COMPUTATIONS IN p-ADIC DISCRETE DYNAMICS AND REAL QUADRATIC FIELDS

Thesis

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

SUSHMA PALIMAR

DEPARTMENT OF MATHEMATICAL AND COMPUTATIONAL SCIENCES
NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA
SURATHKAL, MANGALORE - 575 025

JUNE 2012

DECLARATION

by the Ph.D. Research Scholar

I hereby ***declare*** that the Research Thesis entitled **COMPUTATIONS IN p- ADIC DISCRETE DYNAMICS AND REAL QUADRATIC FIELDS** which is being submitted to the ***National Institute of Technology Karnataka, Surathkal*** in partial fulfillment of the requirements for the award of the Degree of ***Doctor of Philosophy*** in **Mathematics** is a ***bonafide report of the research work carried out by me***. The material contained in this Research Thesis has not been submitted to any University or Institution for the award of any degree.

MA08F03 **Sushma Palimar**

(Register Number Name Signature of the Research Scholar)

Department of Mathematical and Computational Sciences

Place: NITK - Surathkal

Date:

CERTIFICATE

This is to *certify* that the Research Thesis entitled **COMPUTATIONS IN p-ADIC DISCRETE DYNAMICS AND REAL QUADRATIC FIELDS** submitted by **Ms. Sushma Palimar (Register Number: MA08F03)** as the record of the research work carried out by her, is *accepted as the Research Thesis submission* in partial fulfillment of the requirements for the award of degree of **Doctor of Philosophy**.

Dr. B. R. Shankar
Research Guide

Dr. S. M. Hegde
Chairman - DRPC

Acknowledgement

I owe my most sincere gratitude to my guide Dr. B. R. Shankar for considering me as his research student. I thank all faculty members, staff and research students of the Department of Mathematical and Computational Sciences, for their kind and sincere support throughout my work. I am grateful to the former Head of the Department Prof. A. Kandasamy and the present Head of the Department Prof. S. M. Hegde for encouraging me to attend various conferences and workshops, which in turn helped me to understand the current research trends. I sincerely thank my research panel members Prof. K. P. Halemane and Prof. U. Sripati for their valuable suggestions and excellent advice in accomplishing this work. I also acknowledge, with gratitude, *National Institute of Technology Karnataka, Surathkal* for providing financial support throughout my research work.

Abstract

The field of rational numbers $\mathbb{Q}$ is neither complete nor algebraically closed. There is no finite extension of $\mathbb{Q}$ which is algebraically closed. Completions of $\mathbb{Q}$ with respect to p-adic absolute values are the fields of p-adic numbers $\mathbb{Q}_p$. The thesis consists of two parts: p-adic dynamics and real quadratic fields. The first part deals with the p-adic discrete dynamical systems. Two concepts of classical discrete dynamical systems are studied in the context of p-adic fields. Firstly, the notion of topological conjugacy for the p-adic analog of the logistic map and the quadratic map is studied. Secondly, the notion of p-adic backward dynamics for the same maps have also been studied.

In the second part the notion of Mersenne primes has been extended to real quadratic fields with class number 1. Computational results are given. The field $\mathbb{Q}(\sqrt{2})$ is studied in detail with a focus on representing Mersenne primes in the form $x^2 + 7y^2$. It is also proved that x is divisible by 8 and $y \equiv \pm 3 \pmod 8$ generalizing the result of F. Lemmermeyer, first proved by H. W. Lenstra and P. Stevenhagen using Artin's reciprocity law.

Contents

List of Tables

List of Figures

God made integers, all else is the work of man.

Leopold Kronecker

Chapter 1

Introduction

This thesis consists of two parts: p-adic dynamics and real quadratic fields. It is natural to have accumulated truncation errors or round-off errors in a dynamical system even with a small perturbation. These are unavoidable since even with simple repetitive operations, the number of digits of the result can increase so much that the result cannot be held fully in the registers available in the computer. Such errors accumulate one after another from iteration to iteration originating fresh errors. These difficulties motivated to look for an alternate number system which possesses the best features as well as the advantages of both the p-ary and residue number system. Such a number system is the p-adic number system, $\mathbb{Q}_p$, discovered by Kurt Hensel in the late nineteenth century in order to study the properties of algebraic numbers.

Hensel's original description of the p-adic numbers involved an analogy between the ring of integers and the ring of polynomials over the complex numbers, the crux of which was the development of a representation of rational numbers analogous to that of Laurent expansions of rational functions namely, the p-adic expansion. In other words, Hensel sought an analogy between the theory of analytic functions and the rational numbers. Instead of constructing a Taylor series centered at a particular point to obtain local information about an analytic function at the particular point Hensel wrote rational numbers as a sum of powers of a prime number to obtain local information at the *prime*. This idea was motivated by the existence of expansions of

rational numbers with respect to a p-scale:

$$x = \sum_{n=-\infty}^{k} \alpha_n p^n, \qquad \alpha_n = 0, ..., p-1.$$

Such manipulations with rational numbers and series generated the idea that there exists some algebraic structure similar to the system of real numbers $\mathbb{R}$. Thus each $\mathbb{Q}_p$ has the structure of a number field. In fact, the fields of p-adic numbers $\mathbb{Q}_p$ were the first examples of infinite fields that differ from $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and corresponding fields of rational functions.

The p-adic numbers have played a fundamental role in number theory and algebra, and are now finding wider applications in science. In particular, p-adic numbers are useful in investigations of some number-theoretical problems in the field of rational numbers $\mathbb{Q}$. A well-known fact in number theory is that the only non-Archimedean valuations on $\mathbb{Q}$ up to exponentiation are the trivial valuation $|\cdot|_1$ such that $|x|_1 = 1$ for nonzero x, and the p-adic valuation $|\cdot|_p$ defined by $|p^k x|_p = p^{-k}$ where p divides neither the numerator nor the denominator of x.

Real numbers allow only complex numbers as an algebraic extension. For p-adic numbers algebraic extensions of arbitrary dimension are possible. There is no suitable notion of measure on the p-adic analogue of $\mathbb{C}$ because it is not locally compact. The way around this is to use the reduction homomorphism to translate the problem into one of dynamics over $\mathbb{F}_p$.

In Chapter 2 some definitions and background to p-adic numbers are given.

Chapter 3 deals with the study of one-dimensional dynamical systems as a background to the next chapter. Iterating one-dimensional maps has a very long history. After all, to construct an accurate calendar, the Babylonians had to consider (in modern terminology) a rotation of the circle and give a precise estimate for its angle α of rotation based on a piece of its orbit. For this they and later the Greeks considered the line $(t, t\alpha)$ in the plane and developed a continued fraction algorithm

to estimate its slope α. Ever since, continued fractions have played an important role in mathematics and in particular in number theory.

Dynamical systems occur in all branches of science from the differential equations of classical mechanics to physics to the difference equations of mathematical economics and biology. Dynamical systems theory is a classical branch of mathematics which began with Newton around 1665. It provides mathematical models for systems which evolve in time according to a rule, originally expressed in analytical form as a system of ordinary differential equations. These models are called *continuous dynamical systems*. They are also called flows, as the points of the system evolve by flowing along continuous curves.

In the 1880s, Poincaré studied continuous dynamical systems in connection with a prize competition on the stability of the solar system. He found it convenient to replace the continuous flow of time with a discrete analogue, in which time increases in regular, saltatory jumps. These systems are now called discrete dynamical systems. So, for over a century, dynamical systems have come in two flavors: continuous and discrete. Discrete dynamical systems are usually expressed as the iteration of a map (also called an endomorphism) of a space into itself. In these systems, points of the system jump along dotted lines with a regular rhythm.

The mathematical tools that are used in this theory come from different and beautiful branches of mathematics: number theory, topology, ergodic theory, complex analysis, real analysis, general dynamical systems and foliation theory, to name a few.

In chapters 4 and 5 two instances of dynamical systems are studied over p-adic integers, viz., topological conjugacy of quadratic map and backward dynamics of quadratic map with a special focus on the p-adic analog of the standard logistic map. Hensel's Lemma aims at providing solutions to these problems.

The application of completion of $\mathbb{Q}$ with respect to p-adic metric is considered in the previous chapters. The next part of the thesis consists of two chapters with some

definitions of Algebraic number fields and a special focus on real quadratic fields in the last chapter. The fundamental theorem of algebra states that the algebraic closure of the field of real numbers is the field of complex numbers. The algebraic closure of $\mathbb{Q}$, i.e. the field of roots of rational polynomials, is the algebraic numbers. Kummer $(1810-1893)$, Kronecker$(1823-1891)$ and Dedekind $(1831-1916)$ may be considered to be the inventors of modern algebraic number theory. The subject arose basically from the need to solve one particular problem in number theory - Fermat's last theorem. Historically, the desire to generalize Gauss's quadratic reciprocity law, use of arithmetic of cyclotomic fields led to the invention of Algebraic Number Theory.

In the last chapter, the concept of Mersenne primes is studied in real quadratic fields with class number 1. Computational results are given. The field $\mathbb{Q}(\sqrt{2})$ is studied in detail with a focus on representing Mersenne primes in the form x^2+7y^2. It is also proved that x is divisible by 8 and $y \equiv \pm 3 \pmod 8$ generalizing the result of F. Lemmermeyer, first proved by H. W. Lenstra and P. Stevenhagen using Artin's reciprocity law.

Chapter 2

p-adic Numbers

The field of rational numbers is of central importance in physics and mathematics. It is well known that all results of measurements belong to $\mathbb{Q}$, i.e., the irrational numbers cannot be "measured". From a mathematical point of view $\mathbb{Q}$ is the simplest infinite number field. Completion of $\mathbb{Q}$ with respect to the usual absolute value gives the field of real numbers $\mathbb{R}$. Algebraic closure of $\mathbb{R}$ leads to the field of complex numbers $\mathbb{C}$. Although experimental results are given in $\mathbb{Q}$, theoretical models are usually constructed over $\mathbb{R}$ or $\mathbb{C}$. However, it is interesting that in addition to the standard absolute value there exist p-adic norms (valuations) on $\mathbb{Q}$.
An absolute value on a field $\mathbb{F}$ is a group homomorphism:

$$|\cdot| : \mathbb{F}^* \to \mathbb{R}_{>0}$$

where, $\mathbb{R}_{>0}$ is the set of positive reals, that satisfies the following conditions:

1. $|xy| = |x||y|$ $\forall x, y \in \mathbb{F}$
2. $|x + y| \leq |x| + |y| \quad \forall x, y \in \mathbb{F}$ *(the triangle inequality)*
   An absolute value on $\mathbb{F}$ is called *ultrametric* or *non-Archimedean* if it satisfies the additional condition,
3. $|x + y| \leq Max(|x|, |y|)$ *(strong triangle inequality)* otherwise the the absolute value is *Archimedean*.

$|\cdot|$ is extended to $\mathbb{F}$ by setting $|0| = 0$.
Condition 3 implies condition 2, the triangle inequality, since $Max(|x|, |y|)$ does not exceed the sum $|x| + |y|$.

The general notion of absolute value on a field was introduced in 1913 by J. Kürschak. Around 1917, A. Ostrowski described absolute values on some classical fields, including the field of rationals. The whole point of an absolute value is that it provides the notion of *size*, i.e., it can be used to measure distances between numbers, that is, to put a *metric* on a given field, to define the notion of open and closed sets, and in general to investigate the topology of a given field.
The *usual* absolute value $|\cdot|$ on $\mathbb{Q}$ is defined by:

$$x = \begin{cases} x \text{ if } x \geq 0 \\ -x \text{ if } x < 0 \end{cases}$$

It is actually the usual absolute value on the field $\mathbb{R}$ of real numbers, applied to $\mathbb{Q}$ via the inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$. It is easy to see that this absolute value is Archimedean, usually called the *absolute value at infinity* and is denoted by $|\cdot|_\infty$. The only two Archimedean complete fields are $(\mathbb{R}, |\cdot|_\infty)$ and $(\mathbb{C}, |\cdot|_\infty)$ and while $(\mathbb{Q}, |\cdot|_\infty)$ is not complete, $(\mathbb{R}, |\cdot|_\infty)$ is its completion. More generally, an ordered field $\mathbb{F}$ is called Archimedean or, the ordering of a field is called Archimedean if the following holds: given $x, y \in \mathbb{F}$, $x \neq 0$, there exists a positive integer n such that $|nx| > |y|$. This property holds for the *usual* absolute value $|\cdot|_\infty$ on $\mathbb{Q}$ and $\mathbb{R}$. The induced metric $d(x, y) = |x - y|$, is the ordinary Euclidean distance on the number line. The field of real numbers $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to this absolute value. It is easy to see that the Archimedean property is equivalent to the assertion that

$$\sup\{|n| : n \in \mathbb{Z}\} = +\infty.$$

Definition 2.0.1. An absolute value is non-Archimedean if and only if

$$\sup\{|n| : n \in \mathbb{Z}\} = 1$$

Lemma 2.0.2. *Let $\mathbb{F}$ be a field and let $|.|$ be a non-Archimedean absolute value on $\mathbb{F}$. If $x, y \in \mathbb{F}$ and $|x| \neq |y|$, then $|x + y| = Max\{|x|, |y|\}$.*

Proof. Let $|x| > |y|$. Then $|x + y| \leq |x| = Max\{|x|, |y|\}$.
On the other hand, $x = (x + y) - y$, so that

$$|x| \leq max\{|x + y|, |y|\},$$

since $|x| > |y|$, this inequality can hold only if $max\{|x + y|, |y|\} = |x + y|$.
This gives the reverse inequality $|x| \leq |x + y|$ and from this it can be concluded that $|x| = |x + y|$. □

Thus, in an ultrametric space all triangles are isosceles.

Corollary 2.0.3. *If the elements a, x of a non-Archimedean field $\mathbb{F}$ satisfy the inequality $|x - a| < |a|$, then $|x| = |a|$*

Proof. Immediate from the Lemma 2.0.2 □

Remark 2.0.4. The corollary 2.0.3 can be restated in the following way:
for a, b in a non-Archimedean field $\mathbb{F}$, $|a| > |b| \implies |a + b| = |a|$.

Proposition 2.0.5. *Let K be a field with non-Archimedean absolute value.*
i) If $b \in B(a, r)$, then $B(a, r) = B(b, r)$; in other words, every point that is contained in an open ball is a center of that ball.
ii) If $b \in \bar{B}(a, r)$, then $\bar{B}(a, r) = \bar{B}(b, r)$; in otherwords, every point that is contained in a closed ball is a center of that ball.
iii) The set $B(a, r)$ is both open and closed.
iv) If $a, b \in K$ and $r, s \in \mathbb{R}_+^\times$, then $B(a, r) \cap B(b, r) \neq \phi$ if and only if $B(a, r) \subset B(b, s)$ or $B(a, r) \supset B(b, s)$; in other words, in other words any two open balls are either disjoint or contained in one another.
Similar result holds for closed balls

Proof. i) By definition, $b \in B(a, r)$ if and only if $|b - a| < r$. Choose x for which $|x - a| < r$. Then by non-Archimedean property

$$|x - b| \leq Max\{|x - a|, |b - a|\} < r,$$

so that $x \in B(b, r)$. This shows that $B(a, r) \subset B(b, r)$. The other inclusion is obtained by switching a to b, so that the two balls are equal.

ii) is immediate from *i).*
iii) The open ball is always an open set in any metric space. Consider an x in the boundary of $B(a,r)$; this means that any open ball centered in x must contain points that are in $B(a,r)$. Choose a number $s \leq r$, look at the open ball $B(x,s)$ with center x and radius s. Now, since x is a boundary point, $B(a,r) \cap B(x,s) \neq \phi$, so that there exists an element

$$y \in B(a,r) \cap B(x,s).$$

This means that $|y-a| < r$ and $|y-x| < s \leq r$. Applying the non-Archimedean inequality,

$$|x-a| \leq Max\{|x-y|, |y-a|\} < max\{s,r\} \leq r,$$

so that $x \in B(a,r)$. This shows that any boundary point of $B(a,r)$ belongs to $B(a,r)$ which means that, $B(a,r)$ is a closed set.
iv) Let $r \leq s$. If the intersection is not empty, there exists a $c \in B(a,r) \cap B(b,s)$. It is immediate from *i*) that $B(a,r) = B(c,r)$ and $B(b,s) = B(c,s)$. Hence

$$B(a,r) = B(c,r) \subset B(c,s) = B(b,s)$$

as claimed. □

Thus in view of Proposition 2.0.5, the following fact holds:
An ultrametric field is totally disconnected, since any point has a basis of open-closed neighborhoods. More precisely, any closed ball is open. Moreover, any triangle is isosceles. Also, in non-Archimedean geometry, a center of a disc is nothing but a point which belongs to the disc. The image of $\mathbb{Q}_p \backslash \{0\}$ under the p-adic norm is equal to a discrete subset of $\mathbb{R}$, namely $\{p^n : n \in \mathbb{Z}\}$. Therefore the closed and open ball of radius greater than *zero* are equivalent, i.e., $B_r(y) = \bar{B}_{r+\epsilon}(y)$ for all suffiently small ϵ greater than *zero.*

2.1 Discrete Valuation Fields

Definition 2.1.1. A *valued field* is a field $\mathbb{K}$ together with a surjective homomorphism

$$v : \mathbb{K}^* \to \Gamma$$

from the multiplicative group of $\mathbb{K}$ to an ordered abelian group Γ satisfying the following:

- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq inf\{v(x), v(y)\}$ holds whenever $x + y \neq 0$.
- v is non-trivial, that is, there exists $x \in K^*$ with $v(x) \neq 0$

v can be extended to $\mathbb{K}$ by letting $v(0) = +\infty$.

A valuation determines a non-trivial non-Archimedean absolute value and vice-versa. The image $v(\mathbb{K}^*)$ is an additive subgroup of Γ, the value group of v. If $v(\mathbb{K}^*) = \{0\}$, then v is called the *trivial* valuation. Valuations v and cv, for $c > 0$ a real constant, are *equivalent*.
A valuation v on $\mathbb{K}$ is said to be *discrete* if the totally ordered group $v(\mathbb{K}^*)$ is isomorphic to the naturally ordered group $\mathbb{Z}$. If $v(\mathbb{K}^*) = \mathbb{Z}$ then v is called a *normalised discete valuation.*

Relations between non-Archimedean absolute values and valuations:

The following theorem provides a relation between the non-Archimedean absolute values and the valuations on $\mathbb{K}$.

Theorem 2.1.2. *Let $|\cdot|$ be a non-Archimedean absolute value on $\mathbb{K}$ and $s \in \mathbb{R}$, $s > 0$, then the function*

$$\begin{array}{c} v_s : \mathbb{K} \to \mathbb{R} \cup \{\infty\} \\ x \to \begin{cases} -s\, log|x| & if \quad x \neq 0 \\ \infty & if \quad x = 0 \end{cases} \end{array}$$

is a valuation on K. Furthermore, if $s, s' > 0$ and $s \neq s'$, v_s is equivalent to $v_{s'}$. Conversely, if v is a valuation on $\mathbb{K}$ and $q \in \mathbb{R}$, $q > 1$, the function

$$x \to \begin{cases} |\cdot|_q : \mathbb{K} \to \mathbb{R} \\ q^{-v(x)} \qquad if \quad x \neq 0 \\ 0 \qquad\quad if \quad x = 0 \end{cases}$$

Proof. It is easy to check that v_s is a valuation on $\mathbb{K}$. For all $0 \neq x \in \mathbb{K}$,

$$v_s(x) = -s\, log|x| = \left(\tfrac{s}{s'}\right)\left(-s'^{log|x|}\right) = \tfrac{s}{s'} v'_s(x)$$

Thus v_s and $v_{s'}$ are equivalent.
Conversely, $|\cdot|_q$ satisfies axioms of non-Archimedean absolute value on $\mathbb{K}$.
Set $r := \frac{log\, q}{log\, q'}$. For all $0 \neq x \in \mathbb{K}$,

$$|x|_q = q^{-v(x)} = q'^{-rv(x)} = |x|^r_{q'}$$

Consequently $|\cdot|_q$ and $|\cdot|_{q'}$ are equivalent. □

Algebraic properties of valuation

Let $v : \mathbb{K}^* \to \mathbb{R}$ be a valuation corresponding to the absolute value $|\cdot| : \mathbb{F}^* \to \mathbb{R}_{>0}$. Then

$$\mathcal{O} = \mathcal{O}_v = \mathcal{O}_{\mathcal{K}} = \{x \in \mathbb{K} : v(x) \geq 0\} = \{x \in \mathbb{K} : |x| \leq 1\}$$

is a ring called the *valuation ring* of v. $\mathbb{K}$ is its field of fractions, and

$$x \in \mathbb{K} \setminus \mathcal{O} \implies \frac{1}{x} \in \mathcal{O}$$

The set of units in $\mathcal{O}$ is

$$\mathcal{O}^\times = \{x \in \mathbb{K} : v(x) = 0\} = \{x \in \mathbb{K} : |x| = 1\}$$

and

$$\mathcal{M} := \mathcal{O} \setminus \mathcal{O}^\times = \{x \in \mathbb{K} : v(x) > 0\} = \{x \in \mathbb{K} : |x| < 1\} = \{x \in \mathcal{O} : x^{-1} \notin \mathcal{O}\}$$

is an ideal in $\mathcal{O}$. Since $\mathcal{O} = \mathcal{O}^\times \cup \mathcal{M}$, $\mathcal{M}$ is a unique maximal ideal. Hence $\mathcal{O}$ is a local ring. Also, $k = \mathcal{O}/\mathcal{M}$ is a field, called the residue field of v or of $\mathbb{K}$.

The elements with valuation 0 are exactly the invertible elements of $\mathbb{R}$. They are called the *units* of $\mathbb{R}$. A valuation ring $\mathcal{O}$ in $\mathbb{K}$ with residue field k is said to be of equal characteristic if $char(\mathbb{K}) = char(k)$. Otherwise it is said to be of *mixed characteristic.* In this case necessarily $char(\mathbb{K}) = 0$ and $char(k) = p > 0$.

Suppose $v : \mathbb{K} \twoheadrightarrow \mathbb{Z}$ is normalised discrete. Then $\pi \in \mathcal{M}$ with $v(\pi) = 1$ is called a $uniformiser$. Then every $x \in \mathbb{K}^*$ can be written uniquely as

$$x = u\pi^n$$

for a unit $u \in \mathcal{O}^\times$ and $n \in \mathbb{Z}$. Every $x \in \mathcal{O}$ can be written uniquely as

$$x = u\pi^n$$

for a unit $u \in \mathcal{O}^\times$ and $n \in \mathbb{Z}_{\geq 0}$. Every $x \in \mathcal{M}$ can be written uniquely as

$$x = u\pi^n$$

for a unit $u \in \mathcal{O}^\times$ and $n \geq 1$, in particular $\mathcal{M} = (\pi)$. Moreover every ideal I in $\mathcal{O}$ is principal,

$$\mathcal{O} \supset I \neq (0) \implies I = (\pi^n)$$

Proposition 2.1.3. *Let $\mathbb{K}$ be a field with a discrete valuation. Then the set $\mathbb{R}$ of $x \in \mathbb{K}$ such that $v(x) \geq 0$ is a principal domain with a unique non-zero maximal ideal $\mathcal{M}$. Such a ring is called a discrete valuation ring. In particular $\mathbb{R}$ is a local ring (i.e with a unique non-zero prime ideal).*

Proof. Let π be an element such that $v(\pi) = 1$. Every $x \in \mathbb{R}$ can be written in the form $x = \pi^n u$ with $n = v(x)$ and $v(u) = 0$. Now $v(u) = 0$ implies u invertible (because $v(\frac{1}{u}) = 0$ too). So every non-zero ideal of R is of the form $\pi^n\mathbb{R}$ with $n \geq 0$ which shows that $\mathbb{R}$ is indeed a discrete valuation ring. □

Reciprocally if $\mathbb{R}$ is a discrete valuation ring with prime ideal (π), it is easy to see that every non zero element x of the field of fractions $\mathbb{K}$ can be written in in the form $x = \pi^n u$ with u invertible and $n \in \mathbb{Z}$ unique.

