INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

The Local-Global Principle in Number Theory

Amélie Schinck

A Thesis

in

The Department

of

Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements

for the Degree of Master of Science at

Concordia University

Montréal, Québec, Canada

September 2001

ABSTRACT

The Local-Global Principle in Number Theory

Amélie Schinck

"p–adic fields provide remarkable, easy and natural solutions to problems which apparently have no relation to p–adic fields and which otherwise can be resolved, if at all, only by deep and arduous methods".

J.W.S. Cassels

The first Local-Global Principle, as formulated by Hasse in 1921, relates the behaviour of rational quadratic forms in $\mathbb{Q}$ (global field) to their behaviour in the p-adic fields $\mathbb{Q}_p$ (local fields). The notion of using local information as a stepping stone towards understanding more difficult global properties has been generalized and applied to many problems, making Local-Global methods a powerful number theoretic tool. Even when the principle fails, we can sometimes salvage some connection between the local and the global. This thesis aims to give a survey of the basic theory.

Acknowledgements

I wish to thank my thesis supervisor, Dr. Hershy Kisilevsky. His guidance and encouragement helped me stay on course. I am also grateful to Dr. Sebastien Pauli for his help in translating some of Hensel's German text to English, giving me a better understanding of the history. Finally, I would like to thank Craig T. Achen for his loving support throughout the writing of this thesis.

Contents

Preface

Chapter 1 is an overview of p-adic fields in their historical context. It contains important results on p-adic numbers, such as Hensel's Lemma, which will often be referred to throughout the course of this thesis. Chapter 2 contains a statement of the Local-Global Principle (Hasse Principle) and traces its historical development. For this part of my study, I am especially indebted to Dr. Günther Frei, who kindly sent me a copy of the article he wrote on the subject for the Proceedings of the Class Field Theory Conference in Tokyo.

We apply the Local-Global Principle to the study of Diophantine equations in Chapter 3, easily obtaining seemingly difficult results. In Chapter 4, the Hilbert symbol and its properties are reviewed. The proofs of the Hasse-Minkowski Theorem for the representation of a rational number by a quadratic form and the equivalence of quadratic forms are given in Chapter 5 and 6. Both chapters were heavily influenced by Borevich's and Shafarevich's approach in their collaborative text *Number Theory*.

Famous examples of the failure of the Hasse Principle are discussed at length in Chapter 7, among them, the very first counterexample discovered by Reichard in 1942. The Hasse-Minkowski Theorem is extended to finite extensions of the p-adic field in Chapter 8, fully solving Hilbert's eleventh problem. Chapter 9 deduces quadratic reciprocity from a local-global result; The product formula. The Hasse Norm Theorem, of which the Hasse-Minkowski theorem is a particular case, is the focus of Chapter 10. The failure of the Hasse Principle is again the topic of Chapter 11, but this time, put in the language of cohomology, allowing us to discuss the group which measures the obstruction called the Tate-Shafarevich group.

Chapter 1

Introduction

1.1 Hensel's Analogy

In the course of extending Kronecker's work on the factorization of prime ideals in number fields, one of his students was led to the creation of the p-adic numbers. This astute student was Kurt Hensel. Hensel carried over the method of complex analysis of expanding functions locally in order to get information on their global properties to the land of Number Theory. He keenly observed that the linear factors $(x-\alpha)$, the prime ideals of the ring $\mathbb{C}[x]$, play an analogous role in $\mathbb{C}(x)$ to the prime numbers p in $\mathbb{Q}$. Hensel translated the Laurent series expansion of a function $f(x) \in \mathbb{C}(x)$ about a point $\alpha \in \mathbb{C}$

$$f(x) = \sum_{i=N}^{\infty} a_i (x-\alpha)^i$$

into a closely analogous Laurent series expansion of $r \in \mathbb{Q}$ in progressive powers of a prime p

$$r = \sum_{i=N}^{\infty} a_i p^i; \ 0 \le a_i \le p-1.$$

Hensel called the latter the p-adic expansion of r. Any rational number r can be written p-adically with respect to every prime element p of $\mathbb{Z}$. The p-adic expansion gives us local information about r near p, just as each Laurent expansion gives us local information about $f(x)$ near α. Hensel showed that the collection of all such Laurent series in powers of p forms a field, which he dubbed the field of p-adic

numbers and labeled $K(p)$. In modern shorthand this field is denoted $\mathbb{Q}_p$. An interesting historical side note is that, at the time, the definition of a field formulated by Dedekind required that it be a subfield of the field of complex numbers, a requirement the p-adic fields fail to satisfy. The fields of p-adic numbers were the motivation behind the fundamental treatise on abstract Field Theory undertaken by Steinitz. The p-adic fields were the earliest examples of what are now known as Local Fields, with the exception of the fields of real and complex numbers. Local Fields will be discussed further in Chapter 8.

Hensel introduced p-adic numbers in 1897 in a short paper entitled *Über eine neue Begründung der Theorie der algebraischen Zahlen (About a new foundation of the theory of algebraic numbers)*. Hensel's treatment was extremely formal and failed to dazzle the mathematical community. The p-adics were dismissed at the time as imaginative play things, devoid of any real use because no substantial result for which they were indispensable had been found. Hilbert mentioned them in his famous Paris lecture in 1900 yet they went virtually unnoticed for decades. This attitude was in large part due to an error by Hensel.

1.2 The Transcendence of e

From the beginning, Hensel was intent on applying p-adic methods to transcendency questions, a fashionable topic at the end of the 19th century. He gave a flawed proof of the transcendence of e in 1905 during an invited lecture given in Merano, Italy, to the *Versammlung deutscher Naturforscher und Ärtze* (Meeting of German Natural Scientists and Physicians). A discussion of Hensel's erroneous argument can be found in [29]. Hensel later had to admit that "*The proof of the transcendency of e given in my Meran lecture needs an essential completion.*" This blunder did not help the perceived legitimacy of p-adic numbers in mathematical circles. Jean-Paul Bézivin and Philippe Robba obtained a p-adic proof of the Lindemann-Weierstrass Theorem in a 1987 article [4]. This theorem states that the

values taken by the exponential function at different algebraic points are linearly independent over the field of algebraic numbers. The Lindemann-Weierstrass theorem implies that e is transcendental. Referring to their result the authors wrote:

> *"We are glad to vindicate Hensel in his idea that p–adic numbers could be used to prove transcendental results although the proof devised here has nothing to do with the method that Hensel intended to use."*

1.3 The p-adic absolute value

Nevertheless, Hensel continued to develop his theory more fully. He introduced topological notions to the world of p-adics by defining the p-adic absolute value of a rational number x

$$|\ |_p : \mathbb{Q} \hookrightarrow \mathbb{R}, \qquad x \mapsto |x|_p = p^{-\nu_p(x)}$$

where $x = p^{\nu_p(x)}\frac{a}{b}$ with $p \not| \ a$ and $p \not| \ b$. The usual absolute value is written $|\ |_\infty$. By convention, $\nu_p(0) = \infty$, hence $|0|_p = 0$. It is easy to show that the p-adic absolute value is non-archimedean, that is it satisfies the property

$$|x + y|_p \leq \max\{|x|_p, |y|_p\} \qquad (x, y \in \mathbb{Q}).$$

After laying this topological foundation, Hensel mostly concentrated on investigating series which converge with respect to $|\ |_p$. This change of outlook was the first step towards p-adic numbers becoming an essential tool in Number Theory. Kürschak generalized Hensel's work to derive the Theory of Valuations in 1913. The p-adic valuation endows $\mathbb{Q}$ with a metric space structure. From the definition of $|\ |_p$, we see that two rational numbers are deemed close if their difference (expressed in lowest terms) has a numerator divisible by a high power of p.

It has been shown that $\mathbb{Q}$ is not complete with respect to $|\ |_p$, that is, not all Cauchy sequences converge with respect to $|\ |_p$. Recall that a sequence $\{x_i\}_{i\to\infty}$ is Cauchy if

for every $\varepsilon > 0$ in $\mathbb{Q}$, there exists an $N \in \mathbb{N}$ such that if $i, j > N$ then $|x_i - x_j|_p < \varepsilon$. Following the method of completing $\mathbb{Q}$ with respect to the usual absolute value to obtain $\mathbb{R}$, $\mathbb{Q}_p$ can be regarded as the topological field obtained by completing $\mathbb{Q}$ with respect to the p-adic absolute value. In this language, $\mathbb{R}$ is denoted $\mathbb{Q}_\infty$. This absolute value takes on the same value on $\mathbb{Q}_p$ as it does on $\mathbb{Q}$ since the p-adic absolute value of $\sum_{n \geq m_0} a_n p^n = 1/p^{m_0}$ is a rational number.

The p-adic numbers can then be seen, like the reals, as equivalence classes of Cauchy sequences. p-adic analysis is quite simple compared to real analysis since a necessary and sufficient condition for a series to converge in $\mathbb{Q}_p$ is that its terms approach zero. Two absolute values are equivalent if they induce the same topology on $\mathbb{Q}$. The trivial absolute value is the absolute value $|\ |$ such that $|0| = 0$ and $|x| = 1$ for $x \neq 0$. A theorem due to Ostrowski states that every non-trivial absolute value on $\mathbb{Q}$ is equivalent to $|\ |_p$ where p is a prime or $p = \infty$ (see [16], pp.44 for a proof). The modern presentation of the subject normally follows these lines.

The ring of p-adic integers $\mathbb{Z}_p$ is defined to be the set

$$\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

The collection of all invertible elements of $\mathbb{Z}_p$ forms the group of p-adic units $\mathbb{Z}_p^*$. Since we need x and x^{-1} to be elements of $\mathbb{Z}_p$, the group of p-adic units is then described to be the set

$$\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}$$

Concretely, these are the elements of $\mathbb{Q}_p$ that have a p-adic expansion $a_0 + a_1 p + \ldots$ where $a_0 \neq 0$. Every nonzero p-adic number x can be represented uniquely in the form

$$x = p^{v_p(x)} u$$

where u is a p-adic unit.

The field $\mathbb{Q}$ can be identified with the subfield of $\mathbb{Q}_p$ consisting of equivalence classes containing a constant Cauchy sequence (*i.e.* all of whose terms are equal). This shows that $\mathbb{Q}$ is properly contained in $\mathbb{Q}_p$ for any p

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p$$

This is analogous to the inclusion

$$\mathbb{C}(x) \hookrightarrow \mathbb{C}((x-a))$$

The field $\mathbb{C}(x)$ is not equal to $\mathbb{C}((x-a))$ since for example the series for $e^x = \sum \frac{x^n}{n!}$ is not an expansion of a rational function. Herein lies a paradox; The bigger field $\mathbb{Q}_p$ (respectively $\mathbb{C}((x-a))$) gives us local information about the smaller global field $\mathbb{Q}$ (respectively $\mathbb{C}(x)$).

In general, given a valuation v_p on a number field K, we can extend K to its completion K_p. Piecing together information about the distinct completions K_p helps us study properties of K. The following proposition is a simple example of solutions to a global problem being deduced from local information.

Theorem 1.1 (Global Square Theorem)
A rational number x is a square in $\mathbb{Q}$ if and only if x is a square in $\mathbb{Q}_p$ for all $p \leq \infty$.

Proof [$\Rightarrow$] Clear, since $\mathbb{Q}$ sits inside $\mathbb{Q}_p$.

[$\Leftarrow$] Suppose x is a square in $\mathbb{Q}_p$ for all $p \leq \infty$. If $x = 0$ we are done. Suppose $x \neq 0$. We can write $x = \prod_{p<\infty} p^{v_p(x)}$. If x is a square in $\mathbb{R}$, then x is positive. If x is a square at each prime $p < \infty$, then $v_p(x)$ is even for all p, which implies that x is a positive number and is an even power. Thus x is a square in $\mathbb{Q}$. $\square$

To discuss squares, we will sometimes need the notational ease of the Legendre symbol introduced in 1798.

Definition 1.1 (Legendre Symbol)

Let p be an odd prime number and a an integer such that $(p,a) = 1$. The Legendre symbol of a and p is then:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \bmod p \text{ is solvable in } \mathbb{Z} \\ -1 & \text{otherwise} \end{cases}$$

The Legendre symbol has the multiplicative property $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

1.4 Hensel's Lemma

Hensel also produced a theorem which is now a standard tool in p-adic analysis. It is amicably known as Hensel's Lemma. This lemma has its roots in Newton's Method for finding the zeroes of a polynomial equation by successive refinements of an initial approximate solution. Hensel's Lemma allows us to lift non-trivial solutions of congruences modulo p to non-trivial p-adic solutions of polynomials. Any field complete under a non-archimedean valuation, also satisfies Hensel's Lemma. As J.W.S. Cassels states in [11] pp.83:

> "*In the literature there is a variety of results that go under this name. Their common feature is that the existence of an approximate solution of an equation or system of equations in a complete valued field implies the existence of an exact solution to which it is an approximation, subject to conditions to the general effect that the approximate solution is 'good enough'* ".

We will use the following versions of Hensel's Lemma;

Theorem 1.2 (Hensel's Lemma)

Let $f(x) = a_n x^n + ... + a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}_p[x]$. Let $f'(x) = n a_n x^{n-1} + ... + a_1$ be the derivative of $f(x)$. Suppose there exists a $\beta \in \mathbb{Z}_p$ such that $f(\beta) \equiv 0 (\mathrm{mod} p)$ and $f'(\beta) \not\equiv 0 (\mathrm{mod} p)$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that

$$i)\ f(\alpha) = 0$$

$$ii)\ \alpha \equiv \beta (\mathrm{mod} p).$$

Hensel's Lemma, among other things, allows us to determine the p-adic squares.

Corollary 1.1 $p \neq 2$

Let $u \in \mathbb{Z}_p^{\times}$ be a p-adic unit. If there exists an $\alpha \in \mathbb{Z}_p$ such that $\alpha^2 \equiv u (\mathrm{mod} p\mathbb{Z}_p)$, then u is a square in $\mathbb{Z}_p$.

Proof Let $u \in \mathbb{Z}_p^{\times}$. Suppose there exists a $\alpha \in \mathbb{Z}_p$ such that $\alpha^2 \equiv u (\mathrm{mod} p\mathbb{Z}_p)$. By Hensel's Lemma, this solution lifts to a p-adic solution since $p \neq 2$ and $\alpha \in \mathbb{Z}_p^{\times}$ thus $2\alpha \not\equiv 0 (\mathrm{mod} p)$.

□

We will sometimes need to use the stronger version of Hensel's Lemma.

Theorem 1.3 (Hensel's Lemma)

Let $\beta \in \mathbb{Z}_p$ satisfy the condition $|f(\beta)|_p < |f'(\beta)|_p^2$. Then there exists an $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \beta (\mathrm{mod} p)$.

The equation $x^2 - 17 = 0$ is a case in point for the need of Theorem 1.3 because it does indeed have roots in $\mathbb{Q}_2$ (try $\beta = 1$). An immediate consequence of Theorem 1.3 is the following Corollary.

Corollary 1.2 A 2-adic unit u is a square in $\mathbb{Z}_2$ if and only if $u \equiv 1 (\mathrm{mod}\, 8\mathbb{Z}_2)$.

Proof Let $u \in \mathbb{Z}_2^*$ and $f(x) = x^2 - u$. Assume $u \equiv 1 (\mathrm{mod}\, 8\mathbb{Z}_2)$. Then $|f(1)| \leq 2^{-3}$ is strictly smaller than $|f'(1)|^2 = 2^{-2}$. By Theorem 1.3 there exists an $\alpha \in \mathbb{Z}_2$ such that $\alpha^2 = u$. The other direction follows from the fact that $u^2 = (1+2n)^2 \equiv 1 (\mathrm{mod}\, 8\mathbb{Z}_2)$. □

Now recall that every nonzero p-adic number x can be represented uniquely in the form $x = p^n u$, where u is a p-adic unit and $n = v_p(x) \in \mathbb{Z}$. So, putting Corollary 1.1 and 1.2 together, we obtain

Theorem 1.4

Let $x = up^n$, $u \in \mathbb{Z}_p^*$, $n \in \mathbb{Z}$, x is a p-adic square if

1. $n \equiv 0 (\mathrm{mod}\, 2)$
2. $\alpha^2 \equiv u (\mathrm{mod}\, p\mathbb{Z}_p)$ for $p \neq 2$, $u \equiv 1 (\mathrm{mod}\, 8\mathbb{Z}_2)$ for $p = 2$.

Note that squaring $u = 1 + 8k$ where $k \in \mathbb{Z}_2$ results in the fourth powers in $\mathbb{Z}_2^*$. For any $k \in \mathbb{Z}_2$, we find that $(1+8k)^2$ is congruent to 1 modulo 16. It turns out that the fourth powers in $\mathbb{Z}_2^*$ exactly correspond to the elements which are congruent to 1 modulo 16.

The following is an n-variable version of Hensel's Lemma, which will prove quite useful later on.

