The Hasse-Minkowski Principle and Two Big Ideas

Igor Tolkov

March 12, 2010

Abstract

This paper discusses two ideas related to the Hasse-Minkowski theorem on the existence of rational zeros of quadratic forms. The p-adic numbers are introduced in sufficient detail to state the theorem. We then transition the discussion to Hilbert's generalization of the Legendre symbol that is used in the proof of the Hasse-Minkowski theorem.

Contents

1 Introduction

A central question to the study of curves is the existence therein of rational solutions. Precisely, if $f(x_1, ..., x_n) \in \mathbb{Q}[x_1, ..., x_n]$, we are interested in the existence of nontrivial roots of f over $\mathbb{Q}$. If f is a monic polynomial in $\mathbb{Z}$, then all of its rational roots must be integers. For these polynomials, it is not hard

to prove that a root does not exist by considering the equation modulo primes p. If for some p, the monic polynomial has no root, then it doesn't have a root in any of the p equivalence classes, so there is no integral root. For example, suppose we would like to show that the following polynomial f has no rational roots:

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

One approach is to use the rational root test. Neither ± 1 nor ± 17 are roots, and there cannot be others. Another is to reduce the equation modulo a prime. The magic number p in this case is 5. Note that $f(5) \neq 0$ and in $\mathbb{F}_5$, the polynomial reduces to

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

We check that this polynomial has no roots:

$$f(0) = 2 \qquad f(1) = 1 \qquad f(2) = 1 \qquad f(3) = 3 \qquad f(4) = 3$$

Indeed, f has no roots over $\mathbb{F}_5$, so it does not have any roots over $\mathbb{Z}$.

It is useful to extend this method and establish a converse, that is, a criterion that determines whether a given polynomial has a rational root. In full generality, such a criterion is unknown, but one does exist when f is a quadratic form, that is, a homogenous polynomial of degree 2. To do so, we will define the notion of a p-adic number and the related field $\mathbb{Q}_p$.

2 p-Adic Numbers

In this section we introduce the p-adic numbers and highlight several of their properties. We shall present two separate constructions of p-adic numbers.

2.1 Analytical Construction

The analytic construction of p-adic numbers is an attempt at a different completion of $\mathbb{Q}$. Much of the content of this section is described in more detail in [2]. Recall a bit of analysis:

Definition 1. *A sequence $x_1, \ldots$ is* Cauchy *iff for every $\varepsilon > 0$ there is an $N > 0$ such that for every $m, n > N$, $\|x_m - x_n\| < \varepsilon$.*

Definition 2. *The metric space $M = (X, \|\cdot\|)$, is* complete *iff every Cauchy sequence in X converges to an element of X. A* completion *of M is the smallest metric space $\bar{M} = (\bar{X}, \|\cdot\|)$ such that $M \subseteq \bar{M}$ and $\bar{M}$ is complete.*

In what follows, let X be the set $\mathbb{Q}$. (The theory is much more general, however.) The completion of M clearly depends on the definition of norm, or distance function. By using appropriate distance functions, we obtain the p-adic numbers.

2.1.1 The p-adic Metric

Define the *p-adic norm* as follows: first introduce the *p-adic valuation*:

Definition 3. *For any integer $x \neq 0$, define the* p-adic valuation $\nu_p(x)$ *as the biggest power of p dividing x. For a rational $x = q/r$, with q, r integers, define*

$$\nu_p(x) = \nu_p(q) - \nu_p(r).$$

If $x = 0$, define $\nu_p(x) = +\infty$.

Note that it does not matter that $(p, q) = 1$, as any extra factor of p in q and r contributes equally to $\nu_p(q)$ and $\nu_p(r)$ and thus cancels in their difference, while any other factor contributes to neither $\nu_p(q)$ nor $\nu_p(r)$, and again doesn't change the value of $\nu_p(x)$. We can now define the p-adic norm:

Definition 4. *For $x \in \mathbb{Q}$, let $\nu_p(x)$ be defined as above. Then the* p-adic norm *is*

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

For example, $520/14 = 2^2 \cdot 5 \cdot 7^{-1} \cdot 13$, so

$$\left|\frac{520}{14}\right|_2 = 2^{-2} = \frac{1}{4} \qquad \left|\frac{520}{14}\right|_5 = 5^{-1} = \frac{1}{5}$$

$$\left|\frac{520}{14}\right|_7 = 7^1 = 7 \qquad \left|\frac{520}{14}\right|_{13} = 13^{-1} = \frac{1}{13}$$

For any other prime p,

$$\left|\frac{520}{14}\right|_p = p^0 = 1$$

We now have a metric.

