Introduction to p-adic Numbers and Hasse–Minkowski theorem

Selim Virtanen

School of Science

Bachelor's thesis
Espoo 06.01.2021

Supervisor

Prof. Camilla Hollanti

Advisors

Dr Louna Seppälä

Prof. Guillermo Mantilla-Soler

Aalto University
School of Science

Aalto University
School of Science

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi
Abstract of the bachelor's thesis

Author Selim Virtanen

Title Introduction to p-adic Numbers and Hasse–Minkowski theorem

Degree programme Science and Technology

Major Mathematics **Code of major** SCI3029

Teacher in charge Prof. Camilla Hollanti

Advisors Dr Louna Seppälä, Prof. Guillermo Mantilla-Soler

Date 06.01.2021 **Number of pages** 38+1 **Language** English

Abstract

p-adic numbers are an infinite class of complete fields that play an important role in modern number theory. Real numbers can be constructed from rationals by filling the gaps between them according to the concept of distance induced by the traditional absolute value, whereas we get the p-adic numbers if we use the p-adic absolute value that is determined by how many times a number is divisible by the prime p. This divisibility by a prime power creates a strong connection to modular arithmetic in finite fields. Completeness, on the other hand, allows us to use results from analysis. In addition, the ultrametric property of the p-adic absolute value gives the field a hierarchical structure.

In this thesis we seek to construct the p-adic numbers in an approachable way while emphasising the analogy to real numbers. We begin by looking at the p-adic absolute value and show through Ostrowski's theorem that there are no other exotic absolute values over the rationals. Next we complete the rationals with regard to the p-adic absolute value by proving the field properties of a quotient ring that we get by associating the Cauchy sequences that approach the same limit. We define this field to be the p-adic numbers and provide a power series representation that is analogous to the decimal form of reals. Furthermore, we present the p-adic integers and Hensel's lemma that corresponds to Newton's method.

In the second half of the thesis we apply the p-adic numbers to quadratic forms, which are multivariate polynomials consisting of only second degree terms. We reduce rational quadratic forms to a simpler form and present the deep Hasse–Minkowski theorem. The theorem states that if a rational quadratic form has nontrivial zeros over every local field, that is the p-adics and the reals, it must also have nontrivial zeros over the global field, rationals. This is a surprising and strong result, as a solution over the rationals automatically works in the local fields that contain the rationals, but the converse does not hold in general. The proof of the theorem is long and requires that we look at Hilbert sybols, which can be seen as a generalisation of the Legendre symbol, and investigate the square structures of the local fields using Hensel's lemma.

Keywords p-adic numbers, Hensel's lemma, quadratic forms, local–global principle, Hasse–Minkowski theorem

Aalto University
School of Science

Aalto-yliopisto, PL 11000, 00076 AALTO
www.aalto.fi
Tekniikan kandidaatintyön tiivistelmä

Tekijä Selim Virtanen

Työn nimi Johdatus p-adisiin lukuihin ja Hasse–Minkowski-teoreemaan

Koulutusohjelma Teknistieteellinen kandidaattiohjelma

Pääaine Matematiikka **Pääaineen koodi** SCI3029

Vastuuopettaja Prof. Camilla Hollanti

Työn ohjaajat Dr Louna Seppälä, Prof. Guillermo Mantilla-Soler

Päivämäärä 06.01.2021 **Sivumäärä** 38+1 **Kieli** Englanti

Tiivistelmä

p-adiset luvut on ääretön luokka täydellisiä kuntia, joilla on tärkeä rooli modernissa lukuteoriassa. Reaaliluvut voidaan johtaa rationaaliluvuista täyttämällä niiden välissä olevat aukot perinteisen itseisarvon antaman etäisyyden käsitteen mukaisesti, kun taas p-adiset luvut saadaan käyttämällä p-adista itseisarvoa, joka määräytyy suuruusjärjestyksen sijaan sen mukaan, kuinka monta kertaa luku on jaollinen alkuluvulla p. Tämä alkuluvun potenssilla jaollisuus luo vahvan yhteyden modulaariaritmetiikkaan äärellisissä kunnissa. Täydellisyyden kautta puolestaan päästään hyödyntämään analyysin menetelmiä. Lisäksi p-adisen itseisarvon ultrametrisyys antaa kunnalle hierarkisen rakenteen.

