The Hasse-Minkowski Theorem

Tristan Pang

Department of Mathematics
The University of Auckland

Supervisor: Dr Jeroen Schillewaert

A dissertation submitted in partial fulfillment of the requirements for the degree of BSc(Hons) in Mathematics, The University of Auckland, 2019.

Abstract

The Hasse-Minkowski theorem is a local global principle for solutions of nondegenerate quadratic forms in any number field. In this dissertation, we will prove this for the rationals – that a nondegenerate quadratic form has a non-trivial solution in the rationals, $\mathbb{Q}$, if and only if it has non-trivial solutions in the p-adic numbers, $\mathbb{Q}_p$, and the reals, $\mathbb{R}$. Serre's outline [1] will be followed, starting with an introduction of p-adic numbers, which we will define in two equivalent ways, as an infinite sum, and more abstractly, as an inverse limit.

We will also study tools that will help prove the Hasse-Minkowski theorem. Hilbert symbols detect whether a polynomial $aX^2 + bY^2 = Z^2$ has a non-trivial solution. Hensel's Lemma is a p-adic version of Newton's approximation method, wchich "lift" solutions from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$, the p-adic integers. Dirichlet's theorem states that there are infinitely many primes in an arithmetic progression where the initial term and the difference are coprime. All of these tools, are interesting on their own, and will be investigated in this dissertation.

Acknowledgements

First and foremost, I would like to thank my supervisor Dr Jeroen Schillewaert for his guidance, support and encouragement throughout the course of completing this research. This dissertation would certainly not have been possible without his help.

And my sincere thanks to Professor Steven Galbraith who made the Number Theory course interesting which provided intellectual stimulation to help with this research.

I am also very grateful to the then HoD Professor Eamonn O'Brien and the mathematics department who fought for me to enter the university as an underage student.

Last, but not least, my deepest gratitude goes to my beloved mum who has been accompanying me on Campus as requested by the admission office. If not for her, I wouldn't be where I am now.

Contents

Introduction

The p-adic numbers were first introduced by German mathematician Kurt Hensel in 1897. They were built from the rational numbers, just like the real numbers, except in a totally novel way. The p-adic numbers provided the first system of things that were recognisably numbers but had no obvious relations to the real or complex numbers except that both systems contained the rational numbers.

In 1916, Alexander Ostrowski proved a connection between the real numbers and the p-adic numbers; that there are only two types of ways to complete the rationals – either using the usual real absolute value, or using a p-adic absolute value.

Past mathematicians found Hensel's new numbers interesting but impractical. He then revealed that they could be used to develop the basics of algebraic number theory in a different way, though some of what he did had subtle errors. The whole situation changed in 1923 when Hensel's student Helmut Hasse discovered a way to make the p-adic numbers a crucial tool for number theorists. Hasse showed that it was possible to solve a problem locally in all cases, to conclude that it holds globally. Solving a problem locally and putting the local pieces together has become a major practise in modern number theory. Hasse's finding led to the simplification of existing proofs of deep results using class field theory as well as the discovery of new ones including Wiles' proof of Fermat's last theorem. This is known as the Hasse principle or the local-global principle.

In this dissertation, I will show a proof of a specific case of the Hasse principle – the Hasse-Minkowski Theorem. The Hasse-Minkowski theorem states that a nondegenerate quadratic form has a root in the rationals, if and only if it has roots in the p-adic numbers (for every prime) and the real numbers. It is a fundamental result of number theory. This theorem was proved in the rationals by Hermann Minkowski and then generalised to number fields by Helmut Hasse.

The proof of Hasse-Minkowski Theorem requires a lot of background, including a study of Hilbert symbols (introduced by David Hilbert in 1897), Hensel's lemma, and quadratic forms. We will also need to use Dirichlet's Theorem, that there are infinitely many primes in an arithmetic progression where the initial term and the difference are coprime. Interesting on its own, we will provide motivation and a proof of Dirichlet's Theorem, as proved by Dirichlet in 1837.

Chapter 1

p-adic Numbers

Throughout this dissertation, we let $\Bbbk$ be an arbitrary field and p a prime number, unless otherwise stated.

1.1 An introduction to p-adic Numbers

1.1.1 Motivation

In standard base 10 notation, real numbers, say 37 and $\pi = 3.1415\ldots$ can be written as a linear combination of powers of p,

$$37 = 3 \cdot 10^1 + 7 \cdot 10^0, \quad \pi = 3 \cdot 10^0 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + \cdots .$$

We generalise this using prime numbers.

Let p a prime. We can write any natural number, $a \in \mathbb{N}$ as a unique sum of powers of p. For example, for $p = 7$ and $a = 92$, we have,

$$a = p^2 + 6p + 1.$$

We can extend this to the rationals. For $p = 3$ and $a = 11$, $b = 5$, then

$$a = 2 + p^2, \quad b = 2 + p.$$

We first expand $\frac{1}{b}$. To do this, first note that $5 \mid (1 - p^4)$, and that

$$1 - p^4 = -16 \cdot 5.$$

It follows that,

$$\frac{1}{b} = 1 - \frac{4}{5} = 1 + \frac{4 \cdot 16}{1 - p^4} = 1 + c(1 + p^4 + p^8 + \cdots),$$

Where the last step follows from the formula for a geometric series. We will see later why we can do this, but for now, we shall say that instead of using the "normal" norm on $\mathbb{R}$, we define a special norm called the p-adic norm, so that the infinite sum converges. Note that also, $c = 64 = 1 + p^2 + 2p^3$ and that $\frac{1}{b}$ is 4-periodic. Hence,

$$\frac{a}{b} = \frac{2 + p^2}{2 + p} = p + 2p^2 + x^4 + 2x^5 \cdots .$$

Thus, we loosely claim that any rational number can be written as a Laurent series in powers of p^n that is finite on the left (for small powers). It will be shown that the set of all Laurent series in powers of p^n that are finite on the left form a field. This in fact forms a field called $\mathbb{Q}_p$, the p-adic numbers, as we shall see in the next section.

Now, what happens when we use our standard base 10 notation? For example, let

$$a = \ldots 212890625.$$

This is in fact an idempotent number ($a^2 = a$), as we shall see. We construct a as so.

Let $a = \ldots b_3 b_2 b_1 b_0$ be its expansion and note

$$a = \sum_{i=0}^{\infty} b_i 10^i.$$

Set the partial sums as

$$a_n = \sum_{i=0}^{n} b_i 10^i = a \mod 10^{i+1}.$$

Setting $a^2 = a$, it is clear that for all $i \in \mathbb{N}_0$,

$$a_i = a_i^2 \mod 10^{i+1}.$$

We choose $a_0 = 5$. Let $k \in \mathbb{N}$, then $a_k = b_k 10^k + a_{k-1}$. It follows that

$$\begin{aligned} a_k &= a_k^2 && \mod 10^{k+1} \\ &= (b_k 10^k + a_{k-1})^2 && \mod 10^{k+1} \\ &= b_k^2 10^{2k} + 2b_k a_{k-1} 10^k + a_{k-1}^2 && \mod 10^{k+1} \\ &= b_k \Big(\frac{a_{k-1}}{5}\Big) 10^{k+1} + a_{k-1}^2 && \mod 10^{k+1} \\ &= a_{k-1}^2 && \mod 10^{k+1}. \end{aligned}$$

Hence, each b_k is precisely the k-th digit of a_{k-1}^2. Concretely,

$$a_0 = 5,\ a_1 = 25,\ a_2 = 625,\ a_3 = 0625,\ a_4 = 90625,\ a_5 = 890625,\ \ldots$$

We have the limit, a, satisfies

$$a^2 = a \implies 0 = a \cdot (a-1),$$

and thus it is a zero divisor. Hence, the 10-adic numbers do not form a field. It is necessary for p to be prime.

1.1.2 General Notation

Before we dive into the main content, we clarify some notation.

Definition 1.1.1
We define the natural numbers as $\mathbb{N} = \{1, 2, 3, ...\}$. We also use $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Definition 1.1.2
An integer, is **square-free** if it has no square factors.

Definition 1.1.3
A property P holds almost everywhere (on an infinite set I) if P holds on all but a finite number of $i \in I$.

Note 1.1.4
We will use $\mathbb{Z}_p$ to mean the p-adic integers, not the cyclic group of order p. For the latter, we use the standard $\mathbb{Z}/n\mathbb{Z}$ notation, for $n \in \mathbb{N}$.

1.2 A Formal Algebraic Construction of the p-adic Numbers

1.2.1 p-adic Integers

Definition 1.2.1
The sets A_n with homomorphisms $\varphi_n : A_n \to A_{n-1}$, indexed over the natural numbers, form an inverse system

$$\cdots \longrightarrow A_3 \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_1} A_1.$$

The **inverse limit** of a inverse system is

$$\varprojlim A_n = \left\{ \mathbf{a} = (\ldots, a_2, a_1) \in \prod_{n\in\mathbb{N}} A_n \ : \ a_n = \varphi_n(a_{n+1}),\ \forall n \in \mathbb{N} \right\}.$$

Definition 1.2.2
The ring of p**-adic integers**, $\mathbb{Z}_p$, is the inverse limit

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z},$$

where $A_n = \mathbb{Z}/p^n\mathbb{Z}$ and the associated homomorphisms are the canonical

$$\varphi_n(a_n) = a_n \mod p^{n-1}.$$

Definition 1.2.3
The p**-adic valuation** of $n \in \mathbb{Z} \setminus^* \{0\}$ is $v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{R}$, where $v_p(a)$ is the index of the first non-zero entry. If $n = 0$, set $v_p(0) = +\infty$. Note that indeed, $v_p(a)$ is the largest power of p dividing a.

Proposition 1.2.4
For $a, b \in \mathbb{Q}$,

$$v_p(a + b) \geq \min(v_p(a), v_p(b)).$$

Proof.
Let $a = p^n a', b = p^m b'$ and wlog suppose $m \leq n$. Then,

$$v_p(a + b) = v_p(p^n a' + p^m b') = v_p(p^m(p^{n-m}a + b)) \geq m = \min(v_p(a), v_p(b)).$$

□

Definition 1.2.5
The p**-adic norm** of $a \in \mathbb{Q}_p \setminus \{0\}$ is

$$|a|_p = e^{-v_p(a)}.$$

We also set $|0|_p = 0$.

Proof.
To show that $|\cdot|_p$ is a norm, we check the three conditions. Let $a, b \in \mathbb{Z}_p$

1. Clearly, $|a|_p = e^{-v_p(a)} \geq 0$ and is 0 if and only if $a = 0$.
2. $|ab|_p = |a|_p|b|_p$ is also clear.
3. By Proposition 1.2.4, $|a+b|_p \leq e^{-\min(v_p(a),v_p(b))} = \max(e^{v_p(a)}, e^{v_p(b)}) \leq e^{v_p(a)} + e^{v_p(b)} = |a|_p + |b|_p$. □

Definition 1.2.6
The p**-adic metric** of $a, b \in \mathbb{Q} =$ is $d(a,b) = |a-b|_p$.

Definition 1.2.7
Let $a = (\ldots, a_2, a_1) \in \mathbb{Z}_p$. Define $b_0 = a_1$, and inductively define

$$b_{n-1} = \frac{a_n - a_{n-1}}{p^{n-1}},$$

so that

$$a_n = \sum_{i=v_p(a)}^{n-1} b_i p^i \equiv a \mod p^n.$$

In fact, if we defined the $b_n \in \{0, 1, \ldots, p-1\}$ first, then

$$a = \sum_{i=v_p(a)}^{\infty} b_i p^i \in \mathbb{Z}_p.$$

To see this sum converges with the p-adic norm, consider each $b_i p^i \in \mathbb{Z}_p$ with $v_p(b_i p^i) = i$. Then,

$$|a| \leq \sum_{i=v_p(a)}^{\infty} |b_i p^i|_p = \sum_{i=v_p(a)}^{\infty} |b_i| e^{-v_p(p^i)} = \sum_{i=v_p(a)}^{\infty} |b_i| e^{-i} < \infty.$$

since the b_i are bounded by $p-1$, and $\sum e^{-i}$ converges. We also have that two p-adic numbers are close when they share large powers of p.

Write the p**-adic expansion** of a as

$$a = \ldots b_1 b_0 . b_{-1} \ldots b_{k+1} b_k = (\ldots, a_1, a_0 . a_{-1}, \ldots, a_{k+1}, a_k).$$

Remark 1.2.8
Definition 1.2.1 coincides with Definition 1.2.7, and we will use the notation interchangeably, where applicable.

This equivalence holds since (using the notation of Definition 1.2.7) $a_0 = b_0$ and each

$$\sum_{i=0}^{n} b_i p^i \in \mathbb{Z}/p^n\mathbb{Z}$$

corresponds to a_n (for all $n \in \mathbb{N}$). Checking the homomorphism condition:

$$\varphi_n \left(\sum_{i=0}^{n} b_i p^i \right) = \sum_{i=0}^{n-1} b_i p^i.$$

Now we check the valuation. In the previous section, we said $v_p(a)$ is the largest power of p dividing a. Then, the sum terminates at $v_p(a)$:

$$\sum_{i=v_p(n)}^{\infty} b_i p^i,$$

which means $a_n = 0$ for all $n < v_p(a)$, showing that $v_p(a)$ is indeed the index of the first non-zero entry.

1.2.1.1 Exact Sequences

Definition 1.2.9
Let A_i be groups and $f_i : A_i \to A_{i+1}$ be homomorphisms. Then, the sequence

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \cdots \xrightarrow{f_n} A_n$$

is an **exact sequence** if for every k,

$$\operatorname{im} f_k = \ker f_{k+1}.$$

Theorem 1.2.10
A short sequence,

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0,$$

is exact if and only if f is injective, g is surjective, and $\operatorname{im}(f) = \ker(g)$.

In particular, $B/\operatorname{im} f \cong C$.

Proof.
See page 12 of [8] for a discussion on exact sequences. □

Proposition 1.2.11
Let $n \in \mathbb{N}$ and $a = (\ldots, a_2, a_1) \in \mathbb{Z}_p$ be a p-adic number. Let p^n denote the map $a \to p^n a$ and π_n denotes the map $a \to a_n$, then

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\pi_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

is an exact sequence.

Proof.
Clearly, $p^n a = (\ldots, p^n a_2, p^n a_1, 0, \ldots (n \text{ times}), 0)$, and hence, the map p^n is injective. The image of p^n are p-adic numbers that have n leading zeros, in particular, the n-th component of $p^n a$ is 0. Thus $\pi_n(\operatorname{im} p^n) = 0$ and $\operatorname{im} p^n \subset \ker \pi_n$.

Conversely, let $x_n \in \mathbb{Z}/p^n\mathbb{Z}$, $b_i = x_n \mod p^i$, and $b = (\ldots, b_i, \ldots, b_2, b_1) \in \mathbb{Z}_p$. Then, clearly, $\pi_n(b) = x_n$ and π_n is surjective. Now, let $a \in \ker \pi_n$, then $\pi_n(a) = a_n = 0$, and thus, $a_m = 0$ for $m < n$. It is also necessary that for $m > n$, $a_m = 0 \pmod p)^n$, so there exists $c_{m-n} \in \mathbb{Z}/p^{m-n}\mathbb{Z}$ such that $a_m = p^n c_{m-n}$. Now, $a = p^n(\ldots, c_2, c_1)$, thus, $\ker \pi_n \subset \operatorname{im} p^n$. Hence, the sequence is exact. □

Corollary 1.2.12
$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Proof.
Since the exact sequence given in the previous proposition is a short sequence, the result follows by applying Theorem 1.2.10. □

Proposition 1.2.13
$(\mathbb{Z}_p, v_p)$ is an integral domain.