Theorem 1. *The norm $|\cdot|_p$ as defined above defines a metric by $d(x, y) = |x - y|_p$.*

Proof. Fix a prime p. We need to check the axioms of a metric:

- $|x|_p \geq 0$: if $x = 0$, $|x|_p = 0 \geq 0$. Otherwise $|x|_p = p^{\nu_p(x)} \geq 0$ because $p \geq 0$.
- $|x|_p = 0 \iff x = 0$: if $x = 0$, then we have defined $|x|_p = 0$. Assume $x \neq 0$. Then $|x|_p = p^{\nu_p(x)}$. $\nu_p(x)$ is clearly finite, so $|x|_p \neq 0$.

- $|x|_p = |-x|^p$: if $x = 0$, then $x = -x$ so $|x|_p = |-x|^p$. Otherwise, let $x = q/r$ and $-x = -q/r$. Since -1 is a unit in $\mathbb{Z}$, q and $-q$ have the same prime factorization so $\nu_p(q) = \nu_p(-q)$. Then $\nu_p(x) = \nu_p(-x)$ so $|x|_p = |-x|^p$.
- $|x+y|_p \leq |x|_p + |y|_p$: again, this holds trivially if $x = -y$ or if either $x = 0$ or $y = 0$. Assume not. Let $x = q_1/r_1$ and $y = q_2/r_2$, and factor out the largest power of p. That is,

$$x = \frac{p_1 q_1}{p_{-1} r_1} \qquad y = \frac{p_2 q_2}{p_{-2} r_2} \qquad p \not| q_1, r_1, q_2, r_2$$

Then

$$x + y = \frac{p_1 q_1 p_{-2} r_2 + p_{-1} r_1 p_2 q_2}{p_{-1} r_1 p_{-2} r_2}$$

The largest power of p in the numerator is $\max\{p_1 p_{-2}, p_{-1} p_2\}$. In the denominator, the power of p is $p_{-1} p_{-2}$. Thus

$$\nu_p(x+y) = \frac{p_1 p_{-2}}{p_{-1} p_{-2}} = \frac{p_1}{p_{-1}} = \nu_p(x) \text{ or } \nu_p(x+y) = \frac{p_{-1} p_2}{p_{-1} p_{-2}} = \frac{p_2}{p_{-2}} = \nu_p(y)$$

And $\nu_p(x+y) \leq \max\{\nu_p(x), \nu_p(y)\}$. If $p > 1$, $|x+y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$, and we are done.

□

2.1.2 The p-adic completion

Let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ under the p-adic metric defined by $\|\cdot\|_p$. The resulting field ends to have interesting topology, as can be seen from the following theorem.

Theorem 2. *Let $a, b \in \mathbb{Q}_p$ and $r, s \geq 0$.*

1. *If $b \in B(a, r)$, then $B(a, r) = B(b, r)$.*
2. *If $b \in \bar{B}(a, r)$, then $\bar{B}(a, r) = \bar{B}(b, r)$.*
3. *$B(a, r)$ is both open and closed.*
4. *if $r \neq 0$, $\bar{B}(a, r)$ is both open and closed.*
5. *$B(a, r) \cap B(b, s) \neq \emptyset$ iff $B(a, r) \subseteq B(b, s)$ or $B(b, s) \subseteq B(a, r)$.*
6. *$\bar{B}(a, r) \cap \bar{B}(b, s) \neq \emptyset$ iff $\bar{B}(a, r) \subseteq \bar{B}(b, s)$ or $\bar{B}(b, s) \subseteq \bar{B}(a, r)$.*

Thus, every ball is both open and closed, and any two balls are either totally disjoint or one is contained in the other. We will not prove this, as the topology of $\mathbb{Q}_p$, while interesting, is not relevant to this paper.

