Hasse-Minkowski and the Local-to-Global Principle

Jeffrey Hatley

April 16, 2009

Abstract

Students in introductory number theory and abstract algebra classes learn that, when given an equation with integer coefficients, it may help to look at this equation modulo a prime; if it has no solutions in $\mathbb{Z}/p\mathbb{Z}$, then it will have no solutions in $\mathbb{Z}$. This idea of looking “locally” to gain “global” information is a powerful tool in number theory, and mathematicians have devised ways to apply this method in more general contexts. This paper develops some of this machinery and culminates with the celebrated Hasse-Minkowski theorem.

1 Introduction

The study of equations and their solutions is an old and fundamental subject in mathematics. In particular, given an equation $f = 0$ where $f \in \mathbb{Z}[x_1, \ldots, x_n]$, it is natural to ask whether $f$ has any solutions consisting entirely of rational numbers (or, equivalently, integers). These are called Diophantine equations, named for the 3rd century Greek mathematician who studied such equations at length. Determining the answer to these questions can be difficult in general. Some cases are easy, however. For example, consider the polynomial

$$f(x) = x^3 - 2x + 17.$$ 

To determine whether this has any integer solutions, we may reduce the coefficients of $f$ modulo 5 to obtain

$$\bar{f} = x^3 + 3x + 2$$

and determine whether $\bar{f}$ has any solutions in $\mathbb{Z}/5\mathbb{Z}$. This is easy since there are only five numbers to check, and we quickly see that $\bar{f}$ has no such solutions. Now, since the map $\phi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ via $\phi(x) = x \pmod{5}$ is a ring homomorphism, we have that any solution $x \in \mathbb{Z}$ of $f$ would map to a solution $\phi(x) \in \mathbb{Z}/5\mathbb{Z}$ of $\bar{f}$; since $\bar{f}$ has no such solutions, we can conclude that $f$ has no integer solutions. (Note, however, that if we had found a solution of $\bar{f}$ in $\mathbb{Z}/5\mathbb{Z}$, this would not allow us to conclude that $f$ had a solution in $\mathbb{Z}$.)
This strategy of looking modulo a prime is referred to as looking locally, and our example illustrates the “local-to-global” principle: look locally (in \( \mathbb{Z}/5\mathbb{Z} \)) to obtain information globally (in \( \mathbb{Z} \)). While this method worked great in our example, sometimes it yields no information (like when \( \bar{f} \) does have a zero), and other times it cannot be applied at all (e.g. if \( f \in \mathbb{Q}[x] \)). In an effort to extend the scope of the local-to-global principle, we will need to explore the p-adic numbers. Henceforth, \( p \) will denote a rational prime unless otherwise noted. Our final goal is a discussion of the Hasse-Minkowski theorem, which gives a strong local-to-global correspondence for a special family of equations.

2 p-Adic Numbers

2.1 Definition

First introduced by Kurt Hensel, the p-adic numbers give an alternate completion of the rational numbers \( \mathbb{Q} \) than the standard completion \( \mathbb{R} \); it is denoted \( \mathbb{Q}_p \). (A completion of a field \( K \) is an extension \( \bar{K} \) such that every cauchy sequence in \( K \) converges in \( \bar{K} \). The reader should not worry if cauchy sequences and completions are unfamiliar; we will be focusing mostly on the algebraic aspects of \( \mathbb{Q}_p \).)

The crucial point of departure from the standard completion of \( \mathbb{Q} \) is the definition of a \textit{p-adic norm} on \( \mathbb{Q} \). Recall that a norm on a field \( K \) is a function \( |\cdot|: K \to \mathbb{R}_+ \) satisfying

\begin{itemize}
  \item[i)] \( |x| = 0 \iff x = 0 \)
  \item[ii)] \( |xy| = |x||y| \) for all \( x,y \in K \)
  \item[iii)] \( |x + y| \leq |x| + |y| \) for all \( x,y \in K \).
\end{itemize}

In addition, a norm is called \textit{non-archimidean} if it satisfies an additional property:

\begin{itemize}
  \item[iv)] \( |x + y| \leq \max\{|x|, |y|\} \) for all \( x,y \in K \).
\end{itemize}

Note that (iv) implies (iii), so being non-archimidean is a stronger property.

The standard absolute value on \( \mathbb{Q} \) yields the standard completion \( \mathbb{R} \); to obtain each \( \mathbb{Q}_p \), a different absolute value on \( \mathbb{Q} \) is used. Before defining these absolute values, we first define the \textit{p-adic valuation} on \( \mathbb{Q} \).

For every \( x \in \mathbb{Z} - \{0\} \), there exist unique integers \( n, x' \in \mathbb{Z} \) such that \( x = p^n x' \) and \( p \nmid x' \). We set \( \nu_p(x) = n \); we call \( n \) the p-adic valuation of \( x \). Thus, we have

\[ x = p^{\nu_p(x)} x'. \]

We can easily extend this function to \( \mathbb{Q} \): for \( \frac{a}{b} \in \mathbb{Q} - \{0\} \), we let

\[ \nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b). \]
Hence, for every nonzero rational number, we have $x = p^{\nu_p(x)} \frac{a}{b}$ where $p \nmid ab$; in this way, one can think of $\nu_p(x)$ as the “maximum” number of times that $p$ divides $x$, where the “maximum” may be negative. By convention we set $\nu_p(0) = \infty$.

The valuation function has several nice properties. In particular, the reader may wish to verify that for all $x, y \in \mathbb{Q}$ we have

$$\nu_p(xy) = \nu_p(x) + \nu_p(y) \quad (1)$$

and

$$\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}. \quad (2)$$

These properties follow easily from the characterization $x = p^{\nu_p(x)} x'$ where $p \nmid x'$. In particular, $\nu_p(x + y) > \min\{\nu_p(x), \nu_p(y)\}$ only if $\nu_p(x) = \nu_p(y)$.

Using the $p$-adic valuation, we may now define the $p$-adic absolute value (or $p$-adic norm), denoted by $| \cdot |_p$.

**Definition 1.** For every $x \in \mathbb{Q}$, the $p$-adic absolute value of $x$ is

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

if $x \neq 0$ and $|0|_p = 0$.

That $| \cdot |_p$ satisfies the definition of a norm follows immediately from equations 1 and 2.

This absolute value is quite different from the standard absolute value. A moment’s reflection on the definition reveals that a rational number $\frac{a}{b} \in \mathbb{Q}$ in lowest form is “small” if $a$ is highly divisible by $p$, it is “large” if $b$ is largely divisible by $p$, and $|\frac{a}{b}| = 1 \iff p \nmid ab$.