Theorem 1.5 (Hensel's Lemma; n-variable version)

Let $f(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$. Suppose there exists $\beta_1, \beta_2, ..., \beta_n \in \mathbb{Z}_p$ such that $f(\beta_1, \beta_2, ..., \beta_n) \equiv 0 (\mathrm{mod}\, p)$ and for some i the partial derivative of f with respect to x_i satisfies $\partial f / \partial x_i (\beta_1, \beta_2, ..., \beta_n) \not\equiv 0 (\mathrm{mod}\, p)$, then there exists $\alpha_1, ..., \alpha_n \in \mathbb{Z}_p$ such that:

$$i)\ f(\alpha_1, ..., \alpha_n) = 0$$

$$ii)\ \alpha_i \equiv \beta_i (\mathrm{mod}\, p), \text{for } 1 \leq i \leq n.$$

Chapter 2

The Hasse Principle

The theme of this chapter is the link between the behaviour of quadratic forms (with rational coefficients) over the rational field $\mathbb{Q}$ and over the various p-adic fields $\mathbb{Q}_p$ ($\mathbb{Q}_\infty = \mathbb{R}$). The main result in this area is the Hasse-Minkowski Theorem which reduces questions over $\mathbb{Q}$ about quadratic forms with rational coefficients to the corresponding questions over $\mathbb{Q}_p$.

2.1 Helmut Hasse

As previously mentioned, the events of 1905 left the impression that p-adic numbers were an *unfruchtbarer Seitenweg* (fruitless sideway; Quote of Richard Courant found in [21], Vol. 1, pp.viii). Fortunately for the legacy of p-adic numbers, a mathematically gifted young man named Helmut Hasse stumbled upon a copy of Hensel's 1913 text *Zahlentheorie* in a Göttingen second-hand bookstore in March of 1920. In the last chapter of this book, Hensel applies p-adic methods to binary and ternary quadratic forms with rational coefficients, obtaining necessary conditions for the representability of a rational number.

Hasse was so fascinated by the theory of p-adic numbers that he decided to study them at the source. Less than two months after that fateful day in March, Hasse matriculated at Marburg University to study under Hensel. Hensel urged Hasse to

continue the work done in the last chapter of *Zahlentheorie*. In particular, Hensel gave his student the task of determining whether the necessary conditions he had found were also sufficient. In addition, Hasse was to examine quaternary quadratic forms for analogous conditions.

Hasse quickly delivered. One short year after entering Marburg, Hasse graduated as *Doctor Philisophiae*. In his doctoral dissertation (1921), Hasse completely solves the problem Hensel had given him not only for ternary forms, but for n-ary forms. A theorem dating back to Legendre was key in Hasse's solution to the problem. Legendre had reduced the problem of deciding if a homogeneous quadratic form with rational coefficients has a rational zero to

Theorem 2.1 (Legendre's Theorem)
Let a,b,c be integers other than 0 and not all of the same sign, where abc is square free. Then the equation $ax^2 + by^2 + cz^2 = 0$ has a non-trivial solution $x,\ y,\ z \in \mathbb{Z}$ if and only if $-bc, -ac, -ab$ are quadratic residues modulo $|a|, |b|, |c|$ respectively.

Hasse needed a way to translate Legendre's result to p-adic numbers, which he did not readily see. He wrote to Hensel for guidance, receiving it in the form of a postcard (reproduced in vol I pp.ix of [21]). Hensel's reply helped Hasse see that the conditions given by Legendre are equivalent to saying that the ternary form admits a non-trivial p-adic representation of zero for each prime p. Then Legendre's Theorem itself states that it also admits a non-trivial rational representation of zero.

To see how to interpret Legendre's Theorem p-adically ($p \neq 2$), observe that a,b and c not all being of the same sign (*i.e.* the form is indefinite) guarantees that $ax^2 + by^2 + cz^2 = 0$ has a non-trivial solution over $\mathbb{R}$. Furthermore, since the equation concerned is homogeneous, the distinction between rational and integral solutions vanishes. So we can assume x,y and z are relatively prime integers. Note that if $p \nmid abc$, then $ax^2 + by^2 + cz^2 = 0$ has a non-trivial p-adic solution. To show

this, let $z = 1$ and consider the congruence $ax^2 \equiv -c - by^2 (\mathrm{mod} p)$. Since ax^2 takes on $\frac{p+1}{2}$ values modulo p and so does $-c - by^2$, they thus have a value in common which is the solution modulo p. This solution, say (x_0, y_0, z_0), lifts to a p-adic solution since all partial derivatives evaluated at (x_0, y_0, z_0) are not congruent to 0 mod$p$.

Suppose $ax^2 + by^2 + cz^2 = 0$ has a non-trivial p-adic solution for all p. To show $-ab$ is a quadratic residue mod$c$ it is necessary and sufficient to show $\left(\frac{-ab}{p}\right) = 1$ for all $p|c$ (by the Chinese Remainder Theorem). Assume $p|c$. If $p|x$ and $p|y$ then $p|z$ which is a contradiction. Thus x and y are prime to p. The congruence $ax^2 + by^2 \equiv 0 (\mathrm{mod} p)$ is solvable in $\mathbb{Z}$ which implies that $-ab$ is a quadratic residue mod$p$ for all primes p dividing c. So, $-ab$ is a quadratic residue mod$c$.

Now, assume $-bc \equiv u^2 (\mathrm{mod} p)$ where $p \nmid bcu$ and let $f = f(x,y,z) = ax^2 + by^2 + cz^2$. There exists an integer d such that $cd \equiv u (\mathrm{mod} p)$. We then have $-bc \equiv c^2 d^2 (\mathrm{mod} p)$ thus $0 \equiv cd^2 + b (\mathrm{mod} p)$. This results in $f(0,1,d) = b + cd^2 \equiv 0 (\mathrm{mod} p)$. Since $p \neq 2$ and $p \nmid b$ then $\partial f / \partial y (0,1,d) = 2b \not\equiv 0 (\mathrm{mod} p)$. By Hensel's Lemma applied to $f(x,y,z) = ax^2 + by^2 + cz^2$ there exists $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_p$ such that

$$f(\alpha_1, \alpha_2, \alpha_3) = a{\alpha_1}^2 + b{\alpha_2}^2 + c{\alpha_3}^2 = 0$$

where $(\alpha_1, \alpha_2, \alpha_3) \equiv (0,1,d) (\mathrm{mod} p)$.

2.2 The Hasse-Minkowski Theorem

Once Hasse had understood the theorem p-adically, he proved that it also holds for any n-ary quadratic form with rational coefficients. Hasse was now in a position to formulate his first Local-Global Principle for the representation of numbers by quadratic forms. Hasse called this the Fundamental Theorem for the representation of numbers by quadratic forms. His result first appeared in the Crelle Journal of

1923 under the title *Uber die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen* (*About the representability of a quadratic form in the field of rational numbers*) [17]:

Theorem 2.2 (Hasse-Minkowski)
A quadratic form f with rational coefficients represents zero non-trivially in the field of rational numbers $\mathbb{Q}$ if and only if f represents zero non-trivially in the field of real numbers $\mathbb{R}$ and in all fields of p-adic numbers $\mathbb{Q}_p$.

The Hasse-Minkowski Theorem is the simplest, purest form of the Local-Global Principle. We will see the proof in Chapter 5. The Hasse-Minkowski Theorem completely solves the problem of deciding whether a quadratic form with rational coefficients represents a given rational number because of the following:

Theorem 2.3
If a nonsingular quadratic form represents zero non-trivially in some field K of characteristic not equal to 2 then it represent all elements of K non-trivially.

Proof First, note that if K is a field of characteristic different from 2, any nonsingular quadratic form $\sum a_{ij}x_ix_j$ $(a_{ij} \in K,\ 1 \le i,\ j \le n)$ can be put into diagonal form

$$a_1x_1^2 + \ldots + a_nx_n^2 \qquad (a_j \in K)$$

by a linear change of variables ([6] pp.392). Let $f(x_1,\ldots x_n) = a_1x_1^2 + \ldots + a_nx_n^2$ be in $K[x_1,\ldots,x_n]$ and let $(\beta_1,\ldots,\beta_n) \in K^n$ be a non-trivial solution to $f = 0$ (*i.e.* $a_1\beta_1^2 + \ldots + a_n\beta_n^2 = 0$). Without loss of generality, we may assume $\beta_1 \neq 0$. Let γ be any element of K. We want to show that f can be made to represent γ. Write $x_1 = \beta_1(1 + t)$, $x_k = \beta_k(1 - t)$ for $k = 2,\ldots n$. Substituting in the form f we obtain

$$f = (a_1\beta_1^2 + \ldots + a_n\beta_n^2)(1 + t^2) + 2a_1\beta_1^2t - 2a_2\beta_2^2t - \ldots - 2a_n\beta_n^2t = 4ta_1\beta_1^2$$

Setting $t = \gamma/(4a_1\beta_1^2)$, we see that f represents γ. □

The Local-Global Principle, also known as the *Hasse Principle*, was the vindication of Hensel's creation. It was the first intimation of the p-adic numbers' true potential. After a reasonably long period of time, their study subsequently regained importance. "[...] *the merits of this approach took a long time to percolate into the collective mathematical consciousness. As late as* 1930 *L.E. Dickson could write a monograph on quadratic forms* [...] *and Mordell could review it* [...] *without either of them betraying the least awareness of the p–adic viewpoint*" (Ref: [9], pp.vi). Minkowski's name appears in the title cf the theorem because he had found an equivalent result in 1890.

Theorem 2.4 (Minkowski's Theorem)

Given a quadratic form $f(x_1,...,x_n)$ with rational coefficients, if $f(x_1,...,x_n) \equiv 0 (\mathrm{mod} p^r)$ has a non-trivial solution for all primes p and positive integer r and if $f(x_1,...,x_n) = 0$ has a non-trivial solution in the reals, then $f(x_1,...,x_n) = 0$ has a non-trivial rational solution.

Minkowski's Theorem is equivalent to the Hasse-Minkowski Theorem. If we are given a quadratic form with rational coefficients $f(x_1,...,x_n)$, the congruence $f(x_1,...,x_n) \equiv 0 (\mathrm{mod} p^k)$ is solvable for all $k \geq 1$ if and only if the equation $f(x_1,...,x_n) = 0$ is solvable in p-adic integers. For instance to solve $x^2 = 2$ in $\mathbb{Q}_7$ we must solve the system of congruences $x^2 \equiv 2 (\mathrm{mod} 7^r)$, for all $r \geq 1$. Doing the calculation, we obtain the square roots of 2: $\sqrt{2} = x_1 = 3 + 1 \times 7 + 2 \times 7^2 + 6 \times 7^3$ and $\sqrt{2} = x_2 = 4 + 5 \times 7 + 4 \times 7^2 + 0 \times 7^3 = -x_1$.

As J.W.S. Cassels states in his article *Diophantine Equations with Special Reference to Elliptic Curves*:

> *"The use of p–adic numbers is at first sight rather artificial compared with the older language of congruences but offers great technical advantages because $\mathbb{Q}_p$ is a field whereas $\mathbb{Z}$ modp^n is not even an integral domain."*

2.3 Hilbert's Eleventh Problem

Hilbert, a close friend of Minkowski, had studied at length the quadratic extensions $\mathbb{Q}(\sqrt{c})$ of $\mathbb{Q}$, which is tantamount to studying binary quadratic forms. He was determined to generalize Minkowski's Theorem to quadratic forms with algebraic numbers as coefficients. This search led him to prove the existence of certain class fields. He stressed the importance he placed on extending Minkowski's Theorem by proposing this as his eleventh problem in his address delivered before the International Congress of Mathematicians in Paris in 1900. Hilbert believed at the time that:

> **11. Quadratic forms with any algebraic numerical coefficients**
> *"Our present knowledge of the theory of quadratic fields puts us in a position to attack successfully the theory of quadratic forms with any number of variables and with any algebraic numerical coefficients."* [34]

The Hasse-Minkowski Theorem as stated above does not completely solve Hilbert's eleventh problem, since we are just over the rationals. We will see in Chapter 8 that Hasse soon generalized the Hasse-Minkowski Theorem to arbitrary algebraic fields.

Chapter 3

Diophantine Equations

Although p-adic numbers have a function theoretic origin, they are at their best when applied to the theory of Diophantine equations. The study of Diophantine equations is the branch of Number Theory dealing with integer or rational solutions to polynomial equations. A curve of genus 0 defined over $\mathbb{Q}$ is birationally equivalent over $\mathbb{Q}$ either to the line or to a conic section $ax^2 + by^2 + cz^2 = 0$, $a,b,c \in \mathbb{Q}$ (See [9] pp.255, for a sketch of the proof). This reduces the study of Diophantine equations of genus 0 curves to the study of conics.

3.1 Equations Modulo p

As one might expect, the Local-Global Principle is often used to answer questions about rational solutions of Diophantine equations. An equation $f = 0$ is said to satisfy the Hasse Principle if the existence of non-trivial local solutions of $f = 0$ implies the existence of a non-trivial global solution. It is often extremely difficult to determine the solvability of a Diophantine equation in the integers or the rationals, such as $x^n + y^n + z^n = 0$, $n > 2$. On the other hand, the solvability modulo a prime p, can be determined in a finite number of steps. Also, the existence of real solutions is easily determined by sign considerations. Thus for each prime $p \leq \infty$, Hensel's Lemma then shows that the question of existence of solutions of any given Diophantine equation over $\mathbb{R}$ or $\mathbb{Q}_p$ is decidable in the sense of mathematical logic.

So in general approaching a problem locally is easier than tackling the same problem globally. Think of the problem of finding a local minimum of a function in comparison to the problem of finding its global minimum. This implies a strategy; The old idea of divide and conquer prevails.

Theorem 3.1 (Necessary Conditions for Solvability)
A necessary condition for the existence of rational solutions to a polynomial equation $f = 0$ with rational coefficients is that it has p-adic solutions for all primes p. If $f = 0$ has integer coefficients then a necessary condition for the existence of integer solutions is that $f \equiv 0 (\mathbf{mod} p)$ has solutions for all primes p.

Hence we can approach $\mathbb{Q}$ through its local fields $\mathbb{Q}_p$ and also approach each $\mathbb{Q}_p$ through the finite fields $\mathbb{F}_p$ by reduction modulo p. Consider the equation

$$3x^2 + 4y^2 - 5z^2 = 0 \qquad (x,y,z \in \mathbb{Q})$$

After clearing the denominators, we may look for $x,y,z \in \mathbb{Z}$ and assume that $\gcd(x,y,z) = 1$. If $5|x$ and $5|y$ then $5^2|(3x^2 + 4y^2) \Rightarrow 5|z$, which contradicts our assumption that $\gcd(x,y,z) = 1$. If $5 \nmid x$ or $5 \nmid y$, the congruence

$$3x^2 \equiv y^2 (\mathrm{mod}\, 5) \Leftrightarrow 3 \equiv (y/x)^2 (\mathrm{mod}\, 5)$$

is impossible since 3 is not a quadratic residue modulo 5. So $3x^2 + 4y^2 - 5z^2 = 0$ has no non-trivial solution in $\mathbb{Q}$. The quadratic equation

$$x^2 + y^2 = -1$$

is also clearly insoluble rationally since no real solution exists. It is easy to see by examples that if a general polynomial equation has a solution modulo p, no conclusions can be drawn. The congruence conditions are not sufficient. For instance $3x^2 + 4y^2 - 5z^2 = 0$ has a non-trivial solution modulo 7, but no non-trivial solution in $\mathbb{Q}$.

Many interesting results may be obtained through congruence considerations. For instance, the equation

$$x_1^3 + 2x_2^3 + 4x_3^3 = 9x_4^3 \qquad \gcd(x_1, x_2, x_3, x_4) = 1$$

with $x_i \in \mathbb{Z}$, only has the trivial solution. This follows easily from the fact that $a^3 \equiv 0, \pm 1 \pmod 9$ for any integer a, so $x_1^3 + 2x_2^3 + 4x_3^3 \equiv 0 \pmod 9$ has the sole solution $x_1 \equiv x_2 \equiv x_3 \equiv 0 \pmod 9$ which results in $x_4 \equiv 0 \pmod 9$.

3.2 Irrationality of $\sqrt{2}$ and the Three Square Theorem

The following is essentially the classical proof of the irrationality of 2 stated in the language of p-adics.

Theorem 3.2 $\sqrt{2}$ is irrational.

Proof Consider the equation $x^2 = 2$. Taking the 2-adic valuation on both sides; If $x^2 = 2$ has a solution α in $\mathbb{Q}_2$ then $\alpha^2 = 2$. So $2v(\alpha) = v(2) = 1$. No such α exists. Thus $x^2 = 2$ has no solution in $\mathbb{Q}_2$. Since $\mathbb{Q}$ is a subfield of $\mathbb{Q}_2$, we certainly do not have any solutions in $\mathbb{Q}$. Similar reasoning yields that $\sqrt{p}$ is irrational for every positive prime p.

