Local-Global Principle

Fajr Fatima

July 2022

1 Introduction

Hasse's discovery regarding Minskowski's work on the quadractic forms over rational numbers showed that a generalisation could be formed by denoting all real and p-adic numbers in terms of quadratic forms. This was the first real step for the importance of p-adic numbers as Hasse emphasized this generalisation to be applied to number theory. This principle came to be known as the Hasse principle or the *local-global principle* which states that *a property of theorem would hold over $\mathbb{Q}$ if and only if it holds over both $\mathbb{R}$ and $\mathbb{Q}_p$*

While this principle does not constitute of a definite theorem, it provides a philosophy in number theory which equates to that of studying global properties of a surface or curve based on local properties near points on the surface or curve in geometry. We consider that $\mathbb{Q}$ is a *global field* and $\mathbb{R}$ and $\mathbb{Q}_p$ are *local fields.*

Using the theorems stating that the sums of two squares in every $\mathbb{R}$ and $\mathbb{Z}_p$. we see what the local-global principle is about. After which, we will look at Hasse's version of Miskowski's theorem over quadratic forms followed by counter-examples to the local-global principle. This would be followed by discussing the results in local-global principle for heights and lastly, powers.

2 Sums of two squares in $\mathbb{Z}$

Theorem 1. *A positive integer n can be denoted as a sum of two squares only if each prime p dividing t with $p = 3 \pmod 4$ has even multiplicity as a factor of t.*

Example 1. Let $t = 15 = 3.5$, The only prime factor congruent to $3 \pmod 4$, in this case. would be 3, which divides 15 only once. The number $t = 45 = 3^2.5$ divides by 3 twice and $45 = 9 + 36 = 3^2 + 6^2$ and therefore, is seen to be a sum of two squares.

Theorem 2. *For a prime $p \equiv 3 \pmod 4$, some nonzero p-adic integer r would be a sum of two squares in $\mathbb{Z}_p$ if and only if $ord_p(r)$ is even.*

Proof. Suppose $r = p^e u$ such that $e \geq 0$ and $u \in Z_p^x$

For some x and y in $\mathbb{Z}_p$, $x^2 + y^2 = u$. Thus, to find a solution in $\mathbb{Z}_p$, we use Hensel's lemma and the pigeonhole principle.

Let us then consider the following sets

$$G = \{y^2 \pmod p : 0 \leq y \leq p-1\},$$

$$H = \{u - x^2 \pmod p : 0 \leq x \leq p-1\}.$$

An odd prime p would have $(p+1)/2$ squares in $\mathbb{Z}_p$ including 0. Therefore, each set $|G|$ and $|S|$ would be $(p+1)/2$. The sets would then use the pigeonhole principle because $|G| + |S| = p + 1 > |\mathbb{Z}_p|$ and we follow the statement that $u \equiv x_0^2 + y_0^2 \pmod p$ since there are x_0 and y_0 from 0 to $p-1$: $y_0^2 \equiv u - x_0^2 \pmod p$ where x_0 or y_0 have at least one nonzero modulo p. We can suppose that $x_0 \not\equiv 0 \pmod p$ as x_0 and y_0 are symmetric in terms of congruence.

We can then denote

$$f(X) = X^2 + (y_0^2 - u) \in \mathbb{Z}_p[X].$$

Using the Hensel's lemma, we get that there is some $x \in \mathbb{Z}_p : f(x) = 0$ and hence, $x^2 + y_0^2 = u$ because we derive that $f(x_0) \equiv 0 \pmod p$ and $f'(x_0) = 2x_0 \not\equiv 0 \pmod p$.

In the case that e is even, we suppose $e = 2k$. Hence, $r = p^{2k}u = p^{2k}(x^2+y^2)$. We can denote it as $r = (p^k x)^2 + (p^k y)^2$.

In the case that e is odd, we need to consider $x = p^n q$ and $y = p^n w$ in that $n \geq 0$ and both q and w are in $\mathbb{Z}_p$. We would denote this as

$$r = x^2 + y^2 = p^{2n}(q^2 + w^2).$$

As per the theorem statement, $q^2 + w^2$ cannot be in $\mathbb{Z}_p^x$ and are thus, $\equiv 0 \pmod p$. We simplify as

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

$$q^2 = -w^2 \equiv \pmod p$$

$$-1 \equiv (q/w)^2 \equiv \pmod 0$$

. Hence, -1 becomes a square in $\mathbb{Z}_p$ when $-1 \pmod p$ cannot be a square in the case that $p \equiv 3 \pmod 4$. □

Theorem 3. *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 every $\mathbb{Z}_p$.*