Proof.
Let $a, b \in \mathbb{Z}_p^*$. Then, $v_p(ab) = v_p(a) + v_p(b) < \infty$ and thus $ab \neq 0$. □

Theorem 1.2.14
A element of $\mathbb{Z}_p$ is a unit if and only if it is not divisible by p. That is,

$$\mathbb{Z}_p^* = U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \langle p \rangle = \{a \in \mathbb{Z}_p : v_p(a) = 0\}.$$

Proof.
Suppose $a \in \mathbb{Z}_p$ is invertible. Then, there exists $b \in \mathbb{Z}_p$ such that $ab = 1$. Then,

$$v_p(a) + v_p(b) = v_p(ab) = v_p(1) = 0.$$

Since for all $x \in \mathbb{Z}_p$, $v_p(x) \geq 0$, it follows $v_p(a) = v_p(b) = 0$, that is, $p \nmid a$.

Conversely, suppose $p \nmid a$. Write $a = (\ldots, a_1, a_0)$, where each $a_i \not\equiv 0 \mod p$. Then, each a_i is invertible in $\mathbb{Z}/p^i\mathbb{Z}$, and it follows, $a^{-1} = (\ldots, a_1^{-1}, a_0^{-1})$.

□

Corollary 1.2.15
Every nonzero element $a \in \mathbb{Z}_p$ can be written uniquely as

$$a = p^{v_p(a)} u, \text{ with } u \in \mathbb{Z}_p^*.$$

Proof.
Let $a \in \mathbb{Z}_p \setminus \{0\}$ and $n = v_p(a)$. Then $a = p^m u$, for some $u \in \mathbb{Z}_p$. Now,

$$n = v_p(a) = v_p(p^n u) = v_p(p^n) + v_p(u) = n + v_p(u),$$

and hence, $v_p(u) = 0$, and $u \in \mathbb{Z}_p^*$. □

Corollary 1.2.16
$\mathbb{Z}_p$ is a principal ideal domain with unique maximal ideal $\langle p \rangle$.

Proof.
Let $\{0\} \neq I \subset \mathbb{Z}_p$ be an ideal, let $n = \min\{v_p(a) : a \in I\}$. Note $n < \infty$ since $I \neq \{0\}$, and $p^n \mid a$. So, $I \subset \langle p^n \rangle$.

Conversely, take $a \in I$ such that $v_p(a) = n$. Write $a = p^n u$, where $u \in \mathbb{Z}_p^*$. Then, $u^{-1}a = p^n \in I$, so $\langle p^n \rangle \subset I$.

Thus, $I = \langle p^n \rangle$, for any ideal. Now, $\langle p^n \rangle \subset \langle p \rangle$. In particular, $\langle p \rangle$ is maximal. □

Theorem 1.2.17
$\mathbb{Z}_p$ is compact.

Proof.
For each $n \in \mathbb{N}$, $\mathbb{Z}/p^n\mathbb{Z}$ is finite, thus compact with respect to the discrete topology. By Tychonoff's theorem (see a topology book, e.g. [9] Theorem 17.8, page 120), the product, $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$, is compact with respect to the product topology. Note that by definition, $\mathbb{Z}_p$ is a subring of $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$. Define $f : \mathbb{Z}_p \to \mathbb{Z}_p$ by

$$f((\ldots, x_1, x_0)) = (\ldots, y_1, y_0), \quad (y_{n-1}) = (\varphi_n(x_n) - x_{n-1}),$$

where the φ_n are as in Definition 1.2.2. Then, f is continuous and $\mathbb{Z}_p = f^{-1}(\{0\})$. Thus, $\mathbb{Z}_p$ is closed in $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$, and thus compact. □

Corollary 1.2.18
$(\mathbb{Z}_p, d)$ is complete.

Proof.
A compact space is complete (again, check a topology textbook). □

Remark 1.2.19
An open set in the product topology is a union of products, $\prod_{i=1}^{\infty} U_i$, such that each U_i is open in $\mathbb{Z}/p^i\mathbb{Z}$, and almost all $U_i = \mathbb{Z}/p^i\mathbb{Z}$ (see a topology textbook). It follows that $p^n\mathbb{Z}_p$ are neighbourhoods of 0. We also have that the operations are continuous with the topology.

1.2.2 p-adic Numbers

Definition 1.2.20
The field of **p-adic numbers**, $\mathbb{Q}_p$, is the field of fractions of $\mathbb{Z}_p$. That is,

$$\mathbb{Q}_p = \text{Quot}(\mathbb{Z}_p) = \mathbb{Z}_p[p^{-1}].$$

Definition 1.2.21
For $a = \frac{x}{y} \in \mathbb{Q}_p$ with $x \in \mathbb{Z}_p$ and $y \in \mathbb{Z}_p \setminus \{0\}$, set

$$v_p(a) = v_p(x) - v_p(y).$$

Remark 1.2.22
Let $a = \frac{x_1}{y_1} = \frac{x_2}{y_2} \in \mathbb{Q}_p$. By the fundamental theorem of arithmetic, $v_p(x_1 y_2) = v_p(x_1) + v_p(y_2)$ and $v_p(x_2 y_1) = v_p(x_2) + v_p(y_1)$. Since $x_1 y_2 = x_2 y_1$, it follows that $v_p(a)$ does not depend on the representation of a.

Remark 1.2.23
We can extend Definition 1.2.7 to work with $\mathbb{Q}_p$. Every element in the field of fractions can be written as $a = \frac{x}{y} \in \mathbb{Q}_p$ with $x \in \mathbb{Z}_p$ and $y \in \mathbb{Z}_p \setminus \{0\}$. By Corollary 1.2.15, $y = p^{v_p(y)} u$ for some invertible $u \in \mathbb{Z}_p^*$. Then,

$$\frac{x}{y} = \frac{xu^{-1}}{p^{v_p(y)}}.$$

Since $xu^{-1} \in \mathbb{Z}_p$, it is clear that any p-adic number can be written as

$$\sum_{i=v_p(x)-v_p(y)}^{\infty} c_i p^i,$$

with coefficients c_i as in the expansion of au^{-1}.

Since smaller powers of p have larger norms, this is also another way to see why p-adic numbers must terminate on the right, but can have very large powers of p^n.

Corollary 1.2.24
Every nonzero element $a \in \mathbb{Q}_p$ can be written uniquely as

$$a = p^{v_p(a)} u, \text{ with } u \in \mathbb{Z}_p^*.$$

And $v_p(a) \geq 0$ if and only if $a \in \mathbb{Z}_p$.

Proof.
The first statement immediately from the previous remark and Corollary 1.2.15. The second statement also follows from the equivalent infinite sum definition of the p-adic numbers. □

Corollary 1.2.25
$\mathbb{Q}_p$ is locally compact.

Proof.
For any $a \in \mathbb{Q}_p$, $a + \mathbb{Z}_p$ is a compact neighbourhood. □

1.2.3 Examples

Example 1.2.26
Take the rational numbers $\frac{8}{9} = 2^3 \cdot 3^{-2}$, $10 = 2 \cdot 5$, and $-\frac{3}{160} = -3 \cdot 2^{-5} \cdot 5$. Then we have the following p-adic norms:

$$\begin{array}{lll} \left|\dfrac{8}{9}\right|_2 = \dfrac{1}{8} & |10|_2 = \dfrac{1}{2} & \left|-\dfrac{3}{160}\right|_2 = 32 \\ \left|\dfrac{8}{9}\right|_3 = 9 & |10|_3 = 1 & \left|-\dfrac{3}{160}\right|_3 = 3 \\ \left|\dfrac{8}{9}\right|_5 = 1 & |10|_5 = \dfrac{1}{5} & \left|-\dfrac{3}{160}\right|_5 = 5. \end{array}$$

For $p = 2$, we have the following expansions. These have been calculated on Maple[1].

$$\begin{aligned} \frac{8}{9}{}_2 &= \ldots\overline{0111001}1000 \\ 10_2 &= \overline{0}1010.\overline{0} = (\ldots, 10, 10, 2, 2, 0.) \\ -\frac{3}{160}{}_2 &= \overline{1100}.11001 \end{aligned}$$

Example 1.2.27
The series, $\sum_{i=0}^{\infty} 2^i$ diverges with the usual Euclidean Norm. But if we consider the 2-adic norm, the sum converges, since $\lim_{i\to\infty} |2^i|_2 = 0$ and thus,

$$\left|\sum_{i=0}^{\infty} 2^i\right|_2 \leq \sum_{i=0}^{\infty} |2^i|_2 = \sum_{i=0}^{\infty} e^{-i} < \infty.$$

Concretely,

$$\left(\sum_{i=0}^{\infty} 2^i\right)_2 = \overline{1}. = -1_2.$$

This is related to "two's complement" as in binary computing.

1.3 Ostrowski's Theorem

Definition 1.3.1
An absolute value on $\Bbbk$ is a function

$$|\cdot| : \Bbbk \to \{x \in \mathbb{R} : x \geq 0\}$$

such that

[1] Maple can be found at https://www.maplesoft.com/products/maple/. The function used was `evalp`.

1. $|x| = 0$ if and only if $x = 0$,
2. $|xy| = |x||y|$ for all $x, y \in \mathbb{k}$,
3. $|x + y| \leq |x| + |y|$ for all $x, y \in \mathbb{k}$ (triangle inequality).

In particular, an absolute value is a special case of a norm.

Definition 1.3.2
Write $|\cdot|_\infty$ as the usual real absolute value and $\mathbb{Q}_\infty = \mathbb{R}$ as the reals. Recall $|\cdot|_p$ is the p-adic absolute value.

Definition 1.3.3
Two absolute values, $|\cdot|$ and $||\cdot||$ on a field $\mathbb{k}$ are equivalent if there exists $\alpha \in \mathbb{R}^+$ such that for every $x \in \mathbb{k}$

$$|x| = ||x||^\alpha.$$

Lemma 1.3.4
Let $|\cdot|$ be an absolute value on $\mathbb{Q}$. Then $|1| = |-1| = 1$.

Proof.
Since $|1| = |1 \cdot 1| = |1|^2$, it follows $|1| = 1$. Similarly, $|1| = |-1 \cdot -1| = |-1|^2$, so $|-1| = 1$ since absolute value are non-negative. □

Theorem 1.3.5 (Ostrowski's Theorem)
Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to either the real or a p-adic absolute value.

Proof.
Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. We consider two cases.

1. $\exists n \in \mathbb{N}$, $|n| > 1$, then $|\cdot|$ is the real absolute value.
2. $\forall n \in \mathbb{N}$, $|n| \leq 1$, then $|\cdot|$ is a p-adic absolute value.

Suppose there exists $n \in \mathbb{N}$ such that $|n| > 1$. Let n_0 be the smallest such n. Let

$$\alpha = \frac{\log|n_0|}{\log n_0},$$

this is well defined since n_0 and $|n_0|$ are both greater than 1. Note that $|n_0| = n_0^\alpha$. We will prove that this α works for all of $\mathbb{Q}$. It is sufficient to show that $|n| = n^\alpha$ for $n \in \mathbb{N}$, since for any rational, $\pm\frac{n}{m}$ with $n, m \in \mathbb{N}$,

$$\left|\frac{n}{m}\right| = \frac{|n|}{|m|} = \frac{n^\alpha}{m^\alpha} = \left(\frac{n}{m}\right)^\alpha.$$

Now, write n in base n_0,

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k,$$

where $a_i \in 0, 1, \cdots, n_0 - 1$ and $k = \lfloor \frac{\log n}{\log n_0} \rfloor$. It follows that

$$\begin{aligned}
|n| &= |a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k| \\
&\leq |a_0| + |a_1| n_0^{\alpha} + |a_2| n_0^{2\alpha} + \cdots + |a_k| n_0^{k\alpha} && \text{(triangle inequality)} \\
&\leq 1 + n_0^{\alpha} + n_0^{2\alpha} + \cdots + n_0^{k\alpha} && (|n_0| \geq 1 \text{ minimal, } a_i < n,\ |a_i| \leq 1) \\
&= n_0^{k\alpha} \left(1 + n_0^{-\alpha} + \cdots + n_0^{-k\alpha}\right) \\
&\leq n_0^{k\alpha} \frac{1 - n_0^{-\alpha(k+1)}}{1 - n_0^{-\alpha}} && \text{(geometric series, } n_0 \neq 1\text{)} \\
&= n_0^{k\alpha} \frac{n_0^{\alpha} - n_0^{-\alpha k}}{n_0^{\alpha} - 1} \\
&\leq n_0^{k\alpha} \frac{n_0^{\alpha}}{n_0^{\alpha} - 1} && (n_0 > 1) \\
&\leq n^{\alpha} \frac{n_0^{\alpha}}{n_0^{\alpha} - 1} && (n_0^k \leq n).
\end{aligned}$$

Since n was arbitrary,

$$|n^i| \leq n^{i\alpha} \frac{n_0^{\alpha}}{n_0^{\alpha} - 1} \implies |n| \leq n^{\alpha} \left(\frac{n_0^{\alpha}}{n_0^{\alpha} - 1}\right)^{\frac{1}{i}}.$$

Taking limits, $i \to \infty$, it follows that the constant goes to 1, and thus $|n| \leq n^{\alpha}$.

To show the converse inequality, first see that $n^{(k+1)\alpha} = |n_0^{k+1}| \leq |n| + |n_0^{k+1} - n|$. So,

$$\begin{aligned}
|n| &\geq n^{(k+1)\alpha} - |n_0^{k+1} - n| \\
&\geq n^{(k+1)\alpha} - (n_0^{k+1} - n)^{\alpha} \\
&= n_0^{(k+1)\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right) \\
&\geq n^{k\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right),
\end{aligned}$$

since $n_0^{k+1} > n \geq n_0^k$. Since n was arbitrary, it again follows by taking powers and limits, $|n| \geq n^{\alpha}$.

Thus, $|n| = n^{\alpha} = |n|_{\infty}^{\alpha}$ and hence, $|x| = |x|_{\infty}^{\alpha}$, for all $x \in \mathbb{Q}$.

Now consider the case where for all $n \in \mathbb{N}$, $|n| \leq 1$. Note that by Lemma 1.3.4, $|-n| \leq 1$ also. Since $|\cdot|$ is non-trivial, not all elements have absolute value 1. In particular, there is a natural number with a norm strictly less than 1 (for if not, then since every rational is a quotient of two natural numbers and ± 1, every rational has norm 1). Let $n_0 \in \mathbb{N}$ be the smallest number such that $|n_0| < 1$. Now, suppose for a contradiction that n_0 is composite, that there exists $a, b \in \mathbb{N} \setminus \{1\}$ such that $n_0 = ab$. Then, both a and b are less than n_0, and thus, $|a| = |b| = 1$. So $|n_0| = 1$, a contradiction. Hence n_0 is prime.

Let $n \in \mathbb{Z}$ such that $\gcd(n, n_0) = 1$. Then, for any $i \in \mathbb{N}$, $\gcd(n^i, n_0^i) = 1$ also. Thus by Bézout's Identity, there exists $x_i, y_i \in \mathbb{Z}$ (so both have absolute value less than 1) such that

$$x_i n^i + y_i n_0^i = 1.$$

It follows that,

$$1 = |1| \leq |n^i x_i| + |n_0^i y_i| \leq |n|^i + |n_0|^i.$$

Since $|n_0| < 1$,

$$\lim_{i \to \infty} |n_0|^i = 0,$$

and hence, $|n|^i \geq 1$ for sufficiently large i. But since n was an arbitrary integer coprime to n_0, we can consider n^i. Hence, for all n coprime to n_0, $|n| \geq 1$, and hence $|n| = 1$.