2.2 Algebraic Construction

There is an analogous algebraic construction of the p-adic field.

Start with the integers. We can consider a chain of homomorphisms

$$\cdots \to \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \cdots \to \mathbb{Z}/p\mathbb{Z}$$

Let $A_n = \mathbb{Z}/p^n\mathbb{Z}$ and $\phi_n : A_n \to A_{n-1}$ be the homomorphism with kernel $p^{n-1}A_n$. We can define the p-adic integers as follows:

Definition 5. *The ring of p-adic integers, denoted $\mathbb{Z}_p$, is the sequence $(..., x_n, x-n-1, ..., x_1)$ where $x_n \in A_n$ and $\phi_n(x_n) = x_{n-1}$ for $n \geq 2$ under element-wise addition and multiplication.*

We prove the following structure about $\mathbb{Z}_p$, being somewhat messy in the distinction between $\mathbb{Z}$ and $\mathbb{Z}_p$. The ring isomorphism between the two is obvious from definition.

Theorem 3. *Let U denote the group of invertible elements of $\mathbb{Z}_p$. Then every non-zero element of $\mathbb{Z}_p$ can be written as $p^n u$ with $n \geq 0$ and $u \in U$.*

Proof. We just need to prove that u is coprime to p if and only if it is invertible in $\mathbb{Z}_p$. Assume $x \in A_n$ with $p \not| x$. then the image of x in $A_1 = \mathbb{Z}/p\mathbb{Z}$ is nonzero, so x is invertible in A_1. In A_n, we have $y, z \in A_n$ such that $xy + pz = 1$ (since $(x, p) = 1$ in A_n). Then

$$xy(1 + pz + \cdots + (pz)^{n-1}) = (1 - pz)(1 + pz + \cdots + (pz)^{n-1}) = 1 - p^n z^n = 1$$

Since $p^n = 0$ in A_n, and we see that x is invertible. This is true for every A_n, so it is true for $\mathbb{Z}_p$.

Conversely, if $x \in \mathbb{Z}_p$ is invertible, then it is invertible in every A_n, so in particular it is invertible in $A_1 = \mathbb{Z}/p\mathbb{Z}$, so $p \not| x$. □

We call n the *p-adic valuation* of x, denoted $n = \nu_p(x)$. This definition is equivalent to the one in the analytic construction, as is the notation $\nu_p(0) = +\infty$.

It can be easily seen that $\mathbb{Z}_p$ has no zero-divisors. It is clearly non-empty, so it is an *integral domain*. We can then define $\mathbb{Q}_p$ as the field of fractions of $\mathbb{Z}_p$.

Definition 6. *The p-adic field $\mathbb{Q}_p$ is the field of fractions of the ring of p-adic integers $\mathbb{Z}_p$.*

In $\mathbb{Q}_p$, we have a similar representation to that in $\mathbb{Z}_p$:

$$q = \frac{p^n u}{p^m v} = p^{n-m}\frac{u}{v}$$

For more details about the algebraic properties of p-adic numbers, refer to [6]. For more basic algebra, [1] is useful.

2.3 The Hasse Minkowski Theorem

We are now ready to state the desired criterion.

Theorem 4 (Hasse-Minkowski)**.** *Let f be a quadratic form with coefficients in $\mathbb{Q}$ and let f_p be the reduction of f over each $\mathbb{Q}_p$ (including $\mathbb{Q}_\infty = \mathbb{R}$. Then there is a non-trivial solution of $f = 0$ if and only if there is a non-trivial solution of $f_p = 0$ for all f_p.*

The proof of this theorem is not inaccessible, but does use more advanced properties of the p-adic numbers than the ones mentioned so far. It also uses some properties of quadratic forms. Those interested in learning more about quadratic forms may wish to consult [5]. A proof of the Hasse-Minkowski theorem can be found in [6]. A more accessible sketch of the proof can be found in [4].

I will now discuss one construct that is used in the proof, but is interesting by itself.

3 Hilbert Symbol

Having introduced p-adic numbers, we turn our attention to quadratic equations over p-adic fields. Important here is the generalization of the Legendre symbol named the Hilbert symbol.

