it will have greater than p elements. By the pigeonhole principle, as there are only $p - 1$ elements in $\mathbb{F}_p^\times$, there must be (x_1, y_1) and (x_2, y_2) that are distinct coordinate pairs such that $ax_1 - y_1 \equiv ax_2 - y_2 \pmod p$. This implies $a(x_1 - x_2) \equiv y_1 - y_2 \pmod p$. All that is left to show is that $x_1 - x_2, y_1 - y_2 \neq 0$.

If $x_1 = x_2$ then $0 \equiv y_1 - y_2 \pmod p$ and as $1 \leq y_1, y_2 < p$ then $y_1 = y_2$. However, this contradicts distinctness. We see a similar result taking $y_1 = y_2$. Therefore, set $x = |x_1 - x_2|$ and $y = |y_1 - y_2|$ and we are done. $\square$

Lemma 2.3. *For all primes $p > 2$, $p \equiv 1 \pmod 4$ if and only if there exists x such that $x^2 \equiv -1 \pmod p$.*

Proof. We begin with the forward direction; assume that $p \equiv 1 \pmod 4$. By Wilson's Theorem:

$$(p-1)! \equiv 1 \cdot ... \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdot ... \cdot (p-1) \equiv -1 \pmod p$$

If we multiply the last $\frac{p-1}{2}$ factors by -1 then:

$$(-1)^{\frac{p+1}{2}} \equiv 1 \cdots ... \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2}\right) \cdot ... \cdot 1$$

And, as $p \equiv 1 \pmod 4$, $\frac{p+1}{2}$ is odd so:

$$-1 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p$$

Therefore, $-1 \in (\mathbb{F}_p^\times)^2$ as required.

Now, consider the reverse direction; assume that there exists x such that $x^2 \equiv -1 \pmod 4$. By Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod 4$. This in turn means that:

$$(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$$

This can only occur when $\frac{p-1}{2}$ is even. So $\frac{p-1}{2} = 2k$ for some $k \in \mathbb{Z}$ or $p \equiv 1 \pmod 4$ as required. □

Lemma 2.4. *If $a^2 \equiv -1 \pmod p$ has solutions for some a, then p can be represented as a sum of two squares.*

Proof. First, $p \nmid a$ as that would imply $a^2 \equiv 0 \pmod p$ which is a contradiction. Therefore, Thue's Theorem states that there exists $x, y \in \{1, 2, ... \lfloor\sqrt{p}\rfloor\}$ such that $ax \equiv \pm y \pmod p$. So:

$$\begin{aligned} a^2 &\equiv -1 \pmod p \\ \implies a^2x^2 &\equiv -x^2 \pmod p \end{aligned}$$

As $ax \equiv \pm y \pmod p$ then $a^2x^2 \equiv y^2 \pmod p$ so:

$$y^2 + x^2 \equiv 0 \pmod p$$

So, for some x, y we have $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}$. All that is left to show is that $k = 1$. Now, as $x, y \geq 1$, $k > 0$. And $x^2, y^2 \leq (\lfloor\sqrt{p}\rfloor)^2 < \sqrt{p}^2$ which implies $x^2 + y^2 < 2p$. Therefore, $k = 1$, and the proof is finished. □

Lemma 2.5. *The product of numbers that can be written as the sum of two squares, can be written as the sum of two squares.*

Proof. This can be shown through the following algebraic manipulation: take $x = a^2 + b^2$ and $y = c^2 + d^2$. Then:

$$\begin{aligned} xy &= (a^2 + b^2)(c^2 + d^2) \\ &= a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 \\ &= (a^2c^2 + 2abcd + b^2d^2) + (a^2d^2 - 2abcd + b^2c^2) \\ &= (ac + bd)^2 + (ad - bc)^2 \end{aligned}$$

□

We can now prove the theorem:

