p-ADIC QUOTIENT SETS AND p-ADIC VALUATION OF LINEAR RECURRENCE SEQUENCES

DEEPA ANTONY

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

GUWAHATI - 781039, INDIA

JUNE 2025

p-Adic quotients sets and p-adic valuation of linear recurrence sequences

by

Deepa Antony

Roll No. 196123104

Department of Mathematics

submitted in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Guwahati
Guwahati - 781039, India

June 2025

This work is dedicated

to

My Guide

Prof. Rupam Barman

Certificate

This is to certify that the thesis entitled **"p-Adic quotient sets and p-adic valuation of linear recurrence sequences"** submitted by **Mrs. Deepa Antony** to the **Indian Institute of Technology Guwahati**, for the award of the Degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by her under my guidance and supervision. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Date: June 23, 2025
Guwahati, India

Prof. Rupam Barman
Professor
Department of Mathematics
Indian Institute of Technology Guwahati

Acknowledgements

I would like to begin by expressing my heartfelt gratitude to my thesis supervisor, Prof. Rupam Barman, for giving me the opportunity to pursue my Ph.D. under his guidance. I am especially thankful to Rupam Sir for providing the right advice at the right time and for believing in me.

I would like to express my gratitude to Professors Anupam Saikia, Jitendriya Swain, and P. A. S. Sree Krishna for continuously assessing my thesis work and providing suggestions for improvement.

I would like to thank my mother, Nirmala, and my father, Antony, for their unwavering love and support throughout my life, which has helped me reach where I am today. I am also grateful to my sister, Deepti, who was my first mentor, and to my niece, Sophia, for bringing so much joy into our lives.

A special thanks to my dear husband, Joseph, for being my cheerleader and supporting me throughout the writing of this thesis.

I am grateful to my teachers at St. Joseph Public School, Pattanakad, especially my maths teacher Miss. Baby Sindu, who inspired me to come out of my comfort zone. I extend my thanks to my teachers at St. Stephen's College, Delhi, whose wonderful teaching helped me grasp the fundamental concepts of mathematics as a beginner. I would also like to thank my professors at IIT Guwahati, particularly Anjan Sir, Pati Sir, and Arup Sir, who taught me the importance of precision.

I appreciate my colleagues, Gurinder, Sulakashna, and Laxmi, for always being available to discuss doubts while reading articles in number theory. I would also like to thank my seniors Ajit bhaiya and Anwita didi for their support.

Finally, I am thankful to Dr. Jaitra Chattopadhyay, Dr. Stevan Gajović, and Dr. Piotr Miska for their valuable time and suggestions while I was working on this thesis. I would also like to thank Prof. Florian Luca for his comments, which helped improve the quality of the work presented in this thesis.

Date: June 23, 2025
Guwahati, India

Deepa Antony

Abstract

For $A \subseteq \mathbb{Z}$, we consider $R(A) = \{a/b : a, b \in A, b \neq 0\}$, called the ratio set or quotient set of A. It is an open problem to study the denseness of $R(A)$ in the set of p-adic numbers. We study the problem for the cases when A is the set of values attained by an integral form, polynomial and when A is the set of integers formed by a linear recurrence relation. We also calculate the p-adic valuation of certain third order linear recurrence sequences.

Firstly, we study the denseness of ratio set of images of cubic forms $ax^3 + by^3$, where a and b are integers. We also prove that if A is the set of nonzero values assumed by a non-degenerate, integral and primitive cubic form with more than 9 variables, then $R(A)$ is dense in $\mathbb{Q}_p$. Then, we extend the results to diagonal binary forms given by $ax^n + by^n$ for all $n \geq 3$. We also study p-adic denseness of quotients of nonzero values attained by diagonal forms of degree $n \geq 3$, where $\gcd(n, p(p-1)) = 1$. Also, we provide a necessary condition for the denseness of ratio sets of values attained by polynomials whose non-linear irreducible factors have degrees which are multiples of an integer $q > 1$.