Now for any $m \in \mathbb{Z}$, write

$$m = n_0^{v_{n_0}(m)} n$$

where $\gcd(n, n_0) = 1$. Then,

$$|m| = |n_0|^{v_{n_0}(m)} |n| = |n_0|^{v_{n_0}(m)}.$$

Write

$$\alpha = -\log |n_0|.$$

It follows that

$$m = |n_0|^{v_{n_0}(m)} = \left(e^{-v_{n_0}(m)}\right)^{\alpha} = |m|_{n_0}^{\alpha}.$$ □

Remark 1.3.6
There are many extensions to Ostrowski's Theorem. One such is extending the theorem to work over any number field (finite field extension of $\mathbb{Q}$). Defining an analogous p-adic norm using prime ideals and the order of an element in that ideal, this version of Ostrowski's Theorem says that any non-trivial absolute value is either this p-adic norm, or an absolute value that comes from either a real or complex embedding of the number field. Refer to [5] for more details.

1.4 Hensel's Lemma

We now show a p-adic analogy of Newton's method.

Definition 1.4.1
Let $F(X) = a_0 + a_1 X + a_2 X^2 + \cdot + a_n X^n \in \Bbbk[X_1, X_2, ..., X_n]$ a polynomial. Then its formal derivative is

$$F'(X) = a_1 + 2a_2 X + \cdot + n a_n X^{n-1}.$$

Theorem 1.4.2 (Hensel's Lemma)
Let $F(X) = c_0 + c_1 X + c_2 X^2 + \cdot + c_n X^d \in \mathbb{Z}_p[X]$ a polynomial. Suppose there exists a p-adic integer, $a \in \mathbb{Z}_p$, such that

$$F(a) \equiv 0 \mod p, \quad \text{and} \quad F'(a) \not\equiv 0 \mod p.$$

Then there exists a unique p-adic integer $b \in \mathbb{Z}_p$ such that

$$b \equiv a \mod p, \quad \text{and} \quad F(b) = 0.$$

Proof.
Let $a_1 = a$. Then by assumption, $F(a_1) \equiv 0 \mod p$ and $F'(a_1) \not\equiv 0 \mod p$. Now suppose as the inductive hypothesis that for $k \in \mathbb{N}$, there exists a unique $a_k \mod p^k$ such that

$$F(a_k) \equiv 0 \mod p^k, \quad \text{and} \quad a_k \equiv a_1 \mod p$$

Since $a_{k+1} \equiv a_n \mod p^n$, write

$$a_{k+1} = a_k + tp^k, t \in \mathbb{Z}.$$

Using Taylor's theorem (see any basic analysis book), it follows that for all $t \in \mathbb{Z}$,

$$\begin{aligned} F(a_{k+1}) &= F(a_k + tp^k) \\ &= F(a_k) + tp^k F'(a_k) + O(p^{2k}) \\ &\equiv F(a_k) + tp^k F'(a_k) \mod p^{k+1} \end{aligned}$$

So a_{k+1} is a solution $\mod p^{k+1}$ if

$$t = -\frac{F(a_n)}{F'(a_n)} \mod p,$$

(which is well defined since $F'(a_{k+1}) \equiv F'(a_k) \not\equiv 0 \mod p$). Hence,

$$a_{k+1} = a_k - \frac{F(a_k)}{F'(a_k)} \mod p^{k+1} \tag{1.1}$$

uniquely satisfies the two conditions.

Thus, by induction, there exists unique solutions of F, $a_n \equiv a_{n+1} \mod p^n$, for all $n \in \mathbb{N}$. In particular, set

$$b = \lim_{n\to\infty} a_n = (\ldots, a_2, a_1) \in \mathbb{Z}_p,$$

then, $b \equiv a_n \mod p^n$ and $F(b) \equiv 0 \mod p^n$ for all n. Thus,

$$F(b) = 0 \quad \text{and} \quad b \equiv a_1 \equiv a \mod p. \qquad \square$$

Example 1.4.3
Hensel's Lemma states that we can lift any equation from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$, with Equation 1.1 giving an explicit formulae. For example, we show that $F(X) = X^2 - 10$ has a solution in $\mathbb{Z}_3$. Clearly, $F(1) = -9 \equiv 0 \mod 3$ and $F'(1) = 2 \not\equiv 0 \mod 3$. Thus, by Hensel's Lemma, there exists a unique 3-adic integer, $b \in \mathbb{Z}_3$ such that $b^2 = 10$ and $b = 1 \mod 3$.

Indeed, $b = \cdots 100121201 = (1, 1, 19, 46, 43264 \ldots)$, that is,

$$\begin{aligned} 10 &\equiv 1^2 && \mod 3 \\ 10 &\equiv 1^2 && \mod 3^2 \\ 10 &\equiv (1 + 2 \cdot 3^2)^2 && \mod 3^3 \\ 10 &\equiv (1 + 2 \cdot 3^2 + 3^3)^2 && \mod 3^4 \\ &\vdots \end{aligned}$$

Similarly, $F(X) = X^2 - 4$ has a solution in $\mathbb{Z}_3$ since $F(1) \equiv 0 \mod 3$ and $F'(1) \not\equiv 0 \mod 3$. Explicitly, $b = \cdots 222221 = (1, 7, 25, 79, 241, 727 \ldots)$, where $b^2 = 4$ and $b \equiv 1 \mod 3$. Note also, $F(2) \equiv 0 \mod 3$ and $F'(2) \not\equiv 0 \mod 3$, and indeed we can lift to $-b = \cdots 11112 \in \mathbb{Z}_3$.

Here is a generalised version of Hensel's Lemma.

Corollary 1.4.4
Let $F(X) = c_0 + c_1 X + c_2 X^2 + \cdot + c_n X^d \in \mathbb{Z}_p[X]$ a polynomial. Suppose there exists a p-adic integer, $a \in \mathbb{Z}_p$, such that

$$|F(a)|_p < |F'(a)|_p^2.$$

Then there exists a unique p-adic integer $b \in \mathbb{Z}_p$ such that

$$b \equiv a \mod p^{v_p(f(a)) - v_p(f'(a))}, \quad \text{and} \quad F(b) = 0.$$

Proof.
This proof is almost identical to the proof of Hensel's Lemma, bar changing the powers of p in the inductive step. See [1] page 14 for a step by step proof. □

Corollary 1.4.5
Let p be an odd prime. Let $c \in \mathbb{Z}_p^*$. Then c is a square in $\mathbb{Z}_p$ if and only if it is a nonzero square $\mod p$. In particular, if $u \in \mathbb{Z}/p^n\mathbb{Z}$, for some $n \in \mathbb{N}$, with $u \equiv a^2 \mod p$, for some $a \in \mathbb{Z}/p\mathbb{Z}$, then u is a square $\mod p^n$.

Proof.
If c is a square in $\mathbb{Z}_p^*$, say $c = b^2$, then $v_p(b)^2 = v_p(c) = 0$ and $b \in \mathbb{Z}_p^*$. Thus, $c \equiv b^2 \not\equiv 0 \mod p$.

Conversely, write $c \equiv a^2 \not\equiv 0 \mod p$ so that $a \not\equiv 0 \mod p$. Define

$$F(X) = X^2 - c.$$

Then, $F(a) \equiv 0 \mod p$ and $F'(a) = 2a \not\equiv 0 \mod p$ (this is the only place we use $p \neq 2$). Hence, by Hensel's Lemma, $F(X)$ has a root $b \in \mathbb{Z}_p$ such that

$$c = b^2 \quad \text{and} \quad c \equiv a \mod p.$$ □

Lemma 1.4.6
Let $m \in \mathbb{N}$ such that $\gcd(m, p) = 1$. Then, there exists $a \in \mathbb{Z}$ such that $a^m \equiv 1 \mod p$ and $a \not\equiv 1 \mod p$ if and only if $\gcd(m, p-1) \neq 1$, and for any such a, the least positive integer m with that property must be a divisor of $p - 1$.

Proof.
Suppose there exists $a \in \mathbb{Z}$ such that $a^m \equiv 1 \mod p$ and $a \not\equiv 1 \mod p$. Then, the order of $a \mod p$ in $(\mathbb{Z}/p\mathbb{Z})^*$ must divide $\varphi(p) = p-1$. Thus, $\gcd(m, p-1) \neq 1$, since $a \not\equiv 1 \mod p$. The least m satisfying the property divides the gcd, and hence divides $p-1$. Conversely, in a cyclic group of order $p-1$, there is an non-identity element of order dividing $p-1$. □

Proposition 1.4.7
$\mathbb{Q}_p$ is not algebraically closed.

Proof.
Let $\gcd(m,p) = 1$. Suppose there is a mth root of unity, say $\omega \neq 1$. Then, then $\omega^m - 1 = 0$ and $|\omega|_p = 1 > 0$, and hence $\omega \in \mathbb{Z}_p$. Now let $a \equiv \omega \not\equiv 1 \mod p$, so that $a^m \equiv 1 \mod p$. By the previous lemma, $\gcd(m, p-1) \neq 1$. That is, if we choose $m \neq 1$ such that $\gcd(m, p-1) = 1$, $\omega \equiv 1 \mod p$. Then, by Hensel's Lemma, this lifts to a solution in $\mathbb{Z}_p$, but by uniqueness, this must be 1. Hence, the only root of $F(X) = X^m - 1$ in $\mathbb{Q}_p$ is 1. Suppose for a contradiction that $\mathbb{Q}_p$ is algebraically closed, then

$$F(X) = X^m - 1 = (X-1)^m.$$

It is clear that for ever p, there is a $m > 1$ satisfying the above conditions (just choose m to be the next prime after p, which is odd). Then, expanding this out,

$$(X-1)^m = \sum_{i=0}^{m} \binom{m}{i} X^i (-1)^{m-i},$$

where $\binom{m}{i}$ is the binomial coefficient. Then, we had the equality

$$\sum_{i=1}^{m-1} \binom{m}{i} X^i (-1)^{m-i} = 0,$$

for every X. Thus, the left hand side must be the 0 function, meaning that each monomial must vanish. Thus each $\binom{m}{i} = 0$, which is clearly a contradiction. Hence, not all mth roots of unity are in $\mathbb{Q}_p$ and thus, $\mathbb{Q}_p$ is not algebraically closed. □

Proposition 1.4.8
For odd prime p, the $(p-1)$th roots of unity are roots of unity of $\mathbb{Q}_p$. If $p = 2$, then ± 1 are roots of unity.

Proof.
Let p be odd. Consider $F(X) = X^{p-1} - 1$. Let $a \in \{1, 2, \ldots, p-1\}$, then $F(a) \equiv 0 \mod p$ and $F'(a) \equiv (p-1)a^{p-2} \not\equiv 0 \mod p$. Hence by Hensel's Lemma, this lifts to a solution, say ω_a in $\mathbb{Z}_p$. Thus, each a lifts to a unique ω_a, in particular all $p-1$ of these $(p-1)$th roots of unity are in $\mathbb{Q}_p$.

If $p = 2$, then consider $F(X) = X^2 - 1$. $F(-1) \equiv 0 \mod p$ and $F'(-1) \not\equiv 0 \mod p$. Hence, this lifts to a solution in $\mathbb{Z}_2$. Similarly, so does 1. □

Remark 1.4.9
It is possible to show that these are the only roots of unity. See [2] page 114 for more details. This requires more background and will be an interesting topic of future research.

Proposition 1.4.10
Let $p \neq q$ primes. Then $\mathbb{Q}_p$ is not isomorphic to $\mathbb{Q}_q$.

Proof.
Wlog suppose $p > q$ (so $p \neq 2$). Let $m \in \mathbb{N}$ and $m \mid p-1$, and $m \nmid q-1$ (e.g. $m = p-1$). Then, there is a m-th root of unity, $\omega \neq 1$, in $\mathbb{Q}_p$. Suppose for a contradiction there is an isomorphism, $\varphi : \mathbb{Q}_p \to \mathbb{Q}_q$. Then, $\varphi(\omega) \in \mathbb{Q}_q$ is a m-th root of unity. Thus, $\varphi(\omega)^m = 1$, and $\varphi(\omega)^{p-1} \equiv 1 \mod p$. Since $\varphi(\omega) \neq 1$, $m \mid p-1$, a contradiction. Hence $\mathbb{Q}_p \ncong \mathbb{Q}_q$. □

Recall that in $\mathbb{R}$, a series cannot be rearranged without affecting the sum. In fact, if the series does not converge absolutely, it can be shown that there exists a rearrangment convering to any element in $\mathbb{R}$ (refer to any basic real analysis textbook).

Proposition 1.4.11
Let $\{a_n \in \mathbb{Q}_p : n \in \mathbb{N}\}$ be a sequence with $\lim_{n\to\infty} a_n = 0$, and (a'_n) a rearangement of (a_n). Then, $\lim_{n\to\infty} a'_n = 0$ and $\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} a'_n$.

Proof.
First note that, since (a_n) converges to zero, any rearangment must converge to zero. Define the N-th partial sums as $S_N = \sum_{N=1}^{\infty} a_n$ and $S'_N = \sum_{N=1}^{\infty} a'_n$, and let $A = \lim_{m\to\infty} S_m$ Then, let $\varepsilon > 0$, then there exists $N \in \mathbb{N}$ such that for any $m > N$, $|a_m|_p < \varepsilon$, $|a'_m|_p < \varepsilon$, $|A - S_N|_p < \varepsilon$. Now define,

$$T_N = \{a_i : |a_i|_p \geq \varepsilon, i \leq m\}, \quad \text{and} \quad T'_N = \{a'_i : |a'_i|_p \geq \varepsilon, i \leq m\},$$

and define the sums of the elements in R_N (resp. T'_N) as R'_N (resp. R'_N). Since we assumed that $|a_m|_p < \varepsilon$ and $|a'_m|_p < \varepsilon$, it is clear that $T_m = T'_m$, and hence $R_N = R'_N$. Now,

$$|S_N - R_N|_p = \left| \sum_{|a_i|_p < \varepsilon} a_i \right|_p \leq \max\{|a_i|_p : |a_i|_p < \varepsilon\} < \varepsilon.$$

Similarly, $|S'_N - R'_N|_p < \varepsilon$. It follows that,

$$|A - S'_N|_p \leq |A - S_N| + |S_N - S'_N|_p < \varepsilon + |S_N - R_N|_p + |R_N - R'_N|_p + |R'_N - S'_N|_p < 3\varepsilon.$$

Since ε was arbitary, it follows that $\lim_{N\to\infty} S'_N = A$, and thus, $\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} a'_n$. □

Chapter 2

Hasse-Minkowski Theorem

In this chapter, we assume that the characteristic of $\Bbbk$ is not 2.

2.1 Motivation

We already know from basic theory that if a polynomial in n variables has integer solutions, then it has solutions in $\mathbb{Z}/p\mathbb{Z}$ for all p. From what we have already done, we can also extend this to if a polynomial has rational solutions, it has solutions in $\mathbb{Q}_p$ for all p. In this section, we study the converse.

Example 2.1.1
Let $F(X) = X^2 - 5X + 1$. Then F has no roots in $\mathbb{Z}$ since there are no roots in $\mathbb{Z}/2\mathbb{Z}$. To see this reduce F modulo 2:

$$F(X) = X^2 + X + 1 \mod 2.$$

It is easy to check that neither 0 nor 1 is a root.