Some history is useful here. (See [3].) In 1897, David Hilbert introduced the *norm residue symbol* $\left(\frac{a,b}{p}\right)$ for integers a, b, b not a perfect square, with respect to a prime p. The value of the symbol was 1 and a is a norm residue over a field $K = \mathbb{Q}[\sqrt{b}]$ if $a \equiv |\beta| \mod p^n$ for all n for some $\beta \in K$. Otherwise the symbol has value -1 and a is a norm non-residue over K. The symbol was a natural extension of the Largange symbol to extensions of $\mathbb{Q}$, but soon found its way into the theory of p-adic numbers. Kurt Hansel gave the definition close to one used today. (The following discussion is from [6] and [4].)

Definition 7. *Let $a, b \in \mathbb{Q}_p^* = \mathbb{Q}_p \backslash \{0\}$. Define*

$$(a,b)_p = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a solution with } x, y, z \in \mathbb{Q}_p^* \\ -1 & \text{otherwise.} \end{cases}$$

$(a, b)_p$ is called "the Hilbert symbol of a and b relative to $\mathbb{Q}_p$.

We would like to first prove a theorem relating the present definition with Hilbert's original definition. In what follows, let $K = \mathbb{Q}_p$.

Theorem 5. *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. Assume $b = c^2$ for some c. Then $z^2 - ax^2 - by^2 = 0$ has a solution $(c, 0, 1)$, so $(a, b) = 1$. Since b is q square, $K_b = K[b] = K$, so $NK_b^* = K^*$, $a \in K^*$, and we are done.

Assume b is not a square in K. Let $\beta \in K_b$ be such that $\beta^2 = b$. Any element of K_b can be written as $z + \beta y$, $y, z \in K$, and $N(z + \beta y) = (z + \beta y)(z - \beta y) = z^2 - by^2$. If $a \in NK_b^*$, then there are $y, z \in K$ such that $a = z^2 - by^2$, so $(z, 1, y)$ is a solution and $(a, b) = 1$.

Conversely, assume $(a, b) = 1$. Then $z^2 - ax^2 - by^2 = 0$ has a nontrivial zero. If b is not a square, we must have $a \neq 0$, and it can be checked that a is the norm of $\frac{z}{x} + \beta\frac{y}{x}$. □

We now stae a few properties of the Hilbert symbol. These should be reminiscent of the properties of the Lagrange symbol.

Theorem 6. *Let $a, a', b, c \in K^*$. The Hilbert symbol statisfies the following properties:*

1. *$(a, b) = (b, a)$ and $(a, c^2) = 1$.*
2. *$(a, -a) = 1$ and $(a, 1 - a) = 1$.*
3. *If $(a, b) = 1$, then $(aa', b) = (a', b)$.*
4. *$(a, b) = (a, -ab), (a, (1 - a)b)$.*

Proof.

1. $(a, b) = 1$ iff $z^2 - ax^2 - by^2 = 0$ has a nontrivial solution. The definition is symmetric with respect to a, b. If b is already a perfect square, $b = \beta^2$, then $z^2 - ax^2 - \beta^2 y^2 = 0$ has a solution $(\beta, 0, 1)$.
2. Plug in $-a$ for b: $z^2 - ax^2 + ay^2 = 0$ always has a solution $(0, 1, 1)$. Plug in $1 - a$ for b: $z^2 - ax^2 - (1 - a)y^2 = z^2 - y^2 - ax^2 + ay^2 = 0$ always has a solution $(1, 1, 1)$.
3. If $(a, b) = 1$, then $a \in NK_b^*$. By group closure, $a' \in NK_b^*$ iff $aa' \in NK_b^*$, so $(aa', b) = (a', b)$.
4. Using the first three properties, $(a, b) = (b, a) = (-ab, a) = (a, -ab)$, $(a, b) = (b, a) = ((1 - a)b, a) = (a, (1 - a)b)$.