□

In 1770, Lagrange proved that every positive integer is a sum of squares of four integers. In 1798, Legendre answered the deeper question: *Exactly what positive integers need all four squares*? Of course, Legendre's proof did not use the following Local-Global argument.

Theorem 3.3 (Legendre's Three Square Theorem)
A positive integer n is a sum of squares of three integers if and only if it is not of the form $4^r(8k+7)$ where $r,\ k \in \mathbb{Z}, r \geq 0$.

Proof By the Hasse-Minkowski Theorem, we must show that n is represented by the

form $f = f(x,y,z) = x^2 + y^2 + z^2$ in $\mathbb{R}$ and all $\mathbb{Q}_p$. The real case is clear. By Theorem 2.3, if $x^2 + y^2 + z^2$ represents 0 over $\mathbb{Q}_p$, then it represents all elements of $\mathbb{Q}_p$, so it certainly represents the positive integer n. We will assume that the condition of Davenport-Cassels Theorem holds (proof [24] pp.46). This theorem states that, under a certain condition, if an integer n is represented by f in $\mathbb{Q}$ then it is also represented by f in $\mathbb{Z}$.

Claim: The form f represents 0 at all completions of $\mathbb{Q}$ except perhaps at $\mathbb{Q}_2$.

Proof of Claim. Since the equation concerned is homogeneous, we may look for $x,y,z \in \mathbb{Z}$. Consider the congruence $x^2 + y^2 + z^2 \equiv 0 (\mathrm{mod} p)$ for all $p \neq 2$. Suppose there is no solution of the given congruence. If there exists a $\beta \in \mathbb{Z}$ such that $\beta^2 \equiv -1 (\mathrm{mod} p)$ the congruence

$$x^2 + y^2 + z^2 \equiv 0 (\mathrm{mod} p)$$

would have the solution $(1,\beta,0)$, so $\left(\frac{-1}{p}\right) = -1$. Also, if we assume $\left(\frac{a}{p}\right) = 1$ for some integer $a \not\equiv 0, -1 (\mathrm{mod} p)$, then $\left(\frac{-(a+1)}{p}\right) = -1$. Otherwise we would be able to find $x,y,z \in \mathbb{Z}$ such that $a \equiv y^2 (\mathrm{mod} p)$, and $-(a+1) \equiv z^2 (\mathrm{mod} p)$ and the congruence $x^2 + y^2 + z^2 \equiv 0 (\mathrm{mod} p)$ would have the solution $(1, a, -(a+1)) = (x,y,z)$. We find that

$$\left(\frac{-1}{p}\right)\left(\frac{-(a+1)}{p}\right) = \left(\frac{(a+1)}{p}\right) = 1$$

which implies that every nonzero residue class modulo p is a quadratic residue modulo p. This is a contradiction since $p > 2$. The mod p solutions all lift to p-adic solutions by Hensel's Lemma. Therefore f represents 0 in $\mathbb{Q}_p$ for all odd primes p.

Now, observe that for any integer x we have $x^2 \equiv 0, 1$ or $4 (\mathrm{mod} 8)$. Hence $x^2 + y^2 + z^2$ cannot be congruent to 7 modulo 8. Furthermore, $x^2 \equiv 0, 1 (\mathrm{mod} 4)$ so if $x^2 + y^2 + z^2 \equiv 0 (\mathrm{mod} 4)$, x,y and z are even, say $x = 2x_1$, $y = 2y_1$, $z = 2z_1$. Hence if $4^r(8k+7) = x^2 + y^2 + z^2$, then $4^{r-1}(8k+7) = x_1^{\,2} + y_1^{\,2} + z_1^{\,2}$. So we see that if

$(x,y,z) \in \mathbb{Z}^3$ is a solution to the equation there exists another integer solution of smaller height ($H(P) = \max\{|x|,|y|,|z|\}$). Continuing in this fashion (descent) would result in $8k+7 = x_r^2 + y_r^2 + z_r^2$, a contradiction.

□

The method of descent seen above was first introduced by Fermat. We can now effortlessly derive Lagrange's result.

Theorem 3.4 (Lagrange's Four Square Theorem)
Any positive integer n is a sum of squares of four integers.

Proof. If n is not of the form $4^r(8k+7)$, it is the sum of 3 squares. Otherwise, $4^{-r}n \equiv -1 \pmod 8$ and thus $4^{-r}n - 1 \equiv 6 \pmod 8$ so $n - 4^r$ is a sum of three squares. Thus $n = (n-4^r) + 4^r$ is the sum of four squares.

□

Chapter 4

The Hilbert Symbol

It is natural at this point to introduce the Hilbert symbol which will make our statements more concise.

4.1 The Hilbert Symbol

Since any quadratic form is equivalent to a diagonal form, we may confine our attention to quadratic forms which are in the diagonal form. In particular any ternary quadratic form with coefficients in K is equivalent to $ax^2+by^2+cz^2$ $(a,b,c \in K)$ which represents zero if and only if $z^2-ax^2-by^2$ $(a,b \in K)$ represents zero. The representability of zero in the field K by a quadratic form in three variables can then be expressed with the Hilbert symbol of a and b relative to K

$$(a,b)_K = \begin{cases} 1 & \text{if } z^2-ax^2-by^2=0 \text{ has a non-trivial solution in } K \\ -1 & \text{otherwise} \end{cases}$$

Proposition 4.1

Let $a,b \in K^\times$ be square free and let $K(\sqrt{b})$. The equation $z^2-ax^2-by^2=0$ has a non-trivial solution in $K^\times$ if and only if a is the norm of an element in $K(\sqrt{b})^\times$.

Proof Let $\alpha = Z+Y\sqrt{b}$ be a typical nonzero element of $K(\sqrt{b})^\times$ and $a=N(\alpha)$ its norm. Since b is not a square, $K(\sqrt{b})^\times$ is a quadratic extension of K. There exists

$Y,Z \in K^\times$ such that $a = Z^2 - bY^2$. The equation $z^2 - ax^2 - by^2 = 0$ then has the solution $(x,y,z) = (1,Y,Z)$ and so $(a,b)_K = 1$. Conversely, if $(a,b)_K = 1$, the equation $z^2 - ax^2 - by^2 = 0$ has a non-trivial solution in K^3. Observe that $x \neq 0$ or else b would be a square so $a = Z^2 - bY^2$ where $Z = z/x$ and $Y = y/x$. We see that a is then the norm of $Z + \sqrt{b}\,Y$.

By Proposition 4.1, one can rewrite the Hilbert symbol in terms of norms

$$(a,b)_K = \begin{cases} 1 & \text{if } a = N(\alpha)\ ;\ \alpha \in K(\sqrt{b})^\times \\ -1 & \text{otherwise} \end{cases}$$

From the multiplicativity of the norm, it follows that

$$(a,b)(a,b') = (a,bb').$$

In particular $(a,b) = 1 \Rightarrow (a,bb') = (a,b')$. Furthermore, since the definition of the Hilbert symbol depends on the solvability of $z^2 - ax^2 - by^2 = 0$, and since (x_0,y_0,z_0) is a solution of $z^2 - ax^2 - by^2 = 0$ then (x_0,z_0,y_0) is a solution of $z^2 - bx^2 - ay^2 = 0$. Thus the Hilbert symbol is symmetric, that is

$$(a,b) = (b,a).$$

Combining these last two properties one gets the bilinearity of the Hilbert symbol

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

Now, the equation $z^2 - ax^2 + ay^2 = 0$ has solutions $x = y$, $z = 0$, the equation $z^2 - ax^2 - y^2 + ay^2 = 0$ has solutions $x = y = z$ and $z^2 - ax^2 \pm c^2y^2 = 0$ has the solutions $(0,\ y,\ z = \pm cy)$ also $(a,-a) = (a,-1)(a,a)$. We thus get the following properties

$$(a,-a) = (a,c^2) = (a,1-a) = 1 \qquad \text{and} \qquad (a,a) = (a,-1).$$

The Hilbert symbol also has that property

$$(a,b) = (a,-ab)$$

For later use, we introduce an explicit means by which to calculate the Hilbert symbol of a and b relative to the p-adic field $\mathbb{Q}_p$, the proof of which is herein omitted.

Theorem 4.1

Let $a,b \in \mathbb{Q}_p$ where $a = up^{v_p(a)}$ and $b = vp^{v_p(b)}$; $u,v \in \mathbb{Z}_p^{\times}$, $p \neq 2$. The values of the Hilbert symbol over $\mathbb{Q}_p$ for different primes p are given by:

$$(a,b)_{\mathbb{Q}_p} = \left(\frac{-1}{p}\right)^{v_p(a)v_p(b)}\left(\frac{u}{p}\right)^{v_p(b)}\left(\frac{v}{p}\right)^{v_p(a)}$$

If $p = 2$

$$(a,b)_{\mathbb{Q}_2} = (-1)^{(u-1)(v-1)/4+v_2(a)(v^2-1)/8+v_2(b)(u^2-1)/8}$$

If $p = \infty$

$$(a,b)_{\mathbb{R}} = \begin{cases} 1 & \text{if } a \text{ or } b > 0 \\ -1 & \text{if } a \text{ and } b < 0 \end{cases}$$

Proof See [24] pp.21.

Corollary 4.1

Let $a,b \in \mathbb{Q}$ where $a = up^n$ and $b = vp^m$; $u,v \in \mathbb{Z}_p^{\times}$. For $p \neq 2,\infty$, if $p \nmid ab$ then the Hilbert symbol $(a,b)_{\mathbb{Q}_p} = 1$. For $p = 2$ if $2 \nmid ab$ and u or v is congruent to 1 modulo 4 then $(a,b)_{\mathbb{Q}_2} = 1$.

Corollary 4.2

Let p and q be odd primes, $p \neq q$. Then

$$i) \qquad (-1,p)_{\mathbb{Q}_2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

$$ii) \quad (2,p)_{\mathbb{Q}_2} = \begin{cases} 1 & \text{if } p \equiv \pm 1 (\text{mod } 8) \\ -1 & \text{if } p \equiv \pm 3 (\text{mod } 8) \end{cases}$$

$$iii) \quad (q,p)_{\mathbb{Q}_2} = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 (\text{mod } 4) \\ 1 & \text{otherwise} \end{cases}$$

4.2 Hilbert's Tenth Problem

10. Determination of the solvability of a Diophantine equation

"Given a Diophantine equation with any number of unknowns and with rational integer coefficients. Devise a process, which could determine by a finite number of operations whether the equation is solvable in rational integers." [34]

Corollary 4.1 implies that there is a method to test whether or not $z^2 - ax^2 - by^2 = 0$ has a solution in $\mathbb{Q}_p$, $p < \infty$ (in a finite number of steps) since we need only consider the primes which divide a or b. By the Hasse-Minkowski Theorem, this means that there is a method to test, in a finite number of steps, whether or not a given ternary quadratic form with rational coefficients has a rational zero. For $p = \infty$ the method is even more simple. This answers Hilbert's Tenth problem for Diophantine equations of degree 2 in three variables. The Hasse-Minkowski Theorem provides an algorithm to determine the solvability of any quadratic form over a field of characteristic other than 2. The general Hilbert's tenth problem has been shown to be impossible to solve by Matijasevic in 1970.

Chapter 5

Proof of the Hasse-Minkowski Theorem

We now have all the necessary tools to prove the Hasse-Minkowski Theorem (stated below). Most important to keep in mind is that even though we assumed solutions in $\mathbb{Q}_p$ $(p \neq 2)$ at the onset, once we have reduced to the diagonal form with relatively prime, square free nonzero a_i, this is equivalent to having a solution in $\mathbb{F}_p$ $(p \neq 2)$ because of Hensel's Lemma.

5.1 Proof for Ternary Quadratic Forms ($n = 3$)

Since all ternary quadratic forms with rational coefficients can be transformed into the form $f(x,y,z) = z^2 - ax^2 - by^2$, we can focus our attention on those forms and rewrite the Hasse-Minkowski Theorem of Chapter 2 as

Theorem 5.1 (Hasse-Minkowski)
The quadratic form $f(x,y,z) = z^2 - ax^2 - by^2 = 0$, where $a,b \in \mathbb{Q}$, has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{Q}_p$ for each $p \leq \infty$.

Proof First, some preliminary remarks. We may assume that a and b are integers. If not, for instance if we have $z^2 - (1/s)x^2 - cy^2 = 0$, simply substitute $x = sx_0$ and we then have $z^2 - s{x_0}^2 - cy^2 = 0$ to work with. We may also assume that a and b are square free by absorbing the square factor into one of the unknowns. We may look

for $x,y,z \in \mathbb{Z}$ since $f(x,y,z) = 0$ can be solved in $\mathbb{Q}$ if and only if it can be solved in $\mathbb{Z}$ (because f is homogeneous). Without loss of generality we may also suppose that $|a| \leq |b|$ and that x,y,z have no common factor. Let us now begin the proof, which is by induction on $m = |a| + |b|$.

If $m = 0 \Rightarrow |a| = |b| = 0$.

The general case $a = 0$ and $b \neq 0$, which covers the cases $m = 1 \Rightarrow a = 0$, $|b| = 1$ and $m = 2$ where $a = 0$ and $|b| = 2$, reduces to the question: *If b is a square modulo p for all $p \leq \infty$ is b a square in* $\mathbb{Q}$? This question was answered by the Global Square Theorem (Theorem 1.1).

If $m = 2$, where $|a| = |b| = 1$, we have the four possibilities:

$$z^2 - x^2 + y^2 = 0, \qquad z^2 - x^2 - y^2 = 0, \qquad z^2 + x^2 - y^2 = 0, \qquad z^2 + x^2 + y^2 = 0$$

The first three equations have solutions in $\mathbb{Q}$ thus trivially in all the p-adic fields $\mathbb{Q}_p$. The last equation has no solutions in $\mathbb{R}$ so it clearly has no solutions in $\mathbb{Q}$, *i.e.* $(1,1)_{\mathbf{R}} = -1 \Rightarrow (1,1)_{\mathbf{Q}} = -1$.

Now suppose $m \geq 3$ and that for $|a| + |b| < k$ and that $(a,b)_{\mathbb{Q}_p} = 1$ for all $p \leq \infty$ implies $(a,b)_{\mathbf{Q}} = 1$. Write

$$|b| = \prod_i p_i$$

where the p_i are distinct primes.

Claim: a is a square modulo p_i for all $p_i | b$.

If $a \equiv 0 (\mathbf{mod}\, p_i)$ then a is a square modulo p_i.

If $a \not\equiv 0 (\mathbf{mod} p_i)$, then since $(a,b)_{\mathbb{Q}_{p_i}} = 1$, $\exists\ x,y,z \in \mathbb{Q}_{p_i}$ not all zero such that $z^2 - ax^2 - by^2 = 0$. This can be reduced to the congruence $z^2 \equiv ax^2 (\mathbf{mod} p_i)$. If a is not a square modulo p_i then $x \equiv 0 (\mathbf{mod} p_i)$ which in turn implies $z^2 \equiv 0 (\mathbf{mod} p_i)$. Hence p_i divides x,y and z, a contradiction.

Now, a is a square modulo p_i for all $p_i|b$, so by the Chinese Remainder Theorem , a is a square modulo b. There thus exist integers t, and b' such that;

$$t^2 = a + bb' \tag{5.1}$$

By inspection of (5.1), $z^2 - ax^2 - bb'y^2 = 0$ has the solution $(1,1,t) = (x,y,z)$, that is to say $(a,bb')_{\mathbb{Q}} = 1$ which trivially implies that $(a,bb')_{\mathbb{Q}_p} = 1 \; \forall p \leq \infty$. Choose t such that $|t| \leq \frac{|b|}{2}$. Then,

$$|b'| = |\frac{t^2 - a}{b}| \leq |\frac{t^2}{b}| + |\frac{a}{b}| \leq \frac{|b|}{4} + 1 < |b|$$

since $|b| \geq 2$. So $|a| + |b'| < k$ and thus, by the hypothesis, we have the implication $(a,b')_{\mathbb{Q}_p} = 1 \; \forall p \leq \infty \Rightarrow (a,b')_{\mathbb{Q}} = 1$. Applying the properties of the Hilbert symbol seen in the previous chapter, we have $(a,b)_{\mathbb{Q}_p} = 1 \; \forall p \leq \infty$ and $(a,bb')_{\mathbb{Q}_p} = 1 \forall p \leq \infty$ thus $(a,b')_{\mathbb{Q}_p} = 1 \; \forall p \leq \infty$ which implies $(a,b')_{\mathbb{Q}} = 1$ by hypothesis. Finally, we have $(a,bb')_{\mathbb{Q}} = 1$ and $(a,b')_{\mathbb{Q}} = 1$, so $(a,b)_{\mathbb{Q}} = 1$. This ends the proof of the Hasse-Minkowski Theorem for ternary quadratic forms.