Example 2.1.2
Let $F(X, Y) = 3X^4 - 5Y^2 + 15X^2 - 25$. But, reducing $\mathrm{mod}\ 3$ gives us $Y^2 = 1$ and reducing $\mathrm{mod}\ 5$ gives us $X^4 = 0$. In both cases, there is a solution, hence we still don't know anything. But what if we consider $\mathbb{Q}_5$? Suppose for a contradiction that (x, y) is a root of F. Considering the valuation of

$$5y^2 = 3x^4 + 15x^2 - 25,$$

with $v_5(x) = a$ and $v_5(y) = b$,

$$v_p(5y^2) = 2b + 1, \quad \text{and} \quad v_p(3x^4 + 15x^2 - 25) \geq \min(4a, 2a + 1, 2).$$

Note that the valuation on both sides must be equal. Since the left is odd, so must the right, and so, $v_p(3x^4 + 15x^2 - 25) = \min(4a, 2a + 1, 2) = 2a + 1$. But, if $a \geq 1$, $\min(4a, 2a + 1, 2) = 4$ and if $a < 1$, $\min(4a, 2a + 1, 2) = 2$, a contradiction. Hence, F has no solutions in $\mathbb{Q}_5$ and thus no rational solutions.

2.2 Background

2.2.1 Quadratic Forms

Definition 2.2.1
A **quadratic form** in $\Bbbk[X_1, X_2, ..., X_n]$ is a homogeneous polynomial of degree 2 in n variables.

Recall that, after a change of variables, any quadratic form can be written in the form

$$F = a_1X_1^2 + \cdots + a_nX_n^2, \quad a_i \in \mathbb{k}^*.$$

Proposition 2.2.2
If $\mathbb{k}$ is a finite field, then any quadratic form over $\mathbb{k}$ in at least 3 variables has a non-zero root.

Proof.
This follows from the Chevalley-Warning theorem (see [1] page 5) since the degree of a quadratic form is 2. □

Definition 2.2.3
A element of $\mathbb{Q}_p^m$ is called **primitive** if one of the coordinates is invertible.

Proposition 2.2.4
Let $F \in \mathbb{Z}_p[X_1, \ldots, X_m]$ be a homogeneous polynomial with coefficients in $\mathbb{Z}_p$. Then if F has a non-zero solution in $\mathbb{Q}_p^m$, then it has a primitive zero in $\mathbb{Z}_p^m$.

Proof.
Let $(x_1, \ldots, x_m) \in \mathbb{Q}_p^m$ be a non-zero of F. Let

$$y = p^{-\min_i\{v_p(x_i)\}}(x_1, \ldots, x_m).$$

Then, $y \in \mathbb{Z}_p^m$ is a primitive zero of F. □

2.3 Squares in $\mathbb{Q}_p^*$

Proposition 2.3.1
Let p be an odd prime and $x = p^n u \in \mathbb{Q}_p^*$ with $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_2^*$, then x is a square in$\mathbb{Q}_p^*$ if and only if n is even and $\left(\frac{u}{p}\right) = 1$. That is, u is a square modulo p.

Proof.
See [1] page 17. □

Lemma 2.3.2
Let $x = 2^n u \in \mathbb{Q}_2^*$ with $n \in \mathbb{Z}$ and $u \in \mathbb{Q}_2^*$, then x is a square in $\mathbb{Q}_2^*$ if and only if n is even and $u \equiv 1 \mod 8$.

Proposition 2.3.3
See [1] page 18.

Proposition 2.3.4
$\mathbb{Q}_p^{*2}$ is an open subgroup of $\mathbb{Q}_p^*$. That is, the squares of $\mathbb{Q}_p^*$ form an open set.

Proof.
See [1] page 18. □

2.3.1 Legendre Symbol

It is expected that the reader has some knowledge on Legendre symbols. This section will only present ideas needed to progress onto Hilbert symbols. All proofs are available in any reputable introductory book on number theory (e.g. Section 3.2 of [3]). It also follows that the Legendre symbol can be extended to the p-adic units in the obvious way (Definition 2.3.6).

Definition 2.3.5
Define the following functions for odd p.

$$\varepsilon(p) = \frac{(p-1)}{2} \mod 2 = \begin{cases} 0 & \text{if } p \equiv 1 \mod 4 \\ 1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

$$\omega(p) = \frac{(p^2-1)}{8} \mod 2 = \begin{cases} 0 & \text{if } p \equiv 1,7 \mod 8 \\ 1 & \text{if } p \equiv 3,5 \mod 8 \end{cases}$$

Definition 2.3.6
The Legendre Symbol of $a \in \mathbb{Z}_p^*$,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \mod p \text{ has a solution,} \\ 0 & \text{if } a \equiv 0 \mod p, \\ -1 & \text{otherwise} \end{cases} .$$

Proposition 2.3.7 (Euler's Criterion)
Let p be an odd prime.

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

Corollary 2.3.8
The Legendre symbol is linear. That is,

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

Proposition 2.3.9

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

$$\left(\frac{2}{p}\right) = (-1)^{\omega(p)} = \begin{cases} -1 & \text{if } p \equiv 1,7 \mod 8, \\ 1 & \text{if } p \equiv 3,5 \mod 8. \end{cases}$$

Proposition 2.3.10 (Quadratic Reciprocity)
Gauss's Quadratic Reciprocity says that if p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\varepsilon(p)\varepsilon(q)} = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \mod 4, \\ \left(\frac{q}{p}\right) & \text{otherwise.} \end{cases}$$

2.4 Hilbert Symbols

Definition 2.4.1
Let $\Bbbk^*$ be the multiplicative group of $\Bbbk$ and let $a, b \in \Bbbk^*$. Then the **Hilbert symbol** of a and b relative to k is

$$(a,b) = \begin{cases} 1 & \text{if } aX^2 + bY^2 = Z^2 \text{ has a non-trivial solution, } (x,y,z) \in \Bbbk^3 \\ -1 & \text{otherwise.} \end{cases}$$

In particular, if $k = \mathbb{Q}_p$, write $(a,b)_p$.

Lemma 2.4.2
Let $a, b \in \Bbbk^*$. Then $(a,b) = 1$ if and only if there exists $x, y \in \Bbbk$ such that $a = x^2 - by^2$.

Proof.
Suppose there exists $x, y \in \Bbbk$ such that $a = x^2 - by^2$. Then, clearly, $(1, y, z)$ is a solution to $aX_1^2 + bX_2^2 = X_3^2$. Thus, $(a,b) = 1$.

Conversely, suppose $(a,b) = 1$. Then $aX^2 + bY^2 = Z^2$ has a non-trivial solution, say (x,y,z). If $x = 0$, then $b = \frac{z^2}{y^2}$ is a square. Then,

$$a = \left(\frac{a+1}{2}\right)^2 - b\left(\frac{y(a-1)}{2z}\right)^2.$$

If $x \neq 0$, then

$$a = \left(\frac{z}{x}\right)^2 - b\left(\frac{y}{x}\right)^2.$$

□

Lemma 2.4.3
For $b \in \Bbbk^*$, $\{x^2 - by^2 \neq 0 : x, y \in \Bbbk\}$ is a subgroup of $\Bbbk^*$.

Proof.
If b is a square, then for all $a \in \Bbbk^*$,

$$a = \left(\frac{a+1}{2}\right)^2 - b\left(\frac{a-1}{2\sqrt{b}}\right)^2 \in \{x^2 - by^2 \neq 0 : x, y \in \Bbbk\}.$$

Thus, $\{x^2 - by^2 \neq 0 : x, y \in \Bbbk\} = \Bbbk^*$.

On the other hand, suppose b is not a square. Let $a_1, a_2 \in \{x^2 - by^2 \neq 0 : x, y \in \Bbbk\}$. Write

$a_1 = x_1^2 - by_1^2$ and $a_2 = x_2^2 - by_2^2$. Then,

$$\begin{aligned} a_1a_2 &= (x_1^2 - by_1^2)(x_2^2 - by_2^2) \\ &= x_1^2x_2^2 - b(x_1^2y_2^2 + x_2^2y_1^2) + b^2y_1^2y_2^2 \\ &= x_1^2x_2^2 + 2bx_1x_2y_1y_2 + b^2y_1^2y_2^2 - b(x_1^2y_2^2 + 2x_1x_2y_1y_2 + x_2^2y_1^2) \\ &= (x_1x_2 + by_1y_2)^2 - b(x_1y_2 + x_2y_1)^2 \in \{x^2 - by^2 \neq 0 : x, y \in \Bbbk\}, \\ \text{and} \quad a_1^{-1} &= \frac{a_1}{a_1^2} \\ &= \frac{x_1^2 - by_1^2}{a_1^2} \\ &= \left(\frac{x_1}{a_1}\right)^2 - b\left(\frac{y_1}{a_1}\right)^2 \in \{x^2 - by^2 \neq 0 : x, y \in \Bbbk\}. \end{aligned}$$

It follows from the two-step subgroup test that $\{x^2 - by^2 \neq 0 : x, y \in \Bbbk\} \leq \Bbbk^*$. □

Remark 2.4.4
Let $b \in \Bbbk^*$, $B = \{x^2 - by^2 \neq 0 : x, y \in \Bbbk\}$. Then by the previous two lemmas, if $a \in \Bbbk^*$, then $(a, b) = 1$ if and only if $a \in B$. Note also that $b \in B$.

Proposition 2.4.5
Let $a, b, c \in \Bbbk^*$. The following are properties of the Hilbert symbol.

1. $(a, 1) = 1$
2. $(a, b) = (b, a)$ and $(a, b^2) = 1$
3. $(a, -a) = 1$ and $(a, 1 - a) = 1$
4. $(a, b) = 1 \implies (ac, b) = (c, b)$
5. $(a, b) = (a, -ab) = (a, (1 - a)b)$
6. $(a, a) = (a, -1)$

Proof.

1. $(0, 1, 1)$ is a solution to $aX^2 + Y^2 = Z^2$.
2. Clearly, the Hilbert symbol is commutative. Also, $aX^2 + b^2Y^2 = Z^2$ has non-zero solution $(0, 1, b)$, so $(a, b^2) = 1$.
3. $aX^2 - aY^2 = Z^2$ clearly has a solution, $(1, 1, 0)$. Similarly, $aX^2 + (1 - a)Y^2 = Z^2$ has the solution, $(1, 1, 1)$.
4. Let B be the group from Lemma 2.4.3. Then by assumption, $a \in B$. Then by properties of a group, $c \in B$ if and only if $ac \in B$. Hence, $(ac, b) = (c, b)$.
5. By 3, $(a, -a) = 1$, thus using commutativity and the implication of 4, $(a, -ab) = (a, b)$. The second equality is similar.

6. Let $b = -a$ and $c = -1$. Then by 3, $(a, b) = 1$, and by 4, $(a, a) = (a, bc) = (a, c) = (a, -1)$. □

Proposition 2.4.6
If $\mathbb{k} = \mathbb{R}$,

$$(a, b)_\infty = \begin{cases} 1 & \text{if either } a \text{ or } b \text{ are positive} \\ -1 & \text{otherwise.} \end{cases}$$

Proof.
If both a and b are negative, since there are no real solutions to $z^2 = -1$, $(a, b) = -1$. Otherwise, wlog consider $a > 0$. Then it follows $(a, b) = 1$, since setting $z = \sqrt{|b|}$, $y = 1$, there is a x such that $ax^2 = |b| - b$. □

Theorem 2.4.7
Let $\mathbb{k} = \mathbb{Q}_p$, for an odd prime p. Write $a = p^\alpha u$ and $b = p^\beta v$ with $u, v \in \mathbb{Z}_p^*$. Then,

$$(a, b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

Proof.
First note that by 2.2.2, there is a non-zero root of $uX^2 + vY^2 - Z^2$ in $\mathbb{Z}/p\mathbb{Z}$. Thus by Hensel's Lemma, this lifts to $\mathbb{Z}_p$. Thus $(u, v)_p = 1$. Now, obviously, from the formula, we only need to consider $\alpha, \beta \in 0, 1$. We consider the three cases for α and β.

1. $\underline{\alpha = 0, \beta = 0}$

   The RHS is 1. $(a, b)_p = (u, v)_p = 1$.

2. $\underline{\alpha = 0, \beta = 1}$

   The RHS is $\left(\frac{v}{p}\right)$. Since $(u, v)_p = 1$, it follows from 4 of Proposition 2.4.5, $(pu, v)_p = (p, v)_p$. If v is a square, then $(p, v)_p = 1 = \left(\frac{v}{p}\right)$, otherwise if v is non-square, then $vY^2 - Z^2$ has no non-zero solutions $\bmod p$, thus $pX^2 + vY^2 - Z^2$ has no non-zero solutions in $\mathbb{Q}_p$. It follows that $(a, b)_p = (pu, v)_p = (p, v)_p = -1$.

3. $\underline{\alpha = 1, \beta = 1}$

   The RHS is $(-1)^{\frac{p-1}{2}}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. Now, by 5 of Proposition 2.4.5, $(pu, pv)_p = (pu, -p^u v)_p = (pu, -uv)_p$. Thus, we can apply the previous case,

$$(a, b)_p = (pu, -uv)_p = \left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{u}{p}\right)\left(\frac{v}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right).$$

□

Lemma 2.4.8
For $p = 2$, ε and ω are homomorphisms from $\mathbb{Z}_2^*$ to $\mathbb{Z}/2\mathbb{Z}$.

Proof.
For ε, it is suffice to check 1 and 3.

$$\varepsilon(1 \cdot 1) = 0 = \varepsilon(1) + \varepsilon(1), \quad \varepsilon(1 \cdot 3) = 1 = \varepsilon(1) + \varepsilon(3), \quad \varepsilon(3 \cdot 3) = 0 = \varepsilon(3) + \varepsilon(3).$$

For ω we need to check $a \in \{3, 5\}$ and $b \in \{1, 7\}$, which is similar to before,

$$\omega(a^2) = \omega(b^2) = 0, \quad \omega(ab) = 1, \quad \omega(3 \cdot 5) = \omega(1 \cdot 7) = 0.$$

□

Theorem 2.4.9
Let $\Bbbk = \mathbb{Q}_2$. Write $a = 2^\alpha u$ and $b = 2^\beta v$ with $u, v \in \mathbb{Z}_2^*$. Then,

$$(a, b)_2 = (-1)^{\varepsilon(u)\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)}.$$

Proof.
Again, from the formula, we only need to consider $\alpha, \beta \in 0, 1$. We consider the three cases for α and β.

1. $\underline{\alpha = 0, \beta = 0}$

   Suppose one of u or v is $1 \mod 4$. Then the RHS is 1. Wlog suppose $u \equiv 1 \mod 4$. Then if $u \equiv 1 \mod 8$, then u is a square (Proposition 2.3.2) and $(u, v)_2 = 1$. Else, $u \equiv 5 \mod 8$ and, $uX^2 + vY^2 - Z^2$ has a non-zero root $\bmod 8$, $(1, 2, x)$ with $x = 1$. Then by Corollary 1.4.4, there is a solution in $\mathbb{Q}_2$. And $(u, v)_2 = 1$.

   Suppose both u and v are $3 \mod 4$. Then the RHS is -1. Suppose for a contradiction, $X^2 - uY^2 - vZ^2$ has a non-zero solution, so $X^2 + Y^2 + Z^2$ has a non-zero solution $\bmod 4$. It is an easy computation to see that the only root is $(0, 0, 0)$, a contradiction. So, $(u, v)_2 = -1$.