We will not go through the construction of $\mathbb{Q}_p$, but instead focus on what elements of $\mathbb{Q}_p$ look like. Toward that end, recall that in our standard base-10 number system, a positive integer $x \in \mathbb{Z}_+$ is written as a juxtaposition of “digits” $x = a_n \cdots a_1 a_0$ where

$$x = \sum_{i=0}^{n} a_i \cdot 10^i \text{ with } 0 \leq a_i \leq 9.$$  

The number 10 in our base system is arbitrary, of course, and we could instead express numbers in terms of powers of primes $p$ if we wished, e.g.

$$x = \sum_{i=0}^{n} a_i \cdot p^i \text{ with } 0 \leq a_i \leq p - 1. \quad (3)$$

We call (3) the $p-$adic expansion of $x$. This construction works perfectly well, and we can add and multiply numbers component-wise (making sure to “carry”
digits in exactly the same way as we did for base-10). Notice also that writing a number in the form \((3)\) allows us to gain information regarding a number’s divisibility by \(p\); namely, \(\nu_p(x) = i\) where \(i\) is the least index in the expansion such that \(a_i \neq 0\).

Such a representation is not limited to integers; in fact, we can express every element of \(\mathbb{Q}\) this way, provided we allow for an infinite number of terms “to the right” in the series and a finite number of terms \(a_ip^i\) with \(i < 0\); more precisely,

\[
\mathbb{Q} \ni \frac{a}{b} = \sum_{n \geq -n_0} a_n p^n \text{ with } 0 \leq a_n \leq p - 1 \text{ and } -n_0 = \nu_p \left( \frac{a}{b} \right) \quad (4)
\]

The necessity of both of these new conditions will be clearest if illustrated by an example. Suppose we wish to find the 5−adic expansion of \(22/85\). First we write the 5−adic expansions of 22 and 85:

\[
22 = 2 \cdot 5^0 + 4 \cdot 5^1
\]

and

\[
85 = 2 \cdot 5^1 + 3 \cdot 5^2.
\]

Note that \(\nu_5 \left( \frac{22}{85} \right) = -1\). Hence we seek to find the coefficients of the 5−adic expansion

\[
\frac{22}{85} = \sum_{i=-1} a_i \cdot 5^i \text{ with } 0 \leq a_i \leq 4.
\]

They key is realizing that this expansion, when multiplied by the 5−adic expansion of 85, must yield the 5−adic expansion of 22. That is, we are trying to solve for the \(a_i\) in the equation

\[
2 + 4p = (2p + 3p^2)(a_{-1}p^{-1} + a_0 + a_1p + a_2p^2 + \ldots) \quad (5)
\]

where we have replaced each instance of 5 with \(p\) to highlight the \(p\)−adic behavior and to make the computations clearer. (Using “\(p\)” cases the computations by suppressing the urge to add terms and by making “carrying” operations more transparent.) Our strategy will be to solve this equation modulo \(p^i\) for each \(i \geq -1\); we will show that we can do this for the first few values of \(i\), after which the method will make it clear that this process can be continued indefinitely.

First we wish to solve the equation modulo \(p\); equation (5) becomes

\[
2 \equiv (2p + 3p^2)(a_{-1}p^{-1} + a_0 + a_1p + a_2p^2 + \ldots) \pmod{p}
\]

\[
\equiv 2a_{-1} \pmod{p}
\]

\[
\Rightarrow a_{-1} = 1
\]

and so we have obtain our first coefficient. Setting \(a_{-1} = 1\), we now look at equation (5) modulo \(p^2\):
\[ 2 + 4p \equiv (2p + 3p^2)(p^{-1} + a_0 + a_1p + a_2p^2 + \ldots) \mod (p^2) \]
\[ \equiv 2 + 2a_0p + 3p \mod (p^2) \]
\[ \Rightarrow 4p \equiv (2a_0 + 3)p \mod (p^2) \]
\[ \Rightarrow 4 \equiv 2a_0 + 3 \mod (p) \]
\[ \Rightarrow a_0 = 3 \]

and so we have obtained our second coefficient. Continuing in this way, at every step we are required to solve an equation modulo \( p \), and this is always possible due to the field structure of \( \mathbb{Z}/p\mathbb{Z} \). Thus we can write \( \frac{22}{5} \) and any other nonnegative rational number in the form (4).

It remains to show that negative rational numbers can be written in the form (4) for a given prime \( p \). It suffices to show this for integers; in fact, we need only show this for \( x = 1 \), and this is easy. Keeping in mind that \( y = -1 \) is the additive inverse of \( x = 1 \), we simply need to find a number

\[ y = \sum_{n \geq 0} a_n p^n \text{ with } 0 \leq a_n \leq p - 1 \]

such that \( 1 + y = 0 \). It is easy to verify, then, that

\[ y = \sum_{n \geq 0} (p - 1)p^n \]

satisfies this equation, remembering that carrying must be done modulo \( p \).

We are now prepared to define the \( p \)–adic rational numbers. Although a precise definition involves the limit of cauchy sequences, the following definition completely characterizes the \( p \)–adics:

**Definition 2.** The \( p \)–adic rational numbers \( \mathbb{Q}_p \) consist of all numbers of the form

\[ x = \sum_{n \geq -n_0} a_n p^n \text{ with } 0 \leq a_n \leq p - 1 \text{ and } -n_0 = \nu_p(x) \]

where the series may contain infinitely many terms. Two \( p \)–adic numbers \( x, x' \in \mathbb{Q}_p \) are equal if \( |x - x'|_p = 0 \).

We also define a subset of \( \mathbb{Q}_p \) to be the \( p \)–adic integers, denoted \( \mathbb{Z}_p \):

**Definition 3.** The \( p \)–adic integers \( \mathbb{Z}_p \) consist of the set

\[ \mathbb{Z}_p = \{ x \in \mathbb{Q}_p : |x|_p \geq 1 \}; \]
equivalently, \( x \in \mathbb{Z}_p \) if and only if \( x \) is of the form

\[
x = \sum_{i=0} a_i p^i.
\]

It is important to point out that, for \( x \in \mathbb{Z}_p \), if we set

\[
\alpha_n = \sum_{i=0}^n a_i p^i
\]

then we have \( \alpha_{n+1} \equiv \alpha_n \mod p^n \) for \( n \geq 0 \). This gives us an alternate way of representing \( x \):

\[
x = \lim_{n \to \infty} (a_0, a_1, \ldots, a_n, \ldots).
\]

We call such a sequence \( (a_i) \) with the congruence condition on consecutive terms a coherent sequence. Thus, \( \mathbb{Z}_p \) consists of (the limits of) all coherent sequences. Once again, the fact that these coherent sequences converge in \( \mathbb{Q}_p \) follows from the \( p \)-adic norm.

An examination of the methods used above reveals that \( \lim(a_i) = x \in \mathbb{Z}_p \) is a unit (that is, there exists \( y \in \mathbb{Z}_p \) such that \( xy = 1 \)) if and only if \( a_0 \neq 0 \).

We are now ready to explore some more subtle properties of the \( p \)-adic numbers.