Proof of Theorem 2.1. First, let $m = s^2n$, where n is square free. Our goal is to show that for m to be the sum of two squares, all odd prime factors of n are $p \equiv 1 \pmod 4$ or have even multiplicity. First, the forward direction: assume that an integer m can be written as the sum of two squares. Let $m = x^2 + y^2$. If $n = 1$ then the statement is trivially true as all prime factors of m will have even multiplicity and $m = s^2 + 0^2$ is a solution. So, take $m > 1$. Now, we can factor out from x and y their greatest common factor, call it d, and say $x = dx_1$ and $y = dy_1$ where $(x_1, y_1) = 1$. So, $m = d^2(x_1^2 + y_1^2)$ which yields:

$$\frac{s^2n}{d^2} = \frac{m}{d^2} = x_1^2 + y_1^2$$

As n is taken to be square free, then d^2 divides s^2, so let $s^2 = td^2$ for some t:

$$tn = x_1^2 + y_1^2$$

So, consider some odd prime p such that $p \mid n$, and assume for contradiction that $p \equiv 3 \pmod 4$. As $p \mid n$ we know $p \mid x_1^2 + y_1^2$ or,

$$x_1^2 + y_1^2 \equiv 0 \pmod p \implies x_1^2 \equiv -y_1^2 \pmod p$$

aS $p = 4k + 3$ for some $k \in \mathbb{Z}$, $p - 1 = 2(2k + 1)$.

$$\begin{aligned} x_1^{2(2k+1)} &\equiv (-1)^{2k+1}(y_1)^{2(2k+1)} \pmod p \\ \implies x_1^{p-1} &\equiv -(y_1)^{p-1} \pmod p \end{aligned}$$

Consider two cases; first if $p \mid x_1$ then $p \mid tn - x_1^2$ which implies $p \mid y_1^2$. However, the greatest common divisor of x_1 and y_1 is 1, so we have reached a contradiction. Therefore, assume $p \nmid x_1, y_1$. By Fermat's Little Theorem, then:

$$1 \equiv -1 \pmod p$$

which is clearly a contradiction. Therefore, if $p \mid n$ then $p \equiv 1 \pmod 4$. So, all prime factors $p \equiv 3 \pmod 4$ of m have even multiplicity, as they divide s^2, not n. This concludes the forward direction.

Now, we turn to the reverse direction. This direction is significantly easier; assume that for every prime factor $p \equiv 3 \pmod 4$, that p has even multiplicity. As $m = s^2 n$, if $p \equiv 3 \pmod 4$, then $p \nmid n$. So, all prime factors of n are congruent to $1 \pmod 4$. How does this help us? Let $n = p_1 p_2 ... p_k$, the unique prime factorization of n. As for every i, $p_i \equiv 1 \pmod 4$ we can apply Lemmas 2.4 and 2.3 to say that each p_i can be written as the sum of two squares. By Remark 2.5, m can be written as the sum of two squares, as required. □

3. Euler's sums of two squares theorem for p-adics

We now turn to the p-adic equivalent of Euler's two square theorem. We first introduce some more machinery.

Theorem 3.1. *(Euler's criterion) A number a is called a* ***quadratic residue*** $\pmod p$ *if a is coprime to p and $a = x^2 \pmod p$ for some integer x. Given any a:*

$$a^{\frac{p-1}{2}} = \begin{cases} 1 \pmod p & \textit{if } a \textit{ is a quadratic residue} \\ -1 \pmod p & \textit{otherwise} \end{cases}$$

Proof. As a and p are relatively prime Fermat's Little Theorem states that $a^{p-1} \equiv 1 \pmod p$, or $a^{p-1} - 1 \equiv 0 \pmod p$. As $p-1$ is even, equivalently $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p$.

