A Survey of the Local-Global Principle

Haofang Zhu

June 2026

1 Introduction

We discuss one of the central organizing themes in number theory: the local-global principle. The principle states that to show an equation has a solution in $\mathbb{Q}$, it often suffices to show there are solutions in the nontrivial completions of $\mathbb{Q}$, specifically $\mathbb{R}$ as well as $\mathbb{Q}_p$ for each prime p, which are $\mathbb{Q}$ completed under the Euclidean metric and the p-adic metrics respectively. Here $\mathbb{Q}$ is known as a global field, while its completions are each known as local fields, hence the name "local-global principle."

The local-global principle was first coined as Hasse's principle after Helmut Hasse. Hasse realized that Minkowski's theorem for solvability of quadratic forms in $\mathbb{Z}$ could be extended to solvability of quadratic forms in $\mathbb{Q}$. This theorem became known as the Hasse-Minkowski theorem. Hasse became an advocate of analyzing equations in $\mathbb{Q}$ by first analyzing these equations in each of the local fields. We will first analyze some examples where the local-global principle is true, from the sum of two squares theorem, to the generalized Hasse-Minkowski theorem. Throughout this paper, familiarity with Hensel's lemma is assumed.

It turns out that the local-global principle does not hold unanimously for all equations. At the end of this paper, we will visit Selmer's celebrated counterexample to the local-global principle.

2 Toy Example: Sum of Two Squares

To witness the local-global principle in action, we start with the sum of two squares problem, which asks the question: when can a positive integer m be

expressed as the sum of two squares?

Theorem 2.1. *A positive integer m can be written as the sum of two squares in $\mathbb{Q}$ if and only if for each of its prime divisors p satisfying $p \equiv 3 \pmod 4$, $\nu_p(m)$ is even (where $\nu_p(m)$ denotes the exponent of the largest power of p that divides m).*

The proof of this theorem is non-central to this paper and requires understanding of how prime integers are factorized in the Gaussian integers, which is the unique factorization domain $\mathbb{Z}[i]$. Therefore, this paper will not cover the proof.

Instead, let's try to find the "local" formulation of this theorem and show that the local-global principle holds. Analyzing the equation in $\mathbb{R}$ is easy: simply take $x^2 + y^2 = 0^2 + (\sqrt{m})^2 = m$. Now we analyze the question in $\mathbb{Q}_p$. We will analyze the cases when the primes are congruent to 1 or 3 modulo 4. Analyzing the equation in $\mathbb{Q}_2$ is left to the reader.

Theorem 2.2. *If $p \equiv 1 \pmod 4$, then the equation $x^2 + y^2 = m$ always has a solution for x and y in $\mathbb{Q}_p$.*

Proof. It suffices to show that there exists an element s in $\mathbb{Q}_p$ such that $s^2 = -1$, since then we could have the following identity:

$$\left(\frac{1+t}{2}\right)^2 + \left(\frac{s(t-1)}{2}\right)^2 = t.$$

By Fermat's theorem on sums of two squares, there exists an element s_0 of $\mathbb{F}_p$ such that $s_0^2 \equiv -1 \pmod p$ since $p \equiv 1 \pmod 4$. Now, we can lift this solution to a solution in $\mathbb{Q}_p$ by Hensel's lemma since the derivative of $s^2 + 1$ with respect to s at $s = s_0$ is $2s_0 \not\equiv 0 \pmod p$. □

Now we present the case when $p \equiv 3 \pmod 4$.

Theorem 2.3. *If $p \equiv 3 \pmod 4$, then the equation $x^2 + y^2 = m$ has a solution for x and y in $\mathbb{Q}_p$ if and only if $\nu_p(m)$ is even.*

Proof. Write $m = p^k r$ where $k = \nu_p(m)$ and $r \in \mathbb{Z}_p^\times$.

Case 1: k is odd.

We show that there is no solution. If $x^2 + y^2 = m$ in $\mathbb{Q}_p$, then we must have $\nu_p(x) = \nu_p(y) = n$ for some integer n. Indeed, if $\nu_p(x) \neq \nu_p(y)$, then $\nu_p(x^2 + y^2) = 2\min(\nu_p(x), \nu_p(y))$, which is even; but $\nu_p(m) = k$ is odd, a

contradiction. Writing $x = p^n x'$ and $y = p^n y'$ with $x', y' \in \mathbb{Z}_p^\times$, we obtain $p^{2n}(x'^2 + y'^2) = p^k r$, so $x'^2 + y'^2 \equiv 0 \pmod{p}$, i.e. $(x'/y')^2 \equiv -1 \pmod{p}$. This is impossible since $p \equiv 3 \pmod{4}$, as -1 is not a quadratic residue mod p in that case.

Case 2: k is even.