### 2.2 Hensel’s Lemma

It is straightforward (though tedious) to check that, under the component-wise addition and multiplication defined in the preceding section, each \( \mathbb{Q}_p \) is a field. In the discussion above, we showed that there is a natural injection \( \mathbb{Q} \hookrightarrow \mathbb{Q}_p \), but it is not immediately obvious that \( \mathbb{Q}_p \) is strictly larger than \( \mathbb{Q} \). We will be able to prove this quite easily after establishing the following fundamental theorem due to Hensel:

**Theorem 4. (Hensel’s Lemma)** Let \( f \in \mathbb{Z}_p[x] \) be a polynomial with coefficients in \( \mathbb{Z}_p \). Suppose there is a \( p \)-adic integer \( \alpha_1 \) such that

\[
|f(\alpha_1)|_p < |f'(\alpha_1)|_p^2
\]

where \( f' \) is the formal derivative of \( f \). Then there is a unique \( p \)-adic integer \( \alpha \) such that

\[
f(\alpha) \equiv 0
\]

and

\[
\alpha \equiv \alpha_1 \mod (p^{\nu_p(f(\alpha_1))} - \nu_p(f'(\alpha_1))).
\]
Proof: We show that, given $\alpha_1$, we can construct a coherent sequence whose limit is a root of the polynomial. Let

$$\nu_p(f(\alpha_1)) = j$$

and

$$\nu_p(f'(\alpha_1)) = k$$

where $0 \leq 2k < j$. Thus we have $f(\alpha_1) = p^i \xi$ and $f'(\alpha_1) = p^k \gamma$ for some $p$-adic units $\xi$ and $\gamma$. We wish to show that there exists $\alpha_2 \equiv \alpha_1 \mod p^{j-k}$ such that $f(\alpha_2) \equiv 0 \mod p^{j+1}$. Thus, we set

$$\alpha_2 = \alpha_1 + b_2 p^{j-k}$$

and show that we can solve for $b_2$. Now, using the Taylor expansion of $f$ we obtain

$$f(\alpha_2) = f(\alpha_1 + b_2)$$

$$= f(\alpha_1) + f'(\alpha_1) b_2 p^{j-k} + \frac{1}{2!} f''(\alpha_1) b_2^2 p^{2j-2k} + \text{terms in } p^n, n \geq p^{j+1}.$$ 

If $p$ is odd, then

$$\nu_p \left( \frac{1}{2!} f''(\alpha_1) b_2^2 p^{2j-2k} \right) \geq 2j - 2k$$

$$> 2j - j = j$$

hence we have

$$f(\alpha_2) \equiv f(\alpha_1) + f'(\alpha_1) b_2 p^{j-k} \mod p^{j+1}. \quad (6)$$

If $p = 2$, we gain only one additional term and the argument is the same, so we complete the proof for $p > 2$. Now, equation (6) yields

$$f(\alpha_2) \equiv f(\alpha_1) + f'(\alpha_1) b_2 p^{j-k} \mod p^{j+1}$$

$$\equiv p^i \xi + b_2 \gamma p^j \mod p^{j+1}$$

hence we wish to solve for $b_2$ in the equation

$$0 \equiv p^i \xi + b_2 \gamma p^j \mod p^{j+1},$$

or equivalently

$$0 \equiv p^i + b_2 \gamma \mod p$$

which is certainly solvable since $\xi, \gamma$ are units in $\mathbb{Z}/p\mathbb{Z}$. Thus we can obtain $\alpha_2$ with the desired properties. The theorem now follows by induction. $\square$

Hensel’s lemma is an invaluable tool when studying $p$-adic numbers, as it tells us that we can sometimes “lift” a local solution of a polynomial to a global

Hensel’s lemma is an invaluable tool when studying $p$-adic numbers, as it tells us that we can sometimes “lift” a local solution of a polynomial to a global
solution. With a simple application of Hensel’s lemma, we can show that $\mathbb{Q}_p$ is strictly larger than $\mathbb{Q}$ for every $p$.

**Proposition 5.** For every prime $p$, we have an embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ where the inclusion $\mathbb{Q} \subset \mathbb{Q}_p$ is strict.

**Proof.** Fix a prime $p$. We have already shown the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. It remains to show that $\mathbb{Q}_p \not\subset \mathbb{Q}$.

Consider the case when $p$ is odd and let $(a/b)$ denote the Legendre symbol. If $p \equiv 1 \mod 4$, then $(−1/p) = 1$; if $p \equiv 7 \mod 8$, then $(2/p) = 1$; and if $p \equiv 3 \mod 8$, then $(−2/p) = 1$. Hence the equation

$$f(x) = \begin{cases} 
  x^2 + 1 & \text{if } p \equiv 1 \mod 4 \\
  x^2 - 2 & \text{if } p \equiv 7 \mod 8 \\
  x^2 + 2 & \text{if } p \equiv 3 \mod 8 
\end{cases}$$

has a solution $\alpha_1$ modulo $p$ for which it is easily seen that $f'(\alpha_1) \neq \mod p$. Thus, by Hensel’s lemma, $f$ has a solution in $\mathbb{Q}_p$ for each $p$. Since none of $−1, 2$, or $2$ are squares in $\mathbb{Q}$, this shows that $\mathbb{Q}_p \not\subset \mathbb{Q}$.

For $p = 2$, consider the equation

$$f(x) = x^3 - 3.$$

Then $f(3) \equiv 0 \mod 8$ but $f'(3) = 3 \neq 0 \mod 2$, hence by Hensel’s lemma this solution lifts to solution in $\mathbb{Q}_2$ and so $\mathbb{Q}_2 \not\subset \mathbb{Q}$. □

The $p$–adic numbers form a fascinating field with many interesting properties. As has been stated several times, each $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ containing $\mathbb{Q}$ as a dense subset. It is a metric space with a topology induced by $|\cdot|_p$; this topological space is totally disconnected. More algebraically, our representation $\mathbb{Z}_p \ni x = \lim(\alpha_i)$ hints at the fact that $\mathbb{Z}_p$ is the inverse limit of the projective system

$$
\cdots \rightarrow (\mathbb{Z}/p^n\mathbb{Z}) \rightarrow \cdots \rightarrow (\mathbb{Z}/p^3\mathbb{Z}) \rightarrow (\mathbb{Z}/p^2\mathbb{Z}) \rightarrow (\mathbb{Z}/p\mathbb{Z}),
$$

and we could instead define $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. All of these things are beyond the scope of this paper; however, the interested reader is encouraged to see [1] or [2].

With some understanding of $\mathbb{Q}_p$, we are ready to move forward in our exploration of the local-to-global principle. One final thing should be noted: by convention, $\mathbb{R}$ is considered to be $\mathbb{Q}_\infty$; that is, $\mathbb{R}$ is the $p$–adic completion of $\mathbb{Q}$ with respect to the “prime at infinity”. We call $\mathbb{Q}$ a global field and each $\mathbb{Q}_p$ a local field, hence the term “local-to-global”.  