Proof. Let us consider a nonzero integer b is a sum of two squares in $\mathbb{R}$ and in every $\mathbb{Z}_p$. Using 2, we understand that some prime p dividing b with $p \equiv 3 \pmod 4$ would have an even multiplicity $\mathrm{ord}_p(m)$. We can also suppose that $b > 0$ since it is supposed to be the sum of two squares and therefore, using 1, we can prove that b is, in fact, a sum of two squares in $\mathbb{Z}$. □

3 Principle in Quadratic Forms

If we suppose quadratic forms $Q(x, y) = ax^2 + by^2$ with $a, b \epsilon \mathbb{Z} - 0$, not just $x^2 + y^2$, there is no guarantee that $Q(x, y) = m$ in $\mathbb{R}$ and each $\mathbb{Z}_p$ would provide a solution in $\mathbb{Z}$.

Example 2. Let us consider $x^2 + 11y^2 = 3$ with no integer solutions would have a solution in $\mathbb{R}$ and $\mathbb{Z}_p$. Solvability in $\mathbb{R}$ becomes clear and solvability in $\mathbb{Z}_p$ for $p \neq 2$ or 11 can be seen from solving the congruence $x^2 \equiv 3 - 11y^2 \pmod{p}$ using the pigeonhole principle and applying Hensel's lemma as we have previously in 2.

To prove solvability in $\mathbb{Z}_2$, from $3/11 \pmod{8}$ we understand that $3/11$ is a square in $\mathbb{Z}_2$ so we can solve $0^2 + 11y^2 = 3$ in $\mathbb{Z}_2$.

Example 3. Suppose $2x^2 + 7y^2 = 1$. There are no integer solutions but there is a real solution and a solution in $\mathbb{Z}_p$ for $p \neq 2$ or 7 by solving the congruence $2x^2 \equiv 1 - 7y^2 \pmod{p}$ with the pigeonhole principle and then using Hensel's lemma.

In $\mathbb{Z}_2$ with $x = 1$ the equation becomes $y^2 = -1/7$ which would have a 2-adic solution since $1/7 \equiv 1 \pmod{8}$.

In $\mathbb{Z}_7$ we can solve $2x^2 = 1$ by Hensel's lemma since $1/2 \equiv 4 \pmod{7}$.

Using the reduction and Chinese remainder theorem, a polynomial equation with integer coefficients that has solutions in $\mathbb{Z}_p$ for all p has a solution as a congruence mod m for all $m \geq 2 : x^2 + 11y^2 \equiv 3 \pmod{m}$ and $2x^2 + 7y^2 \equiv 1 \pmod{m}$ are both solvable for all m. Hence, we can understand the solvability of a polynomial equation as a congruence in every modulus does not particularly mean that we can find a solution to the polynomial equation in $\mathbb{Z}$.

Theorem 4. *Hasse Minskowski Theorem*
Let $Q(x_1, \ldots, x_n)$ be a quadratic form with rational coefficients.

- *For each $c \epsilon Q^x$ the equation $Q(x) = c$ has a solution in $\mathbb{Q}$ if and only if it has a solution in $\mathbb{R}$ and every $\mathbb{Q}_p$.*
- *The equation $Q(x) = 0$ has a solution in $\mathbb{J}$ besides $(0, \ldots, 0)$ if and only if it has a solution in $\mathbb{R}$ and every $\mathbb{Q}_p$ besides $(0, \ldots, 0)$.*

However, it only applies to finitely many cases. Thus, when $n \geq 2$ in both the mentioned cases, its solvability in $\mathbb{Q}_p$ is automatic except when $p = 2$ or a coefficient of $Q(x)$ is absent from $\mathbb{Z}_p^x$.

Example 4. Let us suppose the quadratic form $f(x, y, z) = 5x^2 + 7y^2 - 13z^2$ and attempt to find a nontrivial solution in $\mathbb{Q}_3$ for $f(x, y, z) = 0$.

We initially see that $f(x, y, z) = 0$ has a nontrivial solution in $\mathbb{R}_3$ which is denoted as $(1, 0, \sqrt{5/13})$. Now, we consider p as a prime such as $p \neq 2, 5, 7, 13$. Thus, the number of variables $f(x, y, z)$ would be $3 \pmod{p}$ because $p \neq 5, 7, 13$ and therefore, $\deg f < 3 \pmod{p}$. This quadratic form would have one trivial solution: $(0, 0, 0)$ but it would also have a nontrivial solution (x_0, y_0, z_0).