Secondly, we focus on the denseness problem in the case of linear recurrence sequences. Let $(x_n)_{n\geq 0}$ be a linear recurrence of order $k \geq 2$ satisfying

$$x_n = a_1x_{n-1} + a_2x_{n-2} + \cdots + a_kx_{n-k}$$

for all integers $n \geq k$, where $a_1, \ldots, a_k, x_0, \ldots, x_{k-1} \in \mathbb{Z}$, with $a_k \neq 0$. In a recent paper, Sanna posed an open question to classify primes p for which the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$. We find a sufficient condition for denseness of the quotient set of the kth-order linear recurrence $(x_n)_{n\geq 0}$ satisfying $x_n = a_1x_{n-1} + a_2x_{n-2} + \cdots + a_kx_{n-k}$ for all integers $n \geq k$ with initial values $x_0 = \cdots = x_{k-2} = 0, x_{k-1} = 1$, where $a_1, \ldots, a_k \in \mathbb{Z}$ and $a_k = 1$. We show that if the characteristic polynomial of the recurrence sequence has a root $\pm\alpha$, where α is a Pisot number and if p is a prime such that the characteristic polynomial of the recurrence sequence is irreducible in $\mathbb{Q}_p$, then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$. We also show that given a prime p, there exist infinitely many recurrence sequences of order $k \geq 2$ so that their quotient sets are not dense in $\mathbb{Q}_p$. Further, we answer Sanna's question for certain linear recurrence sequences whose characteristic polynomials are reducible over $\mathbb{Q}$.

Thirdly, we examine p-adic valuations of third order linear recurrence sequences. In a recent paper, Bilu et al. studied a conjecture of Marques and Lengyel on the p-adic valuation of the Tribonacci sequence. We study the p-adic valuation of third order linear recurrence sequences by considering a generalisation of the conjecture of Marques and Lengyel for third order linear recurrence sequences. Suppose that (x_n) is a third order linear recurrence sequence whose characteristic polynomial has a root γ such that $|\gamma| > 1$. We show that if there exists a prime p for which the conjecture holds for (x_n), then the solution set of the Diophantine equation given by $x_n = m!$ in positive integers n, m is finite. We also show that the solutions can be effectively computed when the form of the conjecture is explicitly known.

We conclude the thesis by considering the notion of direction sets which was introduced by Leonetti and Sanna in 2020. Direction sets generalize ratio sets of subsets of positive integers in $\mathbb{R}$. We generalize the notion of direction sets. We also give a partial answer to a question posed by Leonetti and Sanna.

Contents

Introduction

Mathematics, particularly number theory, is filled with intriguing problems that captivate both experts and anyone with a basic understanding of arithmetic due to their elegant simplicity. One prominent story that illustrates this is that of Andrew Wiles, who, as a schoolboy, dreamed of solving Fermat's Last Theorem and ultimately achieved this remarkable feat. Throughout the history of number theory, many seemingly simple problems have taken hundreds of years to solve, leading to the development of various theories and objects that enrich the field of mathematics and pave the way for further exploration. One such object is the set of p-adic numbers, denoted as $\mathbb{Q}_p$. The p-adic numbers were first described by Kurt Hensel in 1897 and later explored more extensively by his student Helmut Hasse, particularly in relation to the local-global principle. In this thesis, we aim to investigate specific subsets of rational numbers and uncover as much information as possible about the denseness of these sets in $\mathbb{Q}_p$.

We consider ratio sets which are subsets of rational numbers. Given a subset A of the set of integers, the set $R(A) = \{a/b : a, b \in A, b \neq 0\}$ is called the ratio set or quotient set of A. It is an open problem to characterise all subsets of $\mathbb{N}$ whose ratio sets are dense in the positive real numbers. Various results have been obtained based on different properties of a set, such as the asymptotic density of a set, sets containing arithmetic progressions, numbers with specific digits, subsets that partition $\mathbb{N}$ etc. See for example [5, 7, 8, 9, 21, 25, 26, 31, 33, 37, 45, 46, 48, 49]. An analogous study has also been conducted for subsets of algebraic number fields. In [18], Garcia showed that the ratio set of Gaussian primes is dense in the set of complex numbers. More general results on ratio sets of primes in arbitrary quadratic number fields were obtained by Sittinger in [43].