3 Hilbert Symbol

This section explores some properties of the Hilbert symbol, named for the eminent German mathematician David Hilbert. The Hilbert symbol is a generalization of the Legendre symbol and is important in the proof of the Hasse-Minkowski theorem. For the remainder of this section, unless otherwise noted, we let $K$ denote either $\mathbb{R}$ or $\mathbb{Q}_p$ for some prime $p$. As usual, $K^*$ denotes $K \setminus \{0\}$. This section follows the proofs from Serre in [2].

**Definition 6.** Let $a, b \in K^*$ where $K = \mathbb{Q}_p$. We define

$$(a, b)_p = 1 \text{ if } z^2 - ax^2 - by^2 = 0 \text{ has a solution } (z, x, y) \neq (0, 0, 0) \text{ in } K^3$$

$$(a, b)_p = -1 \text{ otherwise.}$$

We call $(a, b)_p = \pm 1$ the Hilbert symbol of $a$ and $b$ relative to $K$. If there will be no confusion, we simply write $(a, b)$.

We first present two elementary properties of the Hilbert symbol.

**Proposition 7.** Let $a, b \in K^*$ and let $K_b = K(\sqrt{b})$. Then $(a, b) = 1$ if and only if $a \in NK_b^*$, the group of norms of elements of $K_b^*$.

**Proof.** First, suppose $b = c^2$ for some $c \in K$. Then the equation $z^2 - ax^2 - by^2 = 0$ has the solution $(c, 0, 1)$, so $(a, b) = 1$. Since $b$ is a square, $K_b = K$, so $NK_b^* = K^* \ni a$.

Now suppose $b$ is not a square in $K$. Then there exists $\beta \in K_b$ such that $\beta^2 = b$, and if $x \in K_b$ then $x = z + \beta y$ for some $y, z \in K$, and the norm of $x$ is $N(x) = N(z + \beta y) = z^2 - by^2$. If $a \in NK_b^*$ then $a = z^2 - by^2$ for some $z, y \in K$, hence the quadratic form $z^2 - ax^2 - by^2$ has the zero $(z, 1, y)$:

$$a = z^2 - by^2$$

$$\Rightarrow 0 = z^2 - a - by^2$$

$$= z^2 - a \cdot 1^2 - by^2$$

hence $(a, b) = 1$. Conversely, suppose $(a, b) = 1$. Then $z^2 - ax^2 - by^2 = 0$ has some non-zero solution $(z, x, y) \neq (0, 0, 0)$. If $x = 0$ then $\left(\frac{z}{y}\right)^2 = b$, but we supposed that $b$ was not a square. Hence $x$ is nonzero, and we have that $a$ is the norm of $\frac{z}{x} + \beta \frac{y}{x}$:

$$0 = z^2 - ax^2 - by^2$$

$$\Rightarrow ax^2 = z^2 - by^2$$

$$\Rightarrow a = \frac{z^2}{x^2} - \frac{by^2}{x^2}$$

$$\Rightarrow a = N\left(\frac{z}{x} + \beta \frac{y}{x}\right). \quad \Box$$
Proposition 7 may seem strange at first, but it turns out to be very useful. For starters, it is used to prove the next proposition:

**Proposition 8.** Let \( a, a', b, c \in K^* \), and in formulas (ii) and (iv) below, suppose \( a \neq 0 \). The Hilbert symbol satisfies the following formulas:

i) \((a, b) = (b, a)\) and \((a, c^2) = 1\),
ii) \((a, -a) = 1\) and \((a, 1 - a) = 1\),
iii) \((a, b) = 1 \Rightarrow (aa', b) = (a', b)\),
iv) \((a, b) = (a, -ab) = (a, (1 - a)b)\).

**Proof.**

1. Formula (i) is clear from the definition of the Hilbert symbol.
2. If \( b = -a \), then
   
   \[
   0 = z^2 - ax^2 - by^2 = z^2 - ax^2 + ay^2
   \]
   
   has the zero \((z, x, y) = (0, 1, 1)\). Similarly, if \( b = 1 - a \), the defining quadratic equation has the zero \((z, x, y) = (1, 1, 1)\). This proves formula (ii).
3. If \((a, b) = 1\), then by Prop. 7 we have \( a \in NK_b^* \), which is a group, hence \( a' \in NK_b^* \Leftrightarrow aa' \in NK_b^* \), applying Prop. 7 again proves formula (iii).
4. Formula (iv) follows from formulas (i)-(iii). □

A more general form of formula (iii) above, which we will not prove, is the equivalence \((aa', b) = (a, b)(a', b)\), which says that the Hilbert symbol is bilinear.

Although these propositions are nice, in general, the calculation of \((a, b)\) via the definition would be very difficult. Actually, the case when \( K = \mathbb{R} \) is rather easy: for \( a, b \in \mathbb{R} \), \((a, b) = -1\) if and only if \( a \) and \( b \) are both \(-1\). This follows immediately from the definition of the Hilbert symbol and the familiar properties of the real numbers. The \( p \)-adic fields \( \mathbb{Q}_p \) are decidedly less-familiar; however, a “closed-form” solution exists for these fields as well. First, to ease notation, we define two functions:

\[
\epsilon(z) \equiv \frac{z - 1}{2} \pmod{2}
\]

and

\[
\omega(z) \equiv \frac{z^2 - 1}{8} \pmod{2}.
\]
Then the following theorem allows one to calculate any Hilbert symbol.

**Theorem 9.** Let $K = \mathbb{Q}_p$ and write $a = p^\alpha u, b = p^\beta v$ where $u, v$ are $p$–adic units. Let $(x/y)$ denote the Legendre symbol. Then

$$(a, b) = (-1)^{\alpha \beta e(p)} (u/p)^\beta (v/p)^\alpha$$

if $p \neq 2$ and

$$(a, b) = (-1)^{c(u) + \alpha \omega(v) + \beta \omega(u)}$$

if $p = 2$.

The proof of this theorem is beyond the scope of this paper; the interested reader should see [2].

Another important theorem is the “product formula”, proved by Hilbert himself. Let $V$ be the set of all prime numbers as well as $\infty$. Recall that $\mathbb{Q}_\infty = \mathbb{R}$; thus, for every $v \in V$, we may speak of $\mathbb{Q}_v$.

**Theorem 10. (Product Formula)** If $a, b \in \mathbb{Q}^*$, we have $(a, b)_v = 1$ for almost all $v \in V$ (that is, for all but a finite number), and

$$\prod_{v \in V} (a, b)_v = 1$$

**Proof.** We mentioned above that the Hilbert symbol is bilinear, thus it suffices to prove the theorem when $a$ and $b$ are equal to $-1$ or to a prime number. We thus consider cases and apply Theorem 9 to each.

1. If $a = b = -1$, then $(-1, -1) = (-1, -1)_2 = 1$, and one can see that if $p \neq 2$, then $(-1, -1)_p = 1$. Since there are an even number of $v \in V$ such that $(a, b)_p = -1$, the product of the Hilbert symbols equals 1.