Examples of valuation and valued fields

Example 2.1.4. Any field K with the trivial valuation defined by $v(x) = 0 \qquad \forall x \in \mathbb{K}$

Example 2.1.5. The field $\mathcal{M}$ of meromorphic functions on the plane with $v(f) :=$ the order of vanishing of f at zero.

Example 2.1.6. For any field k the field of Laurent series over $k, k((t))$, is a valued field via

$$v(f) = N \Leftrightarrow f = \sum_{n \geq N} a_n t^n$$

with $a_N \neq 0$

Example 2.1.7. For a prime p and and a non-zero integer m let $k = v_p(m)$ be the maximal integer such that p^k divides m. The function v_p can be extended to the field of rational numbers as follows: if $x = \frac{a}{b} \in \mathbb{Q}^\times$, then

$$v_p(x) = v_p(a) - v_p(b);\ v_p(0) = \infty$$

The p-adic valuation v_p is a discrete valuation with the ring of integers as $\mathbb{Z}$. Then

$$\mathcal{O} = \left\{ \frac{x}{y} : (y, p) = 1 \right\}$$

$$\mathcal{M} = \left\{ \frac{x}{y} : (y, p) = 1,\ p | x \right\} = (p)\mathcal{O}$$

$$\mathcal{O}/\mathcal{M} = k \cong \mathbb{F}_p, \quad \frac{x}{y} \to \frac{x \mod p}{y \mod p}$$

Theorem 2.1.8. *1. Suppose $v : \mathbb{K}^* \twoheadrightarrow \mathbb{Z}$ is a valuation. Then $\mathcal{O}_v$ is a DVR.*

2. If R is a DVR then there exists a unique valuation v on its field of fractions $\mathbb{K}$ such that $R = \mathcal{O}_v$.

Proof. 1. $\mathcal{O} \subset \mathbb{K}$ is a subring, hence an integral domain. It is clear from proposition 2.1.3 that, $\mathcal{O}$ is a local ring and a PID. $\pi^{-1} \in \mathbb{K} \setminus \mathcal{O}$, so $\mathcal{O}$ is not a field.

2. Let R be a DVR. Then R is a local ring so has a unique maximal ideal $\mathcal{M}$, and R is a PID so $\mathcal{M} = (\pi)$ for some $\pi \in R$. Since R is a PID, R is a UFD. If π'

is another irreducible element then (π') is maximal, hence $(\pi) = (\pi')$ so (π') associate to (π). As R is a UFD, every element is uniquely written in the form $u\pi^n$, $u \in R$ is a unit. A function v on R can be defined by letting $v(u\pi^n) = n$, $v(\frac{x}{y}) = v(x) - v(y)$, which is clearly a valuation.

□

The completion of a field $\mathbb{K}$ with respect to a discrete valuation v is a field $\mathbb{K}_v$ in which the elements can be easily described in terms of a uniformizing parameter. (i.e.,$\mathbb{K}_v$ is complete in the v-adic topology.) In addition, $\mathbb{K}_v$ is a topological space where the topology is defined by the metric d_v.

For any field F there is a trivial absolute value on F defined by

$$|f|_{triv} = \begin{cases} 1 & \text{if } f \neq 0 \\ 0 & \text{if } f = 0 \end{cases}$$

2.2 *p*-adic absolute value

Definition 2.2.1. For any $x \in \mathbb{Q}$, the p-adic absolute value of x is defined by

$$|x|_p = p^{-v_p(x)}, \text{ if } x \neq 0$$
$$\text{with } |0|_p = 0$$

Theorem 2.2.2. ***(Ostrowski)****Every nontrivial absolute value on $\mathbb{Q}$ is either equivalent to the real absolute value or to one of the p-adic absolute values.*

Lemma 2.2.3. *$|\cdot|_p$ is a non-Archimedean absolute value on $\mathbb{Q}$.*

Proof. Properties (1) *and* (2) are easy to check.
If $x = 0$ or $y = 0$, or if $x + y = 0$, Property (3) is trivial.
Let $x, y, x + y \neq 0$ and $x = \frac{a}{b}$ and $y = \frac{c}{d}$ be written in their lowest terms. Then $x + y = \frac{ad+bc}{bd}$, and $v_p(x + y) = v_p(ad + bc) - v_pb - v_pd$. Hence

$$v_p(x + y) \geq min\{v_p(ad), v_p(bc) - v_p(b) - v_p(d)\}$$
$$= min\ \{v_p(a) + v_p(d), v_p(b) + v_p(c) - v_p(b) - v_p(d)\}$$
$$= min\ \{v_p(a) - v_p(b), v_p(c) - v_p(d)\}$$
$$= min\{v_p(x), v_p(y)\}$$

Therefore $|x+y|_p = p^{-v_p(x+y)} \leq Max\{p^{-v_p(x)}, p^{-v_p(y)}\} = Max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$. Thus $|\cdot|_p$ is a non-Archimedean absolute value on $\mathbb{Q}$. □

Definition 2.2.4. Let $(\mathbb{K}, |\cdot|)$ be any valued field. The distance $d(x, y)$ between any two numbers $x, y \in \mathbb{K}$ is given by

$$d(x, y) = |x - y|$$

Then $\mathbb{K}$ is a metric space with the metric $d(x, y) = |x - y|$.

Any field with an absolute value $|\cdot|$ can be made in to a metric space by defining $d(x, y) = |x - y|$. The metric induced by the non-Archimedean absolute value is *ultra-metric*. Then $d_p(x, y) = |x - y|_p$, the p-adic distance between x and y defines a metric on $\mathbb{Q}$. Instead of the triangle inequality for the usual metric it satisfies the strong triangle inequality $d_p(x, y) \leq Max\{d_p(x, y), d_p(y, z)\}$, for any $x, y, z \in \mathbb{Q}$. The corresponding metric spaces are *ultra-metric spaces*. As a consequence (in stark contrast to the *Euclidean* norm), the p-adic norm does not permit accumulation of errors in the following sense. If each of k elements $\{x_1, x_2, ..., x_k\}$have p adic norm atmost ϵ, then $|x_1 + x_2 + ... + x_k|_p \leq \epsilon$ as well. This property justifies extensive use of modular arithmetic (*p-adic estimation*) in p-adic calculation.

The topological completion of $\mathbb{K}$ with respect to $|\cdot|$ can be made in to a field, called the *completion* $\hat{\mathbb{K}}$ of $\mathbb{K}$ with respect to $|\cdot|$. There is a natural injection $\mathbb{K} \hookrightarrow \hat{\mathbb{K}}$ by $x \to (x_n)$, and $|\cdot|$ can be extended from $\mathbb{K}$ to $\hat{\mathbb{K}}$ by

$$|(x_n)| = \lim_{n\to\infty} x_n$$

A field $\hat{\mathbb{F}}$ with a discrete valuation $\hat{v}$ is called a completion of $\mathbb{F}$ if $\hat{v} \mid_{\mathbb{F}} = v$. The metric space $(\mathbb{Q}, d_p)$ is not complete, and its completion is the p-adic number field $\mathbb{Q}_p$. The p-adic numbers $\mathbb{Q}_p$ are constructed by taking the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. If $\lambda \in \mathbb{Q}_p$ then the p-adic absolute value on $\mathbb{Q}$ can be extended to $\mathbb{Q}_p$ by defining

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p$$

where (x_n) is a Cauchy sequence in $\mathbb{Q}$ converging to λ. By considering the sequence (x_n) converging to λ it can be proved that $|\cdot|_p$ is a non-Archimedean absolute value on $\mathbb{Q}_p$. Likewise define v_p on $\mathbb{Q}_p$ by $v_p(\lambda) = -log|\lambda|_p$.

2.3 p-adic completion

Lemma 2.3.1. *Let $\mathcal{O}$ be a DVR and v a valuation of it. Let $\mathbb{K}$ be the fraction field of $\mathcal{O}$, $\mathcal{M} = (\pi)$ for a uniformiser π, and $\mathcal{O}/\mathcal{M} = k$ the residue field. Let $A = \{a_i\}$ be any representative of $\mathcal{O}/\mathcal{M}$, $a_i \in \mathcal{O}$, and assume $0 \in A$. Then every $x \in \mathbb{K}^*$ can be written as,*

$$x = \pi^{v(x)} \sum_{n=0}^{\infty} a_n \pi^n$$

with $a_n \in A$ and $a_0 \neq 0$. a_i are called the digits in the π-adic expansion of x.

Proof. Write $x = \pi^{v(x)} u$ for some unit $u \in \mathcal{O}^\times$. Reducing mod π,

$$\mathcal{O}/\mathcal{M} \xrightarrow{\sim} k$$
$$u \to \bar{u}$$

There exists a unique $a_0 \in A$ such that $a_0 = \bar{u}$, so $a_0 - u \in \mathcal{M}$. Now writing u in the form $u = a_0 + \pi u_1$ and reducing u_1 mod π, there exists a unique $a_1 \in A$ such that $\bar{a}_1 = \bar{u}_1$. Now $u = a_0 + \pi a_1 + \pi^2 u_2$ and repeating the above argument, the partial sums,

$$S_N = \sum_{n=0}^{N} a_n \pi^n \to u$$

are obtained in the topology defined by v. Since $v(S_N - u) \geq N$ implies $S_N \to u$, clearly the a_n are unique. □

Remark 2.3.2.

1. The open balls in $\mathbb{K}$ are of the form $x + \pi^n \mathcal{O}$ which is the set of elements of $\mathbb{K}$ whose digits coincide with those of x up to a_{n-1}.
2. A sequence (x_k) in $\mathbb{K}$ is Cauchy if and only if the digits of x_k eventually stabilize.

Example 2.3.3. The field of p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. The ring of p-adic integers is its valuation ring. Let $\pi = p$ and $A = \{0, 1, ...p-1\}$.

Applying Lemma 2.3.1

$$\mathbb{Q} \hookrightarrow \left\{ \sum_{n=n_0}^{\infty} a_n p^n : a_n \in \{0, 1, ..., p-1\} \right\} = \mathbb{Q}_p$$

$$\mathbb{Z} \hookrightarrow \mathcal{O} \hookrightarrow \left\{ \sum_{n=0}^{\infty} a_n p^n : a_n \in \{0, 1, ..., p-1\} \right\} = \mathbb{Z}_p$$

$$\mathcal{M} = (p) = \left\{ \sum_{n=1}^{\infty} a_n p^n : a_n \in \{0, 1, ..., p-1\} \right\}$$

$$\mathbb{Z}_p / \mathcal{M} = \mathbb{F}_p$$

$$\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}$$

The residue field is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the finite field with p elements. The mapping

$$a = \sum_{i \geq 0} a_i p^i \mapsto a_0 \, (mod \, p)$$

defines a ring homomorphism $\epsilon : \mathbb{Z}_p \to \mathbb{F}_p$ called reduction modulo p. This reduction map is obviously surjective, with kernel

$$\{a \in \mathbb{Z}_p : a_0 = 0\} = \left\{ \sum_{i \geq 1} a_i p^i = p \sum_{j \geq 0} a_{j+1} p^j \right\} = p\mathbb{Z}_p$$

Since the quotient is a field, the kernel $p\mathbb{Z}_p$ of ϵ is a maximal ideal of the ring $\mathbb{Z}_p$. The set $p\mathbb{Z}_p$ is a subgroup of index p in $\mathbb{Z}_p$. The residue field of $\mathbb{Q}_p$ is canonically isomorphic to the finite field $\mathbb{F}_p$ with p elements.

The above discussions may be summarized as below:

Theorem 2.3.4. *For each prime $p \in \mathbb{Z}$ there exists a field $\mathbb{Q}_p$ with a non-Archimedean absolute value $|\cdot|_p$ such that :*
i) There exists an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, and the absolute value induced by $|\cdot|_p$ on $\mathbb{Q}$ via this inclusion is the p-adic absolute value.
ii) The image of $\mathbb{Q}$ under this inclusion is dense in $\mathbb{Q}_p$.

iii) $\mathbb{Q}_p$ *is complete with respect to the absolute value* $|\cdot|_p$.
The field $\mathbb{Q}_p$ *satisfying* $(i), (ii)$ *and* (iii) *is unique up to isomorphism preserving the absolute values.*

Proof. Proof is immediate from the above discussion. □

Proposition 2.3.5. *The inclusion* $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ *has dense image. In particular, given* $x \in \mathbb{Z}_p$ *and* $n \geq 1$, *there exists* $\alpha \in \mathbb{Z}$, $0 \leq \alpha \leq p^n - 1$, *such that* $|x - a| \leq p^{-n}$. *The integer* α *with these properties is unique.*

Proof. Choose $x \in \mathbb{Z}_p$ and $n \geq 1$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, it is possible to find $\frac{a}{b} \in \mathbb{Q}$ which is close enough to x such that

$$\left|x - \frac{a}{b}\right| \leq p^{-n} < 1.$$

For $\frac{a}{b}$ as above,

$$\left|\frac{a}{b}\right| \leq max\left\{|x|, \left|x - \frac{a}{b}\right|\right\} \leq 1$$

which says that $\frac{a}{b} \in \mathbb{Q} \cap \mathbb{Z}_p$, that is $p \nmid b$. If $p \nmid b$ there exists an integer $b' \in \mathbb{Z}$ such that

$$bb' \equiv 1 \pmod{p^n},$$

which implies that

$$\left|\frac{a}{b} - ab'\right| \leq p^{-n},$$

$ab' \in \mathbb{Z}$.
Choosing α to be the unique integer such that

$$0 \leq \alpha \leq p^n - 1 \qquad and \qquad \alpha \equiv ab' \pmod{p^n}$$

gives $|x - a| \leq p^{-n}$, the required result. In otherwords, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the p-adic absolute value. □

The ring of ordinary integers $\mathbb{Z}$ is a subring of $\mathbb{Z}_p$ via the natural inclusion

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p$$

$$a \mapsto (a\,(mod\,p),\ a\,(mod\,p^2), ...,\,)$$

The principal ideals of $\mathbb{Z}_p$ have an intersection equal to $\{0\}$:

$$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset ... \supset p^k\mathbb{Z}_p ... \supset \cap_{k\geq 0} p^k\mathbb{Z}_p = \{0\}.$$

where

$$p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$$
$$x \mapsto n\text{th } p\text{-adic digit}$$

Any element $a \neq 0$ has an order $v(a) = k$, hence $a \notin (p^{k+1})$. Infact, these principal ideals are the only nonzero ideals of the ring of p-adic integers.

Each $z \in \mathbb{Q}_p$ can be written in a unique manner as

$$z = \sum_{n \geq v_p(z)} z_n p^n \qquad\qquad (0 \leq z_n < p)$$

Here $v_p(z)$ is the lowest power in the expansion of z as a p-adic number.
The fractional part of z is defined as

$$\{z\} := \sum_{0 > n \geq v_p(z)} z_n p^n$$

Thus,

$$z = [z] + \{z\} : \mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}\left[\frac{1}{p}\right]$$

More formally,

Definition 2.3.6. If $a = \sum_{n=0}^{\infty} d_n p^n$ with $d_n = 0$ for $0 \leq n < k$ and $d_k \neq 0$, then $|a|_p = p^{-k}$, and if $a = \sum_{n=-m}^{\infty} d_n p^n$, where $d_{-m} \neq 0$, then $|a|_p = p^m$

Open balls in $\mathbb{R}$ are the are the open intervals $B(a, r) = |x - a| < r$. In $\mathbb{Q}_p$ open balls are the sets

$$B(a, r) = \{x \in \mathbb{Q}_p : |x - a|_p < r\}.$$

The closed balls are the sets

$$\bar{B}(a,r) = \{x \in \mathbb{Q}_p : |x-a|_p \leq r\}$$

The *sphere* in $\mathbb{Q}_p$ is the set

$$S(a,r) = \{x \in \mathbb{Q}_p : |x-a|_p = r\}$$

Since p-adic norm has a discrete set of values, $\{p^n | n \in \mathbb{Z}\} \cup \{0\}$, only balls of radii $r = p^n, n \in \mathbb{Z}$ are considered.

Proposition 2.3.7. *The sphere $S(a,r)$ is an open set in $\mathbb{Q}_p$.*

Proof. Let $x \in S(a,r)$ and $B(x,\epsilon)$ be an open ball such that $\epsilon < r$.
Claim: $B(x,\epsilon) \subset S(a,r)$:
Let $y \in B(x,\epsilon)$. Then $|x-y|_p < |x-a|_p = r$ and by Corollary 2.0.3 it is clear that $|y-a|_p = |x-a|_p = r$, which means exactly that $y \in S(a,r)$

□

This is very strange since in $\mathbb{R}^n$ the spheres are certainly not open sets. This strange property implies the following. The set of all balls in $\mathbb{R}$ is uncountable since the set of all positive real numbers is uncountable (*Cantor's theorem*), so it is true for the set of all balls $B(a,r)$ in $\mathbb{R}$.

A completely different result holds for the set of all balls in $\mathbb{Q}_p$.

Proposition 2.3.8. *The set of all balls in $\mathbb{Q}_p$ is countable.*

Proof. The center of the ball in its canonical form is given by

$$a = \sum_{n=-m}^{\infty} a_n p^n$$

and let,

$$a_0 = \sum_{n=-m}^{s} a_n p^n$$

Clearly a_0 is a rational number and $|a - a_0|_p < p^{-s}$. i.e., $a_0 \in B(a, p^{-s})$. Then by Proposition 2.0.5

$$B(a_0, p^{-s}) = B(a, p^{-s})$$

Here both centers and radii come from countable sets. Therefore the product set of all pairs (a_0, s) is also countable and so is the set of all balls in $\mathbb{Q}_p$. □

Lemma 2.3.9. *$\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.*

Proof. The proof is easy to verify. □

The ring of p-adic integers $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$. It is not difficult to see that $B(0, p) = \bar{B}(0, 1) = \mathbb{Z}_p$.
and

$$\mathbb{Z}_p^\times = S(0, 1) = (1 + p\mathbb{Z}_p) \cup (2 + p\mathbb{Z}_p) \cup ... \cup ((p-1) + p\mathbb{Z}_p).$$

There exists filtration of subsets

$$\mathbb{Z}_p^\times \supset 1 + p\mathbb{Z}_p \supset 1 + p^2\mathbb{Z}_p \supset ...$$

Lemma 2.3.10. *The ring $\mathbb{Z}_p$ has a unique maximal ideal*

$$p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$$

and the elements of $\mathbb{Z}_p/p\mathbb{Z}_p$ are invertible in $\mathbb{Z}_p$.

Theorem 2.3.11. *The space $\mathbb{Q}_p$ is totally disconnected.*

Proof. For each $a \in \mathbb{Q}_p$ and each $n \in \mathbb{N}$ the set

$$U_n(a) = \{x \in \mathbb{Q}_p : |x - a|_p \leq p^{-n}\} = \{x \in \mathbb{Q}_p : |x - a|_p < p^{-n+1}\}$$

is an open and closed neighborhood of a. Suppose $a \in A$ so that $A \neq \{0\}$. Then there is an $n \in \mathbb{N}$ such that $U_n(a) \cap A \neq A$. Therefore,

$$A = (U_n(a) \cap A) \cup (\mathbb{Q}_p \setminus U_n(a) \cap A),$$

where both $U_n(a)$ and its complement $\mathbb{Q}_p \setminus U_n(a)$ are open and nonempty; this implies that A is not connected. □

Definition 2.3.12. A topological space is *locally compact* if every point has a compact neighbourhood.

Theorem 2.3.13. *The space $\mathbb{Q}_p$ is locally compact.*

Proof. Since $\mathbb{Z}_p$ is a neighbourhood of *zero*, it suffices to show that this is compact. Since $\mathbb{Z}_p$ is a closed set of a complete metric space it is complete. Now to complete the proof it suffices to show that $\mathbb{Z}_p$ is totally bounded. A set is totally bounded if, for each $\epsilon > 0$, the set can be covered with finitely many balls of radius ϵ. Thus it is enough to take $\epsilon = p^{-n}$ for some integer $n \geq 0$. Since every $x \in \mathbb{Z}_p$ can be expanded as

$$x = y_0 + y_1 p + y_2 p^2 + ... + y_j p^j + ..$$

this implies that there are finitely many balls $B(0, p^{-n})$ that cover $\mathbb{Z}_p$. □

2.4 Inverse limits

Definition 2.4.1. A partially ordered set $(I, \leq)$ is called a *directed set* if for every $i, j \in I$ $\exists\, k \in I$ such that, $i \leq k$ and $j \leq k$.

Example 2.4.2. A totally ordered set is a directed set.

Example 2.4.3. $\mathbb{N}$ can be made into a directed set via $(\mathbb{N}, \leq)$ or $(\mathbb{N}, |)$.

Definition 2.4.4. An *inverse system* $\{G_i, \phi_{ij} | i, j \in I, i \geq j\}$ of groups indexed by a directed set I consists of a group G_i for each $i \in I$ and a homomorphism $\phi_{ij} : G_i \to G_j$ whenever $i \geq j$ in I such that $\phi_{ij}\phi_{jk} = \phi_{ik}$ when $i \geq j \geq k$.

Definition 2.4.5. An *inverse limit* of the inverse system is defined as

$$G = \varprojlim_{i \in I}(G_i, \phi_{ij}) = \varprojlim_{i \in I} G_i = \{(g_i)_{i \in I} \in \prod_{i \in I} G_i : \phi_{ij}(g_i) = g_j \forall j \leq i\}$$

such that the natural projection $\phi_i : G \to G_i$, $g = (g_j)_{j \in I} \mapsto g_i$ is a morphism for each $i \in I$. This is a group (ring).

Example 2.4.6. For a set of positive integers N^* define an ordering $n \leq m$ if $n|m$. For the inverse system $(\mathbb{Z}/n\mathbb{Z})_{n\in\mathbb{N}^*}$ of finite rings where the transition map π_{mn} is the natural projection, the inverse limit is

$$\hat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}^*} \mathbb{Z}/n\mathbb{Z}.$$

Consider the ring $\mathbb{Z}$ and its decreasing sequence of ideals $I_n = p^n\mathbb{Z}$. The inclusions $p^{n+1}\mathbb{Z} \subset p^n\mathbb{Z}$ lead to canonical transition homomorphisms

$$\phi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$$

which is surjective and whose kernel is $p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$

Then

$$\mathbb{Z}_p = \varprojlim_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$$

consists of sequences $x = (..., x_n, ..., x_1)$ with $x_n \in \mathbb{Z}/p^n\mathbb{Z}$, and is the ring of p-adic integers. The ring $\mathbb{Z}_p$ is a complete discrete valuation ring with maximal ideal generated by p, the residue field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, and the fraction field

$$\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right] = \cup_{m=0}^{\infty} p^{-m}\mathbb{Z}_p$$

being the field of p-adic numbers.

