The Hasse-Minkowski Theorem

John Ludlum

December 14, 2018

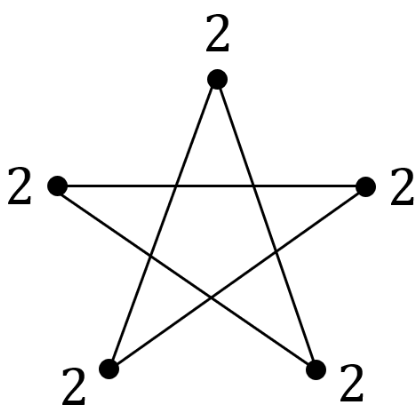
1 Introduction

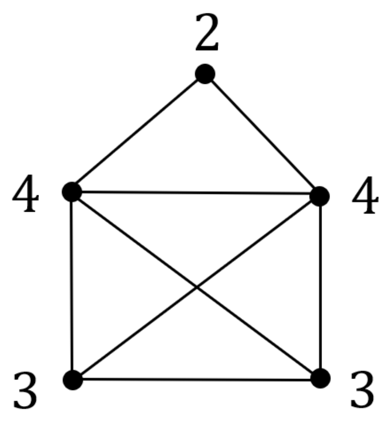
A *local-global principle* is when the local properties of a mathematical object tell you something about the global properties of the object. Here are a few examples:

Ex: (Graph theory)

Theorem: (Euler, 1735) *A connected graph has an Euler circuit if and only if every vertex has even degree.*

Recall that an Euler circuit is a path starting and ending at the same vertex which traverses each edge of the graph exactly once. According to Euler's Theorem, the left-hand graph in the diagram below has an Euler circuit because every vertex has degree 2, while the right-hand graph does not because the bottom two vertices have degree 3.





Euler's Theorem is an example of a local-global principle: the degrees of the vertices of a connected graph (a local property) tell you whether or not the graph has an Euler circuit (a global property).

Ex: (Differential geometry)

The Gauss-Bonnet Theorem relates the Gaussian curvature of a compact two-dimensional Riemann manifold (a local property) to the Euler characteristic of the manifold (a global property).

Ex: (Number theory)

Let $f(x) = x^3 - 3x + 17$. Suppose we want to solve $f(x) = 0$ for $x \in \mathbb{Z}$ (a global question). One approach is to look at the problem over the finite field $\mathbb{Z}/5\mathbb{Z}$ (a local question). In $\mathbb{Z}/5\mathbb{Z}$, the function $f(x)$ becomes $\tilde{f}(x) = x^3 + 3x + 2$. Furthermore, we can check that the equation $\tilde{f}(x) \equiv 0 \pmod 5$ has no solutions:

$$\tilde{f}(0) \equiv 2 \qquad \tilde{f}(1) \equiv 1 \qquad \tilde{f}(2) \equiv 1 \qquad \tilde{f}(3) \equiv 3 \qquad \tilde{f}(4) \equiv 3$$

Now, we know the map

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z} \qquad x \longmapsto x \pmod 5$$

is a ring homomorphism. This means that if $f(a) = 0$ for some $a \in \mathbb{Z}$, then $f(b) \equiv 0 \pmod 5$ where $b = \phi(a) \in \mathbb{Z}/5\mathbb{Z}$. But there are no such solutions b in $\mathbb{Z}/5\mathbb{Z}$ which implies there are no solutions a in $\mathbb{Z}$.

However, it is important to note that the converse is NOT true: a Diophantine equation may have solutions in $\mathbb{Z}/n\mathbb{Z}$ but not in $\mathbb{Z}$. For example, consider the function $f(x, y) = 3x^2 + 6xy + y^2$. Suppose we want to find the non-trivial solutions of $f(x, y) = 0$ for $(x, y) \in \mathbb{Z}^2$. One can check that $(1, 0)$ and $(2, 0)$ are two non-trivial solutions in $(\mathbb{Z}/3\mathbb{Z})^2$. However, factoring $f(x, y)$ over $\mathbb{R}$, we get

$$f(x, y) = \Big((3 + \sqrt{6})x + y\Big)\Big((3 - \sqrt{6})x + y\Big)$$

In other words, $f(x, y)$ is the product of two irrational lines, which means $f(x, y) = 0$ has no non-trivial solutions in $\mathbb{Q}^2$ and thus none in $\mathbb{Z}^2$.