2. Suppose $a = 1, b = l$ where $l$ is a prime. If $l = 2$, then $(1, 2)_v = 1$ for all $v \in V$, which can easily be seen since the solution $(1, 1, 1)$ exists:

$$1^2 + 1 \cdot 1^2 - 2 \cdot 1^2 = 0.$$  

If $l \neq 2$, then if $v \neq 2, l$ then in applying Theorem 9 to $(a, b)_v$ we have $\alpha = \beta = 0$, hence $(a, b)_v = 1$. Otherwise, $v = 2$ or $l$, and Theorem 9 yields $(-1, l)_2 = (-1, l)_l = (-1)^{\epsilon(l)}$. Once again, taking the product of these Hilbert symbols yields 1.

3. Suppose now that $a = l, b = l'$ with $l, l'$ primes. If $l = l'$, then by formula (iv) of Prop. 8 we have $(l, l')_v = (l, -1)_v$ for each $v \in V$, and the formula follows from case 2 above. Otherwise, we have $l \neq l'$. Suppose $l' = 2$. 

11
Then once again, $\alpha$ and $\beta$ in Theorem 9 are equal to 0 when $v \neq 2, l$, hence $(l, 2)_v = 1$. Otherwise, by Theorem 9 we have

$$(l, 2)_2 = (-1)^{\omega(l)}$$

and

$$(l, 2)_l = (2/l) = (-1)^{\omega(l)}$$

by the properties of the Legendre symbol. Taking the product of the Hilbert symbols yields 1.

If $l$ and $l'$ are distinct odd primes, then once again $(l, l')_v = 1$ for $v \neq 2, l, l'$, and Theorem yields

$$(l, l')_2 = (-1)^{\omega(l)\omega(l')}$$

and

$$(l, l')_l = (l'/l), (l, l')_l = (l/l').$$

By Quadratic Reciprocity, $(l'/l)(l/l') = (-1)^{\omega(l)\omega(l')}$, and taking the product again equals 1, completing the proof. □

We state without proof two more theorems regarding the Hilbert symbol which will be needed for the proof of the Hasse-Minkowski theorem. Once again, the interested reader is encouraged to see [2] for the proofs. The first theorem gives necessary and sufficient conditions for the existence of rational numbers with give Hilbert symbols.

**Theorem 11.** Let $(a_i)_{i \in I}$ be a finite family of elements in $\mathbb{Q}^*$ and let $(\epsilon_{i,v})_{i \in I, v \in V}$ be a family of numbers equal to $\pm 1$. Then there exists $x \in \mathbb{Q}^*$ such that $(a_i, x)_v = \epsilon_{i,v}$ for all $i \in I, v \in V$ if and only if

1. Almost all the $\epsilon_{i,v}$ are equal to 1,
2. For all $i \in I$ we have $\prod_{v \in V} \epsilon_{i,v} = 1$, and
3. For all $v \in V$ there exists $x_v \in \mathbb{Q}^*_v$ such that $(a_i, x_v)_v = \epsilon_{i,v}$ for all $i \in I$.

The second theorem is actually proved as a lemma on the way to proving Theorem 11. We have stated already that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ for each $p$. This theorem tells us that $\mathbb{Q}$ is also dense in the product of a finite number of $\mathbb{Q}_p$; thus, given $(x_1, \ldots, x_n) \in \prod^n \mathbb{Q}_p$, we can find $x \in \mathbb{Q}$ arbitrarily close to $x_i$ in $\mathbb{Q}_p$.

**Theorem 12. (Approximation Theorem)** Let $S$ be a finite subset of $V$. The image of $\mathbb{Q}$ in $\prod_{v \in S} \mathbb{Q}_v$ is dense in this product (for the product topology of those $\mathbb{Q}_v$).

Having met both the $p$–adic fields $\mathbb{Q}_p$ and the Hilbert symbol, we may now discuss the celebrated Hasse-Minkowski theorem.
4 The Hasse-Minkowski Theorem

This paper began with an example of the local-to-global principal on an elementary level. With the tools of $p$–adic fields, such methods may now allow us to solve a wider range of problems. For example, consider the equation

$$11y^2 = 11^2 - 2^211x^2 + 2^3x^4.$$ 

One might ask whether this equation has any non-trivial solutions $(x, y) \in \mathbb{Q}^2$. With the tools we started with, we might hope that reducing this equation modulo 2 or 11 would yield information – specifically, if there were no solutions to this equation in $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/11\mathbb{Z}$, then we would know there were no rational solutions. However, reducing modulo 2 yields the equation

$$y^2 = 1$$

which has solutions $(x, 1)$ for all $x \in \mathbb{Q}$, and reducing modulo 11 yields

$$0 = 2^3 x^4$$

which has solutions $(0, y)$ for all $y \in \mathbb{Q}$. Thus, this method gives no information in this example. However, we may use $p$–adic numbers to attack this problem. Since $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, if we can find a $p$ such that the equation has no solutions in $\mathbb{Q}_p$, then we will know the equation has no solutions in $\mathbb{Q}$. Let us consider the equation in $\mathbb{Q}_{11}$, and suppose there exists a non-trivial solution $(x, y)$ in $\mathbb{Q}_{11}$. We will consider the 11–adic valuations of each side, which must be equal. Let $\nu_{11}(y) = j$ and $\nu_{11}(x) = k$. On the left-hand side, we have

$$\nu_{11}(11y^2) = 2j + 1,$$

and on the right side we have

$$\nu_{11}(11^2 - 2^211x^2 + 2^3x^4) \geq \min\{2, 1 + 2k, 4k\}.$$ 

Since the 11–adic valuation of the left side is odd, we must have that the 11–adic valuation of the right side is odd. This implies that

$$\nu_{11}(11^2 - 2^211x^2 + 2^3x^4) = \min\{2, 1 + 2k, 4k\} = 1 + 2k.$$ 

But if $k \geq 1$, $\min\{2, 1 + 2k, 4k = 2\}$, and if $k < 1$ then $\min\{2, 1 + 2k, 4k\} = 4k$. This contradiction allows us to conclude that our equation has no solutions in $\mathbb{Q}_{11}$ and hence no solutions in $\mathbb{Q}$.

The use of $p$–adic fields has greatly increased the scope of our local-to-global principle, but all is not perfect. For instance, finding a solution in $\mathbb{Q}_{11}$ still would not have guaranteed the existence of a solution in $\mathbb{Q}$. Indeed, Ernest Selmer showed that the equation

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

has no solutions in $\mathbb{Q}$. Therefore, the local-to-global principle is not always valid.
is everywhere locally solvable but not globally solvable - that is, it has a solution in each \( \mathbb{Q}_p \) but not in \( \mathbb{Q} \).

Sometimes, however, things work out exactly as they “should”, and the Hasse-Minkowski theorem describes just such an instance. Before stating the theorem, we need a few more definitions.