Tässä tekstissä pyrimme konstruoimaan p-adiset luvut helposti lähestyttävällä tavalla painottaen analogiaa reaalilukuihin. Aloitamme tarkastelemalla p-adista itseisarvoa ja näytämme Ostrowskin teoreeman kautta, että muita eksoottisia rationaalilukujen itseisarvoja ei ole. Seuraavaksi täydellistämme rationaaliluvut p-adisen itseisarvon suhteen todistamalla, että Cauchy-jonojen tekijärengas, joka samaistaa samaa arvoa kohti suppenevat jonot, on kunta. Tämän kunnan määrittelemme p-adisiksi luvuiksi, joille annamme reaalilukujen desimaalimuotoa vastaavan potenssisarjaesityksen. Sitten esittelemme vielä p-adiset kokonaisluvut sekä Newtonin menetelmää vastaavan Henselin lemman.

Tekstin loppuosassa sovellamme p-adisia lukuja tarkastellessamme neliömuotoja, eli usean muuttujan polynomeja, joiden jokainen termi on toista astetta. Redusoimme rationaalineliömuodot yksinkertaisempaan muotoon ja esittelemme syvällisen Hasse–Minkowski-teoreeman. Teoreema sanoo, että jos neliömuodolla on epätriviaaleja nollakohtia kaikkien lokaalien kuntien eli p-adisten lukujen ja reaalilukujen yli, on sillä oltava epätriviaaleja nollakohtia myös globaalin kunnan eli rationaalilukujen yli. Tämä on yllättävä ja vahva tulos sillä rationaaliratkaisu tomii automaattisesti myös rationaaliluvut sisältävissä lokaaleissa kunnissa, mutta käänteinen ei päde ylisesti. Teoreeman todistus on pitkä ja vaatii, että tarkastelemme muun muassa Hilbertin symbolia, jonka voi mieltää Legendren symbolin yleistykseksi, sekä lokaalien kuntien neliörakenteita Henselin lemmaa hyödyntäen.

Avainsanat p-adiset luvut, Henselin lemma, neliömuodot, lokaali–globaali-periaate, Hasse–Minkowski-teoreema

Contents

Symbols and abbreviations

Symbols

$\mathbb{P}$	primes: $\{2, 3, 5, 7, ...\}$
$\mathbb{Z}_+$	positive integers: $\{1, 2, 3, 4, ...\}$
$\mathbb{R}_+$	positive real numbers
$\mathbb{N}_0$	non-negative integers: $\{0, 1, 2, 3, 4, ...\}$
$(a_k)_k$	sequence $a_1, a_2, a_3, ...$
$C(\mathbb{Q})$	the set of Cauchy sequences over, with an implicit absolute value
$C_0(\mathbb{Q})$	the set of (Cauchy) sequences over that have limit 0
$\bar{a}$	congruence class with a representative a
$\mathbb{Q}_p$	field of p-adic numbers
$\mathbb{Q}_\infty$	real numbers $\mathbb{R}$
$\mathbb{Q}_\nu$	$\mathbb{Q}_p$ or $\mathbb{R}$: $\nu \in \mathbb{P} \cup \{\infty\}$
$\mathbb{Z}_p$	ring of p-adic integers: $\{q \in \mathbb{Q}_p \mid \lvert q\rvert_p \leq 1\}$
$R[x]$	polynomial ring over the ring R

Operators

gcd	greatest common divisor
ord_p	p-adic order of an element
$\lvert\cdot\rvert_p$	p-adic absolute value: $\lvert q\rvert_p = p^{-\mathrm{ord}_p(q)}$
$\lvert\cdot\rvert_\infty$	ordinary absolute value $\lvert\cdot\rvert$
$\lvert\cdot\rvert_0$	trivial absolute value
ker	kernel: $\ker(\varphi) = \{a \mid \varphi(a) = 0\}$

1 Introduction

p-adic numbers are an infinite class of number systems which are in several ways similar to the real numbers $\mathbb{R}$ that we are very familiar with. The redeeming properties of $\mathbb{R}$ are that it contains the rational numbers $\mathbb{Q}$, that it is a field and that it is complete. The field property implies in simple terms that the basic arithmetic operations addition, subtraction, multiplication and division follow the usual rules. On the other hand, completeness means that every Cauchy sequence converges, *i.e.* sequences that seem to converge indeed have their limit within the field. This allows us to use results from analysis, such as differentiation by taking the limit of difference quotient. The real numbers are also complete with respect to Dedekind cuts, which is a stronger property for ordered sets, but we will consider only the Cauchy completeness as the p-adic numers are not ordered.