□

5.2 Proof for $n > 3$

The idea behind the proof of the Hasse-Minkowski Theorem for four variables is to construct an integer r which is simultaneously represented by the forms $g = a_1x_1^2 + a_2x_2^2$ and $h = -a_3x_3^2 - a_4x_4^2$ $(a_i \in \mathbb{Q})$ resulting in a rational representation of zero by the indefinite form

$$f(x_1,x_2,x_3,x_4) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$$

We will see that the construction of such an integer follows from the p-adic solvability of $f = 0$ at all primes. The existence of the integer r with the required properties will then be proved using Dirichlet's Theorem on primes in arithmetic progressions.

Theorem 5.2 (Dirichlet's Theorem)

If a and m are relatively prime integers greater than 0, then there exist infinitely many primes p such that $p \equiv a (\mathrm{mod}\, m)$.

Theorem 5.3

Let K be a field with more than five elements. If $a_1x_1^2 + ... + a_nx_n^2 = 0 \quad (a_i \in K)$ has a non-trivial solution in K then it has solution in K for which all the variables take non-zero values.

Proof [6] pp.394.

Theorem 5.4

The quaternary quadratic form with rational coefficients

$$f(x_1,x_2,x_3,x_4) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 0$$

where the $a_i's$ are square free, is solvable in $\mathbb{Q}$ if and only if it is solvable in $\mathbb{Q}_p$ for all $p \leq \infty$.

Proof (Ref. [6] pp.68). Since the form f is solvable in $\mathbb{R}$, it is indefinite, say $a_1 > 0$ and $a_4 < 0$. We will consider the forms

$$g = a_1x_1^2 + a_2x_2^2 \qquad \text{and} \qquad h = -a_3x_3^2 - a_4x_4^2$$

Let S denote the set of distinct odd primes which divide the coefficients a_1, a_2, a_3 and a_4, together with the prime 2 and the infinite prime. Since $f = 0$ is solvable in $\mathbb{Q}_p$ for all $p \leq \infty$, it is in particular solvable for all $p \in S$. By Theorem 5.3, we can choose a representation of zero for each prime $p \in S$

$$a_1\beta_1^2 + a_2\beta_2^2 + a_3\beta_3^2 + a_4\beta_4^2 = 0 \qquad (\beta_i \in \mathbb{Q}_p)$$

where all $\beta_i \neq 0$. Fix $b_p = a_1\beta_1^2 + a_2\beta_2^2 = -(a_3\beta_3^2 + a_4\beta_4^2)$. If some $b_p = 0$, then h and g represent zero in $\mathbb{Q}_p$, hence they represent all numbers by Theorem 2.3. So we may assume that our representation is such that each b_p is a nonzero p-adic integer divisible by at most the first power of p.

Consider the system of congruences

$$\begin{aligned} r &\equiv b_2 (\mathrm{mod}\, 16) \\ r &\equiv b_{p_1} (\mathrm{mod} p_1^{\,2}) \\ r &\equiv b_{p_2} (\mathrm{mod} p_2^{\,2}) \\ &\cdots \\ r &\equiv b_{p_s} (\mathrm{mod} p_s^{\,2}) \end{aligned}$$

The integer $r \neq 0$, which we may choose to be positive, is uniquely determined modulo $m = 16p_1^{\,2}\cdots p_s^{\,2}$ by the Chinese Remainder Theorem. Since b_{p_i} is divisible by at most the first power of p_i, then $|b_{p_i} r^{-1}|_{p_i} = 1$ (*i.e.* $b_{p_i} r^{-1}$ is a p_i-adic unit) and $b_{p_i} r^{-1} \equiv 1 (\mathrm{mod} p_i)$. Hence $b_{p_i} r^{-1}$ is a quadratic residue modulo $p\mathbb{Z}_p$ and thus $b_{p_i} r^{-1}$ is a p_i-adic square (Corollary 1.1) . Also, $2^2 \nmid b_2$, so $b_2 r^{-1} \equiv 1 (\mathrm{mod}\, 8\mathbb{Z}_2)$ and $b_2 r^{-1}$ is a 2-adic square (Corollary 1.2). Since b_p and r always differ by a square factor in all $\mathbb{Q}_p$ for $p \in S$, both the forms

$$-a_3 x_3^{\,2} - a_4 x_4^{\,2} - r x_0^{\,2} \quad \text{and} \quad a_1 x_1^{\,2} + a_2 x_2^{\,2} - r x_0^{\,2}$$

represent zero in $\mathbb{Q}_p$ for all $p \in S$. Since we assumed $a_1 < 0$ and $a_4 > 0$, both forms are indefinite and thus have a solution in $\mathbb{R}$. If $p \notin S$ and $p \nmid r$ then p does not divide any of the coefficients of the ternary forms and thus the forms represent zero in $\mathbb{Q}_p$ (Corollary 4.1). If there is one more prime $q \notin S$ such that $q \mid r$, we can use the fact that if a quadratic form with rational coefficients f represents zero in all fields $\mathbb{Q}_p$ for all $p \leq \infty$ except possibly for $\mathbb{Q}_q$ for some prime q, then f also represents zero in $\mathbb{Q}_q$. The reason why this is true will become clear in Chapter 9. Now, by the ternary case of the Hasse-Minkowski Theorem proved above, there exists rational numbers $c_1, c_2,\ c_3$ and c_4 such that $r = a_1 c_1^{\,2} + a_2 c_2^{\,2} = -a_3 c_3^{\,2} - a_4 c_4^{\,2}$, so that

$$a_1 c_1^{\,2} + a_2 c_2^{\,2} + a_3 c_3^{\,2} + a_4 c_4^{\,2} = 0 \qquad (c_i \in \mathbb{Q})$$

To prove the existence of such an integer r, we may use Dirichlet's Theorem on prime numbers in arithmetic progressions. Let s be a number satisfying the system of congruences above and let $d = \gcd(s, m)$. Then s/d and m/d are relatively prime

and Dirichlet's Theorem implies that there is a positive integer k such that $s/d + km/d = q$ is prime. We can then let $r = s + km = dq$. The result follows.

For five variables we repeat the argument above, finding an integer r by Dirichlet's Theorem which is represented by $g = a_1x_1^2 + a_2x_2^2$ and $h = -(a_3x_3^2 + a_4x_4^2 + a_5x_5^2)$. Then by Hasse-Minkowski Theorem for three and four variables, g and h represents r in $\mathbb{Q}$, giving us a rational representation of zero by

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2.$$

It is easy to see that repeated application of this process will produce a proof of the n variable Hasse-Minkowski.

□

Theorem 5.5

Any quadratic form in five or more variables with coefficients in $\mathbb{Q}_p$ always has a non-trivial solution in $\mathbb{Q}_p$.

Proof See [6] pp.51.

In combination with the Hasse-Minkowski Theorem, Theorem 5.5 implies the result

Theorem 5.6

Every indefinite quadratic form f in five or more variables has a non-trivial rational zero.

5.3 Artin's Conjecture

The success in applying p-adic numbers to the theory of quadratic forms made it natural to consider applying them to forms of higher order. Artin had conjectured;

Artin's Conjecture

All homogeneous equations in $\mathbb{Q}_p[x_1,...,x_n]$ of degree r in at least r^2+1 variables have a non-trivial solution in $\mathbb{Q}_p$.

Artin's conjecture holds for $r = 2$ by virtue of Theorem 5.5. The conjecture has also been proved for $r = 3$, (Refer to [27]). The general Artin Conjecture remained open for approximately thirty years until a counterexample of degree $r = 4$ in 18 variables was discovered in 1966 by G. Terjanian [28]. Terjanian first notes that it suffices to have a homogeneous polynomial of degree 4, $f(x_1,...,x_9) \in \mathbb{Z}[x_1,...,x_9]$ with the property that $f(x_1,...,x_9) \equiv 0 \pmod 4$ implies all the x_i are divisible by 2 to have a counterexample. Indeed the polynomial

$$f(x_1,...,x_9) + 4f(x_{10},...,x_{18}) \tag{5.2}$$

would then be a counterexample because if it had a zero in $\mathbb{Q}_2$, it would have a primitive zero in $\mathbb{Z}_2$, which is not possible. To verify the last statement, suppose there is a primitive zero in $\mathbb{Z}_2$. The form $f(x_1,...x_9)$ is then congruent to 0 modulo 4 which implies 2 divides x_i for $i = 1,...,9$. So 16 divides (5.2) which implies that 4 divides $f(x_{10},...,x_{18})$ and hence 2 divides x_i for $i = 10,...,18$. Terjanian then constructs the following polynomial:

$$f = n(x_1,x_2,x_3) + n(x_4,x_5,x_6) + n(x_7,x_8,x_9)$$

$$n(x,y,z) = x^2yz + y^2zx + z^2xy + x^2y^2 + x^2z^2 + y^2z^2 - x^4 - y^4 - z^4$$

which has the desired property. It is easily verified that if x,y and z are divisible by 2, then $n \equiv 0 \pmod 4$. If any one of x,y or z is not divisible by 2 then $n \equiv 3 \pmod 4$. Consequently $f(x_1,...,x_9) \equiv 0 \pmod 4$ implies that all x_i's are divisible by 2 and we have a counterexample by the discussion above.

There is a conciliatory theorem [2] which states that

Theorem 5.7

For any natural number r, there exists a finite set S of primes such that any form of degree r over $\mathbb{Q}_p$ represents zero non-trivially for every p not in S, provided that the number of variables is at least $r^2 + 1$.

However, there is no known method for determining the set S of exceptional prime numbers ([24] pp.39). Theorems 5.5 and 5.7 are part of a family of theorems in Number Theory which read, as Borevich-Shafarevich put it: "*All is well as long as the number of variables is sufficiently large*" [6] pp.57. In 1957, B.J. Birch proved in his article *Homogeneous forms of odd degree in a large number of variables* [5] that: Given an odd number d, there exists an n such that every homogeneous equation of degree d in n variables has a non-trivial rational solution.

5.4 Projecting a Conic onto a Line

The Hasse-Minkowski Theorem does not help us find a rational solution, it only tells us whether or not our search would be in vain. If our quadratic equation has a rational solution, it has infinitely many. Once we have explicitly found a rational point $P = (x_0, y_0)$ on a rational conic f, we can derive all others by drawing the rational line $L = y - y_0 = t(x - x_0)$ where t is rational and projecting the conic onto the line from point P. Consider the classical problem of parametrizing the Pythagorean triples. Integer solutions to

$$X^2 + Y^2 = Z^2$$

where X, Y and Z have no common factors correspond tc rational solutions to the unit circle

$$x^2 + y^2 = 1$$

where $x = X/Z$ and $y = Y/Z$ are in lowest term. We will project from the point $(-1, 0)$

onto the y-axis. Let $(0,t)$ be the y-intercept and let L denote the line through $(-1,0)$ and $(0,t)$. Armed with the knowledge of x and y, we may get t easily since the slope of L is $t = \frac{y}{1+x} \in \mathbb{Q}$. The equation of L is then $y = t(x+1)$. If the point (x,y) is on the circle and the line L we obtain the relation

$$(1+x)(1-x) = 1-x^2 = y^2 = t^2(1+x)^2$$

Cancelling out an $(x+1)$, solving for x and using the relation $y = t(1+x)$ to solve for y one gets the familiar parametrization of the unit circle as the set

$$(x = \frac{1-t^2}{1+t^2}, y = \frac{2t}{1+t^2})$$

Clearly x and y are rational if and only if t is rational. All rational points on the unit circle $x^2+y^2 = 1$ may be found by simply plugging in arbitrary rational numbers in place of t. This technique allows us to describe the infinite amount of rational points on any conic completely given one rational point. Hence, the Diophantine theory of conics, dominated by the Hasse Principle, is well-understood.

Chapter 6

Equivalence of Quadratic Forms

Mathematicians of the 18th century were greatly preoccupied by the problem of determining conditions for the existence of solutions to binary quadratic equations $ax^2 + bxy + cy^2 + dx + ey + f = 0$ with integer coefficients and to find algorithms to find all such solutions. It was determined early on that one need only consider equations of the form $(a,b,c) = ax^2 + bxy + cy^2 = n$ where a,b and c are relatively prime *i.e.* primitive forms. When faced with the problem of finding integer solutions for such an equation, it is normal to try to simplify it by doing a change of variables. For instance performing the transformation $x_0 = 30x + 43y$, $y_0 = y$ on $15x^2 + 43xy + 32y^2 = 223$ gives us the simpler equation: $x_0^2 + 71y_0^2 = 13380$. An elementary calculation yields the solutions $x_0 = \pm 94$, $y_0 = \pm 8$. However, the corresponding solutions for our original equation, $x = (1/30)(x_0 - 43y_0)$, $y = y_0$, are not integers.

6.1 Preliminary Results

The need to find invertible transformations led Lagrange to lay the foundation for the classification of quadratic forms. Let K be an arbitrary field of characteristic different from 2. Let $f = \sum_{i,j=1}^{n} a_{ij}x_ix_j$, where $a_{ij} = a_{ji}$ $(a_{ij} \in K)$. Let K be an arbitrary field of characteristic different from 2. The determinant d of the quadratic form f is

the determinant of $A = (a_{ij})$, the matrix of the quadratic form f. If $d = 0$ the form f is said to be singular. Otherwise, it is called nonsingular. Two quadratic forms f and g are called equivalent (denoted by $f \sim g$) if there is a nonsingular linear change of variables, which takes one form to the other. Equivalent forms represent the same numbers. The following theorems were found in the *Algebraic Supplement* of Borevich-Shafarevich [6]. The reader is referred to this text for the proofs.

Theorem 6.1

If two quadratic forms over the field K are equivalent over K, then their determinants differ by a nonzero factor which is a square in K.

Definition 6.1

Let f and g be two nonsingular quadratic forms. The form $f+g$ denotes $f(\mathbf{x}) + g(\mathbf{y})$ where $\mathbf{x}$ and $\mathbf{y}$ are independent sets of variables (*i.e.* we are taking the direct sum of the two quadratic spaces.)

Theorem 6.2 (Witt's Theorem)

Let f,g,h be nonsingular quadratic forms over K. If the forms $f+g$ and $f+h$ are equivalent over K then g and h are equivalent over K.

Theorem 6.3

If a quadratic form f in n variables with coefficients in a field K represents $a \neq 0$ then f is equivalent to $ax^2 + g(x_2,...,x_n)$ over K, where g is a quadratic form in $n-1$ variables with coefficients in K.

6.2 A Local-Global Principle

Hasse applied Hensel's p-adic methods to the problem of equivalence of quadratic forms which resulted in a variant of the Hasse-Minkowski Theorem. Hasse's

Habilitation dissertation (1923) contained a proof of the following

Theorem 6.4 (Hasse-Minkowski)
Two nonsingular quadratic forms with rational coefficients are equivalent over the field of rational numbers, if and only if they are equivalent over $\mathbb{R}$ and all the p-adic fields $\mathbb{Q}_p$.

Proof The proof I give is from [6] pp.70. It is by induction on n, the number of variables. If $n = 1, f = ax^2 \sim g = bx^2$ in $\mathbb{Q}_p$ for all $p \leq \infty$ if and only if a/b is a square in $\mathbb{Q}_p$ for all $p \leq \infty$ which is true if and only if a/b is a square in $\mathbb{Q}$ (Theorem 1.1). If $n > 1$, let $r \in \mathbb{Q}$ be represented by f in all $\mathbb{Q}_p$. Since $f \sim g$ in all $\mathbb{Q}_p$, r is also represented by g in all $\mathbb{Q}_p$. By the Hasse-Minkowski Theorem r is then represented by f and g in $\mathbb{Q}$. Applying Theorem 6.3

$$f \sim rx^2 + f_1 \quad \text{and} \quad g \sim rx^2 + g_1$$

where f_1 and g_1 are quadratic forms in $n-1$ variables. By Witt's Theorem, since $f \sim g$ in all $\mathbb{Q}_p$, then $f_1 \sim g_1$ in all $\mathbb{Q}_p$. By the induction hypothesis, $f_1 \sim g_1$ in $\mathbb{Q}$, so $f \sim g$ in $\mathbb{Q}$.

□

This result was also printed in the Crelle journal of 1923 in the article *Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen (About the equivalence of quadratic forms over the field of rational numbers)* [18]. Minkowski had once again previously stated an equivalent result. See [13], pp.315, for a statement of Minkowski's result.

The importance of the Hasse Principle is that both the representability of a number by a given quadratic form and whether two quadratic forms are equivalent can be determined by local information. This is interesting because questions of equivalence, like representability of a rational number over local fields, are manageable. For instance, Sylvester's Law states that (Ref. [20] pp. 42)

Theorem 6.5 (Sylvester's Law)

Let r_1 be the number of positive terms in the diagonalization of a form and r_2 be the number of negative terms. Two quadratic forms over $\mathbb{R}$ are equivalent if and only if they have the same dimension $n = r_1 + r_2$ and the same signature $r_1 - r_2$.