As $\mathbb{F}_p$ is a field, one factor must be 0 for the statement to hold. Now, suppose that a is a quadratic residue; for some x, $a \equiv x^2 \pmod p$. Then:

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$$

So, if a is a quadratic residue then $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$. By Legrange's Theorem, an application of the polynomial division theorem and properties of $\mathbb{F}_p$, $a^{\frac{p-1}{2}} - 1$ has at most $\frac{p-1}{2}$ solutions; all other elements of $\mathbb{F}_p$ must be solutions to $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$. □

Corollary 3.2. *For all primes p, $\frac{p+1}{2}$ integers in $\mathbb{F}_p$, including 0, are quadratic residues mod p.*

Lemma 3.3. *Let p be a prime such that $p \equiv 1 \pmod 4$. Then every p-adic integer is a sum of two squares of p-adic integers.*

Proof. First, if $p \equiv 1 \pmod 4$ then -1 is a quadratic residue. So, for some k_0, $k_0^2 + 1 \equiv 0 \pmod p$. Now, we can apply Hensel's Lemma to $f(x) = x^2 + 1$ as $f(k_0) \equiv 0 \pmod p$ and $f'(k_0) \equiv 2k_0 \not\equiv 0 \pmod p$. Therefore, there exists a p-adic integer $k \in \mathbb{Z}_p$ such that $k \equiv k_0 \pmod p$ and $f(k) = 0$.

Now, for an arbitrary $t \in \mathbb{Z}_p$:

$$\begin{aligned} (1+t)^2 + (k(t-1))^2 &= 1 + 2t + t^2 + k^2(t^2 - 2t + 1) \\ &= 1 + 2t + t^2 - t^2 + 2t - 1 \\ &= 4t \end{aligned}$$

Solving for t shows that $t = (\frac{1+t}{2})^2 + (\frac{k(t-1)}{2})^2$. Therefore, t can be expressed as the sum of two squares, and we are done.

Note: As we have excluded 2-adic integers, $\frac{1+t}{2}$ and $\frac{k(t-1)}{2}$ are in $\mathbb{Z}_p$.

□

Lemma 3.4. *For prime $p \equiv 3 \pmod 4$, a nonzero integer u is a sum of two squares in $\mathbb{Z}_p$ if and only if its p-adic valuation, $v_p(u)$, is even.*

Proof. Let $u = p^a u'$ such that $p \nmid u'$. First, we will show that u' can be written as the sum of two squares, and then consider the cases when a is even and when a is odd.

Let $A = \{y^2 \pmod p | 0 \leq y \leq p-1\}$ and let $B = \{u' - x^2 \pmod p | 0 \leq x \leq p-1\}$. By Euler's criterion, the number of squares for $p \geq 2$ in $\mathbb{F}_p$ is $\frac{p+1}{2}$ so $|A| = \frac{p+1}{2}$ and $|B| = \frac{p+1}{2}$. Then by the pigeonhole theorem, there must be some element in both A and B, as $|A| + |B| = p + 1 > |\mathbb{F}_p|$. Suppose $k \in A$ and $k \in B$ with $0 \leq k \leq p-1$. Then for some $y_0 \in A$ and $x_0 \in B$:

$$k \equiv y_0^2 \pmod p \text{ and } k \equiv u' - x_0^2 \pmod p$$

Therefore:

$$\begin{aligned} & u' - x_0^2 \equiv y_0^2 \pmod p \\ \implies & u' \equiv x_0^2 + y_0^2 \pmod p \end{aligned}$$

Now, all we must show is that Hensel's Lemma applies and we can lift to find solutions in $\mathbb{Z}_p$. As u does not have a factor of p, x_0^2 or $y_0^2 \not\equiv 0 \pmod p$. Suppose that $x_0 \not\equiv 0 \pmod p$. Then let $f(x) = x^2 + (y_0^2 - u')$. First, $f(x_0) \equiv 0 \pmod p$. Second, $f'(x_0) = 2x_0 \not\equiv 0 \pmod p$. Therefore, we can find a solution in $\mathbb{Z}_p$ as required.