The real numbers can be constructed from the rationals by adding the missing limits of Cauchy sequences. In order to use the Cauchy sequences we need to know which numbers are close to each other and this is given by the metric induced by the ordinary absolute value. However, we can also do this completion process using a different absolute value. Namely, for any given prime number p we can define the p-adic absolute value which is determined by how many times a number is divisible by p. Filling in the gaps in rational numbers with respect to this more exotic absolute value gives us the p-adic numbers $\mathbb{Q}_p$ which is also a complete field that contains $\mathbb{Q}$.

In the first half of the thesis we will construct the p-adic numbers. We will start by defining the p-adic order and absolute value. The p-adic absolute value has the ultrametric property as it obeys a stronger version of the triangle inequality. This gives the p-adic numbers a hierarchical structure with connections to modular arithmetic. We will also prove Ostrowski's theorem which states that the p-adic absolute values are the only exotic absolute values over $\mathbb{Q}$.

Next we will consider Cauchy sequences with respect to the p-adic absolute value and show that they form a ring. The sequences converging to zero give us a maximal ideal, and we will define the p-adic numbers to be the field that we get by taking the corresponding quotient ring. We will then proceed to find the p-adic numbers a power series representation that is similar to the decimal form of real numbers and look at some examples of basic p-adic arithmetic.

Over the integers the p-adic absolute value gives us a strong connection to modular arithmetic. Two integers are p-adically close together if they are congruent modulo a high power of p. We will expand the notion of integers by introducing the p-adic integers $\mathbb{Z}_p$ and showing that this connection extends to them, which allows us to also consider $\mathbb{Z}_p$ modulo powers of p. This is useful for example when we look at Hensel's lemma, which enables us to find p-adic roots of polynomials using iteration analogous to Newton's method if we have a root modulo p with sufficient conditions.

There are practical applications of the basic p-adic theory which take advantage of the hierarchical structure that the ultrametric p-adic absolute value induces. For example, it has been observed that in genetic code different codons are more likely to map to the same amino acid if they are 5-adically and 2-adically close, which might provide useful insight to the evolution of the genetic code [1]. On the other hand,

there exist applications especially in mathematical physics that use deeper results and constructs, such as adeles that contain information over the reals and every p-adic field at the same time [2]. The relevance of p-adic numbers is also highlighted by the recent Fields medal awarded to Peter Scholze for his work on perfectoid spaces built on top of p-adic numbers [3].

The theoretical application that we focus on in the second half of the thesis is the Hasse–Minkowski theorem of quadratic forms. We will define quadratic forms as multivariate polynomials with all terms of the second degree, and reduce them to a simpler form appropriate to our problem of determining the existence of nontrivial roots. The Hasse–Minkowski theorem states that a rational quadratic form has nontrivial roots over the global field $\mathbb{Q}$ if and only if it has nontrivial roots over all local fields $\mathbb{R}$ and $\mathbb{Q}_p$. The second assertion is clear as $\mathbb{Q}$ is included in its completions, but the fact that local roots imply the existence of a global one is a surprising and strong result.

The proof of the Hasse–Minkowski theorem is long. We will have to delve deeper into the quotient group structures that are introduced by p-adic square numbers, which share a conncetion to squares modulo p. This knowledge we are going to apply to Hilbert symbols which tell us whether a form of three terms has roots. Since the same condition for a form of two terms can be determined by Legendre symbol, the Hilbert symbol can be interpreted as its generalisation. After we have learned to explicitly compute values of Hilbert symbols we will connect the symbols over different fields with a product formula and use it to inductively prove the Hasse–Minkowski theorem. Finally we will show how to restrict the number of fields we have to check to a practical finite amount and present an example on applying the theorem.