The Hasse-Minkowski Theorem is a local-global principle that tells us when a quadratic equation such as the one above has rational solutions. In order to understand the theorem, we need to introduce the concept of p-adic numbers.

2 p-adic Numbers

Let $x = \dfrac{a}{b} \in \mathbb{Q}$. Observe that we can write $x = \dfrac{a'}{b'} p^n$ where p is prime, $\dfrac{a'}{b'}$ is in lowest terms, $p \nmid a'b'$, and $n \in \mathbb{Z}$. This leads us to the following definition:

Definition: The *p-adic order* of $x \in \mathbb{Q}$ is

$$\nu_p(x) := \begin{cases} n & x \in \mathbb{Q} \setminus \{0\} \\ \infty & x = 0 \end{cases}$$

Informally stated, the p-adic order measures the degree n to which a prime p divides a rational number x. If $\nu_p(x) > 0$, then p divides a more than it divides b. If $\nu_p(x) < 0$, then p divides b more than it divides a.

Proposition: The p-adic order has the following properties: if $x, y \in \mathbb{Q}$, then

1. $\nu_p(xy) = \nu_p(x) + \nu_p(y)$
2. $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$

where the inequality in Property 2 is an equality if and only if $\nu_p(x) \neq \nu_p(y)$.

Proof: Let $x = \dfrac{a'}{b'}p^n$ and $y = \dfrac{c'}{d'}p^m$ as described at the beginning of the section. Without loss of generality, assume $n \leq m$. Then

$$xy = \frac{a'c'}{b'd'}p^{n+m} \qquad \Longrightarrow \qquad \nu_p(xy) = n + m = \nu_p(x) + \nu_p(y)$$

$$x+y = \left(\frac{a'}{b'} + \frac{c'}{d'}p^{m-n}\right)p^n \qquad \Longrightarrow \qquad \nu_p(x+y) \geq n = \min\{\nu_p(x), \nu_p(y)\}$$

This proves Properties 1 and 2. In addition, suppose n is strictly less than m which means that $\nu_p(x) \neq \nu_p(y)$. Then $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\} = \nu_p(x)$. However, $\nu_p(x) = \nu_p(x + y - y) \geq \min\{\nu_p(x + y), \nu_p(y)\}$. If $\min\{\nu_p(x + y), \nu_p(y)\} = \nu_p(y)$, then $\nu_p(y) > \nu_p(x) \geq \nu_p(y)$ which is impossible. Thus, $\min\{\nu_p(x + y), \nu_p(y)\} = \nu_p(x + y)$. So we have $\nu_p(x + y) \geq \nu_p(x)$ and $\nu_p(x) \geq \nu_p(x + y)$ which means that $\nu_p(x + y) = \nu_p(x) = \min\{\nu_p(x), \nu_p(y)\}$. This proves that the inequality in Property 2 is an equality if and only if $\nu_p(x) \neq \nu_p(y)$. $\square$

Having established the p-adic order and two of its properties, we are ready for another definition:

Definition: The *p-adic absolute value* of $x \in \mathbb{Q}$ is

$$|x|_p := \begin{cases} p^{-\nu_p(x)} & x \in \mathbb{Q} \setminus \{0\} \\ 0 & x = 0 \end{cases}$$

Proposition: The p-adic absolute value has the following properties: if $x, y \in \mathbb{Q}$, then

1. $|x|_p = 0 \iff x = 0$
2. $|xy|_p = |x|_p\, |y|_p$
3. $|x + y|_p \leq \max\{|x|_p, |y|_p\}$

Proof: Property 1 is true by the way $|x|_p$ is defined. Next, observe that

$$|x|_p\, |y|_p = p^{-\nu_p(x)}\, p^{-\nu_p(y)} = p^{-\left(\nu_p(x)+\nu_p(y)\right)} = |xy|_p$$

which proves Property 2. Finally, without loss of generality, let $\max\{|x|_p, |y|_p\} = |x|_p$. This implies that

$$|x|_p \geq |y|_p \qquad \Longrightarrow \qquad p^{-\nu_p(x)} \geq p^{-\nu_p(y)} \qquad \Longrightarrow \qquad \nu_p(x) \leq \nu_p(y)$$

So $\nu_p(x) = \min\{\nu_p(x), \nu_p(y)\} \leq \nu_p(x + y)$. Thus,

$$\max\{|x|_p, |y|_p\} = |x|_p = p^{-v_p(x)} \geq p^{-\left(\nu_p(x)+\nu_p(y)\right)} = |x + y|_p\, .$$