Recently, many mathematicians have been exploring classical number theory problems within the p-adic framework. This approach makes the problems interesting in many ways; one of which is that it translates questions about integer congruences into problems in p-adic analysis, providing powerful analytical tools. The proof of the Skolem-Mahler-Lech theorem is an example of how p-adic analysis can effectively address problems in number theory.

Naturally, the denseness of ratio sets in $\mathbb{Q}_p$ is also a compelling topic of study. This exploration was initiated by Garcia and Luca [20], who showed that the ratio set of Fibonacci numbers is dense in $\mathbb{Q}_p$ for all primes p. Subsequently, Sanna [42] demonstrated that the ratio set of k-generalized Fibonacci numbers is dense in $\mathbb{Q}_p$, leaving the problem open for any arbitrary linear recurrence sequence of order k with $k > 1$.

Garcia, Hong, Luca, Pinsker, Sanna, Schechter, and Starr [19] expanded this investigation by examining various types of sets. They highlighted how the denseness of sets in the real numbers differs from that in the p-adic setting. For instance, the set of ratios derived from the Fibonacci numbers is dense in $\mathbb{Q}_p$ for all primes p, while the ratio set is not dense in $\mathbb{R}$. Conversely, the set of prime numbers has a dense ratio set in $\mathbb{R}$, but is not dense in any $\mathbb{Q}_p$. Furthermore, they demonstrated that the denseness of a quotient set in one p-adic number system is completely independent from its denseness in another system. Specifically, they showed that for each set P of prime numbers, there exists a subset $A \subset \mathbb{N}$ such that the ratio set $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p \in P$.

The representation of integers as sums of squares has its roots in ancient history and gained attention through the works of mathematicians such as Fermat, Lagrange, and Legendre. Lagrange's four-square theorem asserts that every positive integer can be expressed as the sum of four integer squares. Subsequent research has explored more general quadratic forms and the representation of integers as sums of higher powers. This naturally leads to investigations into the denseness of the ratio set formed by the sums of the nth powers of integers. In [19], Garcia et al. considered the sum of squares. One of their results states that if $A = \{x^2 + y^2 : x, y \in \mathbb{Z}\} \setminus \{0\}$, then $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p \equiv 1 \mod 4$. They further posed questions about the denseness of ratio sets associated with quadratic and cubic forms. The denseness of the ratio set of nonzero values assumed by a quadratic form has been completely addressed by Donnay, Garcia, and Rouse [14]. The ratio set generated by a quadratic form Q is $R(Q) = \{Q(\overline{x})/Q(\overline{y}) : \overline{x}, \overline{y} \in \mathbb{Z}^r, Q(\overline{y}) \neq 0\}$. They showed that for a non-singular binary quadratic form Q, $R(Q)$ is dense in $\mathbb{Q}_p$ if and only if the discriminant of Q is a nonzero square in $\mathbb{Q}_p$. They also proved that for a non-singular quadratic form involving at least three variables, $R(Q)$ is always dense in $\mathbb{Q}_p$. Later, Miska [35] provided a shorter proof for the same result. However, the problem remains open for forms of degree greater than 2. In [36], Miska, Murru, and Sanna showed that for any prime p, $R(S_m^3)$ is dense in $\mathbb{Q}_p$ for all integers $m \geq 2$, where $S_m^3 = \{x_1^3 + \cdots + x_m^3 : x_1, \ldots, x_m \in \mathbb{Z}_{\geq 0}\}$. They also considered the case when A is the set of values assumed by p-adic analytic functions. In particular, they studied the denseness of $R(A)$ in $\mathbb{Q}_p$ when A is the image of $\mathbb{N}$ under a polynomial $f \in \mathbb{Z}[X]$ and gave a characterisation for degree 1 and 2 cases. However, the problem of finding an effective criteria that determines the denseness of ratio sets of values assumed by polynomials of degrees greater than 2 remains unsolved.