It suffices to show that r is a sum of two squares in $\mathbb{Q}_p$, for then $m = p^k r = (p^{k/2})^2 \cdot r$ can be written as a sum of two squares by scaling. Let $A := \{a^2 \bmod p : a \in \mathbb{F}_p\}$ and $B := \{r - b^2 \bmod p : b \in \mathbb{F}_p\}$. Since A is the set of quadratic residues including 0, it has $\frac{p+1}{2}$ elements, and so does B. Since $|A| + |B| = p + 1 > p = |\mathbb{F}_p|$, the pigeonhole principle gives $A \cap B \neq \emptyset$: there exist $x_0, y_0 \in \mathbb{F}_p$ with $x_0^2 + y_0^2 \equiv r \pmod{p}$. Moreover x_0 and y_0 cannot both be 0 since $r \in \mathbb{Z}_p^\times$, so without loss of generality $x_0 \not\equiv 0 \pmod{p}$. The polynomial $f(X) = X^2 + (y_0^2 - r) \in \mathbb{Z}_p[X]$ satisfies $f(x_0) \equiv 0 \pmod{p}$ and $f'(x_0) = 2x_0 \not\equiv 0 \pmod{p}$, so Hensel's lemma lifts x_0 to an exact solution $x \in \mathbb{Z}_p$ with $x^2 + y_0^2 = r$. □

Lastly, for the case $p = 2$ which we do not prove, we have the following theorem:

Theorem 2.4. *The equation $x^2 + y^2 = m$ has a solution for x and y in $\mathbb{Q}_2$ if and only if $\frac{m}{2^{\nu_2(m)}} \equiv 1 \pmod{4}$.*

Based on Theorems 2.1, 2.2, 2.3, and 2.4, it is not hard to see that the sum of two squares problem obeys the local-global principle. In fact there is a stronger theorem that generalizes this.

3 The Hasse-Minkowski Theorem

In this section, we look at quadratic forms in general. This is often used as the poster example of the local-global principle. A quadratic form is a homogeneous polynomial of degree 2. In other words, $Q(x_1, x_2, \ldots, x_n)$ is a quadratic form if it can be written in the form $Q(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i,j \leq n} a_{i,j} x_i x_j$ where each $a_{i,j}$ is in $\mathbb{Q}$.

Theorem 3.1 (Hasse-Minkowski)**.** *Let $Q(x_1, x_2, \ldots, x_n)$ be a quadratic form with rational coefficients. Then $Q(x_1, x_2, \ldots, x_n) = c$ has a solution in $\mathbb{Q}$ if and only if it has a solution in $\mathbb{R}$ and in every $\mathbb{Q}_p$. In addition, when $c = 0$, there is a nontrivial solution in $\mathbb{Q}$ if and only if there is a nontrivial solution in each of these local fields.*

One direction of the theorem is straightforward: any rational solution is automatically a solution in each local field, since $\mathbb{Q}$ embeds into $\mathbb{R}$ and into every $\mathbb{Q}_p$. The remarkable content of the theorem is the converse. For a full proof, see [4] or [5].

An important practical remark is that checking local solvability does not require infinitely many verifications. For a quadratic form Q with integer coefficients, solvability in $\mathbb{Q}_p$ is automatic whenever p does not divide twice the discriminant of Q: in that case one can always find a nonsingular zero modulo p (using a pigeonhole argument as in Section 2) and lift via Hensel's lemma. Thus the Hasse-Minkowski theorem reduces rational solvability to a finite check: one verifies solvability in $\mathbb{R}$ and in $\mathbb{Q}_p$ for the finitely many primes p dividing the discriminant and $p = 2$.

Notice also that the sum of two squares problem is a specific instance of Theorem 3.1 at work: asking whether m is a sum of two squares is equivalent to asking whether the ternary form $x^2 + y^2 - mz^2$ has a nontrivial rational zero.

4 Local-Global Principle for Powers

In fact, the Hasse-Minkowski theorem is not the only example of the success of the local-global principle.

Theorem 4.1. *A rational number r 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. As with Hasse-Minkowski and all other instances of the local-global theorem, the "only-if" direction is easy, so we shall prove the "if" direction. The case $r = 0$ is easy, so assume $r \neq 0$. For each prime p satisfying $\nu_p(r) \neq 0$, r is a perfect nth power in $\mathbb{Q}_p$, so $\nu_p(r)$ is divisible by n. By examining each of these primes p, we obtain that $r = \pm k^n$ for some k. We are done if n is odd. The case where n is even could be resolved by taking note of the condition that r is a perfect power in $\mathbb{R}$. □

This theorem itself is not too surprising, but it has a stronger generalization in algebraic number theory by Grunwald and Wang, which we will not prove. One of these corollaries is shown below.

Theorem 4.2 (Corollary of Grunwald-Wang)**.** *A rational number r is an nth power in $\mathbb{Q}$ if and only if it is an nth power in $\mathbb{Q}_p$ for all but finitely many p.*

5 Selmer's Counterexample

Example 5.1 (Selmer, 1951)**.** *The cubic equation*

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a nontrivial solution in $\mathbb{R}$ *and in* $\mathbb{Q}_p$ *for every prime* p*, yet has no nontrivial solution in* $\mathbb{Q}$*.*

We follow the proof of local solvability given by Conrad. The strategy is to find a nonzero solution modulo p in each $\mathbb{F}_p$ and then lift it to a solution in $\mathbb{Q}_p$ using Hensel's lemma.