This proves Property 3. $\square$

These properties of the p-adic absolute value imply that the p-adic absolute value is a metric (in fact, an ultrametric) on $\mathbb{Q}$ if we let $d(x, y) = |x - y|_p$. This leads us to two final definitions:

Definition: A *p-adic Cauchy sequence* is a sequence $\{x_n\}_{n=1}^{\infty}$ in $\mathbb{Q}$ such that

$$\forall \epsilon > 0, \quad \exists N \in \mathbb{N} : \quad \forall\, n, m \geq N, \quad |x_n - x_m|_p < \epsilon$$

Definition: The *p-adic rational numbers* $\mathbb{Q}_p$ are defined as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$. That is, if $\mathcal{C}_p$ is the set of p-adic Cauchy sequences in $\mathbb{Q}$, then

$$\mathbb{Q}_p := \left\{ \lim_{n\to\infty} x_n \;\middle|\; \{x_n\}_{n=1}^{\infty} \in \mathcal{C}_p \right\}.$$

This analytic construction of $\mathbb{Q}_p$ is analogous to how we may define $\mathbb{R}$ to be the set of limits of standard Cauchy sequences in $\mathbb{Q}$.

3 Hensel's Lemma, Chevalley-Warning Theorem

Lemma: (Hensel) *Let p be a prime, $f(x) \in \mathbb{Z}[x]$, and $m, k \in \mathbb{N}$ where $m \leq k$. If $\exists\, r \in \mathbb{Z}$ such that $f(r) \equiv 0 \pmod{p^k}$ and $f'(r) \not\equiv 0 \pmod{p}$, then $\exists\, s \in \mathbb{Z}$ such that $f(s) \equiv 0 \pmod{p^{k+m}}$ where $s \equiv r \pmod{p^k}$. Furthermore, s is unique $\pmod{p^{k+m}}$.*

Proof: Consider the Taylor expansion of $f(x)$ about the point $x = r$:

$$f(x) = f(r) + f'(r)(x-r) + \frac{f''(r)}{2!}(x-r)^2 + ...$$

This Taylor series is just the sum of N terms where $N = deg(f)$, so we don't have to worry about convergence issues. Now, the fact that we have $s \equiv r \pmod{p^k}$ in Hensel's Lemma suggests that $s = r + p^k t$ for some $t \in \mathbb{Z}$. We need to prove that t exists.

If we substitute $s = r + p^k t$ into the Taylor expansion above, we get

$$\begin{aligned} f(s) = f(r + p^k t) &= f(r) + f'(r)p^k t + \frac{f''(r)}{2!}p^{2k}t^2 + ... \\ &\equiv f(r) + f'(r)p^k t \pmod{p^{k+m}}. \end{aligned}$$

In order for $f(s) \equiv 0 \pmod{p^{k+m}}$ to hold, it must be that

$$0 \equiv f(r) + f'(r)p^k t \pmod{p^{k+m}}.$$

Observe that $f(r) = p^k a$ for some $a \in \mathbb{Z}$ since $f(r) \equiv 0 \pmod{p^k}$. This means that

$$0 \equiv \Big(a + tf'(r)\Big)p^k \pmod{p^{k+m}} \equiv a + tf'(r) \pmod{p^m}.$$

Since $f'(r) \not\equiv 0 \pmod{p}$, $f'(r)^{-1}$ exists $\pmod{p^m}$, which means we can solve for t in the equation above. This proves that t exists. Furthermore, the uniqueness of a and $f'(r)$ guarantee the uniqueness of t and thus $s \pmod{p^{k+m}}$. □

Theorem: (Chevalley-Warning) *Let K be a field of characteristic p and let $f_1, ..., f_n \in K[x_1, ...x_n]$ be polynomials in n variables such that the $\sum_{k=1}^{n} deg(f_k) < n$. If V is the set of common zeros of $f_1, ..., f_n$ in K^n, then* Card $V \equiv 0 \pmod{p}$.

Proof: Jean-Pierre Serre, *A Course in Arithmetic*, pg. 5

4 The Hasse-Minkowski Theorem

We are now in a position to state the Hasse-Minkowski Theorem.

Definition: A *quadratic form* f over a field K is a homogeneous degree-2 polynomial with coefficients in K:

$$f(x_1, ..., x_n) = \sum_{1 \leq i,j \leq n} \alpha_{ij} x_i x_j \qquad\qquad \alpha_{ij} \in K$$

f is said to *represent zero* if $\exists\ (a_1, ..., a_n) \in K^n$ such that $f(a_1, ...a_n) = 0$.