Theorem 2.4.7. *The mapping $\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ that associates to the p-adic number $x = \sum a_i p^i$ the sequence $(x_n)_{n\geq 1}$ of its partial sums $x_n = \sum_{i<n} a_i p^i \ mod\ p^n$ is an isomorphism of topological rings.*

Proof. Since the transition homomorphism ϕ_n is given by

$$\sum_{i\leq n} a_i p^i \, mod\, p^n \mapsto \sum_{i<n} a_i p^i \, mod\, p^n,$$

the coherent sequences in the product $\prod \mathbb{Z}/p^n\mathbb{Z}$ are simply the sequences (x_n) of partial sums of a formal series $\sum_{i\geq 0} a_i p^i$ $(0 \leq a_i \leq p-1)$, and those are precisely the

p-adic integers. The relations

$$x_1 = a_0,\ x_2 = a_0 + a_1 p,\ x_3 = a_0 + a_1 p + a_2 p^2, ...$$

and conversely

$$a_0 = x_1, \quad a_1 = \frac{x_2 - x_1}{p}, \quad a_2 = \frac{x_3 - x_2}{p^2}, ..$$

show that the factorization $\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is bijective, and hence an algebraic isomorphism. Since this is a continuous map between two compact spaces, it is a homeomorphism, hence the result. □

The homomorphisms $\mathbb{Z} \to \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ furnish a limit homomorphism $\mathbb{Z} \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, which can be identified with the canonical embedding $\mathbb{Z} \to \mathbb{Z}_p$. The map

$$\sum_{i<n} a_i p^i \ mod\, p^n \mapsto \sum_{i<n} a_i p^i \ mod\, p^n \mathbb{Z}_p,$$

obviously defines an isomorphism $\mathbb{Z}/p^n\mathbb{Z} \mapsto \mathbb{Z}_p/p^n\mathbb{Z}_p$, and in particular

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

More generally, the same argument shows that

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

The restriction of reduction homomorphism $\mathbb{Z}_p \mapsto \mathbb{Z}/p^n\mathbb{Z}$ to the subring

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N} \quad (b, p) = 1\} \subset \mathbb{Q}$$

is already surjective and has kernel $p^n\mathbb{Z}_{(p)}$, hence defines an isomorphism:

$$\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^n\mathbb{Z}$$

Starting with the subring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ it is clear that, $\mathbb{Z}_p$ is a projective limit $\varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_{(p)}$ and hence a completion of $\mathbb{Z}_{(p)}$. These considerations also show that a nonzero p-adic number can also be uniquely written as $x = p^m u$ with $m \in \mathbb{Z}$ and a unit $u \in \mathbb{Z}_p^\times$;

hence

$$\mathbb{Q}_p^\times = \bigsqcup_{m\in\mathbb{Z}} p^m\mathbb{Z}_p^\times$$

is a disjoint union over the rational integers $m \in \mathbb{Z}$.

Remark. If $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ denotes the subring consisting of rational numbers having denominator prime to p, then,

$$\mathbb{Q} = \cup_{m\geq 0} p^{-m}\mathbb{Z}_{(p)} \qquad and \qquad \mathbb{Q}^\times = \bigsqcup_{p\in\mathbb{Z}} p^m\mathbb{Z}_{(p)}^\times$$

$\mathbb{Z}_{(p)}^\times$ consists of the fractions having both numerator and denominator prime to p. This gives an elementary description of the decomposition

$$\mathbb{Q} = \mathbb{Z}_{(p)} + \mathbb{Z}\left[\frac{1}{p}\right]$$

induced by the decomposition

$$\mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}\left[\frac{1}{p}\right]$$

Hensel's Lemma:
Hensel's Lemma is the most important algebraic property of the p-adic numbers and of other fields like $\mathbb{Q}_p$ or which are complete with respect to a non-Archimedean valuation. The test involves finding an approximate root of the polynomial, and then verifying a condition on the derivative of the polynomial.

Theorem 2.4.8. *(Hensel's Lemma) Let $f(X) = a_0 + a_1X + ...a_nX^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. Suppose that there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that,*

$$f(\alpha_1) \equiv 0 (mod\, p\mathbb{Z}_p)$$

and

$$f'(\alpha_1) \not\equiv 0 (mod\, p\mathbb{Z}_p)$$

where $f'(X)$ is the formal derivative of $f(X)$. Then there exists a unique p-adic integer

$\alpha \in \mathbb{Z}_p$ *such that* $\alpha \equiv \alpha_1$ *mod* $p\mathbb{Z}_p$ *and* $f(\alpha) = 0$.

2.5 Algebraic closure

The field $\mathbb{Q}_p$ is not algebraically closed. The algebraic closure of $\mathbb{Q}_p$, denoted by $\bar{\mathbb{Q}}_p$ is of infinite degree over $\mathbb{Q}_p$. Any field extension of $\mathbb{Q}_p$ is also a $\mathbb{Q}_p$- vector space. E.g. $\mathbb{Q}_5(\sqrt{2})$ is a vector space with basis $\{1, \sqrt{2}\}$ over $\mathbb{Q}_5$. $\bar{\mathbb{Q}}_p$ is not complete with respect to $|\cdot|_p$. The completion of algebraic closure of $\bar{\mathbb{Q}}_p$ is denoted by Ω, the smallest field containing $\mathbb{Q}$ that is both complete and algebraically closed with respect to $|\cdot|_p$. The field Ω is a beautiful, gigantic realm, in which p-adic analysis lives (Koblitz, 1984).

Chapter 3

Dynamical Systems

Dynamical systems originally arose in the study of systems of differential equations used to model physical phenomena. Mathematically, dynamical systems is the study of long -term behavior in systems that evolve in time. The term dynamical systems refers to either discrete-time or continuous-time dynamical systems. Most of the concepts and results in dynamical systems have discrete-time and continuous-time version. The continuous-time version can often be deduced from the discrete-time versions.

A *continuous-time* dynamical system consists of a space X and a one parameter family of maps $\{f^t : X \to X | t \in \mathbb{R} \text{ or } t \in \mathbb{R}_0^+\}$, that forms a one-parameter group or semigroup, i.e., $f^{[t+s]} = f^{[t]} \circ f^{[s]}$ and $f^{[0]} = identity$. The dynamical system is called a *flow* if the time t ranges over $\mathbb{R}$, and a *semi-flow* if t ranges over $\mathbb{R}_0^+$. For a flow, the map $f^{[t]}$ is invertible, since $f^{[-t]} = (f^{[t]})^{-1}$.
One simplification in this study is to discretize time, so that the state of the system is observed only at discrete steps of time. This leads to the study of the iterates of a single transformation. One is interested in both quantitative behavior, such as the average time spent in a certain region, and also qualitative behavior, such as whether a state eventually becomes periodic or tends to infinity.
A discrete-time dynamical system consists of a non-empty set X and a map $\phi : X \to X$. For $n \in \mathbb{N}$, the nth iterate of ϕ is the n-fold composition $\phi^{[n]} = \phi \circ \phi \circ ... \circ \phi$ (n times); $\phi^{[0]}$ is defined to be the identity map. If ϕ is invertible, then $\phi^{-n} = \phi^{-1} \circ \phi^{-1} \circ ... \circ \phi^{-1}$ (n times). Since $\phi^{[n+m]} = \phi^{[n]} \circ \phi^{[m]}$, these iterates form a group if ϕ is invertible, and

a semigroup otherwise. For a given α in X, the *forward orbit* of α is the set

$$\mathcal{O}_\phi(\alpha) = \{\phi^n(\alpha) : n \geq 0\}$$

If the orbit $\mathcal{O}_\phi(\alpha)$ is finite then α is said to be a *pre-periodic* point, otherwise α is said to be a *wandering* point. The central problem in dynamics is to classify the points α in the set X according to the behavior of their orbits $\mathcal{O}_\phi(\alpha)$.

In practice X usually has additional structure that is preserved by the map f. For example, (X, f) could be a measure space and a measure preserving map; a topological space and a continuous map; a metric space and an isometry; or a smooth manifold and a differentiable map; a finite set (e.g., finite field) and a polynomial.
A dynamical system with a continuous time or flow on a metric space X is a family $\{\phi_t : t \in \mathbb{R}\}$ of homeomorphisms of X such that the map $(t, x) \to \phi_t(x)$ is continuous.
A dynamical system with discrete time on a metric space X is a family $\{f^n : n \in \mathbb{Z}\}$ of homeomorphisms of X or a family $\{f^n : n > 0\}$ of continuous maps of X.
The iterations of a homeomorphism or a continuous map $f : X \to X$ form a dynamical system.

In the context of a discrete dynamical system, where a given map is iterated, that map might be invertible (because of being one-to-one and onto) or non-invertible (failing one or the other or both of these conditions). So, discrete dynamical systems come in two types, invertible and non-invertible. The invertible maps were introduced by Poincaré, and have been extensively studied ever since. The studies of non-invertible maps have been more sparse until recently, when they became one of the most active areas on the research frontier because of their usefulness in applications.

The basic goal of dynamical systems is to understand the eventual or asymptotic behavior of an iterative process. If the process is a differential equation whose independent variable is time, then the theory attempts to predict the ultimate behaviour of solutions of equations in either the distant future ($t \to \infty$) or the distant past ($t \to -\infty$). If the process is a discrete process such as the iterations of a function, then the theory hopes to understand the eventual behaviour of the points x, $f(x)$, ..., $f^n(x)$

as n becomes large, (Devaney, 1989; Brin and Stuck, 2002; Khrennikov and Nilsson, 2004).

3.1 Symbolic dynamics

Symbolic dynamics arose as an attempt to study such systems by means of discretizing space as well as time. The basic idea is to divide up the set of possible states into a finite number of pieces. Each piece is associated with a "symbol", and in this way the evolution of the system is described by an infinite sequence of symbols. This leads to a "symbolic" dynamical system that mirrors and helps us to understand the dynamical behavior of the original system. Computer simulations of continuous systems necessarily involve a discretization of space, and results of symbolic dynamics help us understand how well, or how badly, the simulation may mimic the original. Symbolic dynamics by itself has proved a bottomless source of beautiful mathematics and intriguing questions.

3.1.1 Sequence spaces

As polygons and curves are to geometry, shift spaces are to symbolic dynamics. The set

$$\Sigma = \{0, 1, 2, ..., m-1\}^{\mathbb{N}}$$

is called the sequence space on m symbols $0, 1, ..., m-1$.
The most important ingredient in the sequence space is the shift map σ. The shift map $\sigma : \Sigma \to \Sigma$ is given by $\sigma((s_0, s_1, s_2, ..)) = (s_1, s_2, s_3, ...)$.
The shift map discards the first entry in the sequence and shifts all other entries one place to the left.
The distance between two sequences $s = (s_0, s_1, ...)$ and $t = (t_0, t_1, ...)$ is given by $d(s,t) = \sum_{i=0}^{\infty} \frac{s_i - t_i}{m^i}$.
For an integer $m > 1$, set $\mathbb{A}_m = \{1, 2, ..., m\}$. Let $\Sigma_m = \mathbb{A}_m^Z$ be the set of infinite two sided sequences of symbols in $\mathbb{A}_m$ and $\Sigma_m^+ = \mathbb{A}_m^N$ be the set of infinite one-sided sequences. The pair (Σ_m, σ) is called the full two sided shift; (Σ_m^+, σ) is called the full one sided shift. The two-sided shift is invertible. For a one-sided sequence, the leftmost

symbol disappears, so the one-sided shift is non-invertible, and every point has m pre-images. Both shifts have m^n periodic points of period n. When the entries are from a finite set the sequence space is usually homeomorphic to the standard Cantor set. The shift spaces are compact topological spaces in the product topology. This topology has a basis consisting of cylinders $C^{n_1,...,n_k}_{j_1,..,j_k}$=$\{x = (x_l) : x_{n_i} = j_i, i = 1, 2, ..., k\}$, $n_1 < n_2 < ... < n_k$ are indices in $\mathbb{Z}$ or $\mathbb{N}$, and $j_i \in \mathbb{A}_m$. Since the preimage of a cylinder is a cylinder, σ is continuous on Σ^+_m and a homeomorphism on Σ_m. The metric $d(x, x') = 2^{-l}$, for $l = min\{|i| : x_i \neq x'_i\}$ generates the product topology on Σ^+_m and Σ_m. Thus both the spaces are compact zero dimensional metric spaces and are homeomorphic to a Cantor set. In the product topology periodic points are dense and hence there are dense orbits. A detailed study can be found in (Devaney, 1989; Kitchens, 1998).

3.2 Some definitions and examples

Definition 3.2.1. The *forward orbit* of x is the set of points $x, f(x), f^{[2]}(x)...$ denoted by $O^+(x)$. If f is a homeomorphism, then the full orbit of x is denoted by $O(x)$ and $f^{[n]}(x), n \in \mathbb{Z}$ as the set of points in the orbit. The backward orbit of x is denoted by $O^-(x)$ with the points $x, f^{[-1]}(x), f^{[-2]}(x), ...$

Definition 3.2.2. The point x is a *fixed point* for f if $f(x) = x$. A point $x_0 \in X$ is said to be a *periodic point* if there exists $r \in \mathbb{N}$ such that $f^{[r]}(x_0) = x_0$. The least positive n for which $f^{[n]}(x) = x$ is called the prime period of x.

Example 3.2.3. The map $f(x) = x$ fixes all points in $\mathbb{R}$, whereas the map $f(x) = -x$ fixes the origin while all other points have period 2 .

Example 3.2.4. The map $f(x) = x^3$ has 0, 1 and -1 as fixed points and no other periodic points. The map $q(x) = x^2 - 1$ has fixed points at $\frac{1\pm\sqrt{5}}{2}$, while the points 0 and 1 lie on a periodic orbit of period 2.

Definition 3.2.5. A point x is *eventually periodic* of period n if x is not periodic but there exists $m > 0$ such that $f^{n+i}(x) = f^i(x)$ for all $i \geq m$. That is $f^i(x)$ is periodic for $i \geq m$.

Example 3.2.6. Let $f(x) = x^2$. Then 1 is fixed since $f(1) = 1$, while -1 is eventually fixed since $f(-1) = 1$.

Definition 3.2.7. The point x is called a *critical point* of f if $f'(x) = 0$. The critical point is *nondegenerate* if $f''(x) \neq 0$ The critical point is *degenerate* if $f''(x) = 0$

Example 3.2.8. The point $f(x) = x^2$ has a nondegenerate critical point; but $f(x) = x^n$ has a degenerate critical point at 0.

Definition 3.2.9. The notion of a topological group is given in the definition. A continuous homomorphism of a topological group to itself is called an endomorphism; an invertible endomorphism is an automorphism. Many important examples of dynamical systems arise as translations or endomorphisms of topological groups.

The above examples and definitions follow from (Devaney, 1989; Brin and Stuck, 2002; Khrennikov and Nilsson, 2004; de Melo and van Strien, 1993).

Definition 3.2.10. Let $\Sigma^n = \{s = (s_0, s_1, ...)|s_j \in \{0, 1, ...(n-1)\}\}$ be the set of sequences of elements in $\{0, 1, 2, ..(n-1)\}$. Then $\Sigma^2 = \{s = (s_0, s_1, ...)|s_j \in \{0, 1\}\}$. Σ^n can be made into a metric space. For two sequences $s = (s_0, s_1, ...)$ and $t = (t_0, t_1, ...)$, define

$$d(s,t) = \sum_{i=0}^{i=\infty} \frac{|s_i - t_i|}{2^i}$$

When the state space is Σ^2, since $|s_i - t_i|$ is either 0 or 1, this infinite series is dominated by the convergent geometric series $\sum_{i=0}^{\infty} \frac{1}{2^i}$ (Devaney, 1989).

3.3 Arithmetic dynamical systems

Classically, discrete dynamics refers to the study of the iteration of self-maps of the complex plane or real line. Arithmetic Dynamics is the study of number theoretic properties of dynamical systems. Arithmetic dynamics is discrete-time dynamics (function iteration) over arithmetical sets, such as algebraic number rings and fields, finite fields, p-adic fields, polynomial rings, algebraic curves, etc. The study of arithmetic dynamics draws on ideas and techniques from both classical (discrete) dynamical

systems and the theory of Diophantine equations. Some constructs of arithmetic dynamics (periodic orbits and their stability), are straightforward adaptations of dynamical concepts. A standard technique in number theory is to attempt to answer questions related to a number field K by first studying analogous questions over each completion K_v of K. In particular, the archimedean completions of K lead back to classical dynamics over $\mathbb{R}$ or $\mathbb{C}$. The connections between dynamical systems and number theory arise in many different ways. One subject may provide a new insight or tool for the other.

In the next two chapters two instances of discrete dynamical systems are studied over the ring of p-adic integers $\mathbb{Z}_p$.

Chapter 4

p-adic Dynamical Systems

The study of the dynamics of polynomial and rational maps over $\mathbb{R}$ and $\mathbb{C}$ has a long history and includes many deep theorems. A more recent development is the creation of an analogous theory over complete local fields such as the p-adic rational numbers $\mathbb{Q}_p$ and the completion $\mathbb{C}_p$ of an algebraic closure of $\mathbb{Q}_p$. The non-Archimedean nature of the absolute value on $\mathbb{Q}_p$ and $\mathbb{C}_p$ makes some parts of the theory easier than when working over $\mathbb{C}$ or $\mathbb{R}$. But as usual, there is a price to pay. For example, the theory of non-Archimedean dynamics must deal with the fact that $\mathbb{Q}_p$ is totally disconnected and far from being algebraically closed, while $\mathbb{C}_p$ is not locally compact. One of the most important gadgets in the number theorist's toolbox is reduction modulo a prime. Thus when studying the number-theoretic properties of an object, it can be reduced modulo a prime, then analyze the properties of the hopefully simpler object, and lift the information back to obtain global information. A typical example is provided by Hensel's lemma, which under certain circumstances allows to lift solutions of a polynomial congruence $f(x) \equiv 0 (mod\, p)$ to solutions in $\mathbb{Z}_p$. Then, using information gathered from many primes, one is sometimes able to deduce results for a global field such as $\mathbb{Q}$. (Silverman, 2007)
This section is devoted to discrete p-adic dynamical systems, namely iteration

$$x_{n+1} = f(x_n)$$

of functions $f : \mathbb{Q}_p \to \mathbb{Q}_p$.

To study dynamical systems in fields of p-adic numbers $\mathbb{Q}_p$ and complex p-adic numbers $\mathbb{C}_p$ as well as finite extensions of $\mathbb{Q}_p$, it is convenient to consider the general case of an arbitrary non-Archimedean field $\mathbb{K}$.

4.1 Monomial dynamical systems

The definitions and theorems below are well known and can be found in any standard text on p-adic dynamics. The most studied p-adic dynamical systems are the so called monomial systems. A discrete monomial system is defined by the function $f(x) = x^n$. The roots of unity in $\mathbb{C}_p$ are essential for the investigations of monomial dynamical systems.

Definition 4.1.1. An element $x \in \mathbb{C}_p$ is said to be an n-th root of unity if $x^n = 1$. If $x^n = 1$ and $x^m \neq 1$ for every $m < n$ then we say that x is a root of unity of order n or a *primitive* n-th root of unity.

The multiplicative group of $\mathbb{F}_{p^f}$ is cyclic and has $p^f - 1$ elements. Since a cyclic group has a cyclic subgroup of order d for each divisor d of $p^f - 1$, for every $d|(p^f - 1)$ there exists $x \in \mathbb{F}_{p^f}^{\times}$ that generates the subgroup of d elements such that, $x^d = 1$. The element x generates a group of d roots of the polynomial $x^d - 1$ in $\mathbb{F}_{p^f}$. By Hensel's lemma, for each $d|(p^f - 1)$, the equation $x^d - 1 = 0$ has d solutions in $\mathbb{C}_p$. The definition of *fixed - point*, *periodic - point* are same as in dynamical systems.

Theorem 4.1.2. *The equation $x^k = 1$ has $gcd(k, p-1)$ solutions in $\mathbb{Q}_p$ when $p > 2$. If $p = 2$ then $x^k = 1$ has two solutions (x=1 and x=-1) if k is even and one solution (x=1) if k is odd.*

Theorem 4.1.3. *If $p = 2$ then the dynamical system $x^k = 1$ has no cycles of order $r \geq 2$.*

Theorem 4.1.4. *Let x and y be two n-th roots of unity in $\mathbb{Q}_p$ and let $x \neq y$. If $p > 2$ then $|x - y|_p = 1$. If $p = 2$ then $|x - y|_p = \frac{1}{2}$.*

4.2 p-adic chaos and random numbers

It is natural to consider chaotic maps as a source of randomness. But from a computational point of view these maps are not suited for machine computation . Since the classical chaotic maps are usually defined on real manifolds and the machine computation always admit discrete set of values.
Woodcock and Smart (1998) introduced the p-adic analog of the standard logistic map

$$x \to 4x(1-x)$$

and the Smale horse-shoe map

$$(x, y) \to (y, ax + by^2 + c)$$

for suitable a, b and c. The associated symbolic dynamics is respectively a one-sided shift and a full shift on two symbols. This is also the case for the p-adic analogues on p symbols rather than on two symbols. The analogous p-adic logistic and Smale horse-shoe maps are considered as idealized random number generator and modification of them is analysed in detail at $p = 2$ (Woodcock and Smart, 1998).

If p denotes a prime number, the p-adic logistic map is defined by

$$g : \mathbb{Z}_p \to \mathbb{Z}_p$$

$$x \to \frac{x^p - x}{p}$$

By Fermat's little theorem $g(x) = \frac{x^p - x}{p} \in \mathbb{Z}$ whenever $x \in \mathbb{Z}$. The case $p = 2$, leads to the analog of standard logistic map $L(x) = \frac{x^2 - x}{2}$. Also, L is sensitive to the initial condition in the sense that, if $x, y \in \mathbb{Z}_p$ with $v_p(x - y) = n \geq 1$ then $v_p(L(x) - L(y)) = n - 1$, (Woodcock and Smart, 1998).

Symbolic dynamics of $(\mathbb{Z}_p, g)$

For $x \in \mathbb{Z}_p$, the reduction modulo p of x is denoted by $\bar{x} \in F_p$ and set $X = \prod_{i\geq 0}(F_p)_i$, which is the direct product of a countable sequence of copies of F_p, each with discrete topology. On X, the continuous shift operator $T : X \to X$ is given by $(T(x))_i = x_{i+1}$ for all $x = (x_i) \in X$. The set X is a Cantor-like set, so in particular totally disconnected. Thus the following result follows:

Theorem 4.2.1. *Any two totally disconnected perfect compact metric spaces are homeomorphic.*

Theorem 4.2.2. *There is a homeomorphism $\Phi : \mathbb{Z}_p \to X$ such that $T \circ \Phi = \Phi \circ g$.*

It can be deduced from the above theorem that, the dynamical systems $(\mathbb{Z}_p, g)$ and (X, T) are toplogically conjugate. Hence many properties of $(\mathbb{Z}_p, g)$ can be directly read off from the symbolic representation (X, T). Thus, one is led to consider iterates of $g(x)$ modulo powers of p and those of $L(x)$ modulo powers of 2. In particular, the map $L(x)$ has been studied in great detail. Let $X_e = \{1, 2, 3, ..., 2^e\}$ and $L_e(x)$ denote the reduction of $L(x)$ modulo 2^e. Then it is shown that $L_e : X_e \to X_e$ defined by $L_e(x) = \frac{x^2-x}{2} \pmod{2^e}$ is a permutation of X_e, in fact an even permutation. It is also shown that as e increases, longer and longer orbits of L_e are got which behave well with respect to randomness and this particular case has been investigated in great detail as a source of generating pseudorandom numbers (Woodcock and Smart, 1998).