Without loss of generality, we can suppose that $x_0 \not\equiv 0 \pmod p$. We can consider $g(x) = 5x^2 + 7y_0^2 - 13z_0^2$ and so $g(x) \equiv 0 \pmod p$. We lift the solution through Hensel's Lemma from (x_0, y_0, z_0) to $(\tilde{x}_0, y_0, z_0)$ in $\mathbb{Q}_p^3$ for all primes p.

In the cases of $p = 2, 5, 7, 13$, our nontrivial solution is denoted as $(1, 0, 1)$ for $\pmod 2$, $(0, 2, 1)$ for $\pmod 5$, $(2, 0, 1)$ for $\pmod 7$ and $(3, 1, 0)$ for $\pmod{13}$.

Similarly, in the cases of $p \neq 2, 5, 7, 13$, we can lift these solutions to $\mathbb{Q}_p^3$ through Hensel's Lemma. Hnece, as f would represent 0 in $\mathbb{R}^3$ and $\mathbb{Q}_p^3$ for all primes p, the Hasse-Minskowski shows that f represents 0 in $\mathbb{Q}^3$.

4 Principle in Heights

Using the local-global principle in terms of heights can be useful to measure the computational complexity of rational numbers in their reduced forms. A relevant application of the local-global principle in heights is that of Hilbert's Product Formula.

Theorem 5. *(Product Formula) Let $a, b \in \mathbb{Q}$. So*

$$\prod_{p,\infty} (a, b)_{\mathbb{Q}p} = 1.$$

Proof. The Hilbert symbol in our equation allows us to reduce the proof to the following three cases

$a = b = -1$. In this case, when $p \neq 2, \infty$, $v_p(-1) = 0$ which would translate to $(-1, -1)_{\mathbb{Q}_p} = 1$. We find through computing in $\mathbb{Q}_2$ that $(-1, -1)\mathbb{Q}_2 = -1$ and since a and b are negative, we derive that $(a, b)_{\mathbb{R}} = -1$. Thus, $\prod_{p,\infty} (-1, -1)_{\mathbb{Q}_p} = 1$.

$a = -1, b = l$**, a prime number.** In this case, $l = 2$ and $p \neq 2, \infty$ so $v_p(-1) = v_p(2) = 0$ and thus, $(-1, 2)_{\mathbb{Q}_p} = 1$. Furthermore, as $z^2 + x^2 = 2y^2$ gives us the nontrivial solution $(1, 1, 1) = (x, y, z)$, we can see that $(-1, 2)_{\mathbb{R}} = 1 = (-1, 2)_{\mathbb{Q}_2} = 1$. Thus, $\prod_{p,\infty} (-1, 2)\mathbb{Q}_p = 1$.

In the case that $l \neq 2$ and $p = 2$, we see that $v_2(-1) = v_2(l) = 0$, and so $(-1, l)_{\mathbb{Q}_2} = (-1)^{(l-1)/2}$. In the case that $l \neq 2, p \neq 2$ where $p \neq l$, it derives $(-1, l)_{\mathbb{Q}_p} = 1$. In the case that $p = l \neq 2$ then $v_2(-1) = 0$ and $v_l(l) = 1$ and thus, $(-1, l)_{\mathbb{Q}_l} = \frac{=1}{l} = (-1)^{(L-1)/2}$.. Hence, our product denoted as $\prod_{p,\infty} (-1, l)_{\mathbb{Q}_p}$ would be equal to 1.

$a = l, b = l'$. In this case, if $l = l'$, we derive from the properties of the Hilbert symbol that $(l, l) = (l, -l^2) = (l, -1))l, l)(l, l)$. Thus, $(l, l)_{\mathbb{Q}_p} = (-1, l)_{\mathbb{Q}_p} \forall p$ which was proven in the prior case. Hence, we suppose that $l \neq l$. If $l' = 2$ and $p \neq 2, l$ then $v_p(l) = v_p(l') = 0$ and so $(l, 2)_{\mathbb{Q}_p} = 1$. In the case where $l' = 2$ and $p = 2$, we see that $(l, 2)_{\mathbb{Q}_2} = (-1)^{(l^2-1)/8}$. In the case that $l' = 2$ and $p = 1 \neq 2, v_l(l) = 1$ and $v_l(2) = 0$ then $(l, 2)_{\mathbb{Q}_l} = \frac{2}{l} = (-1)^{(l^2-1)/8}$. When $l \neq l', l, l'p \neq 2$, we have $(l, l')_{\mathbb{Q}_p} = 1$. If $p = 2$, we get $(l, l')_{\mathbb{Q}_2} = (-1)^{(l-1)(l'-1)/4}$

as $v_2(l) = v_2(l') = 0$. As $v_l(l') = 1 = v_{l'}(l)$, we get the result $(l, l')_{\mathbb{Q}_l} = (\frac{l'}{l})$ and $(l, l')_{\mathbb{Q}'_l} = (\frac{l}{l'}$. Therefore, we get the result of the product as $\prod_{p,\infty}(l, l')_{\mathbb{Q}_p} = (-1)^{(l^2-1)/4}(\frac{l'}{l})(\frac{l}{l'}) = 1$. □