Chapter 7

Failure of the Hasse Principle

The result for quadratic forms with rational coefficients certainly looks encouraging. Unfortunately, a general equation having solutions in $\mathbb{R}$ and all p-adic fields $\mathbb{Q}_p$, by no means guarantees solutions in $\mathbb{Q}$. That the *Local-Global Principle* fails for certain curves was seen early on. The first explicit counterexample, $X^4 - 17 = 2Y^2$, was offered by Reichardt in 1942. We will see in detail that $X^4 - 17 = 2Y^2$ has solutions everywhere locally, but not globally in the proof of Theorem 7.4. Ernst S. Selmer later gave a large number of Diophantine equations for which the Hasse Principle fails, including the now famous $3X^3 + 4Y^3 + 5Z^3 = 0$. Selmer's example will also be discussed at length.

7.1 A Simple Counterexample

First, we will present the considerably simpler counterexample to the Hasse Principle. The equation

$$f(X) = (X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$$

has a root in $\mathbb{Q}_p$ for all $p \leq \infty$, but has no root in $\mathbb{Q}$.

Proof It is clear that f has a solution in $\mathbb{R}$ and no solution in $\mathbb{Q}$ since the numbers 2, 17 and 34 are not squares of rational numbers. It remains to be shown that $f = 0$ has a solution in all completions of $\mathbb{Q}$.

Case 1 $p \neq 2, 17$

If either (or both) $\left(\frac{2}{p}\right) = 1$ or $\left(\frac{17}{p}\right) = 1$, then $\alpha^2 \equiv 2$ or $\alpha^2 \equiv 17 (\mathrm{mod} p)$ is solvable in $\mathbb{Z}/p\mathbb{Z}$. Thus there exists an $\alpha \in \mathbb{Z}/p\mathbb{Z}$ such that $f(\alpha) \equiv 0 (\mathrm{mod} p)$. The derivative $2\alpha \not\equiv 0 (\mathrm{mod}\ p)$ since $p \neq 2$ and $\alpha \not\equiv 0 (\mathrm{mod}\ p)$, so solutions lift by Hensel's Lemma. If $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{17}{p}\right) = -1$, then $\left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{34}{p}\right) = 1$ by multiplicativity of the Legendre symbols.

Case 2 $p = 17$

Since $6^2 \equiv 2 (\mathrm{mod}\, 17)$ then $f(6) \equiv 0 (\mathrm{mod}\, 17)$ and $f'(6) = 12 \not\equiv 0 (\mathrm{mod}\, 17)$.

Case 3 $p = 2$

Here, $17 \equiv 1 (\mathrm{mod}\, 8)$ so 17 is a 2-adic square by Corollary 1.2.

Hence, $(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$ does not have a solution in $\mathbb{Q}$ even though it has a solution in all p-adic fields $\mathbb{Q}_p$.

□

So we see that, in general, there is no analogue of Hasse's principle for curves of genus $g \geq 1$ or even for general nonsingular cubic curves, although there are interesting classes of Diophantine cubic equations for which it is known to hold. For instance, we will see in Chapter 10 that Selmer worked out in 1953 sufficient criteria for the Hasse Principle to hold for the cubic equation $ax^3 + by^3 + cz^3 + dw^3 = 0$, $(a, b, c, d \in \mathbb{Z},\ x, y, z, w \in \mathbb{Q})$. There is no known method to determine in a finite number of steps whether a given rational cubic has a rational point. Moreover, when there are rational solutions, there may not be infinitely many.

7.2 Selmer's Curve

As we have seen in the previous section, the idea of looking modulo p for all primes p is not sufficient for cubic curves. Let us take a closer look at the counterexample due to Selmer (1951)

$$f(X,Y,Z) = 3X^3 + 4Y^3 + 5Z^3 \tag{7.1}$$

where $X,Y,Z \in \mathbb{Q}$. Since the form is homogeneous we may look for $X,Y,Z \in \mathbb{Z}$. Selmer's curve has p-adic solutions for all p, but no rational solution. Selmer proved the global insolubility of $3X^3 + 4Y^3 + 5Z^3 = 0$ by considering factorization in a cubic field $\mathbb{Q}(\delta)$. Selmer rewrites the equation as $N\left(\frac{x+\delta y}{-z}\right) = \frac{5}{3}$ where $\delta^3 = \frac{4}{3}$. For a sketch of Selmer's argument see [7], pp.206. We will go about it in quite a different way. There is a theorem which asserts

Theorem 7.1

A curve of genus 1 over $\mathbb{F}_p$ has a point defined over $\mathbb{F}_p$ and thus over $\mathbb{Q}_p$.

Proof See [10], pp.119.

In our particular example, all primes p except for the primes $p = 2,3$ and 5 have good reduction (since they do not divide the discriminant $D = -2^{12}3^{11}5^2$). By Theorem 7.1, the form thus has a zero in $\mathbb{Q}_p$ for all $p \neq 2,3,5$. Note that for $p = \infty$ the form clearly has a zero. For $p = 2$, the form (7.1) has the zero $(\sqrt[3]{-5/3}, 0, 1)$. This zero is in $\mathbb{Q}_2$ since 3 is the inverse of 3 modulo 8 so $-5/3 \equiv (-5)(3) \equiv -15 \equiv 1 (\mathrm{mod}\, 8)$ hence $-5/3$ is a 2-adic cube. For $p = 3$, note that $-4/5$ is a 3-adic cube because $-4/5 \equiv (-4)(-16) \equiv 10 (\mathrm{mod}\, 27)$ (since -16 is the inverse of 5) and $10 = 1 + 9$ is a 3-adic cube. So (7.1) has the 3-adic zero $(0, 1, \sqrt[3]{-4/5})$. For $p = 5$, $3X^3 \equiv Y^3 (\mathrm{mod}\, 5)$ has the solution $X = 1, Y = 2$. The derivative $f'(1,2,0) = 9 - 12 \not\equiv 0 (\mathrm{mod}\, 5)$ so the solution to $3X^3 + 4Y^3 + 5Z^3 = 0$ lifts to a p-adic solution by Hensel's Lemma.

Now to show that $3X^3 + 4Y^3 + 5Z^3 = 0$ has no rational solutions, we will need the following theory.

Lemma 7.1

Let $\rho^3 = 1$, $\rho \neq 1$ and $\mathbb{Q}(\rho) = K$. Let the Galois group $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) = G$. If $A, B \in K^2$ are distinct Galois conjugate points on the curve $u^3 + v^3 + d = 0$ where $u, v \in \mathbb{Q}$, $d \in \mathbb{Z}$, then the line joining A and B is rational and intersects the curve in a third point with rational coefficients.

Proof

The Galois group G is generated by the automorphism $\sigma : \rho \mapsto \rho^2$. Let $A = (u_1, v_1)$ and $B = (u_2, v_2)$ be such that $\sigma u_1 = u_2$ and $\sigma v_1 = v_2$. The line joining A and B will be denoted by $L : v = mu + b_0$. The slope of L is $m = \dfrac{(v_2 - v_1)}{(u_2 - u_1)}$. Applying σ to the slope we obtain $\sigma m = \dfrac{(\sigma v_2 - \sigma v_1)}{(\sigma u_2 - \sigma u_1)} = \dfrac{(v_1 - v_2)}{(u_1 - u_2)} = m$ so $m \in \mathbb{Q}$. Applying σ to the intersect $b_0 = v_1 - mu_1$ we get $\sigma b_0 = v_2 - mu_2 = b_0$, thus $b_0 \in \mathbb{Q}$. Let $C = (u_3, v_3)$ be the third point of intersection. Substituting the line in the curve

$$0 = u^3 + (mu + b_0)^3 + d = (m^3 + 1)(u - u_1)(u - u_2)(u - u_3)$$

where u_1, u_2, u_3 are the zeros. Comparing the coefficients of u^2 results in $u_1 + u_2 + u_3 = (3m^2 b_0)/(m^3 + 1)$. Now $u_1 + u_2$ and $(3m^2 b_0)/(m^3 + 1)$ are rational thus u_3 is rational. Plugging back into the equation of the line, v_3 is also rational and hence C is a rational point.

□

Theorem 7.2

Let $a, b, c > 1$ be distinct integers such that $d = abc$ is cube free. Suppose there are integers x, y, z not all zero such that $ax^3 + by^3 + cz^3 = 0$. Then there exists integers U, V, W with $W \neq 0$ such that $U^3 + V^3 + dW^3 = 0$.

Proof ([10], pp.86) Let $\rho^3 = 1, \rho \neq 1$. Bear in mind that $1 + \rho + \rho^2 = 0$. Write

$$\xi = ax^3 + \rho by^3 + \rho^2 cz^3 \qquad \text{and} \qquad \eta = ax^3 + \rho^2 by^3 + \rho cz^3$$

Then

$$\xi + \eta = 2ax^3 + (\rho + \rho^2)(by^3 + cz^3) = 3ax^3.$$

Similarly

$$\rho^2\xi + \rho\eta = 3by^3 \qquad \text{and} \qquad \rho\xi + \rho^2\eta = 3cz^3$$

Now $(\xi + \eta)(\rho^2\xi + \rho\eta)(\rho\xi + \rho^2\eta) = \xi^3 + \eta^3 = 3^3(xyz)^3d$. So

$$\xi^3 + \eta^3 + d\gamma^3 = 0$$

where $\gamma = -3xyz$.

The two points $A = (\xi, \rho\eta, \gamma)$ and $B = (\eta, \rho^2\xi, \gamma)$ are solutions to the Selmer curve $U^3 + V^3 + dW^3 = 0$. The points A and B are Galois conjugates over $\mathbb{Q}$, since ξ and η are conjugates, $\rho\eta$ and $\rho^2\xi$ are conjugates and γ is rational. First observe that the line L joining A and B will intersect $U^3 + V^3 + dW^3 = 0$ in a third point C which is not $(1,-1,0)$. If it was, it would imply that $a = b$, but a, b, c are distinct integers. Dehomogenizing with respect to W, we may apply Lemma 7.1. The line L is rational and will intersect $u^3 + v^3 + d^3 = 0$ in a third point with rational coordinates. Putting C in homogeneous coordinates by clearing the denominators we get integers U, V, W with $W \neq 0$ such that $U^3 + V^3 + dW^3 = 0$.

□

Lemma 7.2 The only rational point of $X^3 + Y^3 + 60Z^3 = 0$ is $(1,-1,0)$

Proof (Sketch [10], pp.86)

Let $u = U/W$, $v = V/W$. The Selmer curve $u^3 + v^3 = d$ is birationally equivalent to the Weierstrass curve $y^2 = x^3 - 2^4 3^3 d^2$ under the transformation

$$u = \frac{36d + y}{6x} \qquad v = \frac{36d - y}{6x},$$

for which the inverse transformation is

$$x = \frac{12d}{u+v} \qquad y = \frac{36d(u-v)}{u+v}$$

In our example, $d = -60$ so $X^3 + Y^3 + 60Z^3 = 0$ is birationally equivalent to $Y^2 = X^3 - 2^4 3^3 60^2$. Let $E(\mathbb{Q})$ denote the group of rational points of the elliptic curve. The group $E(\mathbb{Q})/2E(\mathbb{Q})$ for $Y^2 = X^3 - 2^4 3^3 60^2$ is trivial. For a proof, see [10], pp.53. The group

$$E(\mathbb{Q}) = \mathbb{Z}^r + \prod_{i=1}^{n} \mathbb{Z}/p_i\mathbb{Z}$$

(p_i not necessarily distinct) and

$$2E(\mathbb{Q}) = (2\mathbb{Z})^r + \prod_{\substack{i=1 \\ p_i \neq 2}}^{n} \mathbb{Z}/p_i\mathbb{Z}$$

Then $E(\mathbb{Q})/2E(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^{r+s}$ where r is the rank and s is the number of 2-torsion points. If $E(\mathbb{Q})/2E(\mathbb{Q})$ is trivial then $E(\mathbb{Q})$ has no 2-torsion points (and the rank is 0). A calculation with PARI with the function *elltors* shows that the curve has no p-torsion for p odd (it actually shows there is no 2-torsion as well). So $E(\mathbb{Q})$ is trivial.

□

Theorem 7.3

$3X^3 + 4Y^3 - 5Z^3 = 0$ has no rational solutions.

Proof By the two previous results, if $3X^3 + 4Y^3 + 5Z^3 = 0$ had a rational point then there would exist $x,y,z \in \mathbb{Z}$, $z \neq 0$ such that $x^3 + y^3 + 60z^3 = 0$, but by Lemma 7.2, no such point exists.

□

7.3 Reichardt's Equation

We now turn our attention to Reichardt's equation; $X^4 - 17 = 2Y^2$.

Theorem 7.4

$X^4 - 17 = 2Y^2$ has p-adic solutions for all primes $p \leq \infty$, but has no rational solution.

Proof Let $f(X,Y) = X^4 - 17 - 2Y^2 = 0$. Since the reduction of the curve has genus 1 for all p except for $p = 2$ and $p = 17$, we need only take a closer look at what happens to the curve at those primes. Observe that $17 \equiv 1 \pmod{16}$ so 17 a 2-adic fourth power by the discussion following Theorem 1.4. $X^4 - 17 = 2Y^2$ thus has a 2-adic solution $(\sqrt[4]{17}, 0)$. Furthermore, $X^4 - 17 - 2Y^2 \equiv X^4 - 2Y^2 \equiv 0 \pmod{17}$ $\Leftrightarrow a^2 \equiv 2 \pmod{17}$ where $a = X^2/Y$, $Y \neq 0$. The congruence has a non-trivial solution since $\left(\frac{2}{17}\right) = 1$. For example $X = Y = 6$. We can then lift this solution to a 17-adic solution by Hensel's Lemma since $f(6,6) \equiv 0 \pmod{17}$ where $\partial f/\partial X(6,6) \not\equiv 0 \pmod{17}$. Hence our equation has local solutions everywhere.

Now to show that $X^4 - 17 = 2Y^2$ has no global solutions, we will use some Algebraic Number Theory. The following is not the argument used by Reichardt. Let $K = \mathbb{Q}(\sqrt{17})$. Suppose $X^4 - 17 = 2Y^2$ has a rational solution. Set $X = a/c$ in lowest terms. The equation

$$a^4 - 17c^4 = 2b^2 \tag{7.2}$$

where a, b and c are rational integers would then have an integral solution. Note that if a prime p divides a and b this implies that p divides c. Similarly if p divides both b and c it divides a. So $\gcd(a,c) = \gcd(b,c) = \gcd(a,b) = 1$. Both a and c are odd, since the right hand side of (7.2) is even and both a and c cannot be even since $\gcd(a,c) = 1$. Since K has integral basis $\{1, \frac{(1+\sqrt{17})}{2}\}$, this makes $\frac{a^2 + c^2\sqrt{17}}{2}$ and $\frac{a^2 - c^2\sqrt{17}}{2}$ elements of $\mathcal{O}_K$.

Now note that $\frac{a^2+c^2\sqrt{17}}{2}$ and $\frac{a^2-c^2\sqrt{17}}{2}$ are relatively prime, since if a prime ideal $\mathfrak{p} \neq (\sqrt{17})$ divides both, then $\mathfrak{p}$ divides a and c. This contradicts the fact that $\gcd(a,c) = 1$. If $(\sqrt{17})$ divides both, then $(\sqrt{17})$ divides a^2 so (17) divides a^4. By equation (7.2), (17) divides b^2 which is a contradiction (since (17) would then divides all of (7.2)). Now

$$\frac{a^4-17c^4}{4} = \left(\frac{a^2+c^2\sqrt{17}}{2}\right)\left(\frac{a^2-c^2\sqrt{17}}{2}\right) = \frac{b^2}{2}$$

Since both $\frac{a^2 \pm c^2\sqrt{17}}{2}$ are algebraic integers, $\frac{b^2}{2}$ is a rational integer. Hence b is even, say $b = 2b_0$. So

$$\left(\frac{a^2+c^2\sqrt{17}}{2}\right)\left(\frac{a^2-c^2\sqrt{17}}{2}\right) = 2{b_0}^2.$$

The class number of K is 1 we thus have unique factorization. In the field K, 2 splits into

$$2 = \left(\frac{5+\sqrt{17}}{2}\right)\left(\frac{5-\sqrt{17}}{2}\right)$$

Since $\frac{a^2 \pm c^2\sqrt{17}}{2}$ are relatively prime and conjugate to each other, each is divisible by one of $\left(\frac{5 \pm \sqrt{17}}{2}\right)$. We can thus write

$$\left(\frac{a^2+c^2\sqrt{17}}{2}\right) = \left(\frac{5 \pm \sqrt{17}}{2}\right)\eta\mu^2$$

for some unit η. The left hand side and its norm are positive, as are $\left(\frac{5 \pm \sqrt{17}}{2}\right)$,

μ^2 and their norms $\left(N\left(\frac{5 \pm \sqrt{17}}{2}\right) = 2\right)$. So $\eta > 0$ thus $N(\eta) > 0$. A fundamental unit in K is $\varepsilon_0 = 4 + \sqrt{17}$. Every unit in K is thus plus or minus some power of the fundamental unit (*i.e.* $\eta = \pm(\varepsilon_0)^n$). If n odd $N((\varepsilon_0)^n) < 0$ since $N(\varepsilon_0) = -1$. So power even, thus η a square and can be absorbed in μ^2. Put $\eta = 1$, $\mu = \frac{u + v\sqrt{17}}{2} \in \mathcal{O}_K$. Now

$$\frac{a^2 + \sqrt{17}c^2}{2} = \left(\frac{5 \pm \sqrt{17}}{2}\right)\left(\frac{u + v\sqrt{17}}{2}\right)^2$$

$$= \left(5(u^2 \pm 34uv + 17v^2) + \sqrt{17}(10uv \pm u^2 \pm 17v^2)\right)/8.$$

Hence $4a^2 = 5(u^2 \pm 34uv + 17v^2)$. This is not possible over $\mathbb{Q}_{17}$ because $4a^2 \equiv 5u^2 (\mathrm{mod}\, 17) \Leftrightarrow (2a/u)^2 \equiv 5 (\mathrm{mod}\, 17)$ and $\left(\frac{5}{17}\right) = -1$.