4.3 Topologically equivalent dynamical systems

In order to classify dynamical systems, notion of equivalence is needed. If $f : X \to X$ and $g : Y \to Y$ are two dynamical systems then a *semiconjugacy* from (Y, g) to (X, f) is a surjective map $\pi : Y \to X$ satisfying $f \circ \pi = \pi \circ g$.
An invertible semiconjugacy is called a *conjugacy*. If there is a conjugacy from one dynamical system to another, the two systems are said to be conjugate; conjugacy is an equivalence relation. To classify dynamical systems, equivalence classes determined by conjugacies preserving some specified structure are studied.

Definition 4.3.1. (Kuznestov, 1998; Kitchens, 1998; Devaney, 1989) A dynamical system $\{T, \mathbb{R}^n, \phi^t\}$ is called *topologically equivalent* to a dynamical system $\{T, \mathbb{R}^n, \psi^t\}$ if there is a homeomorphism $h : \mathbb{R}^n \to \mathbb{R}^n$ mapping orbits of the first system onto orbits of the second system, preserving the direction of time.

In general one can speak of topological conjugacy for homeomorphism of different topological spaces, $f : X \to X$, $f' : X' \to X'$. Then the conjugacy h is a homeomorphism $h : X \to X'$ if $f = h^{-1} f' h$.

Topological conjugation defines an equivalence relation in the space of all continuous surjections of a topological space to itself. This equivalence relation is very useful in the theory of dynamical systems, since each class contains all functions which share the same dynamics from the topological viewpoint.

This section concentrates on the topological conjugacy of the logistic map defined by Woodcock and Smart (1998) over the p-adic field. As a special case the topological conjugacy of the square map is considered. If h is a homeomorphism and f and g are related by $f = h^{-1} \circ g \circ h$, then f and g generally have similar behaviour; f and g are said to be *topologically equivalent*. The special homeomorphisms $h(x) = ax + b$ of $\mathbb{Q}_p$ (with $a, b \in \mathbb{Q}_p$ $a, b \neq 0$) is applied to the *logistic map* defined by $L(x) = \frac{x^p - x}{p}$ for $p = 2$ as a special case; also, the same homeomorphism is applied to the *quadratic map* and shown that these conjugate maps can behave quite differently and depends very much on the constants a, b and the prime p.

Now let $h(x) = ax + b, a, b \in \mathbb{Q}_p$ and $a \neq 0$. Then $h^{-1}(x) = \frac{x-b}{a}$, both h and h^{-1} are one-to-one, onto and continuous, hence homeomorphisms of $\mathbb{Q}_p$. Further, h is an isometry (preserves distances) if $|a|_p = 1$. The conjugates of the quadratic and logistic maps under such homeomorphisms are considered with the primary goal of being able to do all the computations in integer arithmetic.

Let $g(x) = x^2$. A straightforward calculation gives $f(x) = h^{-1} \circ g \circ h(x) = ax^2 + 2bx + \frac{b^2 - b}{a}$. The fixed points of $g(x)$ are 0 and 1 while those of $f(x)$ are $\frac{-b}{a}$ and $\frac{1-b}{a}$. To compute the sequences $x_i = g(x_{i-1})$ or $x_i = f(x_{i-1})$ in a computer it is

clear that the initial value x_0 must be chosen in $\mathbb{Z}_p \cap \mathbb{Z} = \mathbb{Z}$, as a computer cannot represent a general p-adic integer to arbitrary accuracy. Further some fixed level of p-adic precision is obtained by doing all the computations modulo p^e. This is also justified since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ (consequence of Hensel's lemma).

The simplest case is when $a = 1$ and $h(x) = x + b$, a translation and isometry. The conjugate map is $f(x) = x^2 + 2bx + (b^2 - b)$. If $b \in \mathbb{Z}$ then all iterates of f are integers and the fixed points 0 and 1 get mapped to $-b$ and $(1 - b)$. Both have similar dynamics and are topologically equivalent.

If $a \neq 1$, then for the fixed points $\frac{-b}{a}$ and $\frac{1-b}{a}$ to lie in $\mathbb{Z}$ it is necessary that a divides b and a divides $1 - b$. But this is impossible as b and $1 - b$ are always co-prime. So if a divides exactly one of b or $1 - b$ we get that only one of the fixed points is in $\mathbb{Z}$ while the other may or may not be in $\mathbb{Z}_p$ depending on the p-adic absolute values of a and b. One choice of a and b that makes $\frac{-b}{a}$ and $\frac{1-b}{a}$ to lie in $\mathbb{Z}$ is $a = \frac{1}{p^l}$ and $b = \frac{1}{p^k}$ with $l \geq k$.

Then $f(x) = \frac{1}{p^l}x^2 + \frac{2}{p^k}x + \frac{p^l(1-p^k)}{p^{2k}}$. Clearly values of f and its iterates will not be integers if $l, k > 1$. So, let $l = k = 1$ i.e., $a = b = \frac{1}{p}$. Then $f(x) = \frac{(x+1)^2}{p} - 1$, its fixed points are $\frac{-b}{a} = -1$ and $\frac{1-b}{a} = p - 1$. Since we need all iterates to be in $\mathbb{Z}$, let $x_0 \in \mathbb{Z}$. Then $x_1 = f(x_0) = \frac{(x_0+1)^2}{p} - 1$ and this forces $x_0 \equiv -1(mod\ p)$. In this case $x_1 \equiv -1(mod\ p)$ and so all successive iterates also lie in $\mathbb{Z}$. Moreover, since there is a factor of p in the denominator defining $f(x)$, it is clear that if $g(x)$ is reduced mod p^e then $f(x)$ needs to be reduced mod p^{e+1}. Also, all values of $f(x)$ are $\equiv -1(mod\ p)$ and there are exactly p^e distinct such numbers in the set $\{1, 2, 3, ..., p^{e+1}\}$ namely, $tp - 1$ with $t = 1, 2, 3..., p^e$. Both $f(x)$ and $g(x)$ have similar dynamics and are topologically equivalent.
Two simple examples are given below:

1. Let $a = 3$ and $b = 2$. Then $f(x) = 3x^2 + 4x + \frac{2}{3}$. Clearly iterates of f will not be integers. The fixed points are $\frac{-2}{3}$ and $\frac{-1}{3}$ and they lie in $\mathbb{Z}_p$ if and only if $p \neq 3$.

2. Let $a = 2$ and $b = 3$. Then $f(x) = 2x^2 + 6x + 3$ and so f and all its iterates

will be integers. Here the fixed points are $\frac{-3}{2}$ and -1, and $\frac{-3}{2} \in \mathbb{Z}_p$ if and only if $p \neq 2$.

Finally, the logistic map $L(x) = \frac{x^2-x}{2}$ is considered.
The translations $h(x) = x + b$ with $b \in \mathbb{Z}$ gives $f(x) = \frac{x^2+(2b-1)x+b(b-3)}{2}$ and this is always an integer if x is an integer.
Fixed points are $-b$ and $3-b$ and both belong to $\mathbb{Z}$. Thus, both f and g topologically equivalent. As before, since $p = 2$ here, $a = b = \frac{1}{2}$ and $f(x) = \frac{x^2-5}{4}$, so we need to reduce $f(x)$ mod 2^{e+1} if $L(x)$ is reduced mod 2^e. Also only odd values of x are admissible if $f(x)$ is to be an integer and all iterates of f are odd if x is odd. All the 2^e odd values in the set $\{1, 2, 3, ..., 2^{e+1}\}$ are taken on by f.

Both $L(x)$ as well as $f(x)$ have similar dynamics with respect to cycle lengths and fixed points. All the computations for $f(x)$ is verified as done in (Woodcock and Smart, 1998) and agrees with it. For monomial systems defined by $g(x) = x^n$ $(n > 2)$ the analysis is more involved and will be considered in future.

Chapter 5

p-adic Backward Dynamics

5.1 Backward dynamics

Backward-iteration sequences given by

$$x_n = f(x_{n+1}), \qquad n > 0$$

are of a different nature because a point could have infinitely many pre-images as well as none. If the given forward moving map is a quadratic map, the corresponding backward map is a square root map; if the given map is a cubic map the corresponding backward map is the cube root map and so on. Thus essentially one needs to solve $f(x) = 0$ as a polynomial over the defining set. For e.g., the Julia set can be found as the set of limit points of the set of pre-images of (essentially) any given point. Unfortunately, as the number of iterated pre-images grows exponentially, this is not feasible computationally when the underlying set is the set of Real or Complex numbers.

In general, maps of higher degree (≥ 5) are not suitable for backward dynamics over $\mathbb{R}$ or $\mathbb{C}$. As there is no explicit formula for solving a polynomial of degree ≥ 5, roots can be found by using standard techniques from Numerical Methods over $\mathbb{R}$ or $\mathbb{C}$ and one arrives at either a null sequence or constant sequence after some backward iterations. In such cases nothing can be said about the behavior of trajectories. But when the set is finite (endowed with algebraic structure) and the map is a polynomial it is possible

to retrieve the pre-images (roots), if they exist, with respect to different prime power moduli and thus study the structure of pre-images locally at that prime.
It is shown that this problem can be well understood over the ring of p-adic integers $\mathbb{Z}_p$. This process deals with an important branch of mathematics called *Inverse Limit Theory.*

Definition 5.1.1. Given a dynamical system defined by $x_n = G(x_{n+1})$, an infinite sequence $\{x_n\}$ is said to be *forward admissible (backward admissible)* if $x_n = G(x_{n+1})$ for all $n \in N$ (respectively for all $-n \in N$)(refer 3.2) .

To define infinite inverse sequences of G one must choose x_1 on the ordinate axis. The next point in the sequence x_2 must belong to the pre-image of x_1 under G. If the pre-image of x_1 contains more than one point, one of them is chosen if both the values are admissible and the procedure is repeated. During this process at any step $k \geq 1$, if the pre-image of a point x_k, under G, is empty, the sequence cannot be extended any further and the process must be stopped. The procedure is repeated for all initial points and for all possible combinations of pre-images. (If G is a two-to-one map there may be up to 2^n inverse sequences of length n for each initial point). All the sequences that had to be terminated after a finite number of steps must be discarded because they are not forward admissible according to the Definition 5.1.1.

5.2 Inverse limit theory

Some examples and basic definitions of Inverse limits are discussed in section 2.4.

Universal property of inverse limits:

Definition 5.2.1. A *topological* group is a set G with both the structure of a group, and of a topological space, such that the multiplication law $G \times G \to G$ and the inverse map $G \to G$ are continuous maps of topological spaces.

Definition 5.2.2. A *homomorphism* of topological groups is a homomorphism of the underlying groups which is continuous. An *isomorphism* of topological groups is a homomorphism of the underlying groups which is a homeomorphism.

The definition of isomorphism is equivalent to the existence of an inverse (continuous) homomorphism, but is not equivalent to being a (continuous) bijective homomorphism, because the set-theoretic inverse need not be continuous in general.

Let $I = (I, \leq)$ denote a directed partially ordered set or directed poset. An *inverse* or *projective* system of topological spaces (respectively, topological groups) over I, consists of a collection $\{X_i \mid i \in I\}$ of topological spaces (respectively, topological groups) indexed by I, and a collection of continuous mappings (respectively, continuous group homomorphisms) $\varphi_{ij} : X_i \to X_j$, defined whenever $i \geq j$ such that the diagram of the form

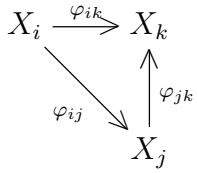

Figure 5.1: Projective limits

commutes whenever they are defined, i.e., whenever i, j, $k \in I$ and $i \geq j \geq k$. Such a system is denoted by $\{X_i, \varphi_{ij}, I\}$ or by $\{X_i, \varphi_{ij}\}$. if the index set I is clearly understood. If X is a fixed topological space (respectively, topological group), denote by $\{X, id\}$ the inverse system $\{X_i, \varphi_{ij}, I\}$, where $X_i = X$ for all $i \in I$, and φ_{ij} is the identity mapping $id : X \to X$. Then $\{X, id\}$ is the constant inverse system on X. Let Y be a topological space (respectively, topological group), $\{X_i, \varphi_{ij}, I\}$ an inverse system of topological spaces (respectively, topological groups) over a directed poset I, and let $\psi_i : Y \to X_i$ be a continuous mapping (respectively, continuous group homomorphism) for each $i \in I$. These mappings ψ_i are said to be compatible if $\varphi_{ij}\psi_i = \psi_j$ whenever $j \leq i$.

One says that a topological space (respectively, topological group) X together with compatible continuous mappings (respectively, continuous homomorphisms)

$$\varphi_i : X \to X_i \qquad \forall i \in I$$

is an *inverse limit* or a *projective limit* of the system $\{X_i, \varphi_{ij}, I\}$ if the following universal property is satisfied:
whenever Y is a topological space (respectively, topological group) and

$$\psi_i : Y \to X_i \quad i \in I$$

is a set of compatible continuous mappings (respectively, continuous homomorphisms), then there is a unique continuous mapping (respectively, continuous homomorphism) $\psi : Y \to X$ such that $\varphi_i \psi = \psi_i \quad \forall \quad i \in I$. One may say that ψ is "induced" or "determined" by the compatible homomorphisms ψ_i.
The maps $\varphi_i : X \to X_i$ are called projections. The projective maps φ_i are not necessarily surjections. The inverse limit is denoted by (X, φ_i), or often simply by X, by abuse of notation. The definitions are depicted in the form of commutative diagram 5.2 below.

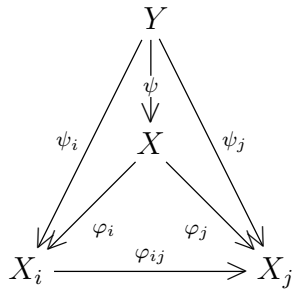

Figure 5.2: Universal property of inverse limits

If $\{X_i, I\}$ is a collection of topological spaces (respectively, topological groups) indexed by a set I, its direct product or Cartesian product is the topological space (respectively, topological group) $\prod_{i \in I} X_i$, endowed with a product topology.
Let $X_0, X_1, X_2, ...$ be a countable collection of spaces, and suppose that, for each $n > 0$, there is a continuous mapping $f_n : X_n \to X_{n-1}$. The seqence of spaces and

mappings $\{X_n, f_n\}$ is called an *inverse limit sequence* and may be represented as

$$... \xrightarrow{f_{n+1}} X_n \xrightarrow{f_n} X_{n-1} ... \xrightarrow{f_2} X_1 \xrightarrow{f_1} X_0$$

Clearly, if $n > m$, there is a continuous mapping $f_{n,m} : X_n \to X_m$ given by the composition $f_{n,m} = f_{m+1} \cdot f_{m+2} \cdots f_{n-1} \cdot f_n$.
Consider a sequence $(x_0, x_1, ..., x_n, ..)$ such that each x_n is a point of the space X_n and such that $x_n = f_{n+1}(x_{n+1}),\ n \geq 0$. Such a sequence can be identified in the product space $\prod_{n=0}^{\infty} X_n$ by considering a function φ from the non-negative integers into $\cup_{n=0}^{\infty} X_n$, given by $\varphi(n) = x_n$. Thus the set of all such sequences is a subset of $\prod_{n=0}^{\infty} X_n$ and has a topology as a subspace. This topological space is the inverse limit space of the sequence $\{X_n, f_n\}$ denoted by $X = \varprojlim(X_n, f_n)$.

Theorem 5.2.3. *Suppose that each space X_n in the inverse limit sequence $\{X_n, f_n\}$ is a compact Hausdorff space. Then X is not empty (Hocking and Young, 1961).*

Theorem 5.2.4. *A space X is a compact Hausdorff space with $dim(X) \leq 0$ if and only if X is an inverse limit of finite discrete spaces (Nagami, 1970).*

A finite discrete space is totally disconnected, compact and Hausdorff and all those properties carry over to inverse limits too.
A detailed study of Inverse limit spaces can be found in (Hocking and Young, 1961).
An important class of such inverse limits is given by rings of p-adic integers $\mathbb{Z}_p$. For every $n \geq 1$, let $A_n = \mathbb{Z}/p^n\mathbb{Z}$. An element of A_n defines in an obvious way an element of A_{n-1} and the homomorphism

$$\varphi_n : A_n \to A_{n-1}$$

is surjective and the kernel is $p^{n-1}A_n$. The sequence

$$... \to A_n \to A_{n-1} ... \to A_2 \to A_1$$

forms a "projective system" indexed by the integers ≥ 1.
Inverse limit of this inverse system is $\mathbb{Z}_p = \varprojlim(A_n, \varphi_n)$. An element of $\mathbb{Z}_p = \varprojlim(A_n, \varphi_n)$ is a sequence $x = (..., x_n, ..., x_1)$ with $x_n \in A_n$ and $\varphi_n(x_n) = x_{n-1}$ if $n \geq 2$. Addition

and multiplication in $\mathbb{Z}_p$ are defined co-ordinate wise. In other words, $\mathbb{Z}_p$ is a subring of the product $\prod_{n\geq 1} A_n$. If A_n is endowed with discrete topology and $\prod_{n\geq 1} A_n$ the product topology, the ring $\mathbb{Z}_p$ inherits a topology which turns it into a compact space.

The connection between congruences and equations is based on the simple remark that, if the equation

$$F(x_1, x_2, ..., x_n) = 0$$

where F is a polynomial with integral coefficients, has a solution in integers, then the congruence

$$F(x_1, x_2, ..., x_n) \equiv 0 \pmod{m}$$

is solvable for any value of the modulus m. On the other hand the situation is more complicated for congruences. For any modulus $m > 1$, there are polynomial congruences having no solutions. For eg., the congruence $x^p - x + 1 \equiv 0 \pmod{m}$ has no solution if p is any prime factor of m by Fermat's theorem. In general, a congruence can have more solutions than its degree, for eg., $x^2 - 7x + 2 \equiv 0 \pmod{10}$ has four solutions $x = 3, 4, 8, 9$. But if the modulus is a prime, a congruence cannot have more solutions than its degree.

Theorem 5.2.5. *If the degree n of $f(x) \equiv 0 \pmod{p}$ is greater than or equal to p, then either every integer is a solution of $f(x) \equiv 0 \pmod{p}$ or there is a polynomial $g(x)$ having integral coefficients, with leading coefficient 1, such that, $g(x) \equiv 0 \pmod{p}$ is of degree less than p and the solutions of $g(x) \equiv 0 \pmod{p}$ are precisely those of $f(x) \equiv 0 \pmod{p}$.*

Theorem 5.2.6. *The congruence $f(x) \equiv 0 \pmod{p}$ of degree n has atmost n solutions.*

Corollary 5.2.7. *If $b_n x^n + b_{n-1} x^{n-1} + ... + b_0 \equiv 0 \pmod{p}$ has more than n solutions, then all the coefficients b_j are divisible by p.*

Theorem 5.2.8. *The congruence $f(x) \equiv 0 \pmod{p}$ of degree n, with leading coefficient $a_n = 1$, has n solutions if and only if $f(x)$ is a factor of $x^p - x$ modulo p, that is,*

if and only if $x^p - x = f(x)q(x) + ps(x)$*, where* $q(x)$ *and* $s(x)$ *have integral coefficients,* $q(x)$ *has degree* $p - n$ *and leading coefficient* 1*, and where* $s(x)$ *is a polynomial of degree less than* n *or* $s(x)$ *is zero.*

The proofs of the above theorems are simple consequences of Fermat's little theorem and its application which can be found in many books on number theory.

5.2.1 Hensel's lifting lemma

As both $\mathbb{Q}$ and $\mathbb{R}$ are not algebraically closed, they do not always contain all roots of polynomials with integer coefficients. Though $\mathbb{C}$ is algebraically closed, as the degree of the polynomial increases, finding roots of the polynomial is computationally not feasible, as it requires high level of precision for machine computation. For this purpose it is natural to turn one's attention to solving polynomial congruences modulo prime powers.
One may note that for any polynomial $f(x) \in \mathbb{Z}[x]$ and any integer r, there is a polynomial $g_r(x) \in \mathbb{Z}[x]$ with $f(x + r) = f(r) + xf'(r) + x^2 g_r(x)$.
This can be seen either through the Taylor expansion for $f(x + r)$ or through the binomial theorem in the form

$$(x + r)^d = r^d + dr^{d-1}x + x^2 \sum_{j=2}^{d} \binom{d}{j} r^{d-j} x^{j-2} \tag{5.2.1}$$

The above standard results mentioned in the form of Theorems can be used to find the solutions to $f(x) \equiv 0 \pmod{p}$. The question is how one may be able to lift a solution to one modulo p^k for various exponents k. With regard to this, Hensel's Lemma is a powerful tool which relates the roots of a given polynomial to its solution modulo a prime. The lemma and its proof both rely on iterative procedures that return an agreeable solution if supplied with a well-behaved seed.

Definition 5.2.9. If $f(a) \equiv 0 \pmod{p}$, then the root a is called *nonsingular* if $f'(a) \not\equiv 0 \pmod{p}$; otherwise it is *singular.*

Two versions of *Hensel's Lemma* are stated below.

Theorem 5.2.10. *(Hensel's Lemma over the ring of integers)*
Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

Theorem 5.2.11. *(Hensel's Lemma over the ring of p-adic integers)*
Let $f \in \mathbb{Z}_p[x]$ be monic. If $a_0 \in \mathbb{Z}$ is a simple root of $f(x) \equiv 0 \pmod{p}$, then $\exists\, y \in \mathbb{Z}_p$ such that $y \equiv a_0 \pmod{p}$ and $f(y) = 0$.

Proof. Suppose that $\exists a_n$ such that $f(a_n) \equiv 0 \pmod{p^n}$. Need to show that a_n can be lifted uniquely to $a_{n+1} \pmod{p^{n+1}}$ such that $a_{n+1} \equiv a_n \pmod{p^n}$ and $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$, then y is the limit of this sequence of $\pmod{p^k}$ solutions.
Since f is a polynomial one can write it in the form $f(x) = \sum_i c_i x^i$. Also consider $tp^n + a_n$ as a possible lift of a_n . Then

$$f(a_n + tp^n) = \sum_i c_i (tp^n + a_n)^i \tag{5.2.2}$$

$$\equiv f(a_n) + p^n t f'(a_n) \pmod{p^{n+1}}. \tag{5.2.3}$$

The equivalence above is a result of Taylor series expansion. Now, solve for t in

$$p^n t f'(a_n) + f(a_n) \equiv 0 \pmod{p^{n+1}}.$$

Thus

$$t f'(a_n) \equiv -\left(\frac{f(a_n)}{p^n}\right) \pmod{p}.$$

But, $f(a_n) \equiv 0 \pmod{p^n}$, (since $a_n \equiv a_0 \pmod{p}$) and $f'(a_n) \not\equiv 0 \pmod{p}$ (simple root), so, t has a unique solution $\pmod{p}$. Thus $a_{n+1} = a_n + tp^n$ is a unique lift of $a_n \pmod{p}$. Thus an infinite sequence of a_i such that $f(a_i) \equiv 0 \pmod{p^i}$, $f'(a_i) \not\equiv 0 \pmod{p^i}$ and $a_{i+1} \equiv a_i \pmod{p}$ is obtained. This sequence is Cauchy, and therefore converges to a unique limit $y \in \mathbb{Z}_p$. □

Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, proof of Theorem 5.2.10 follows directly from Theorem 5.2.11.
It can be verified that proof of Hensel's Lemma is entirely analogous to Newton's

method for locating the root of a differentiable function. Recall Newton's method from calculus as a method of finding roots to a polynomial by choosing a seed and then making better and better approximations based on the polynomial's derivative at that point. In the case of Newton's method, the condition on the seed is that the derivative at that point be non-zero, otherwise it supplies no useful information for improving at each iteration. Hensel's Lemma is similar, it takes a polynomial with coefficients in $\mathbb{Z}_p$ and instead of requiring a guess at a possible root, it requires a p-adic integer that is a root mod p, i.e. some α such that the polynomial $f(x)$ evaluated at α is

$$f(\alpha) \equiv 0 \pmod{p\mathbb{Z}_p}$$

This method will then return roots mod $p, p^2, p^3, ...$ until the desired root of the equation is found.