Recurrence sequences have long been of great interest to number theorists. Considerable research has been conducted on linear recurrence sequences, and a variety of results and applications can be found in the survey by Everest et al. [15]. The problem of denseness of ratio set of linear recurrence sequences is also interesting and has been explored. In [19], Garcia et al. considered the ratio set of second order linear recurrence sequence and extended the result known for Fibonacci sequences to a more general class of second order linear recurrence sequences. In particular, they produced a result for sequences $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ defined as $a_n = ra_{n-1} + sa_{n-2}$ for $n \geq 2$ with initial values $a_0 = 0$ and $a_1 = 1$ where r and s are two fixed integers and $(b_n)_{n\geq 0}$ defined as $b_n = rb_{n-1} + sb_{n-2}$ for $n \geq 2$ with initial values $b_0 = 2$ and $b_1 = r$. In [42, Theorem 1.2], Sanna showed that, for any $k \geq 2$ and any prime p, the ratio set of the k-generalized Fibonacci numbers is dense in $\mathbb{Q}_p$, where k-generalized Fibonacci number $(F_n^{(k)})_{n\geq -(k-2)}$ is defined as

$$F_{-(k-2)}^{(k)} = \cdots = F_0^{(k)} = 0, F_1^{(k)} = 1, F_n^{(k)} = F_{n-1}^{(k)} + F_{n-2}^{(k)} + \cdots + F_{n-k}^{(k)},$$

for all integers $n > 1$. Sanna also posed the question of characterizing primes p for which the ratio set of an arbitrary kth-order linear recurrence sequence is dense in $\mathbb{Q}_p$. This problem remains open.

For a prime p and a nonzero integer n, the p-adic valuation of n, denoted $\nu_p(n)$, is defined as the highest power of p that divides n. Understanding the p-adic valuation is useful for investigating the denseness of sets in the p-adic metric space. Calculating the p-adic valuation of integers with special properties, such as linear recurrence sequences [2, 4, 28, 29, 32, 41, 50] and Stirling numbers [34], among others, is an interesting problem in itself. In [28], Lengyel completely characterized the p-adic valuation of the Fibonacci sequence. Later, Sanna [41] addressed the valuation problem for any second order linear recurrence sequence with initial values $x_0 = 0$ and $x_1 = 1$. Garcia et al. [19] utilized Sanna's result to identify conditions for the denseness of the ratio set of such second order linear recurrence sequences in $\mathbb{Q}_p$.

Unlike the case of second order linear recurrence sequences, finding the p-adic valuation of third order linear recurrence sequences remains largely unsolved. In [32], Marques and Lengyel calculated the 2-adic valuation of the Tribonacci numbers T_n

and applied their findings to solve the Diophantine equation $T_n = m!$ for positive integers n and m. The 2-adic valuations of other generalizations of Fibonacci numbers were also studied, as in [29, 44, 50]. Furthermore, the 2-adic and 3-adic valuations of Tripell sequences were addressed by Bravo et al. in [4]. However, the problem of deriving a closed formula which gives the p-adic valuation of Tribonacci numbers for any prime p remains unsolved. In [32, Conjecture 8], Marques and Lengyel conjectured that the p-adic valuation of a Tribonacci number T_n is either constant or linearly dependent on the p-adic valuation of the index n of the sequence. However, Bilu et al. demonstrated in [2, Theorem 1.5] that this conjecture fails for a specific infinite set of primes with a relative density of $1/12$. They also gave some equivalent conditions for the validity of the conjecture for a prime p. In doing so, they introduced certain notions of zeros of a linear recurrence sequence.