2 p-adic absolute value

We start by introducing the p-adic absolute value, which is the backbone of p-adic numbers, and proving Ostrowski's theorem that connects it with the regular one. In the next section we construct the p-adic numbers by completing the rational numbers $\mathbb{Q}$ with regard to this absolute value. Most proofs are written by the author and inspired by [4] and [5].

The first thing we need to define is what absolute values are and what it means for one to be non-Archimedean.

Definition 1 (absolute value)**.** Let R be a ring. We call a mapping $|\cdot|$ from R to the real numbers $\mathbb{R}$ an *absolute value* if it satisfies the following properties:

A.1. $|a| > 0 \qquad \forall a \in R \setminus \{0\} \quad \text{and} \quad |0| = 0$

A.2. $|ab| = |a||b| \qquad \forall a, b \in R$

A.3. $|a + b| \leq |a| + |b| \qquad \forall a, b \in R$

We call the absolute value *non-Archimedean* if instead of the *triangle inequality* A.3. we have the stronger *non-Archimedean inequality*:

A.3'. $|a + b| \leq \max(|a|, |b|) \qquad \forall a, b \in R$

An absolute value that is not non-Archimedean is *Archimedean*. Absolute values $|\cdot|, |\cdot|_*$ are called *equivalent* if there exists $c \in \mathbb{R}_+$ such that $|a|_* = |a|^c$ for all $a \in R$. The absolute value $|\cdot|_0$ that maps all non-zero elements to 1 is called the *trivial* (non-Archimedean) absolute value.

In order to define the p-adic absolute value we need the concept of p-adic order. As the two are closely related, it is also sometimes more convenient to use the slightly less abstract order instead of absolute value depending on the situation.

Definition 2 (p-adic order)**.** Let p belong to the prime numbers $\mathbb{P}$ and $q \in \mathbb{Q} \setminus \{0\}$. We have a unique representation $q = p^n \frac{a}{b}$, where a and n belong to the integers $\mathbb{Z}$ and b to the positive integers $\mathbb{Z}_+$, with $p \nmid ab$ and $\gcd(a, b) = 1$. We define the *p-adic order*, also known as *p-adic valuation*, to be a mapping from $\mathbb{Q}$ to $\mathbb{R} \cup \{\infty\}$, that maps q to n and 0 to ∞. We denote this by ord_p.

Definition 3 (p-adic absolute value)**.** Let $p \in \mathbb{P}$. The following mapping is called the *(normalised) p-adic absolute value*

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R} : q \mapsto p^{-\text{ord}_p(q)}$$

Here $0 \mapsto p^{-\infty} = 0$.

We have to ensure that the mapping indeed fulfills the properties of an absolute value, and to show that it is non-Archimedean.

Theorem 1. *The p-adic absolute value is a non-Archimedean absolute value*

Proof. A.1. is clear and for A.2. we have

$$|ab|_p = p^{-\mathrm{ord}_p(ab)} = p^{-\mathrm{ord}_p(a)-\mathrm{ord}_p(b)} = p^{-\mathrm{ord}_p(a)}p^{-\mathrm{ord}_p(b)} = |a|_p|b|_p.$$

A.3'. follows from the observation that by assuming $\mathrm{ord}_p(q_1) \geq \mathrm{ord}_p(q_2)$ we get

$$\mathrm{ord}_p(q_1+q_2) = \mathrm{ord}_p\left(p^{n_1}\frac{a_1}{b_1} + p^{n_2}\frac{a_2}{b_2}\right) = \mathrm{ord}_p\left(\frac{p^{n_1-n_2}a_1b_2 + a_2b_1}{b_1b_2}p^{n_2}\right)$$

$$\geq n_2 = \min(\mathrm{ord}_p(q_1), \mathrm{ord}_p(q_2)).$$

Now since $x \mapsto p^{-x}$ is decreasing, we get $|q_1+q_2|_p \leq \max(|q_1|_p, |q_2|_p)$. □

Our ordinary absolute value is very intuitive as it can be interpreted as distance from zero on a number line that is constructed based on the fact that $\mathbb{R}$ is an ordered set. Therefore it may seem strange that with p-adic absolute values the magnitude of a number depends on its prime decomposition instead, making some traditionally large numbers small and vice versa. An absolute value induces the metric $x, y \mapsto d(x,y) = |x-y|$, which tells us the distance between two numbers. In the p-adic case the distance is small if the numbers are congruent modulo p^k for a large k. Let us play with some basic examples.