**Definition 13.** Let \( K \) be a field. A quadratic form over \( K \) is a degree-two polynomial in \( n \) variables of the form

\[
f(x_1, \ldots, x_n) = a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2
\]

with \( a_i \in K^* \) for each \( i \). The number \( n \) of variables is called the rank of \( f \). We define the discriminant of \( f \) to be

\[
d(f) = a_1 \cdots a_n.
\]

For \( a \in K \), we say that \( f \) represents \( a \) if there exists \( (X_1, \ldots, X_n) \in K^n \) with \( (X_1, \ldots, X_n) \neq (0, \ldots, 0) \) such that

\[
f(X_1, \ldots, X_n) = a.
\]

The theory of quadratic forms is vast and rich, and the interested reader should once again consult [2]. We shall simply state without proof three properties of quadratic forms which we will need in the proof of Hasse-Minkowski. Although their proofs are not difficult, they would take us too far afield into the theory of quadratic forms. Their proofs can be found in [2]. The first is a corollary to a theorem of Chevalley and Warning.

**Proposition 14.** Let \( K \) be a finite field. Then every quadratic form over \( K \) in at least 3 variables has a non-trivial zero.

The second proposition is a technical lemma involving the Hilbert symbol. Associated with every quadratic form \( f = \sum a_ix_i^2 \) is a number

\[
\epsilon(f) = \prod_{i<j}(a_i, a_j)
\]

called the Hasse-Witt invariant. This number \( \epsilon \) is clearly equal to \( \pm 1 \); it turns out that this number is also an invariant of \( f \), meaning that it does not change if the \( a_i \) are represented with respect to different orthogonal basis of \( K \). This means that \( \epsilon \), although its definition may seem mysterious, is a fundamental attribute of \( f \). The same is true of the discriminant \( d(f) \) defined above. Of the four parts of the next proposition we will need only parts (2) and (4); the rest are included as a bonus for the reader.

**Proposition 15.** Let \( f \) be a quadratic form over \( K \), let  \( a \in K^*/K^{*2} \), let \( d = d(f) \), and let \( \epsilon = \epsilon(f) \). Then \( f \) represents \( a \) if and only if
1. $f$ is rank 1 and $a = d$,
2. $f$ is rank 2 and $(a, -d) = \epsilon$,
3. $f$ is rank 3 and either $a \neq -d$ or $a = -d$ and $(-1, -d) = \epsilon$, or
4. $f$ is rank $\geq 4$.

The third proposition is the easiest and most intuitive of the three.

**Proposition 16.** Let $g$ and $h$ be two quadratic forms of rank $\geq 1$ over a field $K$, and let $f = g - h$ be the (formal) difference of $g$ and $h$. Then $f$ represents 0 if and only if there exists $a \in K^*$ such that both $g$ and $h$ represent $a$.

In other words, Proposition 16 says that if, for example, $g$ and $h$ are both rank 2 quadratic forms, then letting

$$f = (a_1x_1^2 + a_2x_2^2) - (a_3x_3^2 + a_4x_4^2) = g - h$$

we have that $f$ represents 0 if and only if both $g$ and $h$ represent some non-zero $a$.

With these propositions, we are now ready to state and prove the Hasse-Minkowski theorem. Recall that $V = \{\text{all primes}\} \cup \{\infty\}$.

**Theorem 17. (Hasse-Minkowski)** Let $f$ be a quadratic form over $\mathbb{Q}$, and for $p \in V$ let $f_p$ be the form considered over $\mathbb{Q}_p$ (which makes sense, since $\mathbb{Q} \subset \mathbb{Q}_p$). Then $f$ represents 0 if and only if $f_p$ represents 0 for every $p \in V$.

Before proving this theorem, it is worth taking a moment to understand what it says. In the examples we have considered, we have met instances where a certain polynomial did not have a root in some $\mathbb{Q}_p$, and hence it did not have a root in $\mathbb{Q}$; however, finding a root in $\mathbb{Q}_p$ would not guarantee the existence of a root in $\mathbb{Q}$. In fact, we saw a (degree 3) polynomial which Selmer proved had a root in each $\mathbb{Q}_p$ but not in $\mathbb{Q}$. The Hasse-Minkowski theorem tells us that for every quadratic form over $\mathbb{Q}$, the existence of a root in $\mathbb{Q}$ is equivalent to the existence of a root in each $\mathbb{Q}_p$. Thus, finding a $\mathbb{Q}_p$ without a root would show that $\mathbb{Q}$ has no roots, as it did before, but now if one can show that a quadratic form $f$ has a root in every $\mathbb{Q}_p$, then it is guaranteed to have a root in $\mathbb{Q}$. Note that this is an existence proof; it does not give any hint as to what the solution in $\mathbb{Q}$ might be. Since local fields are in some sense easier to work with than $\mathbb{Q}$, this simplifies the problem of determining whether a root exists, even if it does so by "reducing" the problem to an infinite amount of cases. The proof of the theorem works by patching together local information to obtain global information. We now prove the theorem à la Serre [2].
Proof of the Hasse-Minkowski Theorem.

The "only if" direction is immediate from the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. To prove the other direction, which is the interesting part of the theorem, we let

$$f = a_1 x_1^2 + \ldots + a_n x_n^2, \ a_i \in \mathbb{Q}^*$$

and break the proof into the cases $n = 2, 3, 4, \geq 5$. Since it is clear that the theorem is true for $f$ if and only if it is true for $a_1 f$ (since $a_1 \neq 0$), we may replace $f$ by $a_1 f$ if necessary and therefore suppose throughout the proof that $a_1 = 1$. Keep in mind that our assumption is that $f$ represents 0 in every $\mathbb{Q}_p$, and we wish to show that the same is true in $\mathbb{Q}$.

1. Case $n=2$.

In this case, we have $f = x_1^2 - ax_2^2$ for some nonzero $a \in \mathbb{Q}$. Now, we know that $f$ has a nontrivial root in $\mathbb{Q}_\infty = \mathbb{R}$, hence $a > 0$. Since $a$ is a rational number, it has a "factorization" which may include negative powers of prime numbers. Thus, we may write

$$a = \prod_p p^{\nu_p(a)}$$

where the product runs over all (finite) primes. Since each $f_p$ represents 0, we have

$$a = \frac{x_1^2}{x_2^2}$$

in each $\mathbb{Q}_p$, so $a$ is a square in each $\mathbb{Q}_p$. This implies that $\nu_p(a)$ is even for every $p$, hence $a$ is a square in $\mathbb{Q}$, and so $f$ represents 0 in $\mathbb{Q}$.