Theorem: (Hasse-Minkowski) *A quadratic form f represents 0 over $\mathbb{Q}$ if and only if f represents 0 over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p.*

Remark: The Hasse-Minkowski Theorem is a local-global principle: if we want to know if a quadratic form represents 0 over $\mathbb{Q}$ (a global property), we can check if it represents 0 over $\mathbb{R}$ and $\mathbb{Q}_p$ (local properties).

The proof of the Hasse-Minkowski Theorem is typically done by dividing all quadratic forms into five cases: $n = 1, 2, 3, 4$ and $n \geq 5$ where n is the number of variables in the quadratic form. In this paper, I will not prove the Hasse-Minkowski Theorem. However, I will present an example of how to use the theorem to solve problems which incorporates Hensel's Lemma and the Chevalley-Warning Theorem.

Ex: Consider the quadratic form $f(x, y, z) = 5x^2 + 7y^2 - 13z^2$. Suppose we want to know if the equation $f(x, y, z) = 0$ has a non-trivial solution in $\mathbb{Q}^3$.

First, observe that $f(x, y, z) = 0$ has the non-trivial solution $(1, 0, \sqrt{5/13})$ in $\mathbb{R}^3$.

Next, let p be a prime, $p \neq 2, 5, 7, 13$. Observe that the number of variables of $f(x, y, z)$ is 3 (mod p) because $p \neq 5, 7, 13$, which means deg$f < 3$ (mod p). Furthermore, $f(x, y, z) \equiv 0 \pmod{p}$ has at least one solution, i.e. the trivial solution $(0, 0, 0)$. By the Chevalley-Warning Theorem, there is also a non-trivial solution (x_0, y_0, z_0) since the number of zeros must be 0 (mod p).

Without loss of generality, assume x_0 is the non-zero value in (x_0, y_0, z_0). In other words, $x_0 \not\equiv 0 \pmod{p}$. If we let $g(x) = 5x^2 + 7y_0^2 - 13z_0^2$, then $g(x_0) \equiv 0 \pmod{p}$. Furthermore, $g'(x_0) \not\equiv 0 \pmod{p}$ because $g'(x_0) = 10x = 2 \cdot 5 \cdot x_0$ and $p \not| 2 \cdot 5 \cdot x_0$. By Hensel's Lemma, the solution (x_0, y_0, z_0) lifts to a solution $(\tilde{x}, y_0, z_0)$ in $\mathbb{Q}_p^3$ for all primes p.

In the cases that $p = 2, 5, 7, 13$, after a bit of guessing, one finds that $(1, 0, 1)$ is a non-trivial solution (mod 2), $(0, 2, 1)$ is a non-trivial solution (mod 5), $(2, 0, 1)$ is a non-trivial solution (mod 7), and $(3, 1, 0)$ is a non-trivial solution (mod 13).

Performing the same process as when $p \neq 2, 5, 7, 13$, we can use Hensel's Lemma to lift these solutions to $\mathbb{Q}_p^3$ for all primes p. We just need to define a single variable polynomial g for each solution and check that $g' \neq 0$ at the point in question.

Since f represents 0 in $\mathbb{R}^3$ and $\mathbb{Q}_p^3$ for all primes p, by the Hasse-Minkowski Theorem, f represents 0 in $\mathbb{Q}^3$.

Remark: Unfortunately, the Hasse-Minkowski Theorem is not necessarily true for higher-degree polynomials. For example, in 1951, Ernst Selmer showed that the homogeneous degree-3 polynomial $f(x, y, z) = 3x^3 + 4y^3 + 5z^3$ represents zero in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p but not in $\mathbb{Q}$. Determining why the Hasse-Minkowski Theorem fails for certain higher-degree polynomials is an area of active research.

5 References

Hatley, Jeffrey. *Hasse-Minkowski and the Local-to-Global Principle.* Undergraduate thesis, The College of New Jersey, 2009.

Preszler, Jason. *Notes on p-Adic Numbers.* University of Utah, 2005.

Selmer, Ernst. "The Diophantine Equation $ax^3 + bx^3 + cz^3 = 0$." *Acta Math*, Vol. 85 (1951): 203-362.

Serre, Jean-Pierre. *A Course in Arithmetic.* New York: Springer, 1973.