Example 1. *The number* 1000000 *is relatively large in the* 3*-adic sense as* $|1000000|_3 = 1$*, while* 5*-adically it is very small:* $|1000000|_5 = 5^{-6}$*. In the* 5*-adic case* 1000000 *is far away from* 1 *as* $1000000 \not\equiv 1 \pmod 5$*, whereas with the* 3*-adic absolute value we have* $|1000000-1|_3 = |37037 \cdot 3^3|_3 = 3^{-3}$ *so they are very close.* $\frac{3}{5}$ *is larger than any integer in the* 5*-adic case as* $|\frac{3}{5}|_5 = 5$*, but* 3*-adically it is smaller than most integers.*

While the ordinary absolute value is continuous, the p-adic absolute values are discrete as the value is always a power of p or 0. They also introduce a hirarchical structure to the number set: at layer k all numbers that are at most p^{-k} apart are grouped together. In Figure 1 one can see this applied to 7-adic integers. Out of the coarcest seven groupings the middle one corresponds to integers that are congruent to 0 (mod 7), and the other ones to the other congruence classes respectively. In the grouping representing n (mod 7), the grouping number $m \in \{0, ..., 6\}$ in the next level corresponds to integers congruent to $7n+m$ (mod 7^2), and this pattern continues infinitely deep.

The following theorem motivates why p-adic absolute values are relevant. It turns out that there are no other exotic absolute values over $\mathbb{Q}$. This also shows that p indeed has to be a prime number.

Theorem 2 (Ostrowski)**.** *The* p*-adic absolute values* $|\cdot|_p$*,* $p \in \mathbb{P}$*, and the regular absolute value* $|\cdot|_\infty$ *are the only nontrivial absolute values over* $\mathbb{Q}$ *up to equivalence.*

Proof. This proof follows the one in [6, Thm. 1.].

Let $|\cdot|_*$ be a nontrivial absolute value over $\mathbb{Q}$. By the property A.2. the values of $|\cdot|_*$ over $\mathbb{Z}$ uniquely determine the absolute value over the field of fractions $\mathbb{Q}$, and furthermore $|-k|_* = |k|_*$ so it is enough to prove the statement over $\mathbb{Z}_+$. We split the proof into two cases.

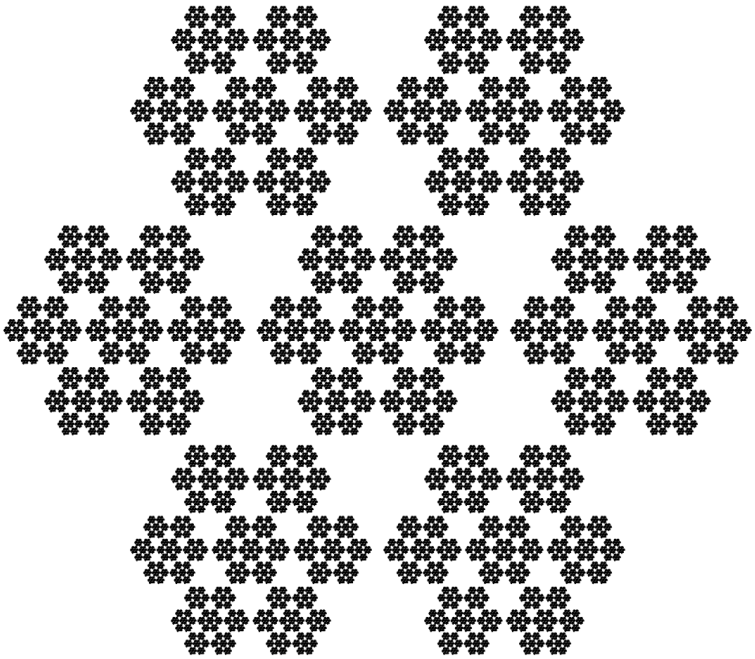

Figure 1: A visualisation of the hierarchical structure of 7-adic integers

1) Assume that there exists $k \in \mathbb{Z}_+$ such that $|k|_* > 1$, and let it be minimal. Now $k > 1$ and therefore $|k|_* = k^c$ for some $c \in \mathbb{R}_+$. Take now $n \in \mathbb{Z}_+$ and express it in base k: $n = \sum_{i=0}^{N} n_i k^i$, where $n_i \in \{0, ..., k-1\}$ and $n_N \neq 0$. We use A.2. and A.3., the fact that by minimality $|n_i|_* \leq 1$, that $n \geq k^N$ and finally that $\sum_{i=0}^{\infty} k^{-ci}$ is some constant C, to get