Solvability in $\mathbb{R}$: We could set $y = 0$ and $z = -1$ and reduce the equation to $3x^3 - 5 = 0$, which has the real solution $x = \sqrt[3]{5/3}$.

Solvability in $\mathbb{Q}_3$: We set $x = 0$ and $z = -1$, an to $4y^3 = 5$, or equivalently $y^3 = 5/4$. We apply a stronger version of Hensel's lemma, specifically Theorem 4.1 of [2]. To show that $\frac{5}{4}$ is a cube in $\mathbb{Z}_3$, it suffices to find α such that $|f(\alpha)|_3 < |f'(\alpha)|_3^2$ where $f(Y) = Y^3 - 5/4$ or $|\alpha^3 - \frac{5}{4}|_3 < |3\alpha^2|_3^2/|3\alpha^2|_3$. It turns out that $\alpha = 2$ works, so $5/4$ is indeed a 3-adic cube, giving the solution $(x, y, z) = (0, y, -1)$ with $y^3 = 5/4$ in $\mathbb{Q}_3$.

Solvability in $\mathbb{Q}_5$: Set $y = z = -1$, reducing to $3x^3 - 4 - 5 = 0$, or $x^3 = 3$. Since $3 \equiv 2^3 \pmod 5$, the element 3 is a nonzero cube modulo 5, and Hensel's lemma (applied to $f(X) = X^3 - 3$ with $f(2) \equiv 0 \pmod 5$ and $f'(2) = 12 \not\equiv 0 \pmod 5$) lifts this to a solution in $\mathbb{Z}_5$.

Solvability in $\mathbb{Q}_p$ **for** $p \neq 3, 5$: We assume the theory of primitive roots or basic group theory for the discussion that follows. We consider two cases.

Case 1: If $p \not\equiv 1 \pmod 3$, then $\gcd(3, p-1) = 1$, so the cubing map on $(\mathbb{Z}/p\mathbb{Z})^\times$ is a bijection: every nonzero element modulo p is a cube. In particular, 3 is a cube modulo p, and Hensel's lemma lifts this to a cube in $\mathbb{Z}_p$. Setting $x^3 = 3$ in $\mathbb{Z}_p$, we get the solution $(x, -1, -1)$.

Case 2: If $p \equiv 1 \pmod 3$ and 3 is not a perfect cube modulo p, the cubes in $(\mathbb{Z}/p\mathbb{Z})^\times$ form a subgroup of index 3, with coset representatives $\{1, 3, 9\}$. As a result, every nonzero residue is of the form b^3, $3b^3$, or $9b^3$ for some $b \not\equiv 0 \pmod p$). We apply this to $a = 5$:

1. If $5 \equiv b^3 \pmod p$, then 5 is a cube in $\mathbb{Q}_p$ by Hensel's lemma. Setting $y^3 = 5$ in $\mathbb{Q}_p$, we check that $3(-y)^3 + 4y^3 + 5(-1)^3 = 0$, So $(-y, y, -1)$ is a solution.

2. If $5 \equiv 3b^3 \pmod{p}$, then $5/3$ is a cube in $\mathbb{Q}_p$ by Hensel's lemma. Setting $x^3 = \frac{5}{3}$, we get $3x^3 + 4(0)^3 + 5(-1)^3 = 0$, so $(x, 0, -1)$ is a solution.

3. If $5 \equiv 9b^3 = 3^2b^3 \pmod{p}$, then $5 \cdot 3 \equiv (3b)^3 \pmod{p}$, so 15 is a cube in $\mathbb{Z}_p$. Setting $t^3 = 15$ and taking $(a, b, c) = (3t, -5, 7)$ yields a valid solution after some messy computations.

This exhausts all primes and confirms local solvability everywhere.

We will not show that Selmer's equation does not have a solution in $\mathbb{Q}$, since it requires some algebraic number theory or elliptic curves. The proof of this could be covered in [3] for instance.

6 Conclusion

The local-global principle is a guiding philosophy in number theory rather than a single theorem. Its most well known success is the Hasse-Minkowski theorem, but there are other examples too, such as the theorem of perfect powers. However, Selmer's example shows that the principle cannot be extended naively to higher-degree equations.

Ultimately, the local-global principle serves as a powerful heuristic even when it fails as a theorem. Local conditions are often far easier to check than global ones, and in fact, local heuristics are often used to formulate or back up conjectures such as the twin prime conjecture, or the even stronger Hardy-Littlewood conjecture.

References

[1] K.Conrad, *The Local-Global Principle*, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf`.

[2] K.Conrad, *Hensel's Lemma*, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`.

[3] K.Conrad, *Selmer's Example*, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf`.

[4] J.Hatley, *Hasse-Minkowski and the Local-to-Global Principle*, `https://www.math.union.edu/~hatleyj/Capstone.pdf`.

[5] K.Sungjin,*Hasse-Minkowski Theorem*,
https://www.csun.edu/ sungjin/HasseMinkowski.pdf.