2. $\underline{\alpha = 1, \beta = 0}$

   The RHS is $(-1)^{\varepsilon(u)\varepsilon(v) + \omega(v)}$. If $v \equiv 1 \mod 8$, v is a square (Proposition 2.3.2) and $(2, v)_2 = 1$. If $v \equiv 7 \mod 8$, $2X^2 + vY^2 - Z^2$ has $(1, 1, 1)$ as a solution $\bmod 8$, hence by Corollary 1.4.4, this lifts to a solution in $\mathbb{Q}_2$. Hence $(2, v)_2 = 1$.

   Now, suppose $(2, v)_2 = 1$, then, $2X^2 + vY^2 - Z^2$ has a non-zero root, then by Proposition 2.2.4, there is a primitive zero in $\mathbb{Z}_p$. In particular, at most one coordinates of the solution are divisible by 2. Hence, there is a non-zero solution $\bmod 2$, say (x, y, z), with $y^2 \equiv z^2 \not\equiv 0 \mod 2$. Going back to $\mathbb{Z}/8\mathbb{Z}$, note that the only squares are 0, 1, 4, and so $y^2 \equiv z^2 \equiv 1 \mod 8$, so $2X^2 + v - 1 \equiv 0 \mod 8$. Computing all cases for X, it follows $v \equiv 1, 7 \mod 8$.

   It follows that $(2, v)_2 = 1$ if and only if $v \equiv 1, 7 \mod 8$. In other words, $(2, v)_2 = (-1)^{\omega(v)}$. Now, by 4 of Proposition 2.4.5, if $(2, v)_2 = 1$ or $(u, v)_2 = 1$, $(2u, v)_2 = (2, v)_2(u, v)_2$. If

$(2,v)_2 = (u,v)_2 = -1$, then by the above and case 1, we must have that $v \equiv 3 \mod 8$ and $u \equiv 3,5 \mod 8$. Thus we have two cases, and it is an easy computation to show that in both cases, $(2u,v)_2 = 1$. Hence, in all cases, $(2,v)_2(u,v)_2 = (2u,v)_2$ also. The correctequation follows by combining the above together.

3. $\underline{\alpha = 1, \beta = 1}$

   The RHS is $(-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)+\omega(u)}$. Now, we know that by 5 of Proposition 2.4.5 and the previous case (since $-uv$ is a unit),

   $$(2u,2v) = (2u,-4uv) = (2u,-uv) = (-1)^{\varepsilon(u)\varepsilon(-uv)+\omega(-uv)}.$$

   Now, noting that $\varepsilon(-1) = 1, \omega(-1) = 0$, and $\varepsilon(u)(1+\varepsilon(u)) = 0$, it follows that

   $$\varepsilon(u)\varepsilon(-uv) + \omega(-uv) = \varepsilon(u)\varepsilon(v) + \omega(v) + \omega(u),$$

   since ε and ω are homomorphisms (Lemma 2.4.8). The result follows. □

Theorem 2.4.10
The Hilbert symbol on $\mathbb{R}$ and $\mathbb{Q}_p$ is bilinear. That is,

$$(a_1a_2,b) = (a_1,b)(a_2,b).$$

Proof.
This is clearly true in $\mathbb{R}$ since a_1a_2 is positive if both a_1 and a_2 have the same sign, and negative otherwise. Now, write $a_1 = p^{\alpha_1}u_1$, $a_2 = p^{\alpha_2}u_2$ and $b = p^{\beta}v$ with $u,v \in \mathbb{Z}_p^*$. Let us consider $p \neq 2$. Then since the Legendre symbol is linear,

$$\begin{aligned}(a_1a_2,b)_p &= (-1)^{(\alpha_1+\alpha_2)\beta\varepsilon(p)}\left(\frac{u_1u_2}{p}\right)^{\beta}\left(\frac{v}{p}\right)^{\alpha_1+\alpha_2}\\ &= (-1)^{\alpha_1\beta\varepsilon(p)}\left(\frac{u_1}{p}\right)^{\beta}\left(\frac{v}{p}\right)^{\alpha_1}(-1)^{\alpha_2\beta\varepsilon(p)}\left(\frac{u_2}{p}\right)^{\beta}\left(\frac{v}{p}\right)^{\alpha_2}\\ &= (a_1,b)_p(a_2,b)_p.\end{aligned}$$

Similarly, for $p = 2$, since ε and ω are homomorphisms (2.4.8),

$$\begin{aligned}(a_1a_2,b)_2 &= (-1)^{\varepsilon(u_1u_2)\varepsilon(v)+(\alpha_1+\alpha_2)\omega(v)+\beta\omega(u_1u_2)}\\ &= (-1)^{\varepsilon(u_1)\varepsilon(v)+\alpha_1\omega(v)+(\beta)\omega(u_1)} + (-1)^{\varepsilon(u_2)\varepsilon(v)+\alpha_2\omega(v)+(\beta)\omega(u_2)}\\ &= (a_1,b)_2(a_2,b)_2.\end{aligned}$$

□

Theorem 2.4.11 (Hilbert's Product Formula)
If $a,b \in \mathbb{Q}^*$. Then, $(a,b)_p = 1$ for almost every prime p, and

$$(a,b)_\infty \prod_{\text{prime } p} (a,b)_p = 1.$$

Proof.
Since the Hilbert symbol is bilinear, it is sufficient to consider a, b primes or -1, since $(1, -1) = 1$, and any non-prime n is a product of primes and -1. Now, consider 3 cases.

1. Let $a = b = -1$. Clearly, $(-1, -1)_\infty = (-1, -1)_2 = 1$. For $p \neq 2$, $(-1, -1)_p = 1$. Hence,

$$(-1, -1)_\infty \prod_{\text{prime } p} (-1, -1)_p = 1.$$

2. Now consider a a prime, and $b = -1$.
   (a) If $a = 2$, clearly, $(2, -1)_\infty = (2, -1)_p = 1$ by considering the solution $(1, 1, 1)$. Hence,

$$(2, -1)_\infty \prod_{\text{prime } p} (2, -1)_p = 1.$$

   (b) Now suppose $a \neq 2$. If $p \neq 2$, $p \neq a$, then $\alpha = \beta = 0$ and $(a, -1) = 1$ by Theorem 2.4.7. If $p = 2$ or $p = a$, then $(a, -1)_2 = (a, -1)_p = (-1)^{\varepsilon(a)}$. Hence,

$$(a, -1)_\infty \prod_{\text{prime } p} (a, -1)_p = (a, -1)_2 (a, -1)_a = (-1)^{2\varepsilon(a)} = 1.$$

3. Now suppose both a and b are primes.
   (a) If $a = b$, then by 6 of Proposition 2.4.5, this reduces to case 2. Thus, consider $a \neq b$.
   (b) Suppose $a = 2$. If $p \neq 2$ and $p \neq b$, then by Theorem 2.4.7 $\alpha = \beta = 0$, and $(2, b) = 1$. If $p = 2$, by Theorem 2.4.9, $\alpha = 1$ and $\beta = 0$. It follows that $(2, b)_2 = (-1)^{\omega(b)}$. If $p = b$, by Theorem 2.4.7, $u = 2$, $\alpha = 0$ and $\beta = 1$. It follows that $(2, b)_p = \left(\frac{2}{b}\right) = (-1)^{\omega(b)}$. Hence,

$$(2, b)_\infty \prod_{\text{prime } p} (2, b)_p = (2, b)_2 (2, b)_b = (-1)^{2\omega(b)} = 1.$$

   (c) Suppose $a \neq 2$ and $b \neq 2$. If $p \neq 2$, $p \neq a$ and $p \neq b$, then by Theorem 2.4.7 $\alpha = \beta = 0$, and $(a, b) = 1$. If $p = 2$, by Theorem 2.4.9 with $\alpha = \beta = 0$, $(a, b)_2 = (-1)^{\varepsilon(a)\varepsilon(b)}$. If $p = a$ or $p = b$, $(a, b)_a = \left(\frac{b}{a}\right)$ and $(a, b)_b = \left(\frac{a}{b}\right)$. Hence, by Quadratic Reciprocity

$$(a, b)_\infty \prod_{\text{prime } p} (a, b)_p = (-1)^{\varepsilon(a)\varepsilon(b)} \left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{2\varepsilon(a)\varepsilon(b)} = 1.$$

□

Corollary 2.4.12
Note that Hilbert's Product Formula is equivalent to Quadratic Reciprocity. Indeed, the previous theorem gives the forward direction.

Proof.
Conversely, suppose Hilbert's Product Formula holds. Let a, b be distinct odd primes. Then, following case 3c, we have that

$$(a,b)_\infty \prod_{\text{prime } p} (a,b)_p = (a,b)_2 (a,b)_a (a,b)_b = (-1)^{\varepsilon(a)\varepsilon(b)} \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = 1.$$

It follows that

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\varepsilon(a)\varepsilon(b)}.$$

□

Remark 2.4.13
The Hilbert Symbol and Hilbert Product Formula can also be extended to number fields (finite field extensions of $\mathbb{Q}_p$). The product formula and quadratic reciprocity are both examples of reciprocity laws. Other reciprocity laws include Kummer reciprocity and Artin reciprocity. These are closely related to Hilbert's ninth problem[1], an unsolved problem in mathematics. The problem is to find a general reciprocity law for a general Hilbert symbol in a number field. David Hilbert stated that solving such a problem will lead to significant progress in the theory of prime power roots of unity.

In the 1920s, Emil Artin made a notable advancement. He established the Artin reciprocity law, which not only opens up its own field of research, but is able to imply all other currently known reciprocity laws. It is also used in the proof of Chebotarev's density theorem, a generalisation of Dirichlet's theorem. It will be interesting to further study this area.

Lemma 2.4.14 (Chinese Remainder Theorem)
Let $a_1, \ldots, a_n \in \mathbb{Z}$ and $m_1, \ldots, m_n \in \mathbb{Z}$ pairwise coprime. Then, there exists $a \in \mathbb{Z}$ such that

$$a \equiv a_i \mod m_i, \quad \text{for all } i.$$

Proof.
See any introductory book on algebra. □

Proposition 2.4.15 (Approximation Theorem)
Let $V = \{v : v \text{ is prime or } \infty\}$ and $S \subset V$ finite. The image of $\mathbb{Q}$ in $\prod_{v \in S} \mathbb{Q}_v$ is dense in this product (for the product topology of those $\mathbb{Q}_v$).

Proof.
Let $S = \{\infty, p_1, \ldots, p_n\}$, where each p_i is a distinct prime. Let

$$(x_\infty, x_1, \ldots, x_n) \in \mathbb{R} \times \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_n} = \prod_{v \in S} \mathbb{Q}_v.$$

By clearing denominators, we can assume each $x_i \in \mathbb{Z}_2 p_i$ for $i \in \{1, \ldots, n\}$. Now we will show that there is a rational number arbitrarily close to each x_i. Let $\varepsilon > 0$ and $N > 0$. Then, by the Chinese

[1] See `https://mathcs.clarku.edu/~djoyce/hilbert/problems.html` for an English version of all Hilbert problems.

Remainder Theorem, with $m_i = p_i^N$ pairwise coprime, there exists$x_0 \in \mathbb{Z}$ such that for all i, $x_0 \equiv x_i \mod p^N$, thus

$$v_{p_i}(x_0 - x_i) \geq N.$$

Now, choose $q \geq 2$ a prime number that is coprime to all p_i. Then, $\{\frac{a}{q^m} : a \in \mathbb{Z},\ m \geq 0\}$ is dense in $\mathbb{R}$ (see any basic book on topology or analysis). Thus, we may choose $u = \frac{a}{q^m}$ such that

$$|x_0 - x_\infty + up_1^N \cdots p^N| \leq \varepsilon.$$

Now, set $x = x_0 + up_1^N \dots p_n^N$. It follows

$$|x - x_\infty| \leq \varepsilon, \quad \text{and} \quad v_{p_i}(x - x_i) \geq N \quad \text{for } i \in \{1, \dots, n\}.$$

The result follows. (Note that the greater v_p is, the smaller $|\cdot|_p$ is.) □

Lemma 2.4.16 (Dirichlet's Theorem)
If $a, m \in \mathbb{Z}$ are coprime, there are infinitely many primes p such that $p \equiv a \mod m$.

Proof.
This is Dirichlet's Theorem. See Chapter 3. Note that the proof does not require anything past this point, and thus there is no circular argument. □

Theorem 2.4.17
Let $I \subset \mathbb{N}$ finite and $V = \{v : v \text{ is prime or } \infty\}$, $\{a_i \in \mathbb{Q}^* : i \in I\}$ and

$$\{\varepsilon_{i,v} \in \{-1, 1\} : i \in I, v \in V\}.$$

Then, there exists $x \in \mathbb{Q}^*$ with $(a_i, x)_v = \varepsilon_{i,v}$ (for all $v \in V$ and $i \in I$) if and only if all the following conditions are satisfied.

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

Proof.
For the forward direction, note that conditions 1 and 2 follow directly from Hilbert's Product Formula. Condition 3 follows if we let $x_v = x$.

Conversely, suppose all three conditions hold. By clearing denominators (multiplying by squares to conserve the Hilbert symbol), we can assume each $a_i \in \mathbb{Z}^*$. Define the following.

$$S = \{\infty, 2, p : p \text{ is prime and } p \mid a_i, \text{ for some } i\}$$

$$T = \{v \in V : \varepsilon_{i,v} = -1, \text{ for some } i \in I\}$$

We consider two cases.

$\underline{S \cap T = \varnothing}$. Let

$$a = \prod_{l \in T \backslash \{\infty\}} l, \quad \text{and} \quad m = 8 \prod_{l \in S \backslash \{2, \infty\}} l.$$

Since $S \cap T = \varnothing$, a and m are relatively prime, and by Dirichlet's Theorem, there exists a prime $p \equiv a \mod m$ (in fact infinitely many), with $p \notin S \cup T$. We claim that $x = ap$ gives $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in V$.

If $v \in S$, $\varepsilon_{i,v} = 1$ since $v \notin T$. If $v = \infty$, then since $x > 0$, $(a_i, x)_\infty = 1$. If $v = l$ a prime, then $x \equiv a^2 \mod m$. Note that $x, a \in \mathbb{Z}_p^*$. If $l = 2$, $x \equiv a^2 \mod 8$ and by $x \equiv 1 \mod 8$ (just check every possible a modulo 8) and by Proposition 2.3.2, x is a square in $\mathbb{Q}_2^*$. Similarly, if $l \neq 2$, $x \equiv a^2 \mod l$ and by Proposition 2.3.1, x is a square in $\mathbb{Q}_l^*$. Hence, in all cases $(a_i, x)_v = 1$.

Now, suppose $v = l \notin S$. Then since $l \neq 2$,

$$(a_i, b)_l = \left(\frac{a_i}{l}\right)^{v_l(b)} \quad \text{for all } b \in \mathbb{Q}_l^*, \tag{2.1}$$

which follows from Theorem 2.4.7 (since a_i is a unit). If $l \notin T \cup \{p\}$, and since $x \in \mathbb{Z}_p^*$, $v_l(x) = 0$. Thus, by Equation 2.1, $(a_i, x)_l = 1 = \varepsilon_{i,l}$. Now, let $l \in T$, so $v_l(x) = 1$. Then, condition 3 says that for all $i \in I$, there is a $x_l \in \mathbb{Q}_l^*$ with $(a_i, x_l)_l = \varepsilon_{i,l}$. Since $l \in T$, one of $\varepsilon_{i,l}$ is -1, so, $v_l(x_l) \equiv 1 \mod 2$ (x_l has odd powers of l). It follows that for all $i \in I$,

$$(a_i, x)_l = \left(\frac{a_i}{l}\right) = (a_i, x_l)_l = \varepsilon_{i,l}.$$

Now, consider $l = p$. Then, by Hilbert's Product Formula and condition 2,

$$(a_i, x)_p = \prod_{v \in V \backslash \{p\}} (a_i, x)_v = \prod_{v \in V \backslash \{p\}} \varepsilon_{i,l} = \varepsilon_{i,p}$$

Hence, $(a_i, x)_v = \varepsilon_{i,l}$ for every $v \in V$ and $i \in I$.