□

7.4 Representation of Integers by Quadratic Forms

A question naturally arises: *If a quadratic form $f(x)$ with integer coefficients has a non–trivial zero in $\mathbb{Z}_p$ for all $p \leq \infty$, does $f(x)$ have a non–trivial zero in $\mathbb{Z}$?* In marked contrast to the question of solutions in rational numbers, the answer is NO. This point is articulated by J.W.S. Cassels, in the introduction to his survey article Diophantine equations with special reference to elliptic curves: *"The field $\mathbb{Q}$ of rational number is already less recalcitrant (because less basic?) than the ring $\mathbb{Z}$ of integers* [...]"

Consider the equation $x^2 - 34y^2 = -1$. The solution $(x,y) = (5/3, 1/3)$ is in $\mathbb{Z}_p$ for all $p \neq 3$. If $p = 3$, the equation has the solution $(3/5, 1/5)$ in $\mathbb{Z}_3$. Yet, $x^2 - 34y^2 = -1$ does not have a solution in $\mathbb{Z}$. To see this, look at $x^2 - 34y^2 = -1$ over the quadratic field $K = \mathbb{Q}(\sqrt{34})$. The fundamental unit in K is $\varepsilon_0 = 35 + 6\sqrt{34}$ where the norm of

ε_0 is 1. Therefore, -1 is not the norm of an algebraic integer (*i.e.* of a unit in $\mathcal{O}_K$). We thus have no nice equivalent to the Hasse-Minkowski Theorem for the representation of an integer by a quadratic form with integer coefficients, although many results in this area still rely heavily on the *Local-Global Principle.* A striking example of such a result due to Conway and Schneeberger (1993) is the following theorem [3]

Theorem 7.5 (The Fifteen Theorem)
If a positive-definite quadratic form having integer matrix represents every positive integer up to 15 then it represents every positive integer.

The criterion is indeed necessary since it is easily seen that $a^2 + 2b^2 + 5c^2 + 5d^2$ represents the integers 0 through 14, but it does not represent 15 because $a^2 + 2b^2 \equiv 0 (\mathrm{mod}\, 5) \Leftrightarrow \left(\frac{3}{5}\right) = 1$ which is false. The original proof of the Fifteen Theorem was never published, but the recent proof by Manjul Bhargava does rely on some Local-Global concepts. For more on this fascinating subject, refer to [12] and [3].

Chapter 8

Finite Extensions of $\mathbb{Q}_p$

Up to this point, Local Field meant the p-adic field $\mathbb{Q}_p$ or $\mathbb{R}$ and Global Field referred to the field of rational numbers $\mathbb{Q}$. However, these are the simplest occurrences of Local and Global Fields. In general a Local Field is a finite, algebraic extension of $\mathbb{R}$, $\mathbb{Q}_p$ or the field of formal power series over some finite field. A Global Field is a finite, algebraic extension of $\mathbb{Q}$ (*i.e.* an algebraic number field) or the field of algebraic functions in one variable over a finite field. We saw that the behaviour of a problem in $\mathbb{Q}$ can sometimes be deduced from it's behaviour in $\mathbb{Q}_p$ and $\mathbb{R}$. In this chapter, we lay the foundation necessary to generalize this idea to finite algebraic extensions of $\mathbb{Q}_p$.

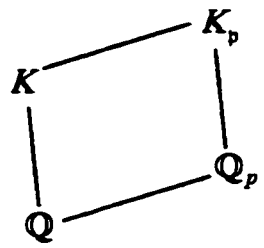
8.1 The p-adic Fields

Let L be a local field of degree n over $\mathbb{Q}_p$. It can be shown that there exists a unique absolute value $|\ |_L$ on L which extends $|\ |_p$ on $\mathbb{Q}_p$ given by [33]:

$$|x|_L = \left(|N_{L/\mathbb{Q}_p}(x)|_p\right)^{1/n} \qquad (x \in L)$$

Now let K be an arbitrary algebraic number field. A finite prime ideal $\mathfrak{p}$ induces a non-archimedean absolute value $|\ |_\mathfrak{p}$ on K which restricts to the usual p-adic absolute value if $\mathfrak{p}|p$. The completion of the algebraic number field K with respect to $|\ |_\mathfrak{p}$ is a

local field (proof see [15], pp.55) called the $\mathfrak{p}$-adic number field. This field is denoted $K_\mathfrak{p}$. Elements of $K_\mathfrak{p}$ are called $\mathfrak{p}$-adic numbers. Pictorially,



By the discussion above, the p-adic absolute value $|\ |_p$ of $\mathbb{Q}_p$ is extended to a unique absolute value $|\ |_\mathfrak{p}$ defined by:

$$|x|_\mathfrak{p} = \left(|N_{K_\mathfrak{p}/\mathbb{Q}_p}(x)|_p\right)^{1/n_\mathfrak{p}}$$

where $n_\mathfrak{p} = [K_\mathfrak{p} : \mathbb{Q}_p]$.

If σ is an embedding $\sigma : K \hookrightarrow \mathbb{C}$, it is called an infinite prime and it induces an archimedean absolute value on K (given by $|\alpha|_\sigma = |\sigma\alpha|$). An archimedean absolute value is an extension of the archimedean absolute value $|\ |_\infty$ on $\mathbb{Q}$. The corresponding completion $K_\mathfrak{p}$ is $\mathbb{R}$ or $\mathbb{C}$. Hilbert was the first to introduce the formal concept of infinite primes [13], pp.239. Let us look at an explicit example. Take $K = \mathbb{Q}(\sqrt{2})$. The Galois group is $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$ where $\sigma : \sqrt{2} \to -\sqrt{2}$. So $|1 + \sqrt{2}|_1 = 1 + \sqrt{2}$ and $|1 + \sqrt{2}|_\sigma = \sqrt{2} - 1$. The prime 7 splits in K into $(3 + \sqrt{2})(3 - \sqrt{2}) = \mathfrak{p}_7\mathfrak{p}_7{}'$. Calculating the various absolute values we find $|3 + \sqrt{2}|_{\mathfrak{p}_7} = 1/7$, $|3 - \sqrt{2}|_{\mathfrak{p}_7} = 1$, $|3 + \sqrt{2}|_{\mathfrak{p}_7{}'} = 1$, and $|3 - \sqrt{2}|_{\mathfrak{p}_7{}'} = 1/7$.

Local fields have many of the same properties as $\mathbb{Q}_p$. If $|\ |_\mathfrak{p}$ is a non-archimedean absolute value, the subset $\{x \in K_\mathfrak{p} : |x|_\mathfrak{p} \leq 1\}$ forms the ring of $\mathfrak{p}$-adic integers denoted $\mathcal{O}_\mathfrak{p}$ and the group of units is $\mathcal{O}_\mathfrak{p}^\times = \{x \in K_\mathfrak{p} : |x|_\mathfrak{p} = 1\}$. Techniques which involve proving theorems about the ground field K by exploring all its embeddings in its completions $K_\mathfrak{p}$ and $\mathbb{R}$ (or $\mathbb{C}$) are called Local methods.

8.2 Hasse-Minkowski for Algebraic Number Fields

Using Takagi's work on class field theory and Hilbert's ideas, Hasse fully solved Hilbert's eleventh problem by extending his *Local-Global Principle* to algebraic number fields in 1924. The problem of representability and equivalence of quadratic forms for an arbitrary number field was thus completely solved. Instead of looking for rational solutions in the usual sense of the word we may look for solutions in a general algebraic number field. The ring of integers of K (*i.e.* the ring of elements of K integral over $\mathbb{Z}$) will be denoted $\mathcal{O}_K$. The more general Hasse-Minkowski Theorem then reads as follows;

Theorem 8.1

Let $f(x_1,...,x_n)$ be a quadratic form with coefficients in some algebraic number field K. Suppose $f(x_1,...,x_n) = 0$ has a non-trivial solution in all $\mathfrak{p}$-adic fields $K_\mathfrak{p}$ for all finite prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ and in all the completions corresponding to the archimedean absolute values. Then $f = 0$ has a non-trivial solution in K.

We will see in Chapter 10 that the proof of Theorem 8.1 follows easily from a beautiful theorem of Hasse's known as the Norm Theorem. Most Local-Global results concerning the relationship between $\mathbb{Q}$ and the p-adic fields $\mathbb{Q}_p$ generalize to algebraic number fields and the corresponding local fields, like the Hasse-Minkowski Theorem. The proofs are often more sophisticated.

The objective of Local Class Field Theory is to describe all abelian extensions of Local Fields. Unlike $\mathbb{R}$, $\mathbb{Q}_p$ possesses many such extensions. The problem of classifying the abelian extensions of $\mathbb{Q}$ is known as the Kronecker-Weber Theorem. A famous theorem of Kronecker and Weber states that: *Every abelian extension of* $\mathbb{Q}$ *is contained in a cyclotomic extension.* This theorem can be proved from the corresponding theorem for the local fields $\mathbb{Q}_p$, [9] pp.151, although historically, the local result was proved using the global theorem.

Chapter 9

The Product Formula and Quadratic Reciprocity

Euler (1707-1783) was led to the discovery of the celebrated law of quadratic reciprocity in the years 1744-46 after examining many individual cases of the solutions of the congruences $x^2 \equiv p(\mathrm{mod}\, q)$ and $x^2 \equiv q(\mathrm{mod}\, p)$. Euler noticed that if p and q are both primes of the form $4k+3$, then only one of the congruences is solvable. On the other hand, if one or both p and q are of the form $4k+1$, then both or neither congruences are solvable. Legendre independently rediscovered this result in 1785. Using the Legendre symbol the quadratic reciprocity law then becomes the familiar

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

As Weil mentions in a letter to Simone Weil [32], the quadratic reciprocity is a startling result because it means that the prime numbers p for which m is a quadratic residue are precisely the ones that belong to a certain arithmetic progression modulo $4m$. For instance $1 = \left(\frac{5}{11}\right) = \left(\frac{5}{31}\right) = \left(\frac{5}{71}\right) = \ldots$ This is quite an astounding statement in light of the fact that the distribution of primes in arithmetic progression seems to be random. Legendre attempted to prove reciprocity, but his proof was flawed in six of the eight cases.

Gauss rediscovered quadratic reciprocity when he was just eighteen years of age. He declared it to be *"The Golden Theorem of Number Theory"*. He gave the first complete proof after one year of intense work in 1795. *"It tortured me for a whole year"* said Gauss *"and eluded my most strenuous efforts before finally I got the proof explained* [...]". A bitter animosity between Legendre and Gauss was sparked when Gauss exposed his proof in his 1801 text *Disquisitiones Arithmeticae* attributing the law to himself, making only a passing remark about Legendre's contribution. Gauss went back to the law of quadratic reciprocity numerous times during his illustrious career, proving it in eight drastically different ways. His ultimate goal was to find an approach which would generalize to higher powers. This quest led to the introduction of Cyclotomy and Gaussian integers by Gauss and eventually was the motivation behind the development of the Theory of Algebraic Numbers.

Gauss' proofs can be found in many Number Theory books. Our goal will be to prove the quadratic reciprocity in Local-Global fashion. This is accomplished by first proving Hilbert's Product Formula, for $a,b \in \mathbb{Q}$, $\prod_{p,\infty} (a,b)_{\mathbb{Q}_p} = 1$ and showing that it is equivalent to quadratic reciprocity. The source of all such product formulas is the p-adic product formula

Theorem 9.1

For any nonzero $x \in \mathbb{Q}$,

$$\prod_{p\leq\infty} |x|_p = 1$$

Proof Let $x \in \mathbf{Z}$. We can write $x = \pm \prod_{p\neq\infty} p^{v_p(x)}$. The sign of x is $\frac{x}{|x|_\infty}$. Thus $x = \frac{x}{|x|_\infty} \prod_{p\neq\infty} p^{v_p(x)}$. Consequently $\prod_{p\leq\infty} |x|_p = p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n} (p_1^{-v_1} p_2^{-v_2} \cdots p_n^{-v_n}) = 1$. The general result for a rational x follows.

□

Note that in Theorem 9.1, $|x|_p = 1$ for almost all prime p in $\mathbb{Q}$.

9.1 Euler's Criterion

Proving Hilbert's Product Formula will require us to become familiar with some preliminary notions.

Theorem 9.2 (Euler's Criterion)

A p-adic unit $u \in \mathbf{Z}_p^*$ is a square if and only if $u^{(p-1)/2} \equiv 1 (\mathrm{mod} p)$

Proof [$\Leftarrow$] Let p be an odd prime. There exists a $\xi \in \mathbf{Z}$ such that $\xi^{p-1} \equiv 1(\mathrm{mod}p)$, $\xi^{(p-1)/2} \equiv -1(\mathrm{mod}p)$ and $\{0, \xi, \xi^2, ..., \xi^{p-1}\}$ is a complete residue system. For some natural number k where $0 \leq k \leq p-1$ we may write $u \equiv \xi^k (\mathrm{mod}p)$ which is true if and only if $u^{(p-1)/2} \equiv (-1)^k (\mathrm{mod}p)$. Suppose $k = 2m$ (*i.e.* $u^{(p-1)/2} \equiv 1(\mathrm{mod}p)$) and let $f(x) = x^2 - u$. Thus $f(\xi^m) = \xi^k - u \equiv 0(\mathrm{mod}p)$ and the derivative $f'(\xi^m) = 2\xi^m \not\equiv 0(\mathrm{mod}p)$ since $p \neq 2$. We can apply Hensel's Lemma to find $z \in \mathbf{Z}_p$ such that $f(z) = z^2 - u = 0$. Thus u is a square.

[$\Leftarrow$] Suppose $u = z^2$ for some $z \in \mathbf{Z}_p$. We have $z \equiv \xi^m (\mathrm{mod}p)$ for some m $\Leftrightarrow u \equiv \xi^{2m} (\mathrm{mod}p) \Leftrightarrow u^{(p-1)/2} \equiv \xi^{m(p-1)} \equiv 1(\mathrm{mod}p)$

□

Recall that in Chapter 1 we saw that if p is an odd prime and u a p-adic unit, then it is necessary and sufficient for u to be a square that $\left(\frac{u}{p}\right) = 1$. In conjunction with Euler's criterion, this result becomes

Lemma 9.1

Let p be an odd prime and let a be an integer such that $p \nmid a$. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\mathrm{mod}p)$$

Euler's Criterion is extremely useful in proving various properties of the Legendre symbol. The following are easy consequences of Euler's criterion.

Corollary 9.1 Let p be an odd prime and let a and b be integers such that $p \nmid a$, $p \nmid b$. Then

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

Proof $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv (a)^{(p-1)/2}(b)^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\mathrm{mod} p)$

□

The first complementary Law of quadratic reciprocity, which is a consequence of Euler's Criterion, was a result already known by Pierre de Fermat. Simply stated the law says that the only prime divisors of $x^2 + 1$ are 2 and primes of the form $4k + 1$. The second law states that 2 is a square in $\mathbb{F}_p$ if and only if $p = 8k \pm 1$.

Corollary 9.2 (Complementary Law 1) Let p be an odd prime, then

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 (\mathrm{mod} 4) \\ -1 & \text{if } p \equiv 3 (\mathrm{mod} 4) \end{cases}$$

Proof Applying Euler's Criterion to -1, $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow (-1)^{(p-1)/2} \equiv 1 (\mathrm{mod} p) \Leftrightarrow 0 \equiv (p-1)/2 (\mathrm{mod} 2) \Leftrightarrow p \equiv 1 (\mathrm{mod} 4)$. Note that clearly, if $p = 2$ then $\left(\frac{-1}{p}\right) = 1$

□

Corollary 9.3 (Complementary Law 2) Let p be an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 (\mathrm{mod} 8) \\ -1 & \text{if } p \equiv \pm 3 (\mathrm{mod} 8) \end{cases}$$

Proof From [24], pp.7. First observe that if 2 has x as a square root x in an algebraic closure of $\mathbb{F}_p$ then $2 \equiv x^2 (\mathrm{mod} p) \Leftrightarrow \left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv x^{p-1} (\mathrm{mod} p)$. Let ζ be a primitive 8^{th} root of unity in an algebraic closure of $\mathbb{F}_p$. We have that $\zeta^4 = -1$ and

$\zeta^2 + \zeta^{-2} = 0$. If we let $x = \zeta + \zeta^{-1}$ then $x^2 = 2$ and

$$x^p = \zeta^p + \zeta^{-p}$$

If $p \equiv \pm 1 (\mathrm{mod}\, 8)$ then $x^p = x \Leftrightarrow x^{p-1} = 1 = \left(\frac{2}{p}\right)$. If $p = \pm 5 (\mathrm{mod}\, 8)$ then $x^p = -(\zeta + \zeta^{-1}) = -x \Rightarrow x^{p-1} = -1 = \left(\frac{2}{p}\right)$

9.2 Proof of the Product Formula

We are now in a position to prove Hilbert's product formula.