$$|n|_* = |\sum_{i=0}^{N} n_i k^i|_* \leq \sum_{i=0}^{N} |n_i|_* |k|_*^i \leq \sum_{i=0}^{N} k^{ci} \leq k^{cN} \sum_{i=0}^{N} k^{-ci} \leq n^c \sum_{i=0}^{\infty} k^{-ci} = Cn^c.$$

In particular this holds for all n^M, so as $M \to \infty$ we get

$$|n|_* = \sqrt[M]{|n^M|_*} \leq \sqrt[M]{Cn^{cM}} = \sqrt[M]{C} n^c \to n^c.$$

Hence $|n|_* \leq n^c$. We use this also for the other direction along with A.3. to get

$$|k^{N+1}|_* = |n + k^{N+1} - n|_* \leq |n|_* + |k^{N+1} - n|_* \leq |n|_* + (k^{N+1} - n)^c.$$

Now by A.2. and since $k^N \leq n < k^{N+1}$ we get an inequality with another constant:

$$|n|_* \geq |k^{N+1}|_* - (k^{N+1} - n)^c \geq k^{(N+1)c} - (k^{N+1} - k^N)^c$$

$$= k^{(N+1)c} \left(1 - \left(1 - \frac{1}{k}\right)^c\right) \geq n^c \left(1 - \left(1 - \frac{1}{k}\right)^c\right) = C' n^c.$$

Now we can use a similar trick with n^M and hence $n^c \leq |n|_*$. In conclusion, $|n|_* = n^c = |n|_\infty^c$ for all $n \in \mathbb{Z}_+$, and therefore $|\cdot|_*$ is equivalent to the ordinary absolute value.

2) Assume that we have $|k|_* \leq 1$ for all $k \in \mathbb{Z}_+$. Since $|\cdot|_*$ is nontrivial, there is some $n \neq 0$ for which $|n|_* < 1$. Since $|\pm 1|_* = 1$, there must therefore be a prime $p \mid n$ with $|p|_* < 1$. Assume that there is another prime q with $|q|_* < 1$. Now there are some $N, M \in \mathbb{Z}_+$, for which $|p|_*^N, |q|_*^M < \frac{1}{2}$. On the other hand, since p^N and q^M are coprime, there are $h, k \in \mathbb{Z}$ with $hp^N + kq^M = 1$. Now we get byA.2. and A.3. that

$$1 = |hp^N + kq^M|_* \leq |h|_*|p|_*^N + |k|_*|q|_*^M \leq |p|_*^N + |q|_*^M < 1,$$

which is a contradiction. Therefore p is the only prime with $|p|_* < 1$. Hence $|k|_*$ only depends on the power of p factor of k. Assume now that $|p|_* = p^{-c}$ for some $c \in \mathbb{R}_+$. If $p \nmid r \in \mathbb{Z} \setminus \{0\}$, we have $|rp^m|_* = |r|_*|p|_*^m = p^{-cm}$ and therefore $|\cdot|_* = |\cdot|_p^c$. In other words our absolute value is equivalent to a p-adic one.

□

Now that we know all possible absolute values of $\mathbb{Q}$ they can be nicely tied together with the following product formula.

Proposition 2.1. *For $q \in \mathbb{Q}^*$ we have*

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |q|_p = 1.$$

Proof. Let $q = (-1)^{n_\infty} \prod_{p \in \mathbb{P}} p^{n_p}$ be the number expressed as its prime decomposition. Now $|q|_p = p^{-n_p}$ for each $p \in \mathbb{P}$ and $|q|_\infty = \prod_{p \in \mathbb{P}} p^{n_p}$. Therefore

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |q|_p = \left(\prod_{p \in \mathbb{P}} p^{n_p} \right) \cdot \prod_{p \in \mathbb{P}} p^{-n_p} = 1.$$

□