Next, consider two cases: either $v_p(u)$ is even, or it is not.

Case 1: If a is even then $a = 2k$ for some $k \in \mathbb{Z}$. Then:

$$\begin{aligned} u &= p^{2k} u' \\ &= p^{2k}(x_0^2 + y_0^2) \\ &= (p^k x_0)^2 + (p^k y_0)^2 \end{aligned}$$

So, in the case when $v_p(u)$ is even, u can be written as a a sum of two squares.

Case 2: Take a to be odd, and suppose $u = x^2 + y^2$ for some $x, y \in \mathbb{Z}_p$. Trivially, x and y are nonzero so consider the following two cases:

a) Suppose that $v_p(x) \neq v_p(y)$. Then $v_p(u) = \max\{v_p(x^2), v_p(y^2)\} = \max\{2v_p(x), 2v_p(y)\}$. Then $v_p(u)$ is even which, again, contradicts our assumption.

b) Suppose that $x = p^n v$ and $y = p^n w$ with $v, w \in \mathbb{Z}_p^\times$, such that x and y have equal valuations. Then:

$$u = x^2 + y^2 = p^{2n}(v^2 + w^2)$$

As $v_p(u)$ is odd and $2n$ is even:

$$v^2 + w^2 \equiv 0 \pmod p$$

$$\implies v^2 \equiv -w^2 \pmod{p}$$

$$\implies -1 \equiv (\frac{v}{w})^2 \pmod{p}$$

But then -1 is a square which contradicts Lemma 2.3 as $p \equiv 3 \pmod 4$. Therefore, when $p \equiv 3 \pmod 4$, a p-adic integer is the sum of two squares if and only if its p-adic valuation is even.

□

Lemma 3.5. *An element $u \in \mathbb{Z}_2$ is a square in $\mathbb{Q}_2$ if and only if $u \equiv 1 \pmod 8$.*

Proof. First, for the forward direction, if $u \in \mathbb{Z}_2$ is a square then in $\mathbb{Z}_8$, $u \equiv 1, 3, 5, 7 \pmod 8$. The squares of the above units are $1, 9, 25, 49$ respectively, all of which are equivalent to $1 \pmod 8$, as required. Now, for the reverse direction, suppose that an element $u \in \mathbb{Z}_2$ is equivalent to $1 \pmod 8$. Consider the function $f(X) = X^2 - u$ and let $a = 1$. First, $|f(1)|_2 = |1-u|_2$ and as $1 - u \equiv 0 \pmod 8$, we have $|1-u|_2 \leq \frac{1}{8}$ and $|f'(1)|_2^2 = |2|_2 = \frac{1}{2}$ so, we can apply Theorem 1.18, to conclude that there exists a unique solution to $X^2 - u = 0$ in $\mathbb{Z}_2$ and u is therefore a square. □

Lemma 3.6. *A nonzero 2-adic integer $2^e u$ with $u \in \mathbb{Z}_2$ is a sum of two squares in $\mathbb{Z}_2$ if and only if $u \equiv 1 \pmod 4$.*

Proof. We will break the above statement into two cases: either $u \equiv 1 \pmod 4$ or $u \equiv 3 \pmod 4$. These are the only cases to consider as $2 \nmid u$.

First, Case 1: if $u \equiv 1 \pmod 4$ then lifting to mod 8, $u \equiv 1 \pmod 8$ or $u \equiv 5 \pmod 8$. By Lemma 3.5, if $u \equiv 1 \pmod 8$ then $u = s^2 + 0^2$ for some $s \in \mathbb{Z}_2$. If $u \equiv 5 \pmod 8$ then $\frac{u}{5} \equiv 1 \pmod 8$ and we can again apply Lemma 3.5 to say that $\frac{u}{5} = s^2$ or some $s \in \mathbb{Z}_2$ so $u = 5s^2 = s^2 + (2s)^2$. As $2 = 1 + 1$, 2 is a sum of two squares, so by Lemma 2.5, $2^e u$ is a product of sums of two squares, and therefore a sum of two squares, as required.