2. Case $n=3$.

The proof of this case is due to the renowned Legendre. We have

$$f = x_1^2 - ax_2^2 - bx_3^2$$

for some nonzero $a, b \in \mathbb{Q}$. Looking at the equation, we see that we may assume that $a$ and $b$ are square-free integers, since otherwise we can multiply them by squares via $x_1^2$ and $x_2^2$ to achieve this. This means that for every finite prime $p$, we have $\nu_p(a)$ and $\nu_p(b)$ are equal to 0 or 1. It is also clear that we can re-number the variables if necessary to assume that $|a| \leq |b|$, where this is the “standard” absolute value on $\mathbb{Q}$. We proceed by induction on the integer $m = |a| + |b|$. If $m = 2$, then we must have

$$f = x_1^2 \pm x_2^2 \pm x_3^2.$$ 

Since $f_\infty$ represents 0, it is clear that $f \neq x_1^2 + x_2^2 + x_3^2$. In each of the other cases, roots in $\mathbb{Q}$ can be found easily by inspection; for instance, $f = x_1^2 - x_2^2 + x_3^2$ has the root $(1, 1, 0)$. 

16
Now suppose $m > 2$, which implies that $|b| \geq 2$. Since $b$ is a square-free integer, we can write

$$b = \pm p_1 \cdots p_2$$

for some distinct primes $p_i$. Let $p$ be one of the $p_i$. We will prove that $a$ is a square modulo $p$. If $a \equiv 0 \pmod{p}$ then is is obvious. Otherwise, $a$ is a $p$-adic unit (since it is an integer). By hypothesis, there exists a non-zero $(x, y, z) \in \mathbb{Q}_p^3$ such that

$$z^2 - ax^2 - by^2 = 0. \quad (7)$$

It is a consequence of the “inverse limit” structure of $\mathbb{Z}_p$ that we may assume that $(x, y, z)$ is primitive; that is, at least one of $x, y, z$ is a $p$-adic unit, and thus not divisible by $p$. Since $p | b$, we have

$$z^2 - ax^2 \equiv 0 \pmod{p}. \quad (8)$$

Now, if $x \equiv 0 \pmod{p}$, then the above equation implies that $z \equiv 0 \pmod{p}$. Then these congruences and equation (7) would imply that $p^2 | by^2$. But $\nu_p(b) = 1$, which implies that $y \equiv 0 \pmod{p}$. This contradicts the fact that $(x, y, z)$ is primitive. Hence $x \not\equiv 0 \pmod{p}$. Then equation (8) implies that $a$ is a square modulo $p$. But since $\mathbb{Z}/b\mathbb{Z} = \prod \mathbb{Z}/p_i\mathbb{Z}$, and $a$ is a square modulo each $p_i$, we have that $a$ is a square modulo $b$. Thus, there exist integers $t, b'$ such that

$$t^2 = a + bb'$$

and by the structure of $\mathbb{Z}/b\mathbb{Z}$ we can choose $t$ such that $|t| \leq \frac{|b|}{2}$. Rearranging this equation, we obtain

$$bb' = t^2 - a$$

which shows that $bb'$ is the norm of some number in the field extension $K(\sqrt{a})/K$ where $K = \mathbb{Q}$ or $\mathbb{Q}_p$. Thus, by the same argument as in the proof of Prop. 7, we see that $f'$ represents 0 in $K$ if and only if the same is true for

$$f' = x_1^2 - ax_2^2 - b'x_3^2.$$ 

By hypothesis, $f'$ represents 0 in each of the $\mathbb{Q}_p$. But due to the bounds we placed on the size of $|t|$ and $|a|$ we have:

$$|b'| = \left| \frac{t^2 - a}{b} \right| \leq \frac{|b|}{4} + 1 < |b| \text{ since } b \geq 2.$$

Write $b'$ in the form $b''u^2$ with $b''$, $u$ integers and $b''$ squarefree. From the above inequality, we clearly have $|b''| < |b|$. But then by the induction hypothesis, the form

$$f'' = x_1^2 - ax_2^2 - b''x_3^2$$

represents 0 in $\mathbb{Q}$, and it is easy to see that $f''$ is equivalent to $f'$; hence $f'$ and therefore $f$ represents 0 in $\mathbb{Q}$ and the theorem is established in this case.
3. Case \( n=4 \)

We can write our quadratic form as

\[
f = ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2)
\]

for some non-zero \( a, b, c, d \in \mathbb{Q} \). Let \( p \in V \). By hypothesis, \( f_p \) represents 0, so by Proposition 16 there exists some \( x_p \in \mathbb{Q}_p^* \) which is represented by both \( g = ax_1^2 + bx_2^2 \) and \( h = cx_3^2 + dx_4^2 \). Recalling the definitions of both \( d(f) \) and \( \epsilon(f) \), we have

\[
\begin{align*}
d(g) &= ab, \\
\epsilon(g) &= (a, b), \\
d(h) &= cd, \text{ and} \\
\epsilon(h) &= (c, d).
\end{align*}
\]

Thus, by Proposition 15 we have

\[
(x_p, -ab)_p = (a, b)_p \text{ and } (x_p, -cd)_p = (c, d)_p \text{ for all } p \in V.
\]

By Hilbert’s Product Formula (Theorem 10), we have

\[
\prod_{p \in V} (a, b)_p = \prod_{p \in V} (c, d)_p = 1,
\]

so the conditions of Theorem 11 are satisfied (look them up!), hence there exists \( x \in \mathbb{Q}^* \) such that

\[
(x, -ab)_p = (a, b)_p \text{ and } (x, -cd)_p = (c, d)_p \text{ for all } p \in V.
\]

If \( z \) is a variable, then the quadratic forms \( g - xz^2 \) and \( h - xz^2 \) both represent 0 in each \( \mathbb{Q}_p \) (by Proposition 15), and since we have already proven the Hasse-Minkowski theorem for rank 3 forms, this implies that \( g \) and \( h \) both represent 0 in \( \mathbb{Q} \). But \( f = g - h = (g - xz^2) - (h - xz^2) \), hence \( f \) represents 0.

4. Case \( n \geq 5 \)

This case is the most difficult to prove. We provide a rather complete sketch of the proof, asking the reader to accept a few facts about quadratic forms, or to see [2] for the requisite theory (or the complete proof). We use induction on \( n \). Just as in the previous case, we can represent \( f \) as the difference of two quadratic forms of ranks 2 and \( n - 2 \):

\[
f = h - g
\]

with

\[
h = a_1x_1^2 + a_2x_2^2
\]
and
\[ g = -(a_3 x_3^2 + \ldots + a_n x_n^2). \]

Let \( S \subset V \) be the subset consisting of \( \infty, 2, \) and the numbers \( p \) such that \( \nu_p(a_i) \neq 0 \) for one \( i \geq 3 \). This set is finite, since the \( a_i \) and their prime divisors are finite. Let \( p \in S \). Since \( f_p \) represents 0 by hypothesis, Prop. 16 implies that there exists \( a_p \in \mathbb{Q}_p^* \) which is represented in \( \mathbb{Q}_p \) by both \( h \) and \( g \); there exist \( x_i^p \in \mathbb{Q}_p, i = 1, \ldots, n \) such that
\[ h(x_1^p, x_2^p) = a_p = g(x_3^p, \ldots, x_n^p). \]

Although this paper did not explore the topology of \( \mathbb{Q}_p \), it can be shown that the squares of \( \mathbb{Q}_p^* \) form an open set. Then by the Approximation Theorem (Theorem 12), there must exist \( x_1, x_2 \in \mathbb{Q} \) such that, if \( a = h(x_1, x_2) \), then \( \frac{a}{a_p} \in \mathbb{Q}_p^{*2} \) for all \( p \in S \). (That is, we can find \( x_1, x_2 \in \mathbb{Q} \) such that \( h(x_1, x_2) \) approximates \( a_p \) in each \( \mathbb{Q}_p \) by at worst a square.)