5 Principle in Powers

Theorem 6. *A rational number is an nth power in $\mathbb{Q}$ if and only if it is an nth power in $\mathbb{R}$ and every $\mathbb{Q}_p$.*

Proof. Let us suppose that $r \in \mathbb{Q}$ in order to solve $x^n = r$ in $\mathbb{R}$ and every $\mathbb{Q}_p$. Let us also assume that $r \neq 0$, and see that for each p prime in r where r is an nth power in $\mathbb{Q}_p$ implies that $\text{ord}_p(r)$ is divisible by n. Hence, all primes in r suppose an nth power in that $r = s^n$ for some $s \in \mathbb{Q}$. In the case of n being odd, it is absorbed into s and r is automatically an nth power in $\mathbb{Q}$. In the case of n being even, r exists as an nth power in $\mathbb{R}$ and therefore, $r > 0$ where $r = s^n$ is still an nth power in $\mathbb{Q}$. □

However, this theorem proves a bit more nuanced outside of a finite sequence such that if $2 \leq n \leq 7$, the nth powers in $\mathbb{Q}^x$ would prove to be the nonzero rational numbers which are nth powers in all but finitely completed cycles of $\mathbb{Q}$. To understand this more, let us look at the example of $n = 8$.

Example 5. Let us show that 16 is an 8th power in all $\mathbb{Q}$ except $\mathbb{Q}_2$. We denote the equation

$$X^8 - 16 = (X^4 - 4)(X^4 + 4) = (X^2 - 2)(X^2 + 2)(X^2 - 2X + 2)(X^2 + 2X + 2).$$

Both the quadratic factors in this case have discriminant -4 which shows that there is an 8th root of 16 in every completion of $\mathbb{Q}$ that has a square root of either 2 or -2 or -4. We understand that 2 is a square in $\mathbb{R}$ and for every odd prime, one of the three numbers meeting the condition are present in $(\mathbb{Z}/(p))^x$. Hence, by Hensel's lemma, 2, -2 or -4 is a square in $\mathbb{Q}_p$. In $\mathbb{Q}_2$, however, since $\text{ord}_2(16)$ is not a multiple of 8, we see that 16 is an 8th power in every completion of $\mathbb{Q}$ except for $\mathbb{Q}_2$. ()

Theorem 7. *(Grunwald-Wang Theorem) An element x in a number field $\mathbb{K}$ is an nth power in K if and only if it is an nth power in $\mathbb{K}_p$ for all but finitely many primes of $\mathbb{K}$.*

The theorem itslef was originally just Grunwald's theorem, however it was prone to many errors until Wang's counterexample (5). Essentially, the Grunwald theorem now states that

$$\mathbb{K}(n, S) : \{x \in \mathbb{K} | x \in \mathbb{K}_p^n \forall p \notin \mathbb{S}\}$$

such that

$$\mathbb{K}(n, S) = \mathbb{K}^n.$$

unless in the special cases that

- $\mathbb{K}$ is $s$special such that 2^{s+1} divides n.
- $\mathbb{S}$ includes the special set consisting of 2-adic primes p, $\mathbb{S}_0 : \mathbb{K}_p$ is s-special.

References

[1] Hatley, Jeffrey. *Hasse-Minskowski and the Local-to-Global Principle*, The College of New Jersey (2009).

[2] Prezler, Jason. *Notes on p-Adic Numbers*, University of Utah (2005).

[3] J.W.S Cassels. *Lectures on Elliptic Curves*, Cambridge Uni. Press, Cambridge (1991).

[4] Zhang, Robin. *The Grunwald Theorem and Isomorphic Radical Extensions*, (2017).

[5] E. Selmer. *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$ Acta Arithmetica **85**(1951).

[6] S. Wang *A Counter-Example to Grunwald's Theorem*, Annals of Math **49**(1948).

[7] G. Whaples, *Non-analytic class field theory and Grunwald's theorem*, Duke Math. J.**9**(1942).

[8] Luedtke, Martin, *The Grunwald-Wang Theorem.* University of Cambridge (2013).

[9] H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (1986).

[10] H. Silverman, *The Arithmetic of Dynamical Systems*, Springer (2007).