□

3.1 Computing the Hilbert Symbol

This section is devoted to proving a concise formula for $(a,b)_p$ by relating it to the Legendre symbol. First define two functions:

$$\begin{aligned} \epsilon(z) &\equiv \frac{z-1}{2} \pmod 2 = \begin{cases} 0 & \text{if } z \equiv 1 \pmod 4 \\ 1 & \text{if } z \equiv -1 \pmod 4 \end{cases} \\ \omega(z) &\equiv \frac{z^2-1}{8} \pmod 2 = \begin{cases} 0 & \text{if } z \equiv \pm 1 \pmod 8 \\ 1 & \text{if } z \equiv \pm 5 \pmod 8 \end{cases} \end{aligned}$$

With these in mind,

Theorem 7. *Let $K = \mathbb{Q}_p$, $a = p^\alpha u$, $b = p^\beta v$, with $u, v \in U_p$. Then*

$$(a,b) = \begin{cases} (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha & \text{if } p \neq 2 \\ \\ (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} & \text{if } p = 2. \end{cases}$$

First prove an easy lemma.

Lemma 1. *Lev $v \in U_p$. If $z^2 - px^2 - vy^2 = 0$ has a nontrivial solution in $\mathbb{Q}_p$, then it has a solution (x,y,z) such that $z, y \in U_p$ and $x \in \mathbb{Z}_p$.*

Proof. We can always find a solution with $x \in \mathbb{Z}_p$ by multiplying all three of x, y, z by the same number. Assume either $y \equiv 0 \pmod p$ or $z \equiv 0 \pmod p$. With $x \in \mathbb{Z}_p$, $z^2 - vy^2 = 0$, and since $v \neq 0 \pmod p$ we must have both $x \equiv y \equiv 0 \pmod p$. But then $z^2 - px^2 - vy^2 \equiv px^2 \equiv 0 \pmod{p^2}$, so $x \equiv 0 \pmod p$, and the solution is trivial. By contraction, a nontrivial solution with $x \in \mathbb{Z}_p$ will have $y, z \neq 0 \pmod p$. □

We will also need the following theorem, not proven here.

Theorem 8. *Let $f(X)$ be a quadratic form with coefficients in $\mathbb{Z}_p$ and discriminant invertible in $\mathbb{Z}_p$. If $p \neq 2$, then any solution mod p lifts to a solution in $\mathbb{Z}_p$. If $p = 2$, then any solution mod 8 lifts to a solution in $\mathbb{Z}_p$.*

Now prove the main theorem. We will omit a few details of the proof related to quadratic forms. We will also omit the proof of the special case $p = 2$. The reader may wish to consult [6] for that as well.

Proof. The case $p \neq 2$: Observe that we only need to worry about the residues of α and β modulo 2. Thus consider three cases:

1. $\alpha = 0$, $\beta = 0$: we want $(a, b) = (u, v) = 1$. By a theorem of Chevalley and Warning, the equation
$$z^2 - ux^2 - vy^2 = 0$$
Has a nontrivial solution modulo p. It is a quadratic form, and it turns out that its discriminant is invertible. By the theorem above, it has a p-adic solution, so $(u, v) = 1$.

2. $\alpha = 1$, $\beta = 0$: we want
$$(a, b) = (pu, v) = \left(\frac{v}{p}\right)$$
Since $(u, v) = 1$, it suffices to show that
$$(p, v) = \left(\frac{v}{p}\right)$$
If v is a perfect square (mod p), then both of those are 1, and equality is satisfied. If v is not a perfect square, then the Legendre symbol is -1. But then $z^2 - px^2 - vy^2 = 0$ doesn't have a nontrivial solution mod p, so it doesn't have a p-adic solution, and thus $(p, v) = -1$. Again, equality is satisfied.

3. $\alpha = 1$, $\beta = 1$: we want
$$(a, b) = (pu, pv) = (-1)^{(p-1)/2} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)$$
But
$$(pu, pv) = (pu, -p^2 v) = (pu, -uv)$$
Therefore
$$(pu, pv) = (pu, -uv) = (p, -uv) = \left(\frac{-uv}{p}\right)$$
By multiplicativity of the Legendre symbol,
$$\left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{u}{p}\right) \left(\frac{v}{p}\right) = (-1)^{(p-1)/2} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)$$
And we are done.

□

One important corollary of the formula is that the Hilbert symbol is bilinear.