Now consider the form \( f_1 = a z^2 - g \) with \( z \) a variable. For each \( p \in S \) we know \( g \) represents \( a_p \) in \( \mathbb{Q}_p \), and since \( \frac{a}{a_p} \in \mathbb{Q}_p^{*2} \) we have that \( g \) also represents \( a \) by Prop. 15 since \( f \) has rank \( n - 1 \geq 4 \). Thus, \( f_1 \) represents 0 in \( \mathbb{Q}_p \).

By the construction of \( f_1 \), it can be shown that \( f_1 \) also represents 0 for each \( p \notin S \); this is a consequence of the fact that, for \( p \notin S \), the coefficients of \( g \) are \( p \)-adic units (by the definition of \( S \)). This implies easily that the discriminant \( d_p(g) \) of \( g \) considered over each \( \mathbb{Q}_p, p \notin S \) is also a unit; less easily, it implies that \( \epsilon_p(g) = 1 \), and these two facts together imply that \( f_1 \) represents 0 in \( \mathbb{Q}_p \) for every \( p \in V \).

Since the rank of \( f_1 \) is \( n - 1 \), our induction hypothesis shows that \( f_1 \) represents 0 in \( \mathbb{Q} \), or in other words \( g \) represents \( a \) in \( \mathbb{Q} \). Since we already showed that \( h \) also represents \( a \), this implies that \( f = h - g \) represents 0, completing the proof of the Hasse-Minkowski theorem. □

5 An Example

At this point, while acknowledging the beauty of the Hasse-Minkowski theorem, the reader may be forgiven for wondering how this theorem makes solving problems any simpler. Indeed, it transforms the problem of finding a solution to an equation in one field to finding a solution in infinitely many fields! However, the local fields \( \mathbb{Q}_p \) are much nicer to work with than \( \mathbb{Q} \) and do indeed simply matters, as this concluding example shows.

Example of the Hasse-Minkowski Theorem’s Application

Let us determine whether the quadratic form
\[ f(x, y, z) = 5x^2 + 7y^2 - 13z^2 \]
(9)
has any non-trivial rational root; that is, if there exists \((x_0, y_0, z_0) \in \mathbb{Q}^3\) such that \(f(x_0, y_0, z_0) = 0\). We will use the Hasse-Minkowski theorem by showing that a root exists in \(\mathbb{Q}_p^3\) for each prime \(p\) and in \(\mathbb{R}^3\). The fact that a root exists in \(\mathbb{R}^3\) is obvious, so we focus our attention on each \(\mathbb{Q}_p\).

1. In \(\mathbb{Q}_p\) where \(p \not| 2 \cdot 5 \cdot 7 \cdot 13\)

In this case, by Proposition 14 there exists a non-trivial solution \((x_0, y_0, z_0) \in (\mathbb{Z}/p\mathbb{Z})^3\) to the congruence

\[
5x^2 + 7y^2 - 13z^2 \equiv 0 \pmod{p}.
\]

Since the solution is non-trivial, at least one of \(x_0, y_0, z_0\) is not divisible by \(p\); suppose \(p \not| x_0\). Then by above,

\[
g(x) = 5x^2 + 7y_0^2 - 13z_0^2
\]

has the root \(x_0\), so \(\nu_p(g(x_0)) \geq 1\), while

\[
g'(x_0) = 10x_0 \not\equiv 0 \pmod{p}
\]

since \(p \not| 2 \cdot 5 \cdot x_0\). So by Hensel’s lemma this lifts to a solution \((\bar{x}, y_0, z_0) \in \mathbb{Q}_p^3\). The same argument works if \(p \not| y_0\) or \(p \not| z_0\).

2. In \(\mathbb{Q}_2\)

Let \(y_0 = 0\) and \(z_0 = 1\), and set

\[
g(x) = 5x^2 + 7y_0^2 - 13z_0^2
= 5x^2 - 13,
\]

so we have

\[
g'(x) = 10x.
\]

Then \(x = 1\) is a root of \(g\) with \(\nu_2(g(1)) = 3\) and \(\nu_2(g'(1)) = 1\), so by Hensel’s lemma we can lift this to a solution \((x, y_0, z_0) \in \mathbb{Q}_2^3\).

3. In \(\mathbb{Q}_5\)

Let \(x_0 = 0\) and \(y_0 = 2\), and set

\[
g(z) = 5x_0^2 + 7y_0^2 - 13z^2
= 28 - 13z^2,
\]

so we have

\[
g'(z) = 26z.
\]

Then \(\nu_5(g(1)) = 1\) and \(\nu_5(g'(1)) = 0\) so by Hensel’s lemma this lifts to a solution \((x_0, y_0, \bar{z}) \in \mathbb{Q}_5^3\).
4. In $\mathbb{Q}_7$
Let $x_0 = 2$ and $y_0 = 0$, and set
\[
g(z) = 5x_0^2 + 7y_0^2 - 13z^2
= 20 - 13z^2,
\]
so we have
\[
g'(z) = 26z.
\]
Then $\nu_7(g(1)) = 1$ and $\nu_7(g'(1)) = 0$, so by Hensel’s lemma this lifts to a solution $(x_0, y_0, z) \in \mathbb{Q}_7^3$.

5. In $\mathbb{Q}_{13}$
Let $x_0 = 3$ and $z_0 = 0$, and set
\[
g(y) = 5x_0^2 + 7y^2 - 13z_0^2
= 45 + 7y^2,
\]
so we have
\[
g'(y) = 14y.
\]
Then $\nu_{13}(g(1)) = 1$ and $\nu_{13}(g'(1)) = 0$, so by Hensel’s lemma this lifts to a solution $(x_0, y, z_0) \in \mathbb{Q}_{13}^3$.

Thus the quadratic form (9) has a solution in every $\mathbb{Q}_p$ including $\mathbb{R}$, so by the Hasse-Minkowski theorem it has a solution in $\mathbb{Q}$. □

As this example illustrates, the Hasse-Minkowski theorem is a powerful tool in modern number theory which generalizes a simple but effective idea from elementary number theory.

6 Acknowledgements

The author would like to thank Dr. Thomas Hagedorn for all of his help and guidance with this paper. The author would also like to thank the entire TCNJ faculty and staff for their devoted instruction and assistance over the past four years, without which this capstone could never have been written.

References