$\underline{S \cap T \neq \varnothing}$. By Proposition 2.3.4, the squares of $\mathbb{Q}_v^*$ are open in $\mathbb{Q}_v^*$. By the Approximation Theorem, the image of $\mathbb{Q}$ meets the open set, and hence there is a $x' \in \mathbb{Q}^*$ such that $\frac{x'}{x_v}$ is a square in $\mathbb{Q}_v^*$ for all $v \in S$. So for all $v \in S$,

$$(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v}.$$

Let $\eta_{i,v} = \varepsilon_{i,v}(a_i, x')_v$, where $(\eta_{i,v} \in \{1, -1\} : i \in I, v \in V)$ satisfies the three conditions. Now since $\eta_{i,v} = 1$ if $v \in S$, we are back in the first case. Thus, there exists $y \in \mathbb{Q}_{p_1}^*$ such that $(a_i, y)_v = \eta_{i,v}$ for all $i \in I$ and $v \in V$. Setting $x = yx'$ gives $(a_i, x)_v = \varepsilon_{i,l}$ for every $v \in V$ and $i \in I$. □

2.5 Invariants

Definition 2.5.1
Let $F = X_1^2 + a_2 X_2^2 + \cdots + a_n X_n^2$ be a quadratic form over $\Bbbk$, with each $a_i \in \Bbbk^*$. Then, the **discriminant** of F is

$$d(F) = a_1 \cdots a_n.$$

The **Hasse invariant** is

$$\varepsilon(F) = \prod_{i<j}(a_i, a_j).$$

Proposition 2.5.2
Let $n \in \mathbb{N} \setminus \{1, 3\}$. Let F be a quadratic form in $\Bbbk[X_1, \ldots, X_n]$, $a \in \Bbbk^*/\Bbbk^{*2}$. Let $d = d(F)$, $\varepsilon = \varepsilon(F)$. Then $F - a$ has a non-zero root if and only if

1. $n = 1$ and $a = d$ (in $\Bbbk^*/\Bbbk^{*2}$),
2. $n = 2$ and $(a, -d) = \varepsilon$,
3. $n = 3$ and either $a \neq -d$ or $a = -d$ and $(-1, -d) = \varepsilon$, or
4. $n \geq 4$.

Proof.
Note that we will only use the case $n = 2$ and $n \geq 4$ in the proof of the Hasse-Minkowski Theorem. See [1] pages 35-38 for a proof of this theorem, and also a discussion on why these are called invariants. □

Lemma 2.5.3
Let F be a quadratic form. Then for any $\mathbf{x} \in \Bbbk^{n*}$,

$$F(\mathbf{x}) = \frac{F(2\mathbf{x}) - 2F(\mathbf{x})}{2}.$$

Proof.
Write $F = a_1X_1^2 + \cdots + a_nX_n^2$ and $\mathbf{x} = (x_1, \ldots, x_n)$, then

$$F(2\mathbf{x}) = 4a_1x_1^2 + \cdots + 4a_nx_n^2 = 4F(\mathbf{x}).$$

Rearranging gets the desired result. □

Lemma 2.5.4
Let F be a quadratic form. Then for any $\mathbf{x}, \mathbf{y} \in \Bbbk^{n*}$ and $b \in \Bbbk$,

$$F(b\mathbf{x} + \mathbf{y}) = b^2F(\mathbf{x}) + F(\mathbf{y}) + b(F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})).$$

Proof.
Write $F = a_1X_1^2 + \cdots + a_nX_n^2$, $\mathbf{x} = (x_1, \ldots, x_n)$, and $\mathbf{y} = (y_1, \ldots, y_n)$, then

$$\begin{aligned} F(\mathbf{x} + \mathbf{y}) &= a_1(x_1^2 + 2x_1y_1 + y_1^2) + \cdots + a_n(x_n^2 + 2x_ny_n + y_n^2) \\ &= F(\mathbf{x}) + F(\mathbf{y}) + 2(a_1x_1y_1 + \cdots + a_nx_ny_n). \end{aligned}$$

Similarly, $F(b\mathbf{x} + \mathbf{y}) = b^2F(\mathbf{x}) + F(\mathbf{y}) + 2b(a_1x_1y_1 + \cdots + a_nx_ny_n)$. Equating and rearranging gets the first result. □

Proposition 2.5.5
Let F a non-zero quadratic form with a non-zero root. Then, F is onto $\Bbbk$.

Proof.
Suppose $F(\mathbf{x}) = 0$ with $\mathbf{x} \in \Bbbk^{n*}$. Let $\mathbf{y} \in \Bbbk^{n*}$ such that $F(\mathbf{x}+\mathbf{y}) \neq F(\mathbf{y})$ (which exists since $\mathbf{x} \neq 0$). Let $a \in \Bbbk$ and define

$$b = \frac{a - F(\mathbf{y})}{F(\mathbf{x}+\mathbf{y}) - F(\mathbf{y})} \in \Bbbk.$$

Then using Lemma 2.5.3 and Lemma 2.5.4,

$$\begin{aligned} F(b\mathbf{x}+\mathbf{y}) &= b^2F(\mathbf{x}) + F(\mathbf{y}) + b(F(\mathbf{x}+\mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})) \\ &= 0 + F(\mathbf{y}) + (a - F(\mathbf{y})) \\ &= a. \end{aligned}$$

Since a was arbitrary, and we constructed $b\mathbf{x}+\mathbf{y} \in \Bbbk^{n*}$, it follows that $F(b\mathbf{x}+\mathbf{y}) = a$, and thus F is onto. □

Corollary 2.5.6
Let G, H be non-zero quadratic forms in at least one variable in $\Bbbk[X_1, \ldots, X_n]$ and $\Bbbk[Y_1, \ldots, Y_m]$ respectively, and let $F = G - H$. Then, F has a non-zero root if and only if there exists $a \in \Bbbk^*$ such that $G - a$ and $H - a$ both have non-zero roots.

Proof.
The converse is obvious. Suppose F has a non-zero root, say $(\mathbf{x}, \mathbf{y})$. Let $a = G(\mathbf{x}) = H(\mathbf{y})$. If $a \neq 0$, we are done. Otherwise, suppose $a = 0$. Then, $G(\mathbf{x}) = 0$, and by Proposition 2.5.5, G is onto. It follows that there is $b \in \Bbbk^*$ such that $H - b$ has a non-zero root, and that b is in the image of G. □

2.6 Hasse-Minkowski Theorem

Theorem 2.6.1 (Hasse-Minkowski)
Let F be a nondegenerate quadratic form over $\mathbb{Q}$. Then F has a non-trivial zero in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{Q}_p$ and $\mathbb{R}$, for all p.

Proof.
The forward direction is obvious. Suppose that F has non-trivial zeros in $\mathbb{Q}_p$ and $\mathbb{R}$. Without loss of generality write

$$F = X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2, \quad a_i \in \mathbb{Z}^* \text{and each } a_i \text{ square free.}$$

We can set $a_1 = 1$ since F has a solution if and only if $a_1^{-1}F$ has a solution. We can multiply through by denominators of each a_i and hence we can consider integer coefficients. And if m is a square factor of a_i, change X_i to $m^{-1/2}X_i$. Consider 4 cases of n: 2, 3, 4, and ≥ 5.

1. $\underline{n = 2}$

   We have $F = X_1^2 - a_2X_2^2$ with a_2 square free. Since F has a non-trivial root in $\mathbb{R}$, $a_2 > 0$. Write

   $$a_2 = \prod_{p \text{ prime}} p^{v_p(a_2)}, \quad v_p \in \{0, 1\}.$$

Let (x_1, x_2) be a non-zero root of F in $\mathbb{Q}_p$. If $x_2 = 0$ then so is x_1, hence $x_2 \neq 0$ and we must have that $a_2 = \frac{x_1^2}{x_2^2}$ a square in $\mathbb{Q}_p$, and so $v_p(a_2) = 0$ for all p. Hence, $a_2 = 1$ in $\mathbb{Q}$, and F has a zero in $\mathbb{Q}$.

2. $\underline{n = 3}$

Write $F = X_1^2 - a_2X_2^2 - a_3X_3^2$, where a_2 and a_3 are non-zero square free integers. Wlog suppose $0 < |a_2|_\infty \leq |a_3|_\infty$. We use strong induction on the value $m = |a_2|_\infty + |a_3|_\infty \geq 2$.

Let $m = 2$. Then, $|a_2|_\infty = |a_3|_\infty = 1$, and so $F = X_1^2 \pm X_2^2 \pm X_3^2$. There are four cases, each satisfying the hypothesis.

(a) $F = X_1^2 + X_2^2 + X_3^2$ has no non-zero solutions in $\mathbb{R}$.
(b) $F = X_1^2 - X_2^2 + X_3^2$ has solution $(1, 1, 0)$.
(c) $F = X_1^2 - X_2^2 - X_3^2$ has solution $(1, 1, 0)$.
(d) $F = X_1^2 + X_2^2 - X_3^2$ has solution $(1, 0, 1)$.

Now, suppose $m > 2$ and that the hypothesis is true for all smaller m. Note that $|a_3|_\infty \geq 2$. Since a_3 is square free, write

$$a_3 = \pm p_1 \cdots p_k = \pm \prod_{p \text{ prime}} p^{v_p(a_3)}, \quad v_p \in \{0, 1\}.$$

We aim to show that a_2 is a square mod a_3 (by the Chinese Remainder Theorem, it is sufficient to show a_2 is a square $\bmod p_i$ for all $i \in \{1, \ldots, k\}$). Let $i \in \{1, \ldots, k\}$ and consider $p = p_i$. If $a_2 \equiv 0 \mod p$, then clearly, a_2 is a square $\bmod p$. Otherwise, a_2 is a p-adic unit. By assumption, there is a $(x_1, x_2, x_3) \in \mathbb{Q}_p^3$ a non-zero root of F. Wlog, by Proposition 2.2.4, (x_1, x_2, x_3) is primitive. Since $p \mid a_3$,

$$x_1^2 = a_2x_2^2 \mod p.$$

If $x_2 = 0 \mod p$, then so is x_1, so $p \mid a_3x_3^2$. Since $v_p(a_3) = 1$, it follows $p \mid x_3$, contradicting primitivity. Hence, $x_2 \neq 0 \mod p$. Thus,

$$a_2 = \frac{x_1^2}{x_2^2} \mod p,$$

in particular, a_2 is a square mod a_3. Write $a_2 = b^2 \mod a_3$ where $|b|_\infty \leq |\frac{a_3}{2}|_\infty$. Then, there exists $c \in \mathbb{Z}$ such that

$$b^2 = a_2 + ca_3.$$

By Lemma 2.4.2, $a_2 = b^2 - ca_3$ implies $(a_2, ca_3) = 1$. Thus, by bilinearity,

$$(a_2, c) = (a_2, a_3), \tag{2.2}$$

where the Hilbert symbols can be in any field (in particular, $\mathbb{Q}_p$, $\mathbb{R}$, and $\mathbb{Q}$). Since $(a_2, a_3)_\infty = (a_2, a_3)_p = 1$, it follows that $X_1^2 - a_2X_2^2 - cX_3^2$ has a non-zero root in $\mathbb{Q}_p$ and $\mathbb{R}$. Now, write

$c = c'u^2$, where c' and u are integers and c' is square free. Then, $X_1^2 - a_2X_2^2 - c'X_3^2$ has a non-zero root in $\mathbb{Q}_p$ and $\mathbb{R}$. Now note that

$$|c'|_\infty \leq |c|_\infty = \left|\frac{b^2 - a_2}{a_3}\right|_\infty \leq \left|\frac{b^2}{a_3}\right|_\infty + \left|\frac{a_2}{a_3}\right|_\infty \leq \frac{|a_3|_\infty}{4} + 1 < |a_3|_\infty, \text{ since } |a_3|_\infty \geq 2.$$

Since $|a_2|_\infty + |c'|_\infty < m$, it follows from the induction hypothesis, $X_1^2 - a_2X_2^2 - c'X_3^2$ has a non-zero root in $\mathbb{Q}$, and so $X_1^2 - a_2X_2^2 - cX_3^2$ has a non-zero root in $\mathbb{Q}$. Thus by Equation 2.2, $X_1^2 - a_2X_2^2 - a_3X_3^2$ has a non-zero root in $\mathbb{Q}$.

3. $\underline{n = 4}$

   Write $F = X_1^2 + a_2X_2^2 - a_3X_3^2 - a_4X_4^2$, where a_2, a_2, and a_3 are non-zero square free integers. Then by Corollary 2.5.6, for $\mathbb{Q}_p$ (respectively $\mathbb{R}$) there exists quadratic forms, $G = X_1^2 + a_2X_2^2$ and $H = a_3X_3^2 + a_4X_4^2$ such that there is a $x_p \in \mathbb{Q}_p^*$ (resp. $x_\infty \in \mathbb{R}$) with $G - x_p$ and $H - x_p$ both having non-zero roots. Now the invariants of G and H are,

   $$\begin{aligned} d(G) &= a_2, & \varepsilon(G) &= (1, a_2), \\ d(H) &= a_3a_4, & \varepsilon(H) &= (a_3, a_4). \end{aligned}$$

   Thus, by Proposition 2.5.2 case 2,

   $$(x_p, -a_2)_p = (1, a_2)_p, \quad \text{and} \quad (x_p, -a_3a_4)_p = (a_3, a_4)_p.$$

   Now by Hilbert's Product Formula,

   $$(1, a_2)_\infty \prod_{p \text{ prime}} (1, a_2)_p = (a_3, a_4)_\infty \prod_{p \text{ prime}} (a_3, a_4)_p = 1$$

   It follows that the conditions for Theorem 2.4.17 are satisfied, thus, there exists $x \in \mathbb{Q}^*$ such that

   $$(x, -a_2)_p = (1, a_2)_p, \quad \text{and} \quad (x, -a_3a_4)_p = (a_3, a_4)_p \quad, \forall p \in \{p : p \text{ is prime or } \infty\}.$$

   Now, the quadratic forms, $G - xZ^2$ and $H - xZ^2$ both have non-zero roots in $\mathbb{Q}_p$ and $\mathbb{R}$ (again by Proposition 2.5.2 case 2). By the proof for $n = 3$, it follows that they also have non-zero roots in $\mathbb{Q}$. Recalling that $F = G - H$, F also has a non-zero root in $\mathbb{Q}$.