5.3 p-adic approximation

It is known that the direct product of totally disconnected spaces is totally disconnected. Also, if the original spaces are discrete, then the limit space $\varprojlim\{X, f\}$ is totally disconnected. This is one way of realizing the p-adic numbers and the Cantor set (as infinite strings). Since the space $\varprojlim\{X, f\}$ is totally disconnected, it is not possible to base the arithmetic structure on $\mathbb{R}$, the set of real numbers. But it is possible to consider the space $\varprojlim\{X, f\}$ to be $\mathbb{Z}_p$, the ring of p-adic integers. This follows from the following two theorems.

Theorem 5.3.1. *Any two totally disconnected perfect compact metric spaces are homeomorphic.*

Theorem 5.3.2. *Let M be a compact, totally disconnected metric space. Then M is homeomorphic to the inverse limit space of an inverse limit sequence of finite, discrete spaces.*

To find the backward iteration of any given polynomial $f(x)$ of arbitrary degree say n, at any point, say x_n of the forward iterating orbit, one needs to solve

$$f(x) \equiv x_n \pmod{p^k} \tag{5.3.1}$$

for some $k \in \mathbb{N}$. For this, first solve the congruence $f(x) \equiv x_n \pmod{p}$, such that the nonzero coefficients of $f(x)$ are relatively prime to p and x_n is chosen as above, so that the corresponding backward iterating orbit of x_n are found modulo p^j, $j \to \infty$. If the degree n of $f(x)$ is greater than p, then by Theorem 5.2.5, $f(x)$ is divisible by $(x^p - x) \bmod p$ and solutions of the resulting polynomial $g(x)$ are the same as those of $f(x) \equiv x_n \pmod{p}$. Since the modulus is prime, the congruence cannot have more solutions than its degree.

Let $a_1, a_2, ..., a_l$ be the roots obtained, by solving the congruence $f(x) \equiv x_n \pmod{p}$ where ($l \leq deg(g(x)$ by Theorem 5.2.6). Now each a_i is lifted modulo p^j, $j = 2, 3, ...$ whenever $f'(a_i) \not\equiv 0 \pmod{p}$, $(i = 1, 2, .., l.)$i.e., whenever the $a_i's$ are nonsingular. Working up to a fixed precision say $j = k$, once the roots are lifted modulo p^k, x_n is replaced by the lifted root and the congruence (5.3.1) is solved now with respect to the new root. The process of replacing the old root by the *new lifted root* is repeated for some finite number of steps. Thus with respect to each nonsingular a_i, we obtain the corresponding backward sequence, generated from the single seed x_n. Thus if there are n nonsingular roots, after the mth step of replacing the old root by the *new lifted root*, there are atmost n^m backward iterating points generated from the single seed x_n. Hence there exists a tree like structure, the roots may be called as leaves and the branches are formed at each new lifted root. A simple code for this program can be written on Python, which computes the sequences effectively.

Sequences thus obtained belong to the *inverse limit space* by definition. It can be verified that the sequence space formed by the above backward iterations is totally disconnected and discrete. Also, if the original spaces are discrete, then the inverse limit space $\varprojlim\{X, f\}$ is totally disconnected. This is one way of realizing the p-adic numbers and the Cantor set.

To study the long time behaviour of a dynamical system it is necessary to introduce a suitable metric. A natural choice would be the one given in section 3.1, i.e., the distance between two sequences $s = (s_0, s_1, ...)$ and $t = (t_0, t_1, ...)$ is given by $d(s,t) = \sum_{i=0}^{\infty} \frac{s_i - t_i}{p^i}$.

Thus by the introduction of a metric, sequence space of backward iteration becomes a compact metric space. The sequence space thus obtained can be identified with the ring of p-adic integers. Since extensive study has been made on the dynamics of the

logistic map, the p-adic analog of the logistic map is deliberately chosen as a practical example for backward dynamics. If p denotes a prime, p-adic logistic map is defined to be

$$\ell : \mathbb{Z}_p \to \mathbb{Z}_p$$

$$x \to cx(1-x)$$

where c is small in the sense $|c|_p < 1$. Denote the reduction of x modulo p by $\bar{x} \in \mathbb{F}_p$ and set $X = \prod_{i\geq 0}(\mathbb{F}_p)_i$ which is the direct product of countably infinite copies of $\mathbb{F}_p$, each with discrete topology. Also, X is a compact Hausdorff space. On X the continuous shift operator is defined as

$$T : X \to X$$

$$T(x)_i = x_{i+1}\, \forall x \in X.$$

The following theorem is basic:

Theorem 5.3.3. *There is a homeomorphism $\varphi : \mathbb{Z}_p \to X$ such that $T \circ \varphi = \varphi \circ \ell$.*

Proof. This follows from theorems 5.3.1 and 5.3.2. □

Since φ is an injective mapping, it induces a natural injective map:

$$\varphi_N : \mathbb{Z}_p/p^N\mathbb{Z}_p \to \prod_{i=1}^{N-1}(\mathbb{F}_p)_i$$

The mapping is surjective for each $N \geq 1$. From the above theorem it is clear that the dynamical systems $(\mathbb{Z}_p, l)$ and (X, T) are topologically conjugate which means that many properties of $(\mathbb{Z}_p, l)$ can be read off directly from the more transparent symbolic representation (X, T). As an illustration, to observe backward moving points in the orbit cycle, the quadratic equation $y = cx(1-x)$, where y is the current value and c is the given constant is considered. On solving, two equations for x are obtained.

$$x_1 = \frac{c + \sqrt{c^2 - 4cy}}{2c}$$

$$x_2 = \frac{c - \sqrt{c^2 - 4cy}}{2c}$$

Both these values may not always lie in $\mathbb{Z}_p$. To find the set of all values in $\mathbb{Z}_p$, the following consequence of Hensel's Lemma is useful.

Theorem 5.3.4. *(Katok, 2007, chapter 1) A polynomial with integer coefficients has a root in $\mathbb{Z}_p$ if and only if it has an integer root modulo p^k for any $k \geq 1$.*

In particular, when the given equation is quadratic, say of degree two, it is known that a rational integer x not divisible by a prime p has a square root in $\mathbb{Z}_p$ if and only if x is a quadratic residue modulo p. To know the set of all admissible backward sequences, we need to check whether $c^2 - 4cy$ is a quadratic residue modulo the base prime p. The backward sequences generated by $y = cx(1 - x)$ will be nonempty, as long as the roots of $y = cx(1 - x)$ are quadratic residues modulo the base prime p, that is to say that the roots of $y = cx(1 - x)$ lie in $\mathbb{Z}_p$.

Since the logistic map $f(x) = cx(1 - x)$ and the quadratic map $g(x) = x^2 + d$ are conjugates of each other through a linear homeomorphism $x = ay + b$, (refer 3.2) for suitable a and b, the maps are equivalent as far as their dynamics are concerned. Since the transformation is done through a homeomorphism, their topological features are preserved. The maps also preserve the properties like pseudorandomness, number of orbit cycles with respect to the given initial point.

Chapter 6

Number Fields

The theory of algebraic number fields has its origin in the attempts to generalize the quadratic reciprocity law and related questions. The development of Algebraic Number Theory is divided into three main periods. The period $(1800 - 1870)$ is considered to be the introductory period. In this sense, it started with Gauss, Eisenstein, Jacobi, and Dirichlet and reached its first peak in the work of Kummer about cyclotomic fields. Kummer restricted his investigations to algebraic numbers connected with the nth roots of unity and the nth roots of such numbers. On the other hand, Dirichlet considered the group of units of the ring generated over $\mathbb{Z}$ by an arbitrary integral algebraic number and determined the structure of this group. It was Dedekind who understood that the basic notion of the theory is the notion of algebraic number field (in German, *algebraischer Zahlkörper*), which was absent in the investigations of his predecessors.

The period $(1871 - 1896)$ is considered as the basic period. During this period the basic notions and theorems were formulated and proved. This was done in three equivalent ways by Dedekind, Kronecker, and Zolotarev. Dedekind formulated the theory by means of ideals, an approach which is now generally accepted. Dedekind's invention of ideals in the 1870s was a major turning point in the development of algebra. His aim was to apply ideals to number theory, but to do this he had to build the whole frame work of commutative algebra: fields, rings, modules and vector spaces.

The study of Class field theory began in the period $(1897 - 1930)$, considerd to be the heroic period. An abelian extension of a field is a Galois extension of the field with abelian Galois group. Class field theory describes the abelian extensions of a number field in terms of the arithmetic of the field. Already Kronecker conjectured that there is a theory of abelian extensions (i.e., normal extensions with abelian Galois groups) of algebraic number fields which is much richer than the theory of algebraic number fields in general. This was based on his investigations about abelian extensions of $\mathbb{Q}$ and of imaginary quadratic extensions. But the first formulations of such a theory go back to D. Hilbert and H. Weber. Hilbert defined what is now called the Hilbert class field of an algebraic number field K. This is the maximal abelian extension $\mathcal{H}$ of K that is unramified at all places. The degree of this extension should be the class number of K and the inertial degree of a prime ideal $\mathfrak{p}$ of K in $\mathcal{H}$ should be equal to the order of its class in the ideal class group of K. Furthermore, Hilbert conjectured that every ideal of K becomes principal in $\mathcal{H}$ (Principal ideal conjecture). The existence of the Hilbert class field has been proved by P. Furtwaïgler in *Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers, Math. Ann. 1907. Bd. 63. S. 137.*

6.1 Basic concepts

An algebraic number field is a finite extension of $\mathbb{Q}$; an algebraic number is an element of an algebraic number field. More precisely,

Definition 6.1.1. A number α in $\mathbb{C}$ is called an *algebraic number* if there exists a polynomial $f(x) = a_n x^n + \cdots + a_0$ such that, $a_0, ..., a_n$, not all zero are in $\mathbb{Q}$ and $f(\alpha) = 0$.
If α is a root of monic polynomial with coefficients in $\mathbb{Z}$ then α is an *algebraic integer*. Clearly all algebraic integers are algebraic numbers. However the converse is not true.

Definition 6.1.2. An algebraic number of degree d is a root of an integral polynomial of degree d and not the root of an integral polynomial of degree less than d. If α is an algebraic number, the field $\mathbb{Q}(\alpha)$ is formed from the adjunction of α to the rational field $\mathbb{Q}$, this is an algebraic number field of degree d over $\mathbb{Q}$ generated by α.

$\mathbb{Q}$ is the smallest algebraic number field of dimension 1 over itself. The simple field extension $\mathbb{Q}(\alpha)$ is the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and α.
Complex numbers that are not algebraic are called transcendental numbers, examples being e and π. Therefore the real numbers $\mathbb{R}$ may be considered as the disjoint union of algebraic and transcendental numbers. Georg Cantor proved that the set of all algebraic numbers is countable, and so, the set of transcendental numbers are uncountable.

Definition 6.1.3. A subfield K of $\mathbb{C}$ is called an *algebraic number field* if its dimension as a vector space over $\mathbb{Q}$ is finite. The dimension of K over $\mathbb{Q}$ is called the degree of K, and is denoted by $[\mathbb{K} : \mathbb{Q}]$.

Definition 6.1.4. Let F be an algebraic number field. If α is algebraic over F, then it has a unique minimal polynomial over F, denoted by $m_{\alpha,F}(x)$, called the *minimal polynomial* of α over $\mathbb{F}$. Conversely, if α is the root of an irreducible, monic polynomial $f(x) \in F[x]$, then f is its minimal polynomial over F. Moreover every polynomial in $F[x]$ for which α is a root must be divisible by $m_{\alpha,F}(x)$.

Let E be an extension field of F, and let K be the set of all elements of E that are algebraic over F. Then K is an algebraic field extension of F.

Definition 6.1.5. The set of all algebraic numbers $\bar{\mathbb{Q}}$ in $\mathbb{C}$ is a subfield of $\mathbb{C}$. In particular all finite extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\alpha)$ for an algebraic number α.

Definition 6.1.6. Let the set of all algebraic integers in $\bar{\mathbb{Q}}$ be denoted by $\mathbb{A}$. Then $\mathbb{A}$ is a subring of $\bar{\mathbb{Q}}$. Then for any algebraic number field F, the intersection $F \cap \mathbb{A}$ is a ring in F called the ring of algebraic integers in F, denoted by $\mathcal{O}_F$. The ring of integers of $\mathbb{Q}$ is $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Definition 6.1.7. Roots of the minimal polynomial $m_{\alpha,F}(x)$ of α are called the *conjugate roots* or *conjugates* of α. If $m_{\alpha,F}(x)$ has degree n, then α has n conjugates. Also, if α is algebraic over F, then $[F(\alpha : F)] = deg(m_{\alpha,F}(x))$. Thus, $F(\alpha)$ can be viewed as a vector space over F of dimension $deg(m_{\alpha,F}(x))$. In particular, all finite extensions of $\mathbb{Q}$ are of the form $\mathbb{Q}(\alpha)$ for an algebraic number α.

Definition 6.1.8. If $F = \mathbb{Q}(\alpha)$ is an algebraic number field of degree d over $\mathbb{Q}$, there exist exactly d embeddings θ_j for $j = 1, 2, ..., d$ of F in $\mathbb{C}$. Furthermore, all of the conjugates of α over $\mathbb{Q}$ are the $\theta_j(\alpha) = \alpha_j$ with $\alpha_1 = \alpha$, and these are precisely the roots of the minimal polynomial $m_{\alpha,F}(x)$ of α over $\mathbb{Q}$.

The following result is well known:

Theorem 6.1.9. *Let $K = \mathbb{Q}(\alpha)$ be an extension field of degree n over $\mathbb{Q}$. Let $\omega_1, ..., \omega_n$ be a basis of K as a vector space of dimension n over $\mathbb{Q}$. Then the matrix $\Omega = (\omega_i^{(j)})$ is invertible.*

Let F be an algebraic number field of degree d over $\mathbb{Q}$, and let θ_j for $j = 1, 2, ..., d$ be the embeddings of F in $\mathbb{C}$. For each element $\alpha \in F$, set

$$T_F(\alpha) = \sum_{j=1}^{d} \theta_j(\alpha)$$

called the *trace* of α from F, and

$$N_F(\alpha) = \Pi_{j=1}^{d} \theta_j(\alpha)$$

called the *norm* of α from F. If α is an algebraic integer then both $T_F(\alpha)$ and $N_F(\alpha)$ are in $\mathbb{Z}$. If F is a number field then the ring of integers in F, is denoted by $\mathcal{O}_\mathcal{F}$. The ring of integers of $\mathbb{Q}$ is $\mathcal{O}_\mathcal{Q} = \mathbb{Z}$.

Definition 6.1.10. The ring $\mathcal{O}_\mathcal{F}$ of integers of an algebraic number field F is an abelian group under addition. Then a basis for $\mathcal{O}_\mathcal{F}$ over $\mathbb{Z}$ or simply a $\mathbb{Z}$-basis, is called an *integral basis* for F or for $\mathcal{O}_\mathcal{F}$. Thus, $\{\alpha_1, \alpha_2, ..., \alpha_s\}$ is an integral basis if and only if all $\alpha_i \in \mathcal{O}_\mathcal{F}$ and every element of $\mathcal{O}_\mathcal{F}$ can be uniquely expressed in the form $a_1\alpha_1 + ... + a_s\alpha_s$ for rational integers $a_1, ..., a_s$.

The following results are basic, proofs which can be found in any standard text on Algebraic Number Theory.

Theorem 6.1.11. *Every algebraic number field F of degree d over $\mathbb{Q}$ has an integral basis, and $\mathcal{O}_F$ is a free abelian group of rank d. As a $\mathbb{Z}-$module*

$$\mathcal{O}_F = \mathbb{Z}\beta_1 \oplus .... \oplus \mathbb{Z}\beta_d.$$

Thus $\mathcal{O}_F$ is a free abelian group of rank d, i.e., where $\{\beta_1, \beta_2, ...\beta_d\}$ is a basis for $\mathcal{O}_F$.

Let K be a number field and $\mathcal{O}_K$ be its ring of integers. An element $\alpha \in \mathcal{O}_K$ is called a unit if $\exists \beta \in \mathcal{O}_K$ such that, $\alpha\beta = 1$. The set of all units in $\mathcal{O}_K$ denoted by $U(K)$ forms a multiplicative subgroup of K^*.

Theorem 6.1.12. ***Dirichlet's Units Theorem***
Let $U(K)$ be the unit group of K. Let $[K : Q] = n$, and $n = r_1 + 2r_2$ where r_1 and $2r_2$ are, respectively, the number of real and complex embeddings of K in $\mathbb{C}$. Then there exist fundamental units $\epsilon_1, ..., \epsilon_r$, where $r = r_1 + r_2 - 1$, such that, every unit $\epsilon \in U(K)$ can be written uniquely in the form

$$\epsilon = \zeta \epsilon_1^{n_1} ... \epsilon_r^{n_r}$$

where $n_1 ... n_r \in \mathbb{Z}$ and ζ is a root of unity in $\mathcal{O}_K$. More precisely, if W_K is the subgroup of U_K consisting of roots of unity, then W_K is finite and cyclic and $U(K) \simeq W_K \times \mathbb{Z}^r$.

Example 6.1.13.
1. For $R = \mathbb{Q}$, $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$
2. For $R = \mathbb{Z}$, the units are ± 1.
3. For $R = \mathbb{Z}[i]$, the units are, $\{\pm 1, \pm i\}$

Theorem 6.1.14. *The group of units U of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$, for d squarefree is as follows:*

- *For $d = -1$, $U = \{\pm 1, \pm i\}$*
- *For $d = -3$, $U = \{\pm 1, \pm\omega, \pm\omega^2\}$*
- *For all other d, $U = \{\pm 1\}$*

Theorem 6.1.15. *The group of units of a real quadratic field $\mathbb{Q}(\sqrt{d})$ is infinite cyclic.*

Proposition 6.1.16. *For a domain D,*

1. *x is a unit if and only if $x|1$.*
2. *Any two units are associates and any associate of a unit is a unit.*

3. x, y are associates if and only if $x|y$ and $y|x$.

4. x is irreducible if and only if every divisor of x is an associte of x or a unit.

5. an associate of an irreducible is irreducible.

Proofs follow directly from the definition. Thus an element a in a domain D is a unit if and only if norm $N(a) = \pm 1$
A domain D is called a *unique factorization domain* if factorization into irreducibles is possible and unique. In a unique factorization domain all irreducibles are prime.

Ideals

An *ideal* is a nonempty subset I of a commutative ring R satisfying:

- If α, $\beta \in I$, then $\alpha - \beta \in I$
- If $r \in R$, and $\alpha \in I$, then $\alpha r \in I$.

Definition 6.1.17. An ideal I in a commutative ring R is called a *principal ideal* if there exists some $a \in R$ such that, $I = (a)$. An integral domain R is called a *principal ideal domain* if every ideal of R is a principal ideal.

Definition 6.1.18. An ideal I in a commutative ring R is called a *prime ideal* if it is a proper ideal and $ab \in I$ implies $a \in I$ or $b \in I$.

Definition 6.1.19. An ideal I in a commutative ring R is a *maximal ideal* if it is a proper ideal and there is no ideal J with $I \subsetneqq J \subsetneqq R$.

Theorem 6.1.20. *A proper ideal I in R is a prime ideal if and only if R/I is a domain. A commutative domain with $1 \neq 0$ is called an integral domain.*

Theorem 6.1.21. *A proper ideal I in R is a maximal ideal if and only if R/I is a field.*

Theorem 6.1.22. *Any prime ideal of $\mathcal{O}_K$ is maximal.*

Remark 6.1.23. If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}$, then $\mathfrak{p}$ contains exactly one prime number $p > 0$ of $\mathbb{Z}$.

The norm $N(\alpha)$ of the principal ideal (α) generated by $\alpha \neq 0$ in $\mathcal{O}$ is the absolute value $|N_K(\alpha)|$ of the norm $N_K(\alpha)$.

Corollary 6.1.24. *For $t \in \mathbb{Z}$, $N(t\mathcal{O}) = |N(t)| = t^2$.*

Lemma 6.1.25. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral ideals. Then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$*

If R is an integral domain, the field of fractions of R, $Frac(R)$ is the field of all equivalence classes of formal quotients a/b, where $a, b \in R$ with $b \neq 0$, and $a/b \sim c/d$ if $ad = bc$.

Definition 6.1.26. An integral domain R is *integrally closed* in its field of fractions if whenever α is in the field of fractions of R and α satisfies a monic polynomial $f(x) \in R[x]$, then $\alpha \in R$.

Every unique factorization domain is integrally closed.

Proposition 6.1.27. *If K is any number field then $\mathcal{O}_K$ is integrally closed.*

Definition 6.1.28. A fractional ideal is nonzero $\mathcal{O}_K$-submodule I of K that is finitely generated as an $\mathcal{O}_K$-module.
A fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is an $\mathcal{O}_K$- module contained in K such that there exists $m \in \mathbb{Z}$ with $m\mathfrak{a} \subset \mathcal{O}_K$. Any ideal of $\mathcal{O}_K$ is a fractional ideal by taking $m = 1$.

Theorem 6.1.29. *Any fractional ideal is finitely generated as an $\mathcal{O}_K$ module.*

Theorem 6.1.30. *Given any fractional ideal $\mathfrak{a} \neq \{0\}$ in K, there exista a fractional ideal $\mathfrak{a}^{-1}$ such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.*

From Theorem 6.1.11, it is immediate that, if K is a number field, then every $\mathcal{O}_K$ ideal I is a subgroup of the free abelian group $\mathcal{O}_F$ of rank $[K : Q] = d$. Hence I is a free abelian group $\mathcal{O}_K$ of rank d. Thus I has a $\mathbb{Z}$ basis $\{\alpha_1, \alpha_2, ..., \alpha_d\} \subset \mathcal{O}_K$, where α_j are called the generators of I and has the $\mathbb{Z}$ module structure of I as

$$I = [\alpha_1, ..., \alpha_d]$$

Ideals in a commutative ring R with identity are called R-ideals for convenience.

Proposition 6.1.31. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Then $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$.*

Proof. Let α be a nonzero algebraic integer in $\mathfrak{a}$ satisfying the minimal polynomial $x^r + a_{r-1}x^{r-1} + ... + a_0 = 0$ with $a_i \in \mathbb{Z} \, \forall i$ and a_0 not zero. Then $a_0 = -(\alpha^r + ... + a_1\alpha)$. Thus, $a_0 \in \mathbb{Z}$ and $\alpha^r + ... + a_1\alpha \in \mathfrak{a}$ □

A ring is called *Noetherian* if every ascending chain $I_1 \subset I_2 \subset I_3 \subset ...$ of ideals terminates, i.e., if there exists n such that $I_n = I_{n+k}$ for all $k \geq 0$.

Theorem 6.1.32. *For any commutative ring R, the following are equivalent.*

- *R is Noetherian*
- *Every nonempty set of ideals contains a maximal element.*
- *Every ideal of R is finitely generated.*

Dedekind Domain

A *Dedekind domain R* is an integral domain satisfying the following properties:

- Every ideal of R is finitely generated.
- Every nonzero prime ideal of R is maximal.
- R is integrally closed in its quotient field.