Theorem 9.3 (The Product Formula)
Let $a, b \in \mathbb{Q}$. Then

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

Proof The following proof is from [24] pp.23.

The properties of the Hilbert symbol allows us to reduce the proof of the general product formula to three special cases $a = b = -1$, $a = -1, b = l$ (l a prime) and $a = l$, $b = l'$ (l and l' distinct primes). The following Hilbert symbols have been calculated using Theorem 4.1.

Case 1. $a = b = -1$. For $p \neq 2, \infty$, $v_p(-1) = 0$ so we have that $(-1,-1)_{\mathbb{Q}_p} = 1$. One has $(-1,-1)_{\mathbb{Q}_2} = -1$ and, since a and b are both negative, $(a,b)_{\mathbb{R}} = -1$. Hence $\prod_{p,\infty} (-1,-1)_{\mathbb{Q}_p} = 1$.

Case 2 $a = -1$, $b = l$ a prime number.
If $l = 2$ and $p \neq 2, \infty$ then $v_p(-1) = v_p(2) = 0$ so $(-1,2)_{\mathbb{Q}_p} = 1$. Moreover, since

$z^2 + x^2 = 2y^2$ has the non-trivial solution $(1,1,1) = (x,y,z)$ we get $(-1,2)_{\mathbb{R}} = 1 = (-1,2)_{\mathbb{Q}_2} = 1$. Hence $\prod_{p,\infty} (-1,2)_{\mathbb{Q}_p} = 1$.

If $l \neq 2$ and $p = 2$, $v_2(-1) = v_2(l) = 0$, so $(-1,l)_{\mathbb{Q}_2} = (-1)^{(l-1)/2}$. If $l \neq 2$, $p \neq 2$ where $p \neq l$, we have $(-1,l)_{\mathbb{Q}_p} = 1$. Now if $p = l \neq 2$, then $v_2(-1) = 0$ and $v_l(l) = 1$, so $(-1,l)_{\mathbb{Q}_l} = \left(\frac{-1}{l}\right) = (-1)^{(l-1)/2}$. The product $\prod_{p,\infty} (-1,l)_{\mathbb{Q}_p}$ is thus equal to 1.

Case 3 $a = l$, $b = l'$. If $l = l'$, by properties of the Hilbert symbol we find that $(l,l) = (l,-l^2) = (l,-1)(l,l)(l,l)$. Hence $(l,l)_{\mathbb{Q}_p} = (-1,l)_{\mathbb{Q}_p}$ for all p. This was dealt with in Case 2. So assume that $l \neq l$. If $l' = 2$ and $p \neq 2, l$ then $v_p(l) = v_p(l') = 0$ thus $(l,2)_{\mathbb{Q}_p} = 1$. If $l' = 2$ and $p = 2$, $(l,2)_{\mathbb{Q}_2} = (-1)^{(l^2-1)/8}$. If $l' = 2$ and $p = l \neq 2$, $v_l(l) = 1$ and $v_l(2) = 0$ so $(l,2)_{\mathbb{Q}_l} = \left(\frac{2}{l}\right) = (-1)^{(l^2-1)/8}$. If $l \neq l'$, $l, l'p \neq 2$, we get $(l,l')_{\mathbb{Q}_p} = 1$. For $p = 2$ we obtain $(l,l')_{\mathbb{Q}_2} = (-1)^{(l-1)(l'-1)/4}$ since $v_2(l) = v_2(l') = 0$. Finally, since $v_l(l') = 1 = v_{l'}(l)$ this results in $(l,l')_{\mathbb{Q}_l} = \left(\frac{l'}{l}\right)$ and $(l,l')_{\mathbb{Q}_{l'}} = \left(\frac{l}{l'}\right)$. We thus obtain $\prod_{p,\infty} (l,l')_{\mathbb{Q}_p} = (-1)^{(l^2-1)/4}\left(\frac{l'}{l}\right)\left(\frac{l}{l'}\right) = 1$. The general result follows.

□

9.3 Quadratic Reciprocity

A direct consequence of the product formula is that for any quadratic form f over $\mathbb{Q}$, the number of primes p, including ∞, for which f has no zero over $\mathbb{Q}_p$ is always even. As previously mentioned, the product formula is equivalent to the classic law of quadratic reciprocity. From the proof of the product formula, we see that in general, if p,q,l are distinct primes not equal to 2, we have $(p,q)_{\mathbb{Q}_l} = 1$. If $l = 2$, then $(p,q)_{\mathbb{Q}_2} = (-1)^{(p-1)(q-1)/4}$ and $(p,q)_{\mathbb{Q}_p} = \left(\frac{q}{p}\right)$. The product formula then becomes

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4} = 1.$$

The product formula $\prod_{p,\infty} (a,b)_{\mathbb{Q}_p} = 1$ is quite useful since if we know all but one value of the Hilbert symbol we can easily determine the missing value. In particular

Lemma 9.2

If a quadratic form with rational coefficients f in three variables represents zero in all fields $\mathbb{Q}_p$ for all $p \leq \infty$ except possibly for $\mathbb{Q}_q$ for some prime q, then f also represents zero in $\mathbb{Q}_q$.

For instance Borevich and Shafarevich prove the Hasse-Minkowski Theorem in their text [6] noting that one never needs to verify the solvability at $p = 2$ in order to deduce global solvability.

9.4 Hasse's Product Formula

There is an analogue of the Product Formula for algebraic number fields. Let K be a finite extension of $\mathbb{Q}$ and let a be an element of $K^\times$. Similarly to Theorem 9.1 we find that

$$\prod_{\mathfrak{p}} |a|_{\mathfrak{p}} = 1$$

where $\mathfrak{p}$ goes through all finite and infinite primes of K. Hilbert had defined the norm residue symbol for quadratic and Kummer extensions of $\mathbb{Q}$, but had verified the product formula only for special cases ([13], pp.262-265). Hasse proved Hilbert's product formula and then generalized the norm residue symbol to abelian extensions. To accomplish this, Hasse worked in $\mathfrak{p}$-adic fields using the adapted Hilbert norm residue. Given a field K, a prime ideal $\mathfrak{p}$ of K and $\nu, \mu \in \mathcal{O}_K$ such that μ is not a square in $\mathcal{O}_K$ we can define the quadratic Hilbert norm residue

$$\left(\frac{\nu,\mu}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } \nu = x^2 - \mu y^2 \text{ is solvable in } K_{\mathfrak{p}} \\ -1 & \text{otherwise} \end{cases}$$

To be consistent with our prior notation, we will denote this norm residue as $(\nu,u)_{K_{\mathfrak{p}}}$. There is a corresponding norm residue symbol for the infinite primes $\mathfrak{p}_\infty$. If K has r real embeddings $\sigma_1 ... \sigma_r$, then for each real embedding we associate an infinite prime $\mathfrak{p}_{\infty_i}$ and

$$(\nu,\mu)_{\mathfrak{p}_{\infty_i}} = \begin{cases} 1 & \text{if } \sigma_i(\nu) = x^2 - \sigma_i(\mu) y^2 \text{ is solvable in } \mathbb{R} \\ -1 & \text{otherwise} \end{cases}$$

As in the case $K = \mathbb{Q}$, we see that $(\nu,u)_{K_{\mathfrak{p}}} = 1$ if ν is the norm of an element in $K_{\mathfrak{p}}(\sqrt{u})$. Hasse then proved the general product formula

$$\prod_{\mathfrak{p},\mathfrak{p}_\infty} (\nu,u)_{K_{\mathfrak{p}}} = 1$$

taken over all primes $\mathfrak{p}$ of the field K. To work comfortably in these fields, Hasse had to prove theorems about $\mathfrak{p}$-adic fields which were analogues of Takagi's results in class field theory. These results paved the way for Local Class Field Theory. Hilbert had managed to prove the above product formula only for a few special cases, such as when K is a field with class number 1 or 2 and with less than two classes or when K is an imaginary extension with an odd class number ([13], pp.238-241). In these cases, Hilbert constructed an extension L of K he called a class field. He then proved various conjectures concerning these special fields.

Chapter 10

The Hasse Norm Theorem

10.1 The Hilbert Norm Theorem

In part III of his report *Zahlbericht* on algebraic number theory to the *Deutsche Mathematiker Vereinigung* (German Mathematical Society), Hilbert reformulated a theorem of Gauss ([13] pp.225)

Theorem 10.1 (Hilbert Norm Theorem)
Let b be a square free integer and a a nonzero integer. If $(a,b)_{\mathbb{Q}_p} = 1$ for all primes $p \leq \infty$ then $a = N(x)$ is solvable in the field $\mathbb{Q}(\sqrt{b})$. That is to say a is a global norm from $\mathbb{Q}(\sqrt{b})$ if and only if it is a local norm everywhere.

We saw in Chapter 4 that $z^2 - ax^2 - by^2 = 0$ has a solution in $\mathbb{Q}_p$ for all $p \leq \infty$ if and only if a is the norm of an element in $\mathbb{Q}_p(\sqrt{b})$. Since a is a norm in $\mathbb{Q}(\sqrt{b})$ if and only if $z^2 - ax^2 - by^2 = 0$ has a solution in $\mathbb{Q}$, we see that the Hilbert Norm theorem is completely equivalent to the Hasse-Minkowski Theorem for rational quadratic forms in three variables.

10.2 The Hasse Norm Theorem for Cyclic Extensions

Let K be a number field. In 1924 Hasse proved that v is the norm of an element in $K(\sqrt{u})$ if and only if v is a local norm everywhere. Hasse later (1930) extended the Norm Theorem from quadratic extensions of K to all cyclic extensions of K. He thus obtained the celebrated Hasse Norm Theorem. The following is the general Norm Theorem that Hilbert had proved only for special cases.

Theorem 10.2 (Hasse Norm Theorem)
Let L/K be a cyclic extension of number fields. An element a in $K^{\times}$ is the norm of an element in $L^{\times}$ (*i.e.* $a \in N(L^{\times})$) if and only if a is the norm of an element in the corresponding local extensions $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ for all prime divisors $\mathfrak{p}$ in K, including infinite primes (i.e. $a \in N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}^{\times})\forall \mathfrak{p}$).

Proof. See [19], Theorem 4.5, p:156. Note: Analogues of the product formula seen in Chapter 8 play a crucial role in the proof of the Hasse Norm Theorem.

In Theorem 10.2, by cyclic extension we mean a Galois extension with cyclic Galois group. In the context of rationals the Hasse Norm Theorem reads as follows: *Let $K/\mathbb{Q}$ be a cyclic extension. A nonzero rational number a is a norm from K if and only if it is a local norm at every prime of K including infinite primes.* In particular, for $L = \mathbb{Q}(\sqrt{b})$ a degree two cyclic extension of $\mathbb{Q}$, the Hasse Norm Theorem reduces to the Hilbert Norm Theorem. It has been observed that one can leave out one particular prime, in the application of the Hasse Norm Theorem (Ref. [19]).

Theorem 10.3

If L/K is a cyclic extension of global fields and $a \in K^{\times}$ is a local norm at all primes of K with the possible exception of one particular prime, then a is a local norm at that prime as well.

Proof. See [19] pp.190. Note: The proof follows from the product formula for the local Artin maps (p:189 of [19]).

10.3 Abelian Extensions

Hasse had at first conjectured that his Norm Theorem for cyclic extensions would hold for abelian extensions. Hasse found the first counterexample to this conjecture himself. The biquadratic field $K = \mathbb{Q}(\sqrt{-39}, \sqrt{-3})$ has the property that $(3,K)_{\mathbb{Q}_p} = 1$ for all $p \in \mathbb{Q}$, but 3 is not a norm in K. Another well-known counterexample is $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$. The extension L is Galois over $\mathbb{Q}$ with non-cyclic Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{1, \delta, \tau, \delta\tau\} = G$, where

$$\delta : \sqrt{13} \to -\sqrt{13} \quad \text{and} \quad \tau : \sqrt{17} \to -\sqrt{17}$$

The norm of an element of α is

$$N_{L/\mathbb{Q}}(\alpha) = \prod_{\sigma} \sigma(\alpha)$$

where $\sigma \in G$. Hence the norm of an element $\alpha = a + b\sqrt{13} + c\sqrt{17} + d\sqrt{13}\sqrt{17}$ from $\mathbb{Q}$ to L is $N_{L/\mathbb{Q}}(\alpha) = \alpha\delta(\alpha)\tau(\alpha)\delta\tau(\alpha)$. It can be shown that -1 is not a norm of any $\alpha \in L$. We will now show that -1 is a local norm everywhere, *i.e.* in each completions $L_{\mathfrak{p}}$. If $p = \infty$, $L_\infty = \mathbb{R}$ and -1 is a norm in $\mathbb{R}$. If $p \neq 13, 17$. The extension L_p is an unramified extension of $\mathbb{Q}_p$ where $[L_p : \mathbb{Q}_p] \leq 2$. By the following result of local class field theory

Theorem 10.4

Let $L_\mathfrak{p}$ be an unramified extension of $\mathbb{Q}_p$ of degree f over $\mathbb{Q}_p$. Let $\beta = p^m u \in \mathbb{Q}_p^\times$, with $u \in U_p, m \in Z$. Then $\beta \in N_{L_\mathfrak{p}/\mathbb{Q}_p}(L_\mathfrak{p}^\times)$ if and only if $f \mid m$. In particular, every unit of $\mathbb{Q}_p$ is the norm of a unit of $L_\mathfrak{p}$.

The number -1 is a norm in L_p for all $p \neq 13, 17$ since -1 is a unit of $\mathbb{Q}_p$, $p \neq 13, 17$. If $p = 13$, $L_{13} = \mathbb{Q}_{13}(\sqrt{13}, \sqrt{17}) = \mathbb{Q}_{13}(\sqrt{13})$ since $17 \equiv 4 (\mathrm{mod}\, 13)$ *i.e.* $\sqrt{17} \in \mathbb{Q}_{13}$ and -1 is the norm of $\alpha = \dfrac{3 - \sqrt{13}}{2} \in L_{13}$. Similarly, $13^8 \equiv (-4)^8 \equiv 1 (\mathrm{mod}\, 17)$ thus 13 is a square in $\mathbb{Q}_{17}$ thus $\mathbb{Q}_{17}(\sqrt{13}, \sqrt{17}) = \mathbb{Q}_{17}(\sqrt{17})$ and -1 is the norm of $4 + \sqrt{17} \in \mathbb{Q}_{17}(\sqrt{17})$. We then see that all local conditions are satisfied.

10.4 Some Applications

Using the Hasse Norm Theorem for cubic cyclic extensions of an algebraic number field K, Selmer proved the following theorem in his 1953 article *Sufficient congruence conditions for the existence of rational points on certain cubic surfaces*

Theorem 10.5

Given $0 \neq a, b, c, d \in \mathbf{Z}$ cube-free integers such that $ad = bc$ then $ax^3 + by^3 + cz^3 + dw^3 = 0$ has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{Q}_p$ for all $p \leq \infty$

Proof (Idea of Selmer's proof). Selmer considers the cubic equation $x^3 + my^3 = n(u^3 + mv^3)$, with integer, cubefree m and n (but not necessarily $(m, n) = 1$). Let K be an algebraic number field. Selmer boils down the question, by an argument about the ideals of the field, to an application of Hasse's Norm Theorem where $K(\rho)$ is his ground field (ρ a complex cube root of unity) and $\Omega = K(\rho)(m^{1/3})$ is the cyclic extension over $K(\rho)$. For more detail, see [25].

Now recall the statement of the generalized Hasse-Minkowski Theorem [13] pp.263,

Theorem

Let $f(x_1,...,x_n)$ be a quadratic form with coefficients in some algebraic number field K. Suppose $f(x_1,...,x_n) = 0$ has a non-trivial solution in all $\mathfrak{p}$-adic fields $K_\mathfrak{p}$ for all finite prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ and in all the completions corresponding to the archimedean absolute values. Then $f = 0$ has a non-trivial solution in K.