4. $\underline{n \geq 5}$

   Now we use induction on n. Write $F = F = X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2$, with each a_i square free. As in the $n = 4$ case, split F into two quadratic forms, $F = G - H$, where $H = X_1^2 + a_2X^2$, and $G = -(a_3X_3^2 + \cdots + a_nx_n^2)$. Let

   $$S = \{2, p, \infty : \exists i \geq 3, v_p(a_i) \neq 0, p \text{ prime}\}.$$

This set is finite since n and each a_i are finite. By assumption, for every $v \in S$, $F - v$ has a non-zero root in each $\mathbb{Q}_v$, so by Corollary 2.5.6, there is a $b_v \in \mathbb{Q}_v^*$ such that $H - b_v$ and $G - b_v$ both have non-zero roots in $\mathbb{Q}_v$. In addition, there exists $x_i^v \in \mathbb{Q}_p$, $i \in \{1, \ldots, n\}$ such that

$$H(x_1^v, x_2^v) = G(x_3^v, \ldots, x_n^v) = b_v.$$

By Proposition 2.3.4, the squares of $\mathbb{Q}_p^*$ form an open set. And by the Approximation Theorem, there exists $x_1, x_2 \in \mathbb{Q}$ such that if $b = H(x_1, x_2)$, then $\frac{b}{b_v} \in \mathbb{Q}_v^{*2}$ for all $v \in S$. Now, consider the quadratic form $F_1 = bZ^2 - G$, where Z is another variable. If $v \in S$, $G - b_v$ has a non-zero root in $\mathbb{Q}_v$. By Proposition 2.5.2 case 4 (since G has $n - 1 \geq 4$ variables), and because $\frac{b}{b_p} \in \mathbb{Q}_v^{*2}$, $G - b$ also has a non-zero root in $\mathbb{Q}_v$. Thus, F_1 has a non-zero root for all $v \in S$.

If $v \notin S$, then all coefficients, $a_3, \ldots a_n$ of G are v-adic units. Thus, the discriminant of G in $\mathbb{Q}_v$, $d_v(G)$, is also a v-adic unit. Since $v \neq 2$, $\varepsilon_v(G) = 1$. It follows that F_1 has non-zero roots in $\mathbb{Q}_v$ for $v \notin S$.

Thus, we have that F_1 has a non-zero root in $\mathbb{Q}_v$ for every $v \in V$. It follows by the induction hypothesis that F_1 must have a non-zero root in $\mathbb{Q}$. Thus, $G - a$ has a root, and F has a non-zero root in $\mathbb{Q}$. □

Remark 2.6.2
Although we are converting a problem in $\mathbb{Q}$ to infinitely many problems in $\mathbb{Q}_p$, it is far easier to solve something in $\mathbb{Q}_p$ since we have Hensel's Lemma (the p-adic analogue of Newton's method).

Example 2.6.3
We will prove that

$$F(X, Y, Z) = X^2 + 3Y^2 - 7Z^2$$

has a non-zero rational root. Note indeed, $(2, 1, 1)$ is a solution, though we shall show this using Hasse-Minkowski and Hensel's Lemma. We consider a few cases.

1. <u>In $\mathbb{R}$</u>

   Clearly, we have a solution since not all coefficients have the same sign (concretely, setting $X = 0, Y = 1$, we have $Z = \sqrt{\frac{3}{7}}$).

2. <u>In $\mathbb{Q}_p$ for $p \notin \{2, 3, 7\}$</u>

   Then by Proposition 2.2.2, there is a non-zero root in $\mathbb{Z}/p\mathbb{Z}$. Call this (x, y, z), so that

   $$x^2 + 3y^2 - 7z^2 \equiv 0 \mod p.$$

   Thus, at least one of x, y, z must not be divisible by p. Suppose that $p \nmid x$. Now let $G(X) = X^2 + 3y^2 - 7z^2$, so that $G'(X) = 2X$. Note that $G(x) \equiv 0 \mod p$, and $G'(x) \not\equiv 0 \mod p$. Now, by Hensel's Lemma, x lifts to a $x' \in \mathbb{Q}_p$, and (x', y, z) is a non-zero root of F in $\mathbb{Q}_p$. If $p \mid x$, then either $p \nmid y$ or $p \nmid z$, and we arrive at a similar conclusion using the same argument.

3. In $\mathbb{Q}_2$

   Consider the non-zero $(x, 1, 0)$, where $x = 1$. Let

   $$G(X) = F(X, 1, 0) = X^2 + 3.$$

   Then, $G'(X) = 2X$, $G(x) \equiv 0 \mod 4$, and $G'(x) \not\equiv 0 \mod 4$. Then by Corollary 1.4.4, there is a non-zero root of G in $\mathbb{Z}/2^n\mathbb{Z}$, for all $n > 2$. Noting that x is also a non-zero root of G in $\mathbb{Z}/2\mathbb{Z}$, it follows that there must be a non-zero root of F in $\mathbb{Q}_2$.

4. In $\mathbb{Q}_3$

   Consider the non-zero $(x, 0, 1)$, where $x = 1$. Let

   $$G(X) = F(X, 0, 1) = X^2 - 7.$$

   Then, $G'(X) = 2X$, $G(x) \equiv 0 \mod 3$, and $G'(x) \not\equiv 0 \mod 3$. Then, by Hensel's Lemma, F this lifts to a the non-zero solution in $\mathbb{Q}_3$.

5. In $\mathbb{Q}_7$

   Similarly, consider the non-zero $(x, 1, 0)$, where $x = 2$. Let

   $$G(X) = F(X, 1, 0) = X^2 + 3.$$

   Then, $G'(X) = 2X$, $G(x) \equiv 0 \mod 7$, and $G'(x) \not\equiv 0 \mod 7$. Then, by Hensel's Lemma, F this lifts to a the non-zero solution in $\mathbb{Q}_3$.

Hence, F has a non-zero root in all $\mathbb{Q}_p$ and $\mathbb{R}$, and thus, by Hasse-Minkowski, F has a non-zero root in $\mathbb{Q}$.

We now give a few tools to help further simplify the problem of the existence of solutions in $\mathbb{Q}_p$.

Proposition 2.6.4
Let F be a quadratic form over $\mathbb{Q}$ in $n \geq 3$ variables. Write

$$F = a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2,$$

with a_i non-zero square free integers as before. Then, for ever $p \nmid (2\prod_{i=1}^n a_i)$, F has a non-trivial zero in $\mathbb{Q}_p$.

Proof.
By Proposition 2.2.2, $F \equiv 0 \mod p$ has a non-trivial solution (since none of the a_i's are divisible by p, and $\mathbb{Z}/p\mathbb{Z}$ is a finite group). Let this solution be $(x_1, \ldots, x_n)$. At least one of the x_i is non-zero $\bmod p$, so wlog, let $x_1 \not\equiv 0 \mod p$. Then, consider $G(X) = F(X, x_2, \ldots, x_n)$. Then $G(x_1) \equiv 0 \mod p$ and $G'(x_1) = 2x_1 \not\equiv 0 \mod p$. By Hensel's Lemma, x lifts to $x' \in \mathbb{Q}_p$ so that $(x', x_2, \ldots, x_n)$ is a non-zero root of F. □

And now, we look at the case where F has 3 variables.

Proposition 2.6.5
Let $a_1, a_2, a_3 \in \mathbb{Z}^*$ be pairwise relatively prime and square-free. Then,

$$F(X,Y,Z) = a_1X^2 + a_2Y^2 + a_3Z^2 = 0$$

has non-trivial solutions in $\mathbb{Q}$ if the following are all satisfied.

1. The a_i do not all have the same sign.
2. For each odd prime $p \mid a_1$, $\left(\frac{-a_2a_3^{-1}}{a_1}\right) = 1$, and similarly for every prime dividing a_2 and a_3.
3. If a_1 is even, then either $a_2 + a_3$ or $a_1 + a_2 + a_3$ is divisible by 8, and similarly for a_2 and a_3.
4. If the a_i are all odd, then there is a $j \neq i$ such that $a_i + a_j \equiv 0 \mod 4$.

Proof.
Condition 1 obviously implies that F has a non-trivial solution in $\mathbb{R}$ (wlog, a_1 and a_2 have different signs, then $(\sqrt{a_1a_2}, a_1, 0)$ is a solution). By Proposition 2.6.4, F has a non-trivial solution in $\mathbb{Q}_p$ for $p \nmid 2a_1a_2a_3$. It remains to show that F has a non-trivial solution in the remaining $\mathbb{Q}_p$, using the other three conditions.

Now, consider $p \mid a_1$, where p is an odd prime. Then, condition 2 says that there is a $r \in \mathbb{Z}$ such that

$$a_2 + r^2a_3 \equiv 0 \mod p.$$

Then, $(1, 1, r)$ is a solution of $F \mod p$. Let $G(Y) = F(1, Y, r) = a_1 + a_2Y^2 + a_3r^2$. Then, $G(1) \equiv 0 \mod p$ and $G'(1) = 2a_2 \not\equiv 0 \mod p$ (since a_1 and a_2 are relatively prime). Thus, by Hensel's Lemma, G and thus F has a non-zero solution in $\mathbb{Q}_p$. Exchanging the roles of a_1 with a_2 then a_3 yields a solution for every $p \mid a_i$.

Finally, we consider $\mathbb{Q}_2$. If the a_i are all odd, then condition 4 holds. Wlog, let

$$a_1 + a_2 \equiv 0 \mod 4.$$

Let $G(X) = a_1X^2 + a_2$. Then, $G(1) \equiv 0 \mod 4$ and $G'(1) = 2a_1 \not\equiv 0 \mod 4$. Then by Corollary 1.4.4, there is a non-zero root of F in $\mathbb{Q}_2$.

If a_1 is even, then condition 3 says that either $a_2 + a_3$ or $a_1 + a_2 + a_3$ is divisible by 8. One of a_2 or a_3 must not be even, wlog say $2 \nmid a_2$. Then, if

$$a_2 + a_3 \equiv 0 \mod 8,$$

let $G(Y) = a_2Y^2 + a_3$. It follows, $G(1) \equiv 0 \mod 4$ and $G'(1) = 2a_2 \not\equiv 0 \mod 4$. Then by the same reasoning as in the previous paragraph, it follows that there must be a non-zero root of F in $\mathbb{Q}_2$. On the other hand, if

$$a_1 + a_2 + a_3 \equiv 0 \mod 8,$$

let $G(Y) = F(1, Y, 1) = a_1 + a_2Y^2 + a_3$. Then, $G(1) \equiv 0 \mod 8$ and $G'(1) = 2a_2 \not\equiv 0 \mod 8$ (since a_2 is not even). By Corollary 1.4.4, G and F have non-zero roots in $\mathbb{Q}_2$.

Thus, given the conditions, F has solutions in $\mathbb{Q}_p$ and $\mathbb{R}$. Hence by Hasse-Minkowski, F has a solution in $\mathbb{Q}$. □

Remark 2.6.6
In fact, the conditions in Proposition 2.6.5 are also necessary. See [2] (page 83) for details. Hence for any quadratic form in three variables, the above conditions determine whether the form as a non-trivial solution in $\mathbb{Q}$.

Example 2.6.7
Revisiting $F(X, Y, Z) = X^2+3Y^2-7Z^2$, it is clear that all conditions of the previous proposition are satisfied, and thus F has a non-trivial solution in $\mathbb{Q}$. In fact, in the calculations done in Example 2.6.3 were all specific cases of the proof of Proposition 2.6.5.

Remark 2.6.8
The Hasse-Minkowski Theorem cannot be extended to polynomials of higher degrees. For example, the cubic form,

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

has non-trivial solutions in each $\mathbb{Q}_p$ and $\mathbb{R}$, but none in $\mathbb{Q}$. Hensel's Lemma can be used to show that F has non-trivial roots locally. For a detailed discussion by Selmer on the lack of roots on $\mathbb{Q}$, see [6] page 205.

Remark 2.6.9
We have seen how useful the Hasse-Minkowski theorem is. This is a special case of the Hasse principle, which is basically the principle of being able to move between local and global solutions. We proved the case of quadratic forms between $\mathbb{Q}$ and $\mathbb{Q}_p$, $\mathbb{R}$. Following a similar proof, and discussion on number fields, one can reach Hasse's conclusion that quadratic forms have a solution in a number field (finite field extension) if and only if it has a solution locally at all places. Note that the places of $\mathbb{Q}$ are $\mathbb{Q}_p$ and $\mathbb{R}$. Further study can take place by investigating the Brauer group. The Brauer-Manin obstruction can sometimes explain why the Hasse principle does not hold. See [11].

2.7 An Application

Here is an example of where the p-adic numbers are useful outside of number theory.

Theorem 2.7.1 (Monsky's Theorem)
A square cannot be dissected into an odd number of triangles of equal area.

(See [4] for a detailed explanation. We sketch a proof here.)

Sketch proof.
Wlog, suppose it is the unit square of area 1. Label the vertices this square as $(0, 0)$, $(1, 0)$, $(0, 1)$, $(1, 1)$. Dissect the square into triangles. Call a vertex the corners of each triangle (which includes the corners of the square).

1. A Sperner colouring is where we label each vertex with one of three colours, a, b, and c, in such a way:

    (a) No edge of any triangle or the square contain vertices of all 3 colours.

(b) Only one edge of the square contains both colour a and c.

Then, Sperner's Lemma ([4], Lemma 2) states that given a Sperner colouring, there is at least one triangle that has vertices of the 3 different colours.

2. Given a point in the square, say (x, y), we give it a colour (either a,b,c) based on the following.

   a if $v_2(x) > 0$ and $v_2(y) > 0$,
   b if $v_2(x) \leq 0$ and $v_2(x) \leq v_2(y)$,
   c if $v_2(y) \leq 0$ and $v_2(y) < v_2(x)$.

   By Chevalley ([4], Page 136), we extend this valuation on $\mathbb{Q}$ to $\mathbb{R}$.

   We claim that if (x_0, y_0) has colour a, then (x_1, y_1) and $(x_1, y_1)-(x_0, y_0)$ have the same colour. To show this, first note that $v_2(x_0) > 0$. We use Proposition 1.2.4. If $v_2(x_1) > 0$, then

   $$v_2(x_1 - x_0) \geq \min\{v_2(x_1), v_2\} > 0.$$

   If $v_2(x_1) \leq 0$, then

   $$v_2(x_1 - x_0) \geq \min\{v_2(x_1), v_2\} = v_2(x_1).$$

   A similar argument works for the second coordinate. Hence, in both cases, (x_1, y_1) and $(x_1, y_1) - (x_0, y_0)$ have the same colour.

   We also claim that any three collinear points on $\mathbb{R}^2$ (regardless of the dissection) does not use all three colours. To prove this, consider three points, A, B, and C with corresponding colours a, b, c respectively. We wish to show these aren't collinear, that is, $B - A = (x_1, y_1)$ and $C - A = (x_2, y_2)$ are not parallel. Consider the matrix,

   $$M = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}.$$

   Then, $\det M = x_1y_2 - x_2y_1$. By the previous claim, $B - A$ has colour b, and $C - A$ is c. So, $v_2(y_2) < v_2(x_2)$ and $V_2(x_1) \leq v_2(y_2)$. Hence, $v_2(x_1y_2) < v_2(x_2y_1)$ and by Proposition 1.2.4,

   $$v_2(\det M) = \min\{v_2(x_1y_2), v_2(x_2y_1)\} \leq 0 < \infty.$$

   It follows $\det M \neq 0$, and thus the three points are not collinear.

3. Let n be odd and consider a dissection with n triangles of equal area. Note by the first claim that no side of the square or triangles have all three colours. Then, $(0, 0)$ has colour a, $(0, 1)$ is c, and both $(1, 0)$ and $(0, 1)$ are b. It can be shown that there are an odd number of edges with endpoints of colour a and c.

   By Sperner's lemma, there is a triangle with vertices of the three different colours, call these A, B and C. Now, modifying the proof of the second claim, it can be shown using Cartesian geometry, the area of the triangle with vertices A, B, and C, has area

   $$V = \frac{x_1y_2 - x_2y_1}{2} = \frac{\det M}{2}.$$

Thus,

$$v_2(V) = v_2\left(\frac{\det M}{2}\right) \leq -1$$

Since the area of the square is 1, each triangle has area $\frac{1}{n}$, but as n is odd,

$$v_2(V) = v_2\left(\frac{1}{n}\right) = 0$$

A contradiction. Hence n must be even. □

Chapter 3

Dirichlet's Theorem

3.1 Motivation

We start by presenting this famous theorem and proof by Euclid.