Thus, an integral domain R is a Dedekind domain if it is noetherian, integrally closed in its field of fractions, and every nonzero prime ideal of R is maximal.

Theorem 6.1.33. *The ring of integers $\mathcal{O}_K$ of a number field K has the following properties:*

1. *It is a domain with field of fractions K.*
2. *It is noetherian*
3. *If $\alpha \in K$ satisfies a monic polynomial equation with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$. i.e., $\mathcal{O}_K$ is integrally closed in its field of fractions K.*
4. *Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.*

Theorem 6.1.34. *If K is a number field, then the ring of integers $\mathcal{O}_K$ is a Dedekind domain.*

Proposition 6.1.35. *Any principal ideal domain is a Dedekind domain.*

Proposition 6.1.36. *Every nonzero prime ideal in $\mathcal{O}_K$ contains exactly one integer prime.*

Lemma 6.1.37. *If R is a Dedekind domain and I is any proper ideal of R, then I contains a product of prime ideals.*

Theorem 6.1.38. *Every proper nonzero ideal in a Dedekind domain R is uniquely representable as a product of prime ideals.*

Theorem 6.1.39. *If R is a Dedekind domain, then every nonzero, prime, integral R-ideal is invertible.*

Ideal Class group

Lemma 6.1.40. *If R is a Dedekind domain, then the set of all fractional ideals forms a multiplicative abelian group, denoted by $\mathfrak{F}(R)$. The set $\mathcal{P}(R)$ consisting of all principal fractional R-ideals is a subgroup of $\mathfrak{F}(R)$.*

Definition 6.1.41. Let R be a Dedekind domain. Then the quotient group $\mathfrak{F}(R)/\mathcal{P}(R)$ is called the class group of R, denoted by $\mathfrak{C}_R$. Two fractional ideals are equivalent if they belong to the same coset of $\mathcal{P}(R)$ in $\mathfrak{F}(R)$. The group of equivalence classes of ideals is called the *ideal class group.*

Definition 6.1.42. The ideal class group denoted by $Cl(K)$, is the quotient group

$$Cl(K) = \mathcal{F}_K/\mathcal{P}_K.$$

The cardinality of $Cl(K)$ denoted by h_K is called the *class number.*

Theorem 6.1.43. *Suppose that R is a Dedekind domain. Then R is a unique factorization domain if and only if $\mathfrak{C}_R$ has order 1.*

Theorem 6.1.44. *If K is a number field, then the class number of K is finite.*

Definition 6.1.45. If K is a number field with signature $\{r_1, r_2\}$, where $[K : \mathbb{Q}] = n = 2r_1 + r_2$. Then the cardinality $|\mathfrak{C}_K|$ is called the class number of $\mathcal{O}_K$, denoted by h_K. The value

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}$$

is called the *Minkowski bound* for K.

Theorem 6.1.46. *Let K be an algebraic number field of degree n over $\mathbb{Q}$. Then each ideal class contains an ideal $\mathfrak{a}$ satisfying*

$$N(\mathfrak{a}) \leq M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}.$$

Chapter 7

Quadratic Fields

Definition 7.0.47. Any algebraic number field of degree two is a *quadratic field.*

Definition 7.0.48. A quadratic field is called a *real* or an *imaginary* quadratic field according as $K \subset R$ or not.

A quadratic field K is real if and only if $K = \mathbb{Q}(\sqrt{d})$ with square free $d > 1$ in $\mathbb{Z}$. The ring of integers of any quadratic field is given by

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv\ 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv\ 1 \pmod 4 \end{cases}$$

The discriminant of the field K is

$$\Delta(\mathcal{O}) = \begin{cases} 4d & \text{if } d \equiv\ 2, 3 \pmod 4 \\ d & \text{if } d \equiv\ 1 \pmod 4 \end{cases}$$

Proposition 7.0.49. *For a quadratic field K with discriminant d, one has $K = \mathbb{Q}(\sqrt{d})$. Further $1, \frac{d+\sqrt{d}}{2}$ is an integral basis of the ring $\mathcal{O}$ of algebraic integers in K.*

Corollary 7.0.50. *The discriminant uniquely determines a quadratic field.*

Let $\mathfrak{p}$ be any prime ideal in $\mathcal{O}$. Then $\mathfrak{p}$ contains a unique prime number $p > 0, p \in \mathbb{Z}$.

Proposition 7.0.51. *For an odd prime p and a quadratic field of discriminant d, the following holds:*

- $p\mathcal{O} = \mathfrak{p}^2$, $\mathfrak{p}$ *prime if and only if* $\left(\frac{d}{p}\right) = 0$
- $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$, $\mathfrak{p}$ *prime if and only if* $\left(\frac{d}{p}\right) = 1$
- $p\mathcal{O} = \mathfrak{p}$ *prime if and only if* $\left(\frac{d}{p}\right) = -1$,

where $\left(\frac{d}{p}\right)$ *is the Legendre symbol.*

Proposition 7.0.52. *Let* $\mathcal{O}$ *be the ring of integers in a quadratic field of discriminant* d*. Then*

- $2\mathcal{O} = \mathfrak{p}^2$, $\mathfrak{p}$ *prime if and only if* $\left(\frac{d}{2}\right) = 0$
- $2\mathcal{O} = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$, $\mathfrak{p}$ *prime if and only if* $\left(\frac{d}{2}\right) = 1$
- $2\mathcal{O} = \mathfrak{p}$ *prime if and only if* $\left(\frac{d}{2}\right) = -1$,

where $\left(\frac{d}{2}\right)$ *is the Kronecker's quadratic residue symbol.*

7.1 Mersenne primes in quadratic fields

It is well known that $a^d - 1$ divides $a^n - 1$ for each divisor d of n, and if $n = p$, a prime, then

$$a^p - 1 = (a-1)(1 + a + a^2 + ... + a^{p-1}) \tag{7.1.1}$$

and if $a^p - 1$ is a prime, then $a = 2$.
Number theorists of all persuasions have been fascinated by prime numbers of the form $2^p - 1$ ever since *Euclid* used them for the construction of perfect numbers. In modern times, they are named after *Marin Mersenne* (1588-1648). A well known result due to Euclid is that, if $2^p - 1$ is a prime, then $2^{p-1}(2^p - 1)$ is perfect. Much later *Euler* proved the converse, every even-perfect number has this form.

Mersenne primes have been studied by amateurs as well as specialists. Mersenne primes are used in cryptography too in generating pseudorandom numbers. By far, the most widely used technique for pseudorandom number generation is an algorithm first proposed by Lehmer, known as the linear congruential method. It is generated

by the recursion $X_{n+1} \equiv aX_n \pmod{M_{31}}$, where M_{31} is the Mersenne prime $2^{31}-1$. Of the more than two billion choices for a only handful of multipliers are useful. One such value is $a = 7^5 = 16807$, which was originally designed for use in the IBM 360 family of computers.

Many have attempted to generalize the notion of Mersenne primes and even-perfect numbers to complex quadratic fields with class number 1. One reason is that they have only finitely many units. Indeed, with the exception of $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, the other seven complex quadratic fields with class number 1 have only two units: ± 1. Spira (1961) defined Mersenne primes over $\mathbb{Q}(\sqrt{-1})$ to give a useful definition of even-perfect numbers over $\mathbb{Z}[i]$, the ring of Gaussian integers. His work was continued later by McDaniel (1974, 1990) to give an analogue of *Euclid-Euler* Theorem over $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. In both the papers the concept of Mersenne primes is used to give a valid definition of even-perfect numbers.
Recently Pedro Berrizbeitia and Iskra (2010) studied Mersenne primes over Gaussian integers and Eisenstein integers. The primality of Gaussian Mersenne numbers and Eisenstein Mersenne numbers are tested using biquadratic reciprocity and cubic reciprocity laws respectively.

Since the concept of Mersenne primes over Real quadratic fields has not been studied, in this chapter the concept of Mersenne primes has been extended to real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with class number 1. As usual, the ring of integers of K is denoted by $\mathcal{O}_K$,

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Since K is a unique factorization domain, irreducibles are primes in these domains. Hence for any $\eta \in K$ the two factorings of η say

$$\eta = \pi_1^{k_1}\pi_2^{k_2}...\pi_r^{k_r} \text{ and } \eta = \epsilon_1\pi_1^{k_1}\epsilon_2\pi_2^{k_2}...\epsilon_r\pi_r^{k_r}$$

are considered to be one and the same, where ϵ_i are units and π_i are irreducibles.

Define $M_{p,\alpha} = \frac{\alpha^p-1}{\alpha-1}$ such that $\alpha \in \mathcal{O}_\mathcal{K}$ is irreducible and $(\alpha-1) = u$ is a unit other than ± 1. Then $M_{p,\alpha}$ may be called as an analog of Mersenne prime if the norm of

$M_{p,\alpha}$ namely $N(M_{p,\alpha}) = N(\frac{\alpha^p-1}{\alpha-1})$ is a rational prime.
The irreducibility of α is tested for $d \equiv 2, 3 \pmod 4$ and for $d \equiv 1 \pmod 4$, for the values of d up to 499.

Possible Questions

- Find all irreducibles α in the ring of integers of $\mathbb{K}$ such that $\alpha - 1$ is some unit u with
- $N(\alpha - 1) = N(u) = \pm 1$ in the ring of integers of $\mathbb{K}$ depending on
- $d \equiv 2, 3 \pmod 4$ and $d \equiv 1 \pmod 4$.

Conditions under which α is irreducible is considered below.

Theorem 7.1.1. *Let $d \equiv 2, 3 \pmod 4$ and $N(\alpha - 1) = -1$. Then α is irreducible if and only if $d = 2$ and $u \in \{1 + \sqrt{2}, 1 - \sqrt{2}, -1 + \sqrt{2}, -1 - \sqrt{2}\}$.*

Proof. Let α be irreducible and $u = a + b\sqrt{d}$. Then $\alpha = (a + 1) + b\sqrt{d}$. Hence, $N(\alpha) = (a + 1)^2 - 2b^2 = N(u) + 2a + 1 = 2a$. Since α is irreducible, $2a$ should be a rational prime. Hence $a = \pm 1$. With $a = 1$, $u = 1 + b\sqrt{d}$ and $N(u) = -1 = 1 - b^2 d$. i.e., $b^2 d = 2$. Since d is square-free, $d = 2$ and $b = \pm 1$.
Similarly with $a = -1$, one obtains $b = \pm 1$ and $d = 2$.
Conversely let $d = 2$ and $u = a + b\sqrt{2}$ be any unit in $\mathbb{Q}(\sqrt{2})$ with $N(u) = -1$. Then $\alpha = (a+1)+b\sqrt{2}$ and $N(\alpha) = (a+1)^2 - 2b^2 = a^2 - 2b^2 + 2a + 1 = N(u) + 2a + 1 = 2a$, is a rational prime, if and only if $a = \pm 1$. As before, we get $b = \pm 1$.
Hence, different choices of u for which α is irreducible are respectively, $1 + \sqrt{2}$, $1 - \sqrt{2}$, $-1 + \sqrt{2}$ and $-1 - \sqrt{2}$. As $1 + \sqrt{2} = u$ is the fundamental unit, these values are, $u, -u^{-1}, u^{-1}, -u$. Corresponding α values are, $2 + \sqrt{2}$, $2 - \sqrt{2}$, $\sqrt{2}$ and $-\sqrt{2}$.

□

Since $2 - \sqrt{2}$ and $-\sqrt{2}$ are the conjugates of $2 + \sqrt{2}$ and $\sqrt{2}$ respectively, $M_{p,\alpha}$ is computed at $\alpha = 2 + \sqrt{2}$ and $\sqrt{2}$.
For $\alpha = 2 + \sqrt{2}$ a few Mersenne primes in $\mathbb{Q}(\sqrt{2})$ are given below:

p	$M_{p,\alpha}$	$N(M_{p,\alpha})$
2	$3+\sqrt{2}$	7
3	$9+5\sqrt{2}$	31
5	$97+67\sqrt{2}$	431
7	$1121+791\sqrt{2}$	5279
11	$152193+107615\sqrt{2}$	732799

Table 7.1: Mersenne primes in $\mathbb{Q}(\sqrt{2})$ for $\alpha = 2+\sqrt{2}$

The next Mersenne primes are found at
$p = 73$, with $N(M_{p,\alpha}) = 851569055172258793218602741480913108991$,
$p = 89$ with $N(M_{p,\alpha}) = 290315886781191681464330388772329064268797313023$,
$p = 233$ with $N(M_{p,\alpha}) = 180604754272820230333680012311664417847378068915378065470653141679119595184985817477128291571565179408372345191779634973245 43$.

With $\alpha = \sqrt{2}$, $M_{p,\alpha} = \frac{(\sqrt{2})^p - 1}{\sqrt{2}-1}$.
Thus, $N(M_{p,\alpha}) = 2^p - 1$, giving all the usual Mersenne numbers.

Theorem 7.1.2. *Let* $d \equiv 1 \pmod 4$ *and* $\alpha - 1 = u = \frac{a+b\sqrt{d}}{2}$ *be a unit such that,* $N(u) = N(\alpha - 1) = -1$. *Then,* α *is irreducible, if and only if,* a *is a rational prime and* b *is some odd integer.*

Proof. By hypothesis, $N(\alpha) = \frac{(a+2)^2 - db^2}{4} = a$ since $N(u) = -1$. For α to be irreducible a should be an odd rational prime.
Indeed if $a = 2$ then $u = \frac{2+b\sqrt{d}}{2}$ and $N(u) = \frac{4-db^2}{4} = -1 \Rightarrow b^2 d = 8$. This is impossible since $d \equiv 1 \pmod 4$. Since $d \equiv 1 \pmod 4$ it is clear that b is some odd integer. Thus, the analogs of Mersenne primes are defined for $d \equiv 1 \pmod 4$ whenever units are of the form $u = \frac{p+(2n+1)\sqrt{d}}{2}$, where $n \in \mathbb{Z}$ and p is an odd rational prime.
The converse is straightforward since the norm of α is $a = p$, a rational prime by assumption. □

The Table below shows the values of $d \equiv 1 \pmod 4$, $d < 500$ for which $N(u) = -1$, α is irreducible and u is the fundamental unit.

$\mathbb{Q}(\sqrt{d})$	u	α	$N(\alpha)$
$\mathbb{Q}(\sqrt{13})$	$\frac{3+\sqrt{13}}{2}$	$\frac{5+\sqrt{13}}{2}$	3
$\mathbb{Q}(\sqrt{29})$	$\frac{5+\sqrt{29}}{2}$	$\frac{7+\sqrt{29}}{2}$	5
$\mathbb{Q}(\sqrt{53})$	$\frac{7+\sqrt{53}}{2}$	$\frac{9+\sqrt{53}}{2}$	7
$\mathbb{Q}(\sqrt{149})$	$\frac{61+5\sqrt{149}}{2}$	$\frac{63+5\sqrt{149}}{2}$	61
$\mathbb{Q}(\sqrt{173})$	$\frac{13+\sqrt{173}}{2}$	$\frac{15+\sqrt{173}}{2}$	13
$\mathbb{Q}(\sqrt{293})$	$\frac{17+\sqrt{293}}{2}$	$\frac{19+\sqrt{293}}{2}$	17

Table 7.2: $K = \mathbb{Q}(\sqrt{d})$; $d \equiv 1 \pmod 4$ and $N(u) = -1$.

As an illustration:

p	$N(M_{p,\alpha})$
5	1231
7	25117
11	9181987
19	1098413907397

Table 7.3: Mersenne primes in $K = \mathbb{Q}(\sqrt{13})$ for $\alpha = \frac{5+\sqrt{13}}{2}$

The next Mersenne prime is found at $p = 41$.

Theorem 7.1.3. *Let* $d \equiv 2, 3 \pmod 4$ *and* $u = a + b\sqrt{d}$ *be a unit, such that* $N(u) = 1$*, then* α *is always reducible.*

Proof. By hypothesis, $\alpha = (a+1) + b\sqrt{d}$ and $N(\alpha) = 2(1+a)$, which is prime only if $a = 0$, which contradicts $N(u) = 1$. Hence α is not irreducible. □

Theorem 7.1.4. *Let* $d \equiv 1 \pmod 4$ *and* $u = \frac{a+b\sqrt{d}}{2}$ *be a unit such that* $N(u) = 1$*. Then,* α *is irreducible, if and only if,* $a + 2$ *is a rational prime and* b *is some odd integer.*

Proof. By hypothesis, $N(\alpha) = \frac{(a+2)^2 - db^2}{4} = a + 2$, since $N(u) = 1$. For α to be irreducible $a + 2$ should be a rational prime. Clearly $a \neq 0$. Hence $a + 2$ is an odd rational prime. Hence, $a^2 \equiv 1 \pmod 4$. Since $d \equiv 1 \pmod 4$ it is clear that b

is some odd integer. Thus, the analogs of Mersenne primes are defined for $d \equiv 1 \pmod 4$ whenever units are of the form $u = \frac{a+(2n+1)\sqrt{d}}{2}$, where $n \in \mathbb{Z}$ and $a+2$ is an odd rational prime.
Converse is straightforward as in Theorem 7.1.2. □

The Table below lists the values of $d < 500$, $d \equiv 1 \pmod 4$ for which $N(u) = 1$, α is irreducible and u is the fundamental unit.

$\mathbb{Q}(\sqrt{d})$	u	α	$N(\alpha)$
$\mathbb{Q}(\sqrt{21})$	$\frac{5+\sqrt{21}}{2}$	$\frac{7+\sqrt{21}}{2}$	7
$\mathbb{Q}(\sqrt{77})$	$\frac{9+\sqrt{77}}{2}$	$\frac{11+\sqrt{77}}{2}$	11
$\mathbb{Q}(\sqrt{93})$	$\frac{29+3\sqrt{93}}{2}$	$\frac{31+3\sqrt{93}}{2}$	31
$\mathbb{Q}(\sqrt{237})$	$\frac{77+5\sqrt{237}}{2}$	$\frac{79+5\sqrt{237}}{2}$	79
$\mathbb{Q}(\sqrt{437})$	$\frac{21+\sqrt{437}}{2}$	$\frac{23+\sqrt{437}}{2}$	23
$\mathbb{Q}(\sqrt{453})$	$\frac{149+7\sqrt{453}}{2}$	$\frac{151+7\sqrt{453}}{2}$	151

Table 7.4: $K = \mathbb{Q}(\sqrt{d})$; $d \equiv 1 \pmod 4$ and $N(u) = 1$

As an illustration consider the following table:

p	$N(M_{p,\alpha})$
17	223358425353211

Table 7.5: Mersenne primes in $K = \mathbb{Q}(\sqrt{21})$, for $\alpha = \frac{7+\sqrt{21}}{2}$

The next Mersenne prime is found at $p = 47$.

Similar calculations are obtained for $\mathbb{Q}(\sqrt{77})$, the fundamental unit is $u = \frac{9+\sqrt{77}}{2}$ and $\alpha = \frac{11+\sqrt{77}}{2}$.

p	$N(M_{p,\alpha})$
2	23
7	10248701

Table 7.6: Mersenne primes in $K = \mathbb{Q}(\sqrt{77})$ for $\alpha = \frac{11+\sqrt{77}}{2}$

The next Mersenne prime is found at $p = 71$.

Remarks

1. In Tables 7.2 and 7.4 above, the fundamental unit u is chosen in $\mathbb{Q}(\sqrt{d})$. However, it is possible that, $\alpha = 1 + u$ is not irreducible with u as fundamental unit and yet $\alpha' = 1 + u'$ is irreducible for some other unit u' in $\mathbb{Q}(\sqrt{d})$.
   As an illustration $\mathbb{Q}(\sqrt{5})$ is considered. Here, $u = \frac{1+\sqrt{5}}{2}$ is the fundamental unit. But, $\alpha = 1 + u = \frac{3+\sqrt{5}}{2} = u^2$ is again a unit!
   However, with $u' = u^2 = \frac{3+\sqrt{5}}{2}$, we get $\alpha' = 1 + u' = \frac{5+\sqrt{5}}{2}$ and $N(\alpha') = 5$, so α' is irreducible. Another choice is $u^5 = u'' = \frac{11+5\sqrt{5}}{2}$ and $\alpha'' = 1 + u'' = \frac{13+5\sqrt{5}}{2}$ is irreducible since $N(\alpha'') = 11$.

2. Theorems 7.1.1 and 7.1.3 imply the following: Among all fields $\mathbb{Q}(\sqrt{d})$, $d \equiv 2, 3 \pmod 4$, $\mathbb{Q}(\sqrt{2})$ is the only field where $\alpha = 1 + u$ is irreducible. There are essentially only two choices for α, namely $\sqrt{2}$ and $2 + \sqrt{2}$.

Similar to usual Mersenne primes in $\mathbb{Z}$, quadratic Mersenne norms have the following properties:

Properties of $M_{p,\alpha}$:

1. If $N(M_{n,\alpha})$ is prime, then n is prime.

2. The sequence $\{N(M_{n,\alpha})\}_{n=1}^{\infty}$ is an increasing sequence of integers that starts at 1.

3. If d divides n then $M_{d,\alpha}$ divides $M_{n,\alpha}$ in $\mathbb{Q}(\sqrt{d})$ and $N(M_{d,\alpha})$ divides $N(M_{n,\alpha})$.

4. If d and n are relatively prime then $M_{d,\alpha}$ is relatively prime to $M_{n,\alpha}$ in $\mathbb{Q}(\sqrt{d})$ and $N(M_{n,\alpha})$ is relatively prime to $N(M_{d,\alpha})$.

Experimental evidence shows that Mersenne primes are sparse in $\mathbb{Q}(\sqrt{d})$ for $d \equiv 1 \pmod 4$. Some interesting properties of Mersenne primes in $\mathbb{Q}(\sqrt{2})$ are given below.

Mersenne primes in $\mathbb{Q}(\sqrt{2})$

1. Since $\alpha = 1 + u = 2 + \sqrt{2} = u\sqrt{2}$, where u is the fundamental unit, we have $\alpha^n = a_n + b_n\sqrt{2} = u^n(\sqrt{2})^n$, for any integer $n > 0$ and $a_n, b_n \in \mathbb{Z}$. A small calculation also reveals that,

$$\alpha^n = \begin{cases} (2^{\frac{n-1}{2}}\sqrt{2})u^n & if\ n\ is\ odd; \\ 2^{\frac{n}{2}}u^n & if\ n\ is\ even. \end{cases}$$

which is

$$\alpha^n = \begin{cases} (2^{\frac{n-1}{2}}\sqrt{2})(v_n + w_n\sqrt{2}) & if\ \ n\ \ is\ \ odd; \quad w_n, v_n \in \mathbb{Z}; \\ 2^{\frac{n}{2}}(v'_n + w'_n\sqrt{2}) & if\ \ n\ \ is\ even; \quad v'_n, w'_n \in \mathbb{Z}. \end{cases}$$

It can be noted that, w_n, the coefficient of $\sqrt{2}$ in u^n is odd if n is odd. Also, $2^{\frac{n+1}{2}}w_n = a_n$ and $2^{\frac{n-1}{2}}v_n = b_n$.
And, w'_n, the coefficient of $\sqrt{2}$ in u^n is even if n is even. Also,

$2^{\frac{n}{2}}v'_n = a_n$ and $2^{\frac{n}{2}}w'_n = b_n$.
For n odd, $N(u)^n = -1$, so

$$N(\alpha^n) = N(2^{\frac{n-1}{2}}\sqrt{2})N(u)^n = N(2^{\frac{n-1}{2}})N(\sqrt{2})(-1)^n = 2^{n-1}(-2)(-1) = 2^n$$

For n even, $N(u)^n = 1$, and

$$N(\alpha^n) = N(2^{\frac{n}{2}})N(u)^n = N(2^{\frac{n}{2}})(1) = 2^n.$$

2. For any odd prime p, let $\alpha^p = a_p + b_p\sqrt{2}$ for some $a_p, b_p \in \mathbb{Z}$.
Then,

$$\begin{aligned} N(\alpha^p - 1) = N((a_p - 1) + b_p\sqrt{2}) &= (a_p - 1)^2 - 2b_p^2 \\ &= a_p^2 - 2b_p^2 - 2a_p + 1 \\ &= 2^p - 2a_p + 1 \end{aligned}$$

But,

$$N(M_{p,\alpha}) = N\left(\frac{\alpha^p - 1}{\alpha - 1}\right) = -N(\alpha^p - 1) = 2a_p - 2^p - 1 = 2^{\frac{p+3}{2}} w_p - 2^p - 1.$$

3. As already noticed, a_p has a factor of $2^{\frac{p+1}{2}}$.

   Hence, $2a_p \equiv 0 \pmod 4$. This further implies that, $N(M_{p,\alpha}) \equiv -1 \pmod 4$ for $p \geq 2$ and $N(M_{p,\alpha}) \equiv -1 \pmod 8$ for $p > 2$.
   The next three properties are consequences of quadratic reciprocity, and $\left(\frac{\cdot}{\cdot}\right)$ denotes the *Legendre* symbol.