Now, Case 2: suppose for the sake of contradiction that $u \equiv 3 \pmod 4$. Let $t = 2^e u$ in $\mathbb{Q}_2$ such that t is a sum of two squares. Then $u = \frac{t}{2^e}$ is a sum of two squares, by Lemma 3.5 and as $\frac{1}{2} = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2$.

Let $u = x^2 + y^2$ for some $x, y \in \mathbb{Z}_2$. Then $u \equiv x^2 + y^2 \pmod 4$. The only squares mod 4, however, are 0 and 1 so $u \equiv 0, 1$ or $2 \pmod 4$, which is a contradiction.

Therefore, x or $y \notin \mathbb{Z}_2$. Suppose, without loss of generality that $x \notin \mathbb{Z}_2$. Now, $y^2 = u - x^2$. As $u \in \mathbb{Z}_2^\times$, $v_2(u) = 0$ which means $|u|_2 = 1$. However, as $x \notin \mathbb{Z}_2^\times$, $|x|_2 > 1$ so $|x|_2^2 > 1$. By Lemma 1.6, $|y|_2^2 = |u - x^2|_2 = |x^2|_2 > 1$.

Let $|x|_2 = |y|_2 = 2^n$ for some $n \geq 1$. Then we can say $x = \frac{v}{2^n}$ and $y = \frac{w}{2^n}$ for some $v, y \in \mathbb{Z}_2$. Now, $v^2 + w^2 = 4^n(x^2 + y^2) = 4^n u \equiv 0 \pmod 4$. At the same time, as $v, w \in \mathbb{Z}_2^\times$, $v^2, w^2 \equiv 1 \pmod 4$, which means $v^2 + w^2 \equiv 2 \pmod 4$, which is a contradiction.

Therefore, we may conclude that $2^e u$ is a sum of two squares in $\mathbb{Z}_2$ if and only if $u \equiv 1 \pmod 4$. □

Theorem 3.7. *A nonzero integer is a sum of two squares in $\mathbb{Z}$ if and only if it is a sum of two squares in $\mathbb{R}$ and in $\mathbb{Z}_p$ for every p.*

Proof. The forward direction is trivially true. For the reverse direction, assume that a nonzero integer m is a sum of two squares in $\mathbb{R}$ and in every $\mathbb{Z}_p$. Then if $p \equiv 3 \pmod 4$ by Lemma 3.4, $v_p(m)$ is even. Therefore, m has even multiplicity by all prime factors $p \equiv 3 \pmod 4$ so Theorem 2.1 states that m is a sum of two squares in $\mathbb{Z}$. □

Acknowledgments. It is a pleasure to thank my mentors, Peter Xu and Yun Cheng, for their instrumental encouragement, wisdom, and mathematical knowledge. I would also like to thank Peter May for his critical and helpful comments, and for his assistance in refining the language and formatting of this paper.

References

[1] Fernando Q. Gouvêa. p-adic Numbers: An Introduction. Universitext. 1993

[2] An Introduction to p-adic Numbers and p-adic Analysis. Andrew Baker. http://www.maths.gla.ac.uk/ ajb/dvi-ps/padicnotes.pdf

[3] Keneth Ireland, Michael Rosen. A Classical Introduction to Modern Number Theory. Springer. 1982.

[4] Neal Koblitz. p-adic numbers, p-adic analysis, and Zeta-functions. Springer. 1977.

[5] Keith Conrad. The Local-Global Principle. http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/localglobal.pdf

[6] Keith Conrad. Hensel's Lemma. http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/hensel.pdf

[7] Jahnavi Bhaskar. Sum of Two Squares. http://www.math.uchicago.edu/ may/VIGRE/VIGRE2008 /REUPapers/Bhaskar.pdf