Theorem 3.1.1
There are infinitely many primes.

Proof.
Suppose for a contradiction that there are finitely many primes. Let these be $p_1, p_2, \ldots, p_n$. Let $N = p_1 p_2 \cdots p_n + 1 \geq 2$. Then, there exists a prime $q \mid N$. Since we assumed there are finitely many primes, $q = p_i$ for some i. Then, we have

$$q \mid N \quad \text{and} \quad q \mid p_1 \cdots p_n.$$

It follows that $q \mid (N - p_1 \cdots p_n) = 1$. But there are no primes dividing 1, a contradiction. Thus there must by infinitely many primes. □

Lemma 3.1.2
If $N \equiv 3 \mod 4$, then there is a prime $q \mid N$ such that $q \equiv 3 \mod 4$.

Proof.
Suppose not. Then, for every prime $q \mid N$, $q \equiv 1 \mod 4$. Then, $N \equiv 1 \mod 4$. □

We modify Euclid's proof.

Theorem 3.1.3
There are infinitely many primes of the form $p \equiv 3 \mod 4$.

Proof.
Suppose for a contradiction that there are finitely many primes of the form $p \equiv 3 \mod 4$. Let these be $p_1, p_2, \ldots, p_n$. Let $N = 4p_1 p_2 \cdots p_n - 1 \geq 2$ with $N \equiv 3 \mod 4$. Then, there exists a prime $q \mid N$ such that $q \equiv 3 \mod 4$ by the lemma. Since we assumed there are finitely many primes $p \equiv 3 \mod 4$, $q = p_i$ for some i. Then, we have

$$q \mid N \quad \text{and} \quad q \mid 4p_1 \cdots p_n.$$

It follows that $q \mid (N - 4p_1 \cdots p_n) = -1$. But there are no primes dividing -1, a contradiction. Thus there must by infinitely many primes. □

The logical next step is to ask the question: for every $a, d \in \mathbb{N}$ coprime, are there infinitely many primes in the set $\{a + nd : n \in \mathbb{N}\}$? This is Dirichlet's Theorem. As in [7] (Theorem 7), we cannot create a "Euclid type proof" for every a, d (the condition given in [7] is that $a^2 \not\equiv 1 \mod d$). Thus, we need to prove Dirichlet's Theorem using other means. To do this, we need to first take a look at L-functions.

3.2 Dirichlet L-Functions

3.2.1 Dirichlet Characters

Definition 3.2.1
A **Dirichlet character** $\bmod n$ is a function $\chi : \mathbb{Z} \to \mathbb{C}$ such that $\chi|_{(\mathbb{Z}/n\mathbb{Z})^*} \to \mathbb{C}^*$ is a homomorphism and $\chi(m) = 0$ if $\gcd(m, n) > 1$. These characters form a cyclic group with $\varphi(n)$ elements (see the remark).

If the homomorphism is the identity, we define the character χ_1, the principal character $\mod n$, as

$$\chi_1(a) = \begin{cases} 0 & \text{if } a \equiv 0 \mod n, \\ 1 & \text{otherwise.} \end{cases}$$

Remark 3.2.2
In fact, the group of characters is dual to $(\mathbb{Z}/n\mathbb{Z})^*$. See [3] pages 214-216.

Proposition 3.2.3
A Dirichlet character maps $(\mathbb{Z}/n\mathbb{Z})^*$ to the $\varphi(n)$-th roots of unity in $\mathbb{C}^*$.

Proof.
Let g be a generator of $(\mathbb{Z}/n\mathbb{Z})^*$. Since χ is a homomorphism,

$$\chi(1) = \chi(g^{\varphi(n)}) = \chi(g)^{\varphi(n)} = 1.$$

□

Proposition 3.2.4 (Orthogonality relations)
Let χ be a character $\bmod n$. Then,

$$\sum_{i=1}^{n} \chi(i) = \begin{cases} \varphi(n) & \text{if } \chi = \chi_1, \\ 0 & \text{otherwise,} \end{cases} \qquad \text{and} \qquad \sum_{\chi}^{\varphi(n)} \chi(i) = \begin{cases} \varphi(n) & \text{if } i \equiv 1 \mod m, \\ 0 & \text{otherwise.} \end{cases}$$

Proof.
If $\chi = \chi_1$, then the sum is counting the elements in the group $(\mathbb{Z}/n\mathbb{Z})^*$, which has $\varphi(n)$ elements. If $\chi \neq \chi_1$, choose $a \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\chi(a) \neq 1$. Then,

$$\chi(a) \sum_{i=1}^{n} \chi(i) = \sum_{i=1}^{n} \chi(a)\chi(i) = \sum_{i=1}^{n} \chi(ai) = \sum_{i=1}^{n} \chi(i),$$

since group multiplication is a bijection. So, $(\chi(a)-1)\sum_{i=1}^{n}\chi(i)=0$, and since $\chi \neq \chi_1$,

$$\sum_{i=1}^{n}\chi(i)=0.$$

The second relationship follows in a similar fashion. If $i \equiv 1 \mod n$, the sum counts the number of characters, $\varphi(n)$. If $i \not\equiv 1 \mod n$, choose χ' such that $\chi'(n) \neq 1$. Then,

$$\chi'(i)\sum_{\chi}^{\varphi(n)}\chi(i)=\sum_{\chi}^{\varphi(n)}\chi'(i)\chi(i)=\sum_{\chi}^{\varphi(n)}\chi'\chi(i)=\sum_{\chi}^{\varphi(n)}\chi(i),$$

since the χ's form a cyclic group. The result follows. □

3.2.2 Dirichlet Series

Definition 3.2.5
From now on, let $a, d \in \mathbb{N}$ coprime and write

$$P_{a,d}=\{a+nd : n \in \mathbb{N}\}.$$

We will also consider characters, $\chi \bmod d$.

Definition 3.2.6
Let $s \in \mathbb{C}$. Then

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

is a **Dirichlet Series**. Define a **Dirichlet L-function** as

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

on its domain of convergence.

Proposition 3.2.7
$L(s,\chi)$ converges absolutely for $\Re(s)>1$ and

$$L(s,\chi)=\prod_{p}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}.$$

Proof.
$L(s,\chi)$ converges absolutely since χ is bounded, and $\sum_{n=1}^{\infty}\frac{1}{n^t}$ converges for $t>1$. To prove the other claim, first note that if S is a finite set of prime numbers, and $N(S)$ the set of natural numbers whose prime factors belong to S. Then, since $\chi(nm)=\chi(n)\chi(m)$,

$$\sum_{n\in N(S)}\frac{\chi(n)}{n^s}=\prod_{p\in S}\left(\sum_{m=0}^{\infty}\chi(p^m)p^{-ms}\right).$$

Letting S increase to the set of all primes, and rearranging the sum (which is possible because of absolute convergence), $N(S) \to \mathbb{N}$, and we get,

$$\begin{aligned} L(s,\chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \\ &= \prod_p \left(\sum_{m=0}^{\infty} \chi(p^m) p^{-ms} \right) \\ &= \prod_p \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} \end{aligned}$$

Where the last equality is possible since for $\Re(s) > 1$, $|\chi(p)p^{-s}| = |p^{-s}| \leq |2^{-s}| < 1$. □

Corollary 3.2.8

$$L(s,\chi) = \prod_{p \nmid d} \left(1 - \frac{\chi(p)}{p^s} \right)^{-1}.$$

Proof.
Since $\chi(p) = 0$ for all $p \mid d$, the result follows. □

Lemma 3.2.9

$$\lim_{s \to 1} \sum_p p^{-s} = -\lim_{s \to 1} \log(s-1)$$

Proof.
This is proved by looking at the Riemann Zeta function. See [1] page 70. □

Lemma 3.2.10
$\sum_p \sum_{n \geq 2} \frac{\chi(p)^n}{np^{ns}}$ is bounded.

Proof.
This is also proved by looking at the Riemann Zeta function. See [1] page 70. □

Theorem 3.2.11
If $\chi \neq \chi_1$, then $L(1,\chi) \neq 0$.

Proof.
To prove this requires a lot of background (such as Abel summations) which i out of the scope of this paper. Refer to [1] pages 64-73 for details. □

Lemma 3.2.12

$$-\lim_{s \to 1} \log(s-1) = \sum_{p \nmid d} \frac{\chi_1(p)}{p^s}.$$

Proof.
Since

$$\sum_{p\nmid d} \frac{\chi_1(p)}{p^s} = \sum_{p\nmid d} p^{-s}$$

differs from $\sum_p p^{-s}$ by a finite number of terms, taking the limit $s \to 1$ and using 3.2.9,

$$\lim_{s\to 1} \sum_{p\nmid d} \frac{\chi_1(p)}{p^s} = \lim_{s\to 1} \sum_p p^{-s} = -\lim_{s\to 1} \log(s-1).$$

□

Lemma 3.2.13
$\lim_{s\to 1} \sum_{p\nmid d} \frac{\chi(p)}{p^s}$ is bounded for $\chi \neq \chi_1$.

Proof.
Let $\chi \neq \chi_1$. Define the logarithm for x such that $|x| < 1$ in the usual way:

$$\log \frac{1}{1-x} = \sum_{n=1}^{\infty} \frac{x^n}{n}.$$

Then, for $\Re(s) > 1$, $|\chi(p)p^{-s}| = |p^{-s}| \leq |2^{-s}| < 1$, so

$$\begin{aligned}
\log L(s,\chi) &= \log \prod_{p\nmid d} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} && \text{(Proposition 3.2.7)}\\
&= \sum_{p\nmid d} \log \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}\\
&= \sum_{p\nmid d} \sum_n \frac{\chi(p)^n}{np^{ns}}\\
&= \sum_{p\nmid d} \frac{\chi(p)}{p^s} + \sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}.
\end{aligned}$$

Now, $\log L(s,\chi)$ is bounded by Theorem 3.2.11. Also the boundedness of $\sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}$ follows from Lemma 3.2.10. Hence $\sum_{p\nmid d} \frac{\chi(p)}{p^s}$ is bounded. □

Lemma 3.2.14

$$\sum_{p\in P_{a,d}} p^{-s} = \varphi(d)^{-1} \sum_{\chi} \left(\chi(a)^{-1} \sum_{p\nmid d} \frac{\chi(p)}{p^s}\right).$$

Proof.

$$\begin{aligned}
\varphi(d)^{-1}\sum_{\chi}\left(\chi(a)^{-1}\sum_{p\nmid d}\frac{\chi(p)}{p^s}\right) &= \varphi(d)^{-1}\sum_{p\nmid d}p^{-s}\sum_{\chi}\left(\chi(a)^{-1}\chi(p)\right)\\
&= \varphi(d)^{-1}\sum_{p\nmid d}p^{-s}\sum_{\chi}\left(\chi(a^{-1}p)\right)\\
&= \begin{cases}\sum_{p\nmid d}p^{-s} & \text{if } a^{-1}p\equiv 1 \mod d\\ 0 & \text{otherwise}\end{cases}\\
&= \sum_{p\in P_{a,d}}p^{-s},
\end{aligned}$$

where the second to last equality follows from Proposition 3.2.4, and swapping sums is possible because of absolute convergence. □

3.3 Dirichlet's Theorem

We now have the tools to prove Dirichlet's Theorem. Let P be the set of prime numbers.

Definition 3.3.1
Let $A\subset P$. Then, the **density** (call this k) of A is

$$k=\lim_{s\to 1}\frac{\sum_{p\in A}\frac{1}{p^s}}{\sum_{p\in P}\frac{1}{p^s}}=\lim_{s\to 1}\frac{-1}{\log(s-1)}\sum_{p\in A}\frac{1}{p^s},$$

so that $0\le k\le 1$. Roughly speaking, this is to say that the density of A is the size of A by the size of P.

Theorem 3.3.2 (Dirichlet's Theorem)
$P_{a,d}$ has density $\frac{1}{\varphi(d)}$.

Proof.
Let χ be a character $\mathrm{mod}\ d$. Then, we have

$$\lim_{s\to 1}\sum_{\chi}\left(\chi(a)^{-1}\sum_{p\nmid d}\frac{\chi(p)}{p^s}\right)=\lim_{s\to 1}\chi_1(a)^{-1}\sum_{p\nmid d}\frac{\chi_1(p)}{p^s}=-\lim_{s\to 1}\log(s-1),$$

since the limit of the sum over $p\nmid d$ is bounded if $\chi\neq\chi_1$ (Lemma 3.2.13), and goes to $-\log(s-1)$ if $\chi=\chi_1$ (Lemma 3.2.12). We also used the fact $\chi_1(a)=1$ (since a and d are coprime). Hence, we have that by Lemma 3.2.14,

$$\lim_{s\to 1}\sum_{p\in P_{a,d}}p^{-s}=\lim_{s\to 1}\varphi(d)^{-1}\sum_{\chi}\left(\chi(a)^{-1}\sum_{p\nmid d}\frac{\chi(p)}{p^s}\right)=-\lim_{s\to 1}\log(s-1)\varphi(d)^{-1}.$$

It follows that

$$k = \lim_{s\to 1} \frac{-1}{\log(s-1)} \sum_{p\in P_{a,d}} p^{-s} = \varphi(d)^{-1}.$$

□

Corollary 3.3.3
For every $a, d \in \mathbb{N}$ coprime, the set $P_{a,d}$ is infinite, that is, there are infinitely many primes of the form $a + nd$, where $n \in \mathbb{N}$.

Proof.
Since a finite set has density 0, the result follows. □

Remark 3.3.4
Many beautiful theorems can come out of Dirichlet's Theorem, such as for $a \in \mathbb{Z}$ (non-square), the set $\{p \text{ prime} : \left(\frac{a}{p}\right) = 1\}$ has density $\frac{1}{2}$ (see [1] page 75). It is of course also used in the proof of 2.6.1. Another extension of Dirichlet's is the Green-Tao theorem (see [10]), which states that any $P_{a,d}$, when ordered, contains arbitrarily long sequences of primes. Future research will be to digest this proofs, and also to investigate further applications of Dirichlet's Theorem.

References

[1] Jean-Pierre Serre, *A Course in Arithmetic*, Springer GTM 7 (1973)

[2] Fernando Q. Gouvêa, *p-adic Numbers: An Introduction*, Springer (1997)

[3] Graham Everest, Thomas Ward, *An Introduction to Number Theory*, Springer GTM 232 (2005)

[4] Martin Aigner, Günter M. Ziegler, *One square and an odd number of triangles*, Proofs from THE BOOK, p 131-138, Springer (2010)

[5] Keith Conrad, *Ostrowski for number fields* (2010)

[6] Ernst S Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$ Acta Mathematica 85.1, p 203-362 (1951).

[7] Ram Murty, Nithum Thain, *Primes in certain arithmetic progressions*, Functiones et Approximatio Commentarii Mathematici 35, p 249-259 (2006)

[8] Saunders MacLane, *Homology*, Springer (1995)

[9] Stephen Willard, *General topology*, Dover Publications (2004)

[10] Ben Green, Terence Tao,*The Primes Contain Arbitrarily Long Arithmetic Progressions*, Annals of Mathematics, vol. 167, no. 2, p 481547 (2008)

[11] Alexei Skorobogatov, *Beyond the Manin obstruction*, Inventiones mathematicae 135.2, p 399-424 (1999)