4. Let p be an odd prime. If $p \equiv \pm 1 \pmod 8$, then

$$2^{\frac{p+3}{2}} = 2^2 2^{\frac{p-1}{2}} \equiv 4 \pmod p.$$

   If $p \equiv \pm 3 \pmod 8$, then

$$2^{\frac{p+3}{2}} = 2^2 2^{\frac{p-1}{2}} \equiv -4 \pmod p.$$

   Combining the above we get,

$$N(M_{p,\alpha}) \equiv \begin{cases} 4w_p - 3 \pmod p & \text{if } p \equiv \pm 1 \pmod 8; \\ -4w_p - 3 \pmod p & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

5. If $N(M_{p,\alpha})$ is a rational prime and q is any other prime then

$$\left(\frac{N(M_{p,\alpha})}{q}\right)\left(\frac{q}{N(M_{p,\alpha})}\right) = \begin{cases} 1 \quad if \quad q \equiv 1 \pmod 4; \\ -1 \quad if \quad q \equiv 3 \pmod 4. \end{cases}$$

6. If $N(M_{p,\alpha})$ is a rational prime then $\left(\frac{2}{N(M_{p,\alpha})}\right) = 1$ since $N(M_{p,\alpha}) \equiv -1 \pmod 8$. Hence, $\sqrt{2} \in \mathbb{F}_{N(M_{p,\alpha})}$, the finite field with $N(M_{p,\alpha})$ elements.

7.1.1 Testing for primality

Several primality tests are available and some are specially designed for special numbers, an example being the famous Lucas-Lehmer Test for the usual Mersenne primes. One can show that the generalized Mersenne numbers of $\mathbb{Q}(\sqrt{2})$ can be put in a special form, so that recent primality tests can be used to determine whether they are prime. Now,

$$N(M_{p,\alpha}) = N\left(\frac{\alpha^p - 1}{\alpha - 1}\right) = 2^{\frac{p+3}{2}} w_p - 2^p - 1,$$

or,

$$N(M_{p,\alpha}) = 2^{\frac{p+3}{2}}(w_p - 2^{\frac{p-3}{2}}) - 1$$

Since w_p is odd, $(w_p - 2^{\frac{p-3}{2}})$ is odd for $p > 3$.
For $p > 3$,

$$N(M_{p,\alpha}) = h.2^{\frac{p+3}{2}} - 1, \quad where \quad h = (w_p - 2^{\frac{p-3}{2}}), \quad odd.$$

An algorithm to test the primality of numbers of the form $h \cdot 2^n \pm 1$, for any odd integer h such that, $h \neq 4^m - 1$ for any m is described in (Bosma, 1993). It can be noted that, h is not equal to $4^m - 1$ in $M_{p,\alpha}$ for any m. Hence, the algorithm given in (Bosma, 1993) can be used to test the primality of $M_{p,\alpha}$.

7.2 Primes of the form $x^2 + 7y^2$

The problem of representing a prime number by the form $x^2 + ny^2$, where n is any fixed positive integer dates back to Fermat. This question was best answered by *Euler* who spent 40 years in proving Fermat's theorem and thinking about how they can be generalized, he proposed some conjectures concerning $p = x^2 + ny^2$, for $n > 3$. These remarkable conjectures, among other things, touch on quadratic forms and their composition, genus theory, cubic and biquadratic reciprocity. Refer (Cox, 1989) for a thorough treatment. Some elementary properties of the form $x^2 + ny^2$ are disussed below.

Lemma 7.2.1. *Let n be a nonzero integer, and p be an odd prime not dividing n.*

Then

$$p|x^2+ny^2,\ gcd(x,y)=1 \iff \left(\frac{-n}{p}\right)=1$$

Euler became intensely interested in this question in the early 1740's and he mentions numerous examples in his letters to Goldbach. One among several of his conjectures stated in modern notation is

$$\left(\frac{-7}{p}\right)=1 \iff p\equiv 1,9,11,15,23,25 \pmod{28}$$

The study of integral quadratic forms in two variables

$$f(x,y)=ax^2+bxy+cy^2, \quad a,b,c\in\mathbb{Z}$$

began with Lagrange, who introduced the concepts of discriminant, equivalence and reduced form. A primitive positive definite form $ax^2+bxy+cy^2$ is said to be reduced if

$$|b|\le a\le c, \ \text{ and } b\ge 0 \quad \text{ if either } \quad |b|=a \ \text{ or } \ a=c$$

The form x^2+ny^2 is always a reduced form with discriminant $-4n$.
The following lemma gives necessary and sufficient condition for a number m to be represented by a form of discriminant D.

Lemma 7.2.2. *Let $D\equiv 0,1 \pmod 4$ and m be an integer relatively prime to D. Then m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue modulo m.*

As a corollary :

Corollary 7.2.3. *Let n be an integer and p be an odd prime not dividing n. Then $\left(\frac{-n}{p}\right)=1$ if and only if p is represented by a primitive form of discriminant $-4n$.*

In 1903, Landau proved a conjecture of Gauss (Theorem 7.2.4 below):
Let $h(D)$ denote the number of classes of primitive positive definite forms of discriminant D, i.e., $h(D)$ is equal to the number of reduced forms of discriminant D.

Theorem 7.2.4. *Let n be a positive integer. Then*

$$h(-4n) = 1 \Leftrightarrow n = 1, 2, 3, 4 \text{ or } 7.$$

Theorem 7.2.4 only gives the value of n when $h(-4n) = 1$. For $h(-4n) > 1$ the theorem fails. For eg., when $n = 5$, $D = -20$. But $h(-20) = 2$ and e,

$$p \equiv 1, 3, 7, 9 \pmod{20} \Longleftrightarrow \left(\frac{-5}{p}\right) = 1$$

$$\Longleftrightarrow p = x^2 + 5y^2 \text{ or } 2x^2 + 2xy + 3y^2$$

In general, two primitive positive definite forms of discriminant D are in the same genus if they represent same the values in $(\mathbb{Z}/D\mathbb{Z})^*$. Equivalent forms represent the same numbers and hence are in the same genus. This turns out to be the basic idea of genus theory (Cox, 1989). In this section the case $n = 7$ is considered to represent $N(M_{p,\alpha})$ in the form $x^2 + 7y^2$ whenever $M_{p,\alpha}$ is a Mersenne prime in $\mathbb{Q}(\sqrt{2})$. By theorem 7.2.4 above, $x^2 + 7y^2$ is the only reduced form of discriminant -28, and it follows that

$$p = x^2 + 7y^2 \Longleftrightarrow p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$$

for primes $p \neq 7$.

The following theorem 7.2.5 provides a classical illustration.

Theorem 7.2.5. *Let p be an odd prime congruent to 1, 2, or 4 mod 7. Then p can be written as*

$$p = x^2 + 7y^2$$

for certain integers x and y; moreover, x and y are uniquely determined up to sign.

7.3 Norms of Mersenne primes of the form $x^2 + 7y^2$ in $\mathbb{Q}(\sqrt{2})$

On March 3, 1998, the birth centenary of *Emil Artin* was celebrated at the Universiteit van Amsterdam. The paper (Lenstra and Stevenhagen, 2000) is based on two lectures given on the occasion. To quote from (Lenstra and Stevenhagen, 2000): "Artin's

reciprocity law is one of the cornerstones of *class field theory*. To illustrate its usefulness in elementary number theory, we shall apply it to prove a recently observed property of Mersenne primes." The property of Mersenne primes referred to is the following:

Theorem 7.3.1. *If* $M_p = 2^p - 1$ *is prime and* $p \equiv 1 \pmod 3$*, then* $M_p = x^2 + 7y^2$ *for some integers* x*,* y *and one always has* $x \equiv 0 \pmod 8$ *and* $y \equiv \pm 3 \pmod 8$*.*

This was first observed by *Franz Lemmermeyer* and proved in (Lenstra and Stevenhagen, 2000) using Artin's reciprocity law. The special property of the usual Mersenne primes referred to in Theorem 7.3.1 has the following generalization over $\mathbb{Q}(\sqrt{2})$.

7.4 Main theorem

Theorem 7.4.1. *If* $N(M_{p,\alpha})$ *is a rational prime, with* $\alpha = 2 + \sqrt{2}$*, then* $N(M_{p,\alpha})$ *is always a quadratic residue* $\pmod 7$*, and hence it can be written as* $x^2 + 7y^2$*. Also,* x *is divisible by* 8*, and* $y \equiv \pm 3 \pmod 8$*.*

The first few Mersenne primes in $\mathbb{Q}(\sqrt{2})$ with $\alpha = 2 + \sqrt{2}$, as well as the representations of their norms as $x^2 + 7y^2$ is given below.

p	$M_{p,\alpha}$	$x^2 + 7y^2$
5	431	$16^2 + 7 \cdot 5^2$
7	5279	$64^2 + 7 \cdot 13^2$
11	732799	$856^2 + 7 \cdot 3^2$

Table 7.7: Representation of Mersenne primes as $x^2 + 7y^2$ in $\mathbb{Q}(\sqrt{2})$

For $p = 73$,

$$N(M_{p,\alpha}) = 851569055172258793218602741480913108991 =$$

$$(28615996544447548272)^2 + 7 \cdot (2161143775888286749)^2$$

For $p = 89$,

$$N(M_{p,\alpha}) = 290315886781191681464330388772329064268797313023 =$$

$$(363706809248848497658560)^2 + 7 \cdot (150253711001099458172317)^2$$

For $p = 233$,

$$N(M_{p,\alpha}) = 180604754272820230333680012311664417847378068915378065470653141 6$$

$$791195951849858174771282915715651794083723451917796349732454 3.$$

The corresponding representation is

$$(865273456032586778183783265738424079290310705903212235241825 84)^2 +$$

$$7 \cdot (388651402565631046393562909823492944773807092189525854233736 29)^2.$$

The proof is based on Artin reciprocity law, one of the main results from an important branch of algebraic number theory called **class field theory**. The theorem is proved in two steps: In the first step it is shown that $N(M_{p,\alpha})$ is always a quadratic residue (mod 7). Next an outline of the proof that x is divisible by 8, and $y \equiv \pm 3 \pmod 8$ is given.

Now it is shown that, if $N(M_{p,\alpha})$ is a prime then, $N(M_{p,\alpha})$ can be written as $x^2 + 7y^2$. Since $N(M_{p,\alpha}) = 2^{\frac{p+3}{2}} w_p - 2^p - 1$, representing a prime in the form $x^2 + 7y^2$ depends on w_p. The values of v_p and w_p are found (mod 7). It is clear from the previous discussion that, for any odd n, $N(u^n) = v_n^2 - 2w_n^2 = -1$.
If $u^n = v_n + w_n\sqrt{2}$, then v_n and w_n satisfy the following recursions:
$v_{n+1} = v_n + 2w_n$ and $w_{n+1} = v_n + w_n$, with initial conditions: $v_1 = 1$, $w_1 = 1$. The above recursions are used to show that v_n and w_n satisfy the following:

$$v_{n+2} = 3v_n + 4w_n \,;\; w_{n+2} = 2v_n + 3w_n$$

$$v_{n+3} = 7v_n + 10w_n \,;\; w_{n+3} = 5v_n + 7w_n$$

$$v_{n+4} = 17v_n + 24w_n \,;\; w_{n+4} = 12v_n + 17w_n$$

$$v_{n+5} = 41v_n + 58w_n \,;\; w_{n+5} = 29v_n + 41w_n$$

$$v_{n+6} = 99v_n + 140w_n \,;\; w_{n+6} = 70v_n + 99w_n$$

From the above one may also easily obtain the following congruences:

$$\{v_{6k+1}\} \equiv 1 \pmod 7 \,;\; \{w_{6k+1}\} \equiv 1 \pmod 7 \tag{7.4.1}$$

$$\{v_{6k+5}\} \equiv 6 \pmod 7 \,;\; \{w_{6k+5}\} \equiv 1 \pmod 7 \tag{7.4.2}$$

Since only odd prime powers greater than 3 are considered, equations (7.4.1) and (7.4.2) are meaningful.

Hence,

$$N(M_{p,\alpha}) = 2^{\frac{p+3}{2}} w_p - 2^p - 1 \equiv 2^{\frac{p+3}{2}} - 2^p - 1 \pmod 7 \tag{7.4.3}$$

Let us solve equation (7.4.3) for $p > 3$.
If $p = 3k + 1$ then $2^p \equiv 2 \pmod 7$ and $2^{\frac{p+3}{2}} \equiv 4 \pmod 7$, so

$$N(M_{p,\alpha}) \equiv 1 \pmod 7.$$

If $p = 3k + 2$ then $2^p \equiv 4 \pmod 7$ and $2^{\frac{p+3}{2}} \equiv 2 \pmod 7$, so

$$N(M_{p,\alpha}) \equiv 4 \pmod 7.$$

Thus from Theorem 7.2.5 it is straightforward that, $N(M_{p,\alpha})$ can always be represented as $x^2 + 7y^2$. As a background to the proof of theorem 7.4.1, the following lemma is proved.

Lemma 7.4.2. *If $N(M_{p,\alpha})$ is a rational prime and $N(M_{p,\alpha}) = x^2 + 7y^2$, then $x \equiv 0 \pmod 4$, and $y \equiv \pm 3 \pmod 8$.*

Proof. From the previous discussion, we know

$$N(M_{p,\alpha}) = x^2 + 7y^2. \tag{7.4.4}$$

But $N(M_{p,\alpha}) = 2^{\frac{p+3}{2}} w_p - 2^p - 1$. Clearly we may take $p > 6$. So either $p = 6k + 1$ or $p = 6k + 5$.

If $p = 6k + 1$, then

$$N(M_{p,\alpha}) = 2^{\frac{6k+4}{2}} w_p - 2^{6k+1} - 1 \equiv -1 \equiv 7 \pmod 8. \tag{7.4.5}$$

If $p = 6k + 5$, then also,

$$N(M_{p,\alpha}) = 2^{\frac{6k+5}{2}} w_p - 2^{6k+5} - 1 \equiv 7 \pmod 8. \tag{7.4.6}$$

But right hand side of equation (7.4.4) is $x^2 + 7y^2$. We show that x must be even and y odd.

For, if x is odd and y is even, then $x^2 \equiv 1 \mod 8)$ and either $y^2 \equiv 0 \pmod 8)$ or $y^2 \equiv 4 \pmod 8)$. If $y^2 \equiv 0 \pmod 8$, then $x^2 + 7y^2 \equiv 1 \pmod 8)$ contradicting equations (7.4.5) and (7.4.6); and if $y^2 \equiv 4 \pmod 8$, then

$$x^2 + 7y^2 \equiv 1 + 7.4 \equiv 5 \pmod 8,$$

again contradicting equations (7.4.5) and (7.4.6). Thus x is even and y is odd.

Hence by equation (7.4.4)

$$7 \equiv x^2 + 7y^2 \equiv x^2 + 7 \pmod 8,$$

since $y^2 \equiv 1 \pmod 8$ and so, $x^2 \equiv 0 \pmod 8$ implying $x \equiv 0 \pmod 4$.

We now prove that $y \equiv \pm 3 \pmod 8$

Let $p \equiv 1 \pmod 6$. From equation (7.4.5)

$$N(M_{p,\alpha}) = x^2 + 7y^2 = 2^{\frac{6k+4}{2}} w_p - 2^{6k+1} - 1.$$

Reducing modulo 16, we get $N(M_{p,\alpha}) \equiv -1 \pmod{16}$. But $N(M_{p,\alpha}) = x^2 + 7y^2$ and $x \equiv 0 \pmod 4$. Hence $7y^2 \equiv -1 \pmod{16}$, yielding $y^2 \equiv 9 \pmod{16}$. This proves that $y \equiv \pm 3 \pmod 8$. The same result follows from equation (7.4.6) when $p \equiv 5 \pmod 6$. □

Below some known results about Artin Reciprocity are discussed which follow mainly from (Lenstra and Stevenhagen, 2000).

7.4.1 Artin's reciprocity law

Frobenius map

Let R be a ring in which one has $p = 0$, and consider the pth power map

$$F : R \to R$$

defined by $F(x) = x^p$. Then F respects the addition $F(a + b) = F(a) + F(b)$, and multiplication as well given by $F(ab) = F(a)F(b)$ if R is commutative and finally $F(1) = 1$. These three properties constitute the definition of a ring homomorphism, which leads to the following theorem.

Theorem 7.4.3. *Let p be a prime number and R a ring in which $p = 0$. Then the pth power map $R \to R$ is a ring homomorphism from R to itself.*

The map in the theorem is called the *Frobenius map* after Georg Ferdinand Frobenius. Many reciprocity laws including Artin's, are concerned about classifying which ring homomorphism $R \to R$ is Frobeninus. In particular, the Frobenius map $F : F_p \to F_p$ is the identity. Thus for any integer a, one has $a^p \equiv a \bmod p$, proving Fermat's little theorem. Consider the quadratic extensions of F_p. Let d be a nonzero integer, and p be a prime number not dividing $2d$. Consider the ring $F_p[\sqrt{d}]$, the elements of which are by definition formal expressions of the form $u + v\sqrt{d}$, with u and v ranging over F_p. Applying Frobeninus map F to a typical element $u + v\sqrt{d}$, one can find

$$F(u + v\sqrt{d}) = (u + v\sqrt{d})^p = u^p + v^p d^{\frac{p-1}{2}}\sqrt{d}$$

This leads to investigate the value of $d^{\frac{p-1}{2}}$ in F_p. Thus from Fermat's theorem

$$0 = d^p - d = d.(d^{\frac{p-1}{2}} - 1)(d^{\frac{p-1}{2}} + 1).$$

Since F_p is a field, one of the three factors d, $(d^{\frac{p-1}{2}} - 1)$, $(d^{\frac{p-1}{2}} + 1)$ must vanish. As p does not divide $2d$, it is exactly one of the last two. The quadratic residue symbol $\left(\frac{d}{p}\right)$ distinguishes between the two cases: for $d^{\frac{p-1}{2}} = 1$ in F_p, $\left(\frac{d}{p}\right) = 1$ and for $d^{\frac{p-1}{2}} = -1$ in F_p, $\left(\frac{d}{p}\right) = -1$. The Frobenius map is one of the two obvious automorphisms

of $F_p[\sqrt{d}]$: for $\left(\frac{d}{p}\right) = 1$ it is the identity and for $\left(\frac{d}{p}\right) = -1$ it is the map sending $u + v\sqrt{d}$ to $u - v\sqrt{d}$. The assignment $u + v\sqrt{d}$ to $u - v\sqrt{d}$ is clearly reminiscent of complex conjugation, and it defines an automorphism in more general circumstances involving square roots.

Artin symbol

Consider higher degree extensions. Instead of $X^2 - d$, let $f \in Z[X]$ be any monic polynomial of positive degree n such that the discriminant $\Delta(f) \neq 0$. Instead of $F_p[\sqrt{d}]$, for a prime number p consider the ring $F_p[\alpha]$ consisting of all p^n formal expressions

$$u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1}$$

with coefficients $u_i \in F_p$ and $f(\alpha) = 0$. The coeffcients of f are integers in F_p. In the same manner replacing F_p by $\mathbb{Q}$, one may define the ring $\mathbb{Q}[\alpha]$, which is a field if and only if f is irreducible.

Now, instead of two automorphisms assume that there exists a finite abelian group G of ring automorphisms of $\mathbb{Q}[\alpha]$ such that $f = \prod_{\sigma \in G}(X - \sigma(\alpha))$ with coefficients in $\mathbb{Q}[\alpha]$. The existence of G is a strong assumption. For example, in the important case that f is irreducible it is equivalent to $\mathbb{Q}[\alpha]$ being a Galois extension of $\mathbb{Q}$ with an abelian Galois group.

The precise statement is as follows:

Theorem 7.4.4. *Let p be a prime not dividing $\Delta(f)$. Then there is a unique element $\varphi_p \in G$ such that the Frobenius map of the ring $F_p[\alpha]$ is the reduction of φ_p mod p, in the following sense: in the ring $\mathbb{Q}[\alpha]$, one has*

$$\alpha^p = \varphi_p(\alpha) + p \cdot (q_0 + q_1\alpha + ... + q_{n-1}\alpha^{n-1})$$

for certain rational numbers $q_0, q_1, ..., q_{n-1}$ of which the denominators are not divisible by p.

The element φ_p of G is referred to as the Artin symbol of p. In the case $n = 2$ it is virtually identical to the quadratic symbol $\left(\frac{\Delta(f)}{p}\right)$. Here are two illustrative results which are immediate from theorem 7.4.4.

Result 1

The degree of each irreducible factor of the polynomial $f \pmod p$ in $F_p[X]$ is equal to the order of φ_p in the group G. In particular, $\varphi_p = 1$ in G if and only if $f \pmod p$ splits into n linear factors in $F_p[X]$.

Result 2

The polynomial f is irreducible in $\mathbb{Z}[X]$ if and only if G is generated by the elements φ_p, as p ranges over all prime numbers not dividig $\Delta(f)$.

Artin's quadratic reciprocity law

There exists a group homomorphism

$$(\mathbb{Z}/4d\mathbb{Z})^* \to \{\pm 1\}$$

with

$$p \pmod{4d} \to \left(\frac{d}{p}\right) \text{ for any prime } p \text{ not dividing } 4d.$$

To generalize Artin's quadratic reciprocity law to the situation of theorem 7.4.4 it is natural to guess that $4d$ is replaced by $\Delta(f)$ and $\left(\frac{d}{p}\right)$ by φ_p respectively.

Artin reciprocity over $\mathbb{Q}$

There exists a group homomorphism

$$(\mathbb{Z}/\Delta(f)\mathbb{Z})^* \to G \quad \text{with} \quad p \pmod{\Delta(f)} \to \varphi_p$$

for any prime number p not dividing $\Delta(f)$. It is surjective if and only if f is irreducible. Here φ_p determines the splitting behaviour of the polynomial $f \bmod p$. Thus Artin reciprocity yields a relation between $f \pmod p$ and $p \pmod{\Delta(f)}$.

7.4.2 Primes in a quadratic field

Let $K = \mathbb{Q}(\sqrt{d})$. Finding primes in K is equivalent to solving the minimal polynomial of K in finite fields F_p, for p prime, i.e., finding a ring homomorphism from $\mathcal{O}_K \to F_p$, where $\mathcal{O}_K$ is the ring of integers of K.