Proof $(n = 2,3)$ The two variable case $n = 2$ is a direct consequence of the theorem: $a \in K$ is a square in K which is true if and only if a is a square in $K_\mathfrak{p}$ for all $\mathfrak{p}$ and in each real embeddings; the proof of which is similar to that of Theorem 1.1. The 3 variable case $n = 3$ is a particular case of the Hasse Norm Theorem since $f(x) = ax^2 + by^2 + cz^2 = 0$ has a non-trivial solution if and only if $-ab$ is a norm of an element of $K(\sqrt{-bc})$. Moreover, $f(x) = 0$ has non-trivial solutions in all $K_\mathfrak{p}$ and in $\mathbb{R}$ implies that $-ab$ is a local norm of an element in $K_\mathfrak{p}(\sqrt{-bc})$ with respect to $K_\mathfrak{p}$. The general case is obtained in the same manner as the previous case for $\mathbb{Q}$ (see the proof of Theorem 5.4).

□

There is a finite set of primes which must be taken into consideration when applying the Hasse Norm Theorem. Using the Hasse Norm Theorem, Voncenzo Acciaro constructed an algorithm in order to answer the following question: Let $L = \mathbb{Q}(\alpha)$ be a cyclic extension of the rationals of prime degree q and let $a \in \mathbb{Q}^\times$. Does the equation

$$N_{L/\mathbb{Q}}(\lambda) = a$$

admit any solution in L? (*i.e.* Is a the norm of some element in L. It is worth noting that we are not asking how to find such a λ, but only whether a solution exists. See Voncenzo Acciaro's Doctoral thesis for a detailed account see [1] Chapter 4.) Although the Norm Theorem gives a satisfactory criterion for establishing

whether or not a given element of K is the norm of an element from the cyclic extension L of K, it does not help in identifying what integers of K are norms of integers of L. In particular, there is no systematic way to determine which quadratic extensions have a unit of norm -1. Refer to the discussion about the representation of integers by quadratic forms in Section 7.4.

Chapter 11

Measuring the Failure

Even when the Hasse Principle does not hold, there sometimes remains a close interaction between the local and the global. We have already seen that the Hasse Principle fails for

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

It has been conjectured that although the Hasse Principle fails for elliptic curves, it does not fail that badly, that is the measure of the obstruction to the Hasse Principle is finite. Since studying the extent of the obstruction to the Hasse Principle is an active area of research in Number Theory, this chapter aims to give a brief glimpse at the rich theory involved. Hasse's principle may be expressed cohomologically. This formulation, is essential in measuring the failure of the Local-Global Principles. We thus begin by getting reacquainted with some definitions and theory from the cohomology of groups and Galois cohomology. The content of this chapter relies heavily on the references [10], [26] and some useful notes on the subject written up by David S. Dummit.

11.1 First Cohomology Group

Let G be a finite group and let A be a G-module written additively (*i.e.* A is an abelian group on which G acts on the left). The action is written $\sigma(a)$ where $\sigma \in G$ and $a \in A$. The group G acts on itself by $\sigma(\tau) = \sigma\tau\sigma^{-1}$ where $\sigma, \tau \in G$. A 1-*cocycle* is a map

$$f: G \to A$$

$$\sigma \mapsto a_\sigma$$

which satisfies the cocycle identity

$$f: \sigma\tau \to a_{\sigma\tau} = a_\sigma + \sigma a_\tau$$

for all $\sigma, \tau \in G$. If f and g are 1-cocycles then $f+g$ is also a 1-cocycle where $(f+g)(a) = f(a) + g(a)$. The 1-cocycles thus form a group denoted $Z^1(G,A)$. The group G acts trivially on A if and only if $\sigma(a) = a$ for all $\sigma \in G$ and all $a \in A$. If $f \in Z^1(G,A)$ and G acts trivially on A, then $a_{\sigma\tau} = a_\sigma + \sigma a_\tau = a_\sigma + a_\tau$ which is true if and only if $f \in \mathrm{Hom}(G,A)$. The map f is called a 1-*coboundary* if and only if there exists an element $b \in A$ such that

$$f: \sigma \to a_\sigma = \sigma b - b$$

for all $\sigma \in G$. A coboundary is a cocycle because

$$\begin{aligned} a_{\sigma\tau} &= \sigma\tau(b) - b \\ &= \sigma\tau(b) - \sigma(b) + \sigma(b) - b \\ &= \sigma(\tau(b) - b) + \sigma(b) - b \\ &= \sigma a_\tau + a_\sigma \end{aligned}$$

The coboundaries in fact form a subgroup of $Z^1(G,A)$ since the sum of two coboundaries is again a coboundary. The group of coboundaries is denoted $B^1(G,A)$. Note that if G acts trivially on A then $B^1(G,A) = \{0\}$. The quotient group $Z^1(G,A)/B^1(G,A)$ is called the first cohomology group and is denoted by $H^1(G,A)$. If G acts trivially on A

$$H^1(G,A) = \mathrm{Hom}(G,A)$$

The cohomology group $H^0(G,A)$ is the set of elements of A fixed by G, $\{a \in A \mid \sigma a = a \; \forall \sigma \in G\}$, denoted A^G. There are higher order cohomology groups $H^n(G,A)$, but we will not need them. If G is a topological group and A is a topological A-module (*i.e.* A is a topological group and G acts continuously on A) then the continuous cohomology is defined as above except that the cocycles are continuous functions (as are the coboundaries).

11.2 Hasse Principle

Given an elliptic curve E defined over $\mathbb{Q}$, we can look at E over $\overline{\mathbb{Q}}$, over which it acquires points. Write

$$G = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$$

and let

$$G_p = Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$$

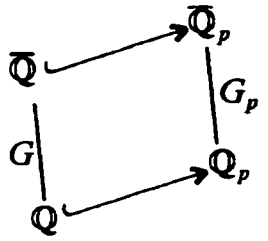
be the decomposition group of the prime p. We can view G_p as a subgroup of G. The embedding of fields

$$\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$$

induces the embedding of groups

$$G_p \hookrightarrow G$$

The diagram looks like



Let $E(\mathbb{Q})$ be the group of rational points of E. The elliptic curve E will be identified with its group of algebraic points which will be denoted by

$$E = E(\overline{\mathbb{Q}})$$

By restricting all cocycles in $Z^1(G,E)$ to G_p we get a canonical group homomorphism

$$H^1(G,E) \to H^1(G_p,E)$$

called a *localization*. If P is a point on the curve E it gives rise to a coboundary $\sigma \to \sigma P - P \in B^1(G,E) \subset B^1(G_p,E)$. The map

$$E(\overline{\mathbb{Q}}) \hookrightarrow E(\overline{\mathbb{Q}}_p)$$

induces the sequence

$$H^1(G,E) \to H^1(G_p,E) \xrightarrow{j_p} H^1(G_p,E(\overline{\mathbb{Q}}_p))$$

where j_p is the localization map. If a cocycle f is a coboundary we say f is trivial (in the trivial class). We would like to answer the question: If a cocycle f when restricted to G_p is an element of $B^1(G_p,E)$ for all p, is f an element of $B^1(G,E)$? In other words, if f is locally trivial for all p (E has a local point) is f globally trivial (E has a global point).

11.3 Principal Homogeneous Spaces

Now the elliptic curves over $\mathbb{Q}$ which become isomorphic to E over $\overline{\mathbb{Q}}$ are called twists of E. To each element of $H^1(G,E)$, we can associate a certain twist of E called a *Principal Homogeneous Space*. The concept of Principal Homogeneous Spaces was introduced by Weil [10]. The following two definitions are taken from [26].

Definition 11.1

Let $E/\mathbb{Q}$ be an elliptic curve. A principal homogeneous space for $E/\mathbb{Q}$ consists of a pair (C,μ), where $C/\mathbb{Q}$ is a smooth curve and a morphism

$$\mu : C \times E \to C$$

defined over $\mathbb{Q}$ by $\mu(p_0,P) = p_0 + P$ with the following properties:

i) $p_0 + O = p_0$ for all $p_0 \in C$.

ii) $(p_0 + P) + Q = p_0 + (P + Q)$ for all $p_0 \in C$, $P,Q \in E$.

iii) For all $p_0,q \in C$ there is a unique $P \in E$ satisfying $p_0 + P = q$.

Definition 11.2

Two homogeneous spaces C and $\mathcal{D}$ for $E/\mathbb{Q}$ are equivalent if there is an isomorphism θ : $C \to \mathcal{D}$ which preserves the action of E on C *i.e.* such that for all $p_0 \in C$ and $P \in E$ we have $\theta(p_0 + P) = \theta(p_0) + P$.

Note that E is a principal homogeneous space for E and that any other principal homogeneous space is in the same class as E, that is in the trivial class, if and only if it has a point in $\mathbb{Q}$.

Theorem 11.1

Let $E/\mathbb{Q}$ be an elliptic curve. There is a natural bijection

$$H^1(G,E) \leftrightarrow \left\{ \begin{array}{c} \text{Set of equivalence classes of} \\ \text{Principal Homogeneous Spaces} \\ \text{for } E/\overline{\mathbb{Q}} \text{ which have rational points in } \overline{\mathbb{Q}} \end{array} \right\}$$

defined as follows:

Let $C/\mathbb{Q}$ be a homogeneous space and choose a point $p_0 \in C$. Then

$$\{\sigma \to \sigma p_0 - p_0\} \to \{C/\mathbb{Q}\}$$

where $\{\ \}$ indicates an equivalence class and $\sigma p_0 - p_0$ means (iii) in definition 11.1. For a proof see [26], pp.291.

11.4 The Tate-Shafarevich Group

The group $H^1(G,E)$ is called the Weil-Chatelet group which we will denote WC. The trivial class of WC corresponds to the class of Principal Homogeneous Spaces having a rational point. So the problem of checking the triviality of the Weil-Chatelet group is equivalent to answering the Diophantine equation of whether a given curve has a rational point. We have the exact sequence

$$0 \to E(\mathbb{Q})/mE(\mathbb{Q}) \to H^1(G,E_m) \to [H^1(G,E)]_m \to 0$$

where E_m is the group of elements of $E(\overline{\mathbb{Q}})$ of order exactly m and $[...]_m$ denotes the subgroup of elements of $E(\overline{\mathbb{Q}})$ of order dividing m. The principal homogeneous spaces come into the computation of the weak Mordell-Weil group $E(\mathbb{Q})/mE(\mathbb{Q})$. This problem

may be reduced to determining whether each associated homogeneous space has a rational point. One can either explicitly find such a point or show that there is some local completion of $\mathbb{Q}$ for which it has no point. The difficulty is that there are homogeneous spaces that have points locally everywhere, yet have no rational point, that is the Hasse Principle fails. So we are interested in the elements of $H^1(G,[E]_m) = S_m$, the m-Selmer group, which are images of $E(\mathbb{Q})/mE(\mathbb{Q})$. Since the sequence is exact, these are precisely the elements of the kernel of the map

$$S_m = H^1(G,[E]_m) \to H^1(G,E) = WC$$

Being in the kernel of the latter map means that there is a point on C defined over $\mathbb{Q}$. Let the Russian letter Ш (sha) denote the elements of WC for which there is a point on C everywhere locally (elements of WC for which f restricted to G_p is an element of $B^1(G_p,E)$ for all p, *i.e.* having a $\mathbb{Q}_p$ point for all p). These elements form a group called the *Tate-Shafarevich Group.* It counts the number of equivalence classes of homogeneous spaces of C which have points in all local fields. The group Ш is the intersection of the kernels of all localization maps j_p. We get the exact sequence

$$0 \to E(\mathbb{Q})/mE(\mathbb{Q}) \to S_m \to [Ш]_m \to 0$$

The Tate-Shafarevich group then measures the obstruction to the Local-Global Principle for the elliptic curve E, that is, it measures the gap between rational solvability and everywhere local solvability. It was conjectured in the 60's that the Tate-Shafarevich group is finite. The conjecture remains unproved. Establishing the finiteness of the Tate-Shafarevich group is tantamount to proving that the Hasse Principle holds up to a finite obstruction for curves of genus 1. The problem is that there are no algorithms for computing Ш for a curve from the initial data. Rubin with help of some ideas by Francsico Thaine gave the first concrete examples of elliptic curves over number fields with a Tate-Shafarevich group proved to be finite [22]. It is now known that if $E(\mathbb{Q})$ is finite then $|Ш| < \infty$. For more on the conjectured finiteness theorems concerning Tate-Shafarevich look at Ju. I. Manin, Cyclotomic fields and modular curves, Russian Mathematical Surveys 26 (1971), 7-78.

Bibliography

[1] Vincenzo Acciaro, *Local global methods in number theory*, thesis (Ph.D.), Carleton University, 1995, Ottawa: National Library of Canada, 2 microfiches.

[2] J. Ax and S. Kochen. *Diophantine problems over local fields* I. Amer. J. Math., **87** (1965), 605-630

[3] M. Bhargava, *On the Conway-Schneeberger Fifteen Theorem*, Contemporary Mathematics, **272** (2000), 26-37.

[4] Jean-Paul Bézivin and Philippe Robba, *A new p-adic method for proving irrationality and transcendence results*, Ann. Math., II. Ser. **129** (1989), 151-160.

[5] B.J. Birch, *Homogeneous forms of odd degree in a large number of variables*, Mathematika, **4**, 1957, 102-105.

[6] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[7] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, Jour. London Math. Soc. **41** (1966), 193-291.

[8] J.W.S. Cassels, *Rational Quadratic Forms*, Academic Press, New York, 1978.

[9] J.W.S. Cassels, *Local Fields*, London Mathematical Society Student Texts, Vol.3 (Cambridge University Press), 1986.

[10] J.W.S. Cassels, *Lectures on Elliptic Curves*, London Mathematical Society, Student Texts 24, Cambridge University Press, 1991.

[11] J.W.S. Cassels and A. Frölich, *Algebraic Number Theory*, Academic Press, London and New York, 1967.

[12] J.H. Conway, *Universal Quadratic Forms and the Fifteen Theorem*, Contemporary Mathematics, **272** (2000), 23-26.

[13] J. Dieudonné, *Abrégé d'histoire des mathématiques* I, Hermann, Paris, 1978.

[14] Günter Frei, *How Hasse was led to the Theory of Quadratic Forms, the Local-Global Principle, the Theory of the Norm Residue Symbol, the Reciprocity Laws, and to Class Field Theory*, Article for the Proceedings of the Class Field Theory Conference in Tokyo.

[15] Larry J. Goldstein, *Analytic Number Theory*, Prentice-Hall, New Jersey, 1971.

[16] Fernando Q. Gouvêa, *p-adic numbers; An Introduction*. Springer-Verlag, second edition, 1997.

[17] Helmut Hasse, *Uber die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 129-148.

[18] Helmut Hasse, *Uber die Aquivalenz quadratischer Formen im Körper der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 205-224.

[19] G.J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1975.

[20] T.Y. Lam, *The Algebraic Theory of Quadratic Forms*, W.A. Benjamin Inc., Massachusetts, 1978.

[21] Heinrich Wolfgang Leopoldt and Peter Roquette, *Mathematische Abhandlungen*, 3 vols., Berlin, New York, Walter de Gruyter, 1975.

[22] Barry Mazur, *On the Passage from local to global in number theory*, Bull. Amer. Math. Soc. (N.S.), **29** (1993), no.1, 14–50.

[23] L.J. Mordell, *Diophantine Equations*, Academic Press, London and New York, 1969.

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

[25] Ernst S. Selmer, *Sufficient congruence conditions for the existence of rational points on certain cubic surfaces*, Math. Scan.**1**,113-119,1953.

[26] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Text in Mathematics **106**, Springer-Verlag, New York, 1986.

[27] T. Springer, Some properties of cubic forms over fields with discrete valuation, Koninkl. Nederl. Akad. van Wetenss, 17 (1955), pp.512-516

[28] G. Terjanian, *Un contre-exemple à une conjecture d' Artin*, Comptes Rendus Acad. Sci. Paris, **262** (1966), 612.

[29] Peter Ullrich, *Der Henselsche Beweisversuch für die Transzendenz von e* Tagungsband der Tagung der Fachsektion Geschichte der Mathematik der DMV in Rummelsberg bei Altdorf/Nünberg (Juni 1995).

[30] Peter Ullrich, *On the origin of p-adic analysis*, Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics (Munich, 1993), 459—473, Sympos. Gaussiana, de Gruyter, Berlin, 1995.

[31] Peter Ullrich, *The genesis of Hensel's p-adic numbers*. Charlemagne and his heritage; 1200 years of civilization and science in Europe, Vol.2 (Aachen, 1995), 163—178, Brepols, Turnhout, 1998.

[32] André Weil, *Oeuvres Scientifique*, collected papers Vol I, p:244-255, Springer-Verlag, 1980.

[33] Edwin Weiss, *Algebraic Number Theory*, McGraw Hill Book Company, New York, 1963.

Websites

[33] http://www-groups.dcs.st-and.ac.uk/history/Mathematicians/Hensel.html
[34] http://aleph0.clarku.edu/~djoyce/hilbert/problems.html