Theorem 9. *The Hilbert symbol satisfies the following additional property*

5. $(aa', b) = (a, b)(a', b)$

This follows directly from the formula. Again, some manipulation is required with the case $p = 2$.

3.2 Hilbert Product

Having established a formula for $(a,b)_p$, we prove the following theorem, due to Hilbert. Let V be the set of prime numbers together with ∞ with the convention that $\mathbb{Q}_\infty = \mathbb{R}$ (where $(a,b) = 1$ if $a > 0$ and $b > 0$ and -1 if both $a, b < 0$).

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

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

Proof. This proof relies on the formula for $(a,b)_p$ and that fact that $(a,b)_p$ is bilinear. Thus it is enough to prove the theorem for a, b equal to -1 or a prime. Therefore examine three cases, which will have lots of subcases.

1. $a = -1$, $b = -1$: $(-1,-1)_\infty = -1$, $(-1,-1)_2 = -1$ (from formula). Let $p \neq 2$. Then $\alpha = \beta = 0$ so $(a,b) = 1$ (again, from formula). The condition is satisfied and there are an even number of v yielding -1, so the product is 1.

2. $a = 1$ and $b = l$ with l prime. If $l = 2$, then $(-1,2)_v = (-1, 1-(-1)) = 1$ for all $v \in V$. Assume $l \neq 2$. If $v \neq 2$, then $\alpha = \beta = 0$ so $(-1,l)_v = 1$. Conversely, if $v = 2$ or l, $(-1,l)_2 = (-1,l)_l = (-1)^{\epsilon(l)}$, the product of which is 1.

3. Suppose $a = l$ and $b = l'$ with both l, l' prime. If $l = l'$, then $(a,b)_p = (a,-1)_p$ and the problem is reduced to case 2. Assume $l \neq l'$. Suppose $l' = 2$. Then $\alpha = \beta = 0$ and thus $(a,b)_p = 1$ unless $v = 2$ or $v = l$. If the latter is true,

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

   And

   $$(l,2)_l = \left(\frac{2}{l}\right) = (-1)^{\omega(l)}$$

   By a property of the Legendre symbol. The product of these is 1.

   Finally assume $l \neq l' \neq 2$. Then $(l,l')_v = 1$ unless v is either of 2, l, l'. We have

   $$\begin{aligned} (l,l')_2 &= (-1)^{\epsilon(l)\epsilon(l')} \\ (l,l')_l &= \left(\frac{l'}{l}\right) \\ (l,l')_{l'} &= \left(\frac{l}{l'}\right). \end{aligned}$$

   By quadratic reciprocity,

   $$\left(\frac{l'}{l}\right)\left(\frac{l}{l'}\right) = (-1)^{\epsilon(l)\epsilon(l')}$$

So the product of the three is 1.

□

4 Conclusion

With this we conclude the brief discussion of p-adic numbers and Hilbert symbols. The theory itself is very interesting, and this discussion seems to want to be expanded into a more comprehensive treatment of the theory. We hope that the little that is here intrigues the reader to learn more about quadratic forms and local-to-global methods such as the Hasse-Minkowski theorem. Serre's book on "arithmetic" provides a very good introduction to these ideas, and Jones's monograph provides a good basic introduction to quadratic forms.

4.1 Acknowledgements

I would like to thank Professor William Stein for inspiring this paper through his class on number theory in Winter term of 2010.

References

[1] Michael Artin. *Algebra*. Prentice-Hall, New Jersey, 1991.

[2] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction*. Springer-Verlag, New York, (2003).

[3] Jeremy Gray and Karen H. Parshall. *Episodes in the history of modern algebra (1800-1950)*. American Matematical Society, Rhode Island, 2007.

[4] Jeffrey Hatley. "Hasse-Minkowski and the Local-to-Global Principle". Senior capstone, UM Amherst: `http://www.math.umass.edu/~hatley/Capstone.pdf`, 2009.

[5] Burton W. Jones. *The Arithmetic Theory of Quadratic Forms*. "The Carus Mathematical Monographs", Mathematical Association of America, 1961.

[6] Jean-Pierre Serre. *A Course in Arithmetic*. Springer-Verlag, New York, 1973.