For $K = \mathbb{Q}(\sqrt{-7})$, the element $\omega = \frac{1+\sqrt{-7}}{2}$ is an integer of K, which is a zero of the polynomial $X^2 - X + 2$. Finding a ring homomorphism from $\mathcal{O}_K$ to another ring is equivalent to finding a zero of $X^2 - X + 2$, in that ring. The element $-2 \in \mathbb{Z}/8\mathbb{Z}$ satisfies $(-2)^2 + (-2) + 2 = 8 = 0$. Also, $8 = \omega + 2\bar{\omega} + 2 \in \omega + 2\mathcal{O}_K$.

Thus there is a ring homomorphism from

$$O_K \to \mathbb{Z}/8\mathbb{Z}$$

$$a + b\omega \to (a - 2b) \bmod 8$$

Kernel $\mathfrak{a}$ of the map is generated by 8 and $\omega + 2$. Thus $\mathfrak{a} = (\omega + 2)\mathcal{O}_K$.

For eg., over F_2, $X^2 - X + 2 = X(X - 1)$, giving 2 ring homomorphisms $\mathcal{O}_K \to F_2$, mapping ω to 0 and 1 in F_2. Their kernels are prime ideals of index 2 in $\mathcal{O}_K$ with generators ω and $\bar{\omega}$. Also, the identity $\omega\bar{\omega} = 2$ and $\omega + 2 = -\omega^3$ shows that the ideal $\mathfrak{a}$ factors as the cube of prime $\omega\mathcal{O}_K$.

Theorem 7.4.5. *Let K be a number field, and let L be an abelian extension of K with group G. Then for every prime $\mathfrak{p}$ of K that does not divide $\Delta(L/K)$ there is a unique element $\varphi_p \in G$ with the property that the automorphism of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ induced by φ_p is the Frobenius map of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ relative to $\mathfrak{p}$.*

From Results 7.4.1 and 7.4.1 it is clear that φ_p determines the splitting behaviour of $f \pmod p$. Thus, Artin reciprocity yields a relation between $f \pmod p$ and $p \pmod{\Delta(f)}$. So, for $p \equiv 1, 2, 4 \pmod 7$, $X^2 - X + 2$ splits completely and Artin symbol equals 1, whereas $X^2 - X + 2$ is irreducible in $F_p[X]$ for $p \equiv 3, 5, 6 \pmod 7$ and the Artin symbol equals -1.

For a prime $\mathfrak{p}$ of K, write $k(\mathfrak{p})$=$\mathcal{O}_\mathcal{K}/\mathfrak{p}$, a finite field, and its cardinality, $\mathfrak{n}_\mathfrak{p}$, is called the norm of $\mathfrak{p}$. Consider a ring homomorphism $k(\mathfrak{p}) \to R$ for a suitable ring R and for some prime $\mathfrak{p}$ of K. The Frobenius map F of such a ring is the map $R \to R$ defined by $F(x) = x^{\mathfrak{n}_\mathfrak{p}}$. It is a ring homomorphism. It was proved by Galois in 1830 that the

Frobenius map of the finite field $k(\mathfrak{p})$ itself is the identity. This generalizes Fermat's little theorem.
The inclusion map $\mathcal{O}_K \to \mathcal{O}_L$ induces a ring homomorphism $k(\mathfrak{p}) \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. The element $\varphi_p \in G$ is called the Artin symbol of $\mathfrak{p}$. To give an example, let $K = \mathbb{Q}[\sqrt{-7}] = \mathbb{Q}[\omega]$ with the minimal polynomial $\omega^2 - \omega + 2 = 0$. Let $L = K[\beta]$, where β is a zero of $X^2 - \omega X - 1$. Since the discriminant is $\omega^2 + 4 = \omega + 2$ is non-zero, and L has dimension 2 over K, it is automatic that L is abelian over K with group G of order 2.
The non-identity element ρ of G satisfies $\rho(\beta) = \omega - \beta = -1/\beta$. (β is a zero of $X^2 - \omega X - 1$). The ring of integers of L equals $\mathcal{O}_L = \mathcal{O}_K + \mathcal{O}_K.\beta$, and $\Delta(L/K)$ is the $\mathcal{O}_K$ ideal generated by the polynomial discriminant $\omega + 2$; it is the ideal $\mathfrak{a} = (\omega\mathcal{O}_K)^3$.
One may compute φ_p for the prime $\mathfrak{p} = \sqrt{-7}\mathcal{O}_K$ of norm 7:
note that the field $k(\mathfrak{p}) = F_7$, $2\omega - 1 = \sqrt{-7} = 0$, and therefore $\omega = 4$. Because, in F_7, $2\omega = 1 \implies \omega = 2^{-1} \equiv 4 \bmod 7$.
The ring $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is the quadratic extension $F_7[\beta]$ of F_7 defined by $\beta^2 = \omega\beta + 1 = 4\beta + 1$. Also, an easy computation shows that, $\beta^7 = 4 - \omega = 4 - \beta$. This is same as the image of $\rho(\beta) = \omega - \beta$ in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Thus, $\varphi_\mathfrak{p} = \rho$. It can be checked easily that, the primes $(8 \pm 3\sqrt{-7})$ of norm 127 has Artin symbol 1, i.e., $\beta^{127} = 1$ in F_7.

The generalization of Artin reciprocity law to K can be drawn from theorem 7.4.5 like this: since every ingredient of the law for $\mathbb{Q}$ has a meaningful analog over K, the natural replacement for the group $(\mathbb{Z}/m\mathbb{Z})^*$ defined for any non-zero integer m, is the group of invertible elements $(\mathcal{O}_K/\mathfrak{m})^*$ of the finite ring $\mathcal{O}_K/\mathfrak{m}$, for a non-zero $\mathcal{O}_K$ - ideal $\mathfrak{m}$. A closer inspection reveals the difficulty:
If $\mathfrak{p}$ is a prime of K coprime to $\Delta(L/K)$, there is no way to give a meaningful definition to $\mathfrak{p}$ mod $\Delta(L/K)$ as an element of $(\mathcal{O}_K/\Delta(L/K))^*$.

Ray class group

This problem can be resolved by defining a suitable multiplicative group modulo $\mathfrak{m}$ that contains an element $\mathfrak{p}$ *modulo* $\mathfrak{m}$ for each $\mathfrak{p}$ coprime to $\mathfrak{m}$ and that generalizes $(\mathbb{Z}/m\mathbb{Z})^*$; this group is called the **ray class group** modulo $\mathfrak{m}$ denoted by $Cl_\mathfrak{m}$.
The description of $Cl_\mathfrak{m}$ by means of generators and relations:

one generator $[\mathfrak{p}]$ for each prime $\mathfrak{p}$ of $\mathcal{O}_K$ coprime to $\mathfrak{m}$, and one relation $[\mathfrak{p}_1].\ [\mathfrak{p}_2]...[\mathfrak{p}_t] = 1$ for every sequence $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_t$ of prime ideals for which there exists $v \in \mathcal{O}_K$ satisfying

$$\mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_t = v\mathcal{O}_K, \quad v \equiv 1 \pmod{\mathfrak{m}}, \quad v >> 0$$

An element $\nu \in K$ is called **totally positive**, denoted as $\nu >> 0$, if each field embedding $K \to R$ maps ν to a positive real number and (in case there are no such embeddings) $\nu \neq 0$.

$Cl_{\mathfrak{m}}$ is a finite abelian group, and using the unique prime ideal factorization, the definition can be reformulated as follows: $Cl_{\mathfrak{m}}$ is the multiplicative group of equivalence classes of nonzero ideals $\mathfrak{a}$ of $\mathcal{O}_K$ that are co-prime to $\mathfrak{m}$. The ideal $\mathfrak{a}_1$ belongs to the same class as $\mathfrak{a}_2$ if and only if there exists $v_1, v_2 \in \mathcal{O}_K$ with

$$v_1\mathfrak{a}_1 = v_2\mathfrak{a}_2, v_1 \equiv v_2 \equiv 1 \pmod{\mathfrak{m}} \quad v_1 >> 0, \quad v_2 >> 0$$

Thus, there is a group homomorphism from $\mathcal{O}_K/\mathfrak{m}$ to $Cl_{\mathfrak{m}}$ that sends (v mod $\mathfrak{m}$) to the class of $v\mathcal{O}_K$ whenever $v >> 0$; and although in general it is neither injective nor surjective, it is both for $K = \mathbb{Q}$.

Artin's reciprocity law

There is a group homomorphism

$$Cl_{\Delta(L/K)} \to G$$

with

$$[\mathfrak{p}] \to \varphi_p$$

for every prime $\mathfrak{p}$ of K coprime to $\Delta(L/K)$. It is surjective if and only if L is a field. This is now called the **Artin map**. Thus, by definition of $Cl_{\Delta(L/K)}$, theorem 7.4.5 asserts that, $\varphi_{\mathfrak{p}_1}.\varphi_{\mathfrak{p}_2}...\varphi_{\mathfrak{p}_t} = 1$ whenever $\mathfrak{p}_1.\mathfrak{p}_2...\mathfrak{p}_t = v\mathcal{O}_K$ for some $v \equiv 1 \pmod{\Delta(L/K)}$ with $v >> 0$.

Mersenne primes

Consider

$$K = \mathbb{Q}[\sqrt{-7}] = \mathbb{Q}[\omega], \qquad \omega^2 - \omega + 2 = 0$$

$$L = K[\beta], \qquad \beta^2 - \omega\beta - 1 = 0.$$

Then $\Delta(L/K) = \mathfrak{a}$ is the kernel of the map $\mathcal{O}_K \to \mathbb{Z}/8\mathbb{Z}$ sending ω to -2. It is the cube of the prime $\omega\mathcal{O}_K$ of norm 2. Hence,

$$(\mathbb{Z}/8\mathbb{Z})^* \approx (\mathcal{O}_K/\mathfrak{a})^* \to Cl_{\mathfrak{a}}$$

and its kernel is $\{\pm 1\}$. Thus $Cl_{\mathfrak{a}}$ is identified with the group $(\mathbb{Z}/8\mathbb{Z})^*/\{\pm 1\}$ of order 2.

Consider the Artin map $Cl_{\mathfrak{a}} \to G = \{1, \rho\}$. The Artin symbol of $\sqrt{-7}\mathcal{O}_K$ is ρ; hence it is an isomorphism and hence L is a field. Also, the discriminant of the polynomial defining L is $\omega^2 + 4 = \omega + 2 = -\omega^3$ not a square in K, and $\omega\bar{\omega} = 2$, it is immediate that, $L = K[\sqrt{-\omega}]$.

7.4.3 Recipe for calculating Artin symbol

If $\mathfrak{p} = \pi\mathcal{O}_K$ is a prime of $K = \mathbb{Q}[\sqrt{-7}] = \mathbb{Q}[\omega]$ different from $\omega\mathcal{O}_K$, then $\varphi_p = 1$ or ρ according as π maps to ± 1 or to ± 3 under the map $\mathcal{O}_K \to \mathbb{Z}/8\mathbb{Z}$ that sends ω to -2. For eg., $\sqrt{-7} = 2\omega - 1$ maps to 3 mod 8 and the number $8 \pm 3\sqrt{-7}$ maps to $\pm 3.3 = \pm 1$ mod 8. This is because, $\sqrt{-7} = 2\omega - 1$ and ω maps to -2 under $\mathbb{Z}/8\mathbb{Z}$. Now it is easy to see that,

$$8 \pm 3\sqrt{-7} \equiv \pm 3(2(-2) - 1) \equiv \pm 1 \bmod 8.$$

Consider an element of the form $x + \sqrt{-7}y$ having norm $x^2 + 7y^2$ which is a rational prime. The Artin symbol equals 1 if $x + 3y$ is ± 1 mod 8, and ρ otherwise.

From Lemma 7.4.2 it is clear that, $x \equiv 0 \pmod 4$ and $y \equiv \pm 3 \pmod 8$. Hence, the Artin symbol is 1 if and only if x is divisible by 8.
Lemmermeyer's observation is equivalent to the assertion that any prime of $K =$

$\mathbb{Q}[\sqrt{-7}]$ of norm M_p has trivial Artin symbol in the quadratic extension $L = K[\sqrt{-\omega}]$.

Theorem 7.4.6. *Let $M_p = 2^p - 1$ be a Mersenne prime with $p \equiv 1 \pmod 3$, and write $M_p = x^2 + 7y^2, x, y \in \mathbb{Z}$. Then x is divisible by 8.*

Proof. Consider the extension $N = K[\sqrt{-\omega}, \sqrt{-\bar{\omega}}]$ of K that is composed of the quadratic extension $L = K[\sqrt{-\omega}]$ and its conjugate $K[\sqrt{-\bar{\omega}}]$. It is of dimension 4 over K with a basis consisting of $1, \sqrt{-\omega}, \sqrt{-\bar{\omega}}$ and $\sqrt{-\omega}.\sqrt{-\bar{\omega}} = \sqrt{2}$. It is enough to prove the congruence $\xi^{M_p} \equiv \xi \pmod{M_p\mathbb{Z}_N}$ for all $\xi \in \mathbb{Z}_N$, since it implies that the Artin symbols of both the primes of norm M_p of K in the subextension L of N are trivial. It turns out that N can also be realized in a second way: since $\sqrt{2} \in N$, it may be viewed as an extension of dimension 4 of the field $E = \mathbb{Q}(\sqrt{2})$. Since

$$(\sqrt{-\omega} \pm \sqrt{-\bar{\omega}})^2 = -(\omega + \bar{\omega}) \pm 2\sqrt{-\omega}\sqrt{-\bar{\omega}} = -1 \pm 2\sqrt{2}$$

it follows that N is the composition of two conjugate quadratic extensions of E got by adjoining square roots of $-1 + 2\sqrt{2}$ and $-1 - 2\sqrt{2}$; the product of these square roots is a square root of -7. Thus, N is an abelian extension of E .
In the new base field $E = \mathbb{Q}(\sqrt{2})$, one can explicitly factor M_p:
$M_p = 2^p - 1 = \frac{\sqrt{2}^p - 1}{\sqrt{2}-1}.\frac{\sqrt{2}^p+1}{\sqrt{2}+1}$.
Denote by v_p and $\bar{v}_p$ the two factors on the right. They belong to $\mathbb{Z}_E = \mathbb{Z} + \mathbb{Z}.\sqrt{2}$, are conjugate in E and generate two primes of E of norm M_p. As v_p and $\bar{v}_p$ are coprime with the product M_p, the congruence to be proved is equivalent to

$$\xi^{M_p} \equiv \xi \pmod{v_p\mathbb{Z}_N}$$

and

$$\xi^{M_p} \equiv \xi \pmod{\bar{v}_p\mathbb{Z}_N}$$

for all $\xi \in \mathbb{Z}_N$; i.e., it is sufficient to show that the Artin symbols of $v_p\mathbb{Z}_E$ and $\bar{v}_p\mathbb{Z}_E$ in the abelian extension N of E are both the identity. Let γ and δ denote the roots of the quadratic polynomials $X^2 - (1 + \sqrt{2})X + 1$ and $X^2 - (1 - \sqrt{2})X + 1$ of discriminants $-1 + 2\sqrt{2}$ and $-1 - 2\sqrt{2}$ respectively. An automorphism of N is the identity if it is so on both $E[\gamma]$ and $E[\delta]$. Thus it is enough to show that the Artin symbols of $v_p\mathbb{Z}_E$ and $\bar{v}_p\mathbb{Z}_E$ are trivial. This is shown to be true via Artin reciprocity. The

discriminant of each of these extensions divides $(-1+2\sqrt{2})(-1-2\sqrt{2})\mathbb{Z}_E = 7\mathbb{Z}_E$. From $p \equiv 1 \pmod 6$, and $(\sqrt{2})^6 = 8 \equiv 1 \pmod 7$ thus $(\sqrt{2})^p \equiv \sqrt{2} \pmod 7$, so the generators v_p and $\bar{v}_p$ of the Mersenne prime M_p are both 1 mod $7\mathbb{Z}_E$. They are also both totally positive and hence, by the Artin reciprocity law, their Artin symbols must be trivial. □

7.4.4 Proof of Main theorem

The proof given in theorem 7.4.6 carries over word-for-word, and so, an outline of the proof is given. By definition, $N(M_{p,\alpha}) = \frac{(2+\sqrt{2})^p-1}{1+\sqrt{2}}.\frac{(2-\sqrt{2})^p-1}{1-\sqrt{2}}$. Denote the two factors on the right by v_p and $\bar{v}_p$. It is easy to see that v_p and $\bar{v}_p$ are both totally positive. Thus it is enough to compute the Artin symbols of $v_p\mathbb{Z}_E$ and $\bar{v}_p\mathbb{Z}_E$, and show that they are both trivial.

It is enough to consider only two cases: $p \equiv 1 \pmod 6$ and $p \equiv 5 \pmod 6$. Since $\sqrt{2} \equiv 3, 4 \pmod 7$, by taking $\sqrt{2} = 4$ in v_p and $\sqrt{2} = 3$ in $\bar{v}_p$, a straightforward computation shows that, $v_p \equiv 1 \pmod 7$ and $\bar{v}_p \equiv 1 \pmod 7$. This completes the proof.

Bibliography

Bosma, W. (1993), 'Explicit Primality Criteria for $h.2^k \pm 1$', *Math. Comp.* **61**(203), 97–109.

Brin, M. and Stuck, G. (2002), *An Introduction to Dynamical Systems*, Cambridge University Press, United Kingdom.

Bruhat, F. and Lal, S. (1963), 'Lectures on Some Aspects of p-adic Analysis', Tata Institute of Fundamental Research Bombay.

Cox, D. A. (1989), *Primes of the form $x^2 + ny^2$*, Wiley -Interscience.

Crivelli, F., Pink, R. et al. (2008), 'Absolute values, valuations and completion', Electronic Notes.

de Melo, W. and van Strien, S. (1993), *One-Dimensional Dynamics*, Vol. 1, 1 edn, Springer-Verlag.

Devaney, R. L. (1989), *An Introduction to Chaotic Dynamical Systems*, 2 edn, Addison-Wesley, USA.

Dokchitser, T. (2007), 'Local Fields', Electronic Notes.

Gouvea, F. Q. (2003), *p-adic Numbers An Introduction*, 2 edn, Springer-Verlag, Germany.

Hocking, J. G. and Young, G. S. (1961), *Topology*, Addison-Wesley, USA.

Katok, S. (2007), *p-adic Analysis Compared with Real*, Vol. 37, 1 edn, American Mathematical Society, USA.

Khrennikov, A. Y. and Nilsson, M. (2004), *p-adic Deterministic and Random Dynamics*, Vol. 1 of *Mathematics and its Applications*, Kluwer Academic, The Netherlands.

Kitchens, B. P. (1998), *Symbolic Dynamics*, 1 edn, Springer-Verlag, Germany.

Koblitz, N. (1984), *p-adic Numbers, p-adic Analysis, and Zeta-Fuctions*, 2 edn, Springer-Verlag, New York.

Kuznestov, Y. A. (1998), *Elements of Applied Bifurcation Theory*, Applied Mathematical Sciences, 2 edn, Springer-Verlag, New York.

Lang, S. (2002), *Algebra*, 3 edn, Springer-Verlag, New York.

Lenstra, H. W. and Stevenhagen, P. (2000), 'Artin Reciprocity and Mersenne Primes', *Nieuw Arch. Wiskd. (5)* **1**, 44–54.

McDaniel, W. L. (1974), 'Perfect Gaussian Integers', *Acta Arith.* **25**, 137–144.

McDaniel, W. L. (1990), 'An Analogue in certain Unique Factorization Domains of the Euclid-Euler theorem on Perfect numbers', *Int. J. Math. Math. Sci.* **13**(1), 13–24.

Medio, A. and Raines, B. (2007), 'Backward dynamics in Economics, The Inverse limit approach', *J. Econ. Dynam. Control* **31**(5), 1663–1671.

Nagami, K. (1970), *Dimension theory*, Academic Press Inc., USA.

Nilsson, M. (2000), 'Cycles of Monomial and perturbated monomial p-adic dynamical systems', *Ann. Math. Blaise Pascal* **7**(1), 37–63.

Niven, I., H S Zuckerman and Montgomery, H. L. (2006), *An Introduction to the theory of Numbers*, John Wiley & Sons, Inc., Canada.

Pedro Berrizbeitia and Iskra, B. (2010), 'Gaussian and Eisenstein Mersenne primes', *Math. Comp.* **79**(271), 1779–1791.

Ritzenthaler, C. (2005), 'AGM for Elliptic Curves', Electronic Notes.

Robert, A. M. (2000), *A Course in p-adic Analysis*, Springer-Verlag, USA.

Schikoff, W. H. (1984), *Ultrametic Calculus: An introduction to p-adic analysis*, Cambridge Studies in Advanced Mathematics 4, Cambridge University Press, Cambridge.

Silverman, J. H. (2007), *The Arithmetic of Dynamical Systems*, 1 edn, Springer-Verlag, New York.

Spira, R. (1961), 'The Complex Sum of Divisors', *Amer. Math. Monthly* **68**(2), 120–124.

Stallings, W. (2006), *Cryptography and Network Security: Principles and Practices*, Prentice Hall India,.

Thiel, U. (2010), 'Discrete Valuation Fields of Higher Rank', Electronic Notes.

Woodcock, C. F. and Smart, N. P. (1998), 'p-adic Chaos and Random Number Generation', *Exp. Math.* **7**(4), 333–3421058–6458.

Bio-Data

Sushma Palimar
Research Scholar
Department of Mathematical and Computational Sciences
National Institute of Technology Karnataka
P O Srinivasanagar
Mangalore - 575 025.
Email: sushmapalimar@gmail.com

Education: M.Sc.(Mathematics), Mangalore University, 2004.

Papers (Published/Presented)

International Journals

1. Sushma Palimar and B. R. Shankar, Dynamical Systems, Inverse limit theory and p-adic Integers; *Adv. Stud. Contemp. Math.(Kyungshang)*, **20** (2010), 433–436. ISSN 1229-3067.

2. Sushma Palimar and B. R. Shankar: Mersenne Primes in Real Quadratic Fields; *J. Integer Seq.*, **15** (2012), Article 12.5.6. ISSN 1530-7638.

Conference Proceedings (Refereed)

1. B. R. Shankar and Sushma Palimar : *Dynamical Systems over the p-adic fields* $\mathbb{Q}_p$*;* in *Nonlinear Dynamics*, M. Daniel, S. Rajasekhar (Eds.), Narosa Publishing House, India, (2009), pp. 265-268. (Papers presented in honour of Prof. M. Lakshmanan's 60th Birthday.)

2. Shankar B. R. and Sushma Palimar: *Representations of Mersenne Primes in Number Fields,* 5th International Conference of IMBIC on "Mathematical Sciences for Advancement of Science and Technology" (MSAST 2011), Avishek Adhikari and M. R. Adhikari, (Eds.), Kolkata. Dec 18-20, 2011. pp.174-180.

Conferences (Papers Presented)

1. Sushma Palimar and Shankar B. R. : *Dynamical Systems and Ultrametric Calculus,* The 22nd International Conference of Jangjeon Mathematical Society, August 13-15, 2009, AIT, Chickmagalur, India.

2. Sushma Palimar and Shankar B. R. : *Primes of the form* $x^2 + 7y^2$ *in* $\mathbb{Q}(\sqrt{2})$, National Conference on Graph Theory and Number theory, NCGNIT, University of Mysore, March 21-22, 2012.