For a linear recurrence sequence (x_n), $n \in \mathbb{Z}$ is said to be a zero of the sequence if $x_n = 0$. In [2], Bilu et al. generalized the concept of zeros by introducing the notions of twisted integral zeros and twisted rational zeros. Moreover, in [3], they established that the number of twisted rational zeros of a non-degenerate linear recurrence sequence is finite which generalises the Skolem-Mahler-Lech theorem. They also calculated the set of twisted rational zeros of the Tribonacci sequence explicitly.

In this thesis, we study the problem of the denseness of ratio sets of values assumed by polynomials and forms of degree greater than 2. We also investigate the denseness problem for different types of linear recurrence sequences, thereby addressing the question posed by Sanna for several linear recurrence sequences. Furthermore, we examine the p-adic valuation of certain third order linear recurrence sequences and demonstrate how this valuation is useful in solving a Diophantine equation involving the terms of the sequence. We also calculate the twisted integer zeros of certain third order linear recurrence sequences explicitly. Additionally, we consider a generalization of ratio set in $\mathbb{R}$, known as the direction set.

Organization of the Thesis

We present the entire work of this thesis in seven chapters as described below.

- Chapter 1: Preliminaries
- Chapter 2: p-Adic quotient sets: cubic forms
- Chapter 3: p-Adic quotient sets: polynomials and integral forms
- Chapter 4: p-Adic quotient sets: linear recurrence sequences- I
- Chapter 5: p-Adic quotient sets: linear recurrence sequences- II
- Chapter 6: p-Adic valuation of third order linear recurrence sequences
- Chapter 7: Direction sets

In Chapter 1, we define p-adic numbers and describe some properties of the set of p-adic numbers. We also state some theorems that will be used to prove our results in the subsequent chapters.

In Chapter 2, we consider the ratio set of images formed by cubic forms and study its denseness in the set of p-adic numbers. In particular, we study the denseness problem for the cubic forms ax^3+by^3, where a and b are integers. We also prove that if A is the set of nonzero values assumed by a non-degenerate, integral and primitive cubic form with more than 9 variables, then $R(A)$ is dense in $\mathbb{Q}_p$. Additionally, we show that for $p \neq 3$, the ratio set of a diagonal cubic form containing more than 6 variables is dense in $\mathbb{Q}_p$.

In Chapter 3, we extend the results to the diagonal binary forms ax^n+by^n for all $n \geq 3$. We also consider diagonal forms of degree $n \geq 3$, where $\gcd(n, p(p-1)) = 1$ and find that $\lceil \frac{n+1}{2} \rceil$ is the least number r such that for every integral diagonal form F of degree n depending essentially on at least r variables, the ratio set of values assumed by F is dense in $\mathbb{Q}_p$. We also study the problem for values assumed by polynomials and give some necessary conditions for the denseness of the ratio set by giving bounds for the number of irreducible factors of the polynomial.

In Chapter 4, we study the problem of denseness for ratio set of linear recurrrence sequences. We find a sufficient condition for the denseness of the quotient set of the kth-order linear recurrence $(x_n)_{n\geq 0}$ satisfying $x_n = a_1x_{n-1} + a_2x_{n-2} + \cdots + a_kx_{n-k}$ for all integers $n \geq k$ with initial values $x_0 = \cdots = x_{k-2} = 0, x_{k-1} = 1$, where $a_1, \ldots, a_k \in \mathbb{Z}$ and $a_k = 1$. We show that if the characteristic polynomial of the recurrence sequence has a root $\pm\alpha$, where α is a Pisot number and if p is a prime such that the characteristic polynomial of the recurrence sequence is irreducible in $\mathbb{Q}_p$, then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$. Also, we show that given a prime p, there exist infinitely many recurrence sequences of order $k \geq 2$ so that their quotient sets are not dense in $\mathbb{Q}_p$. We also study the quotient sets of linear recurrence sequences with coefficients in some arithmetic and geometric progressions.

In Chapter 5, we examine the denseness of ratio sets of linear recurrence sequences whose characteristic polynomials are reducible over $\mathbb{Q}$. Specifically, we focus on kth-order linear recurrence sequences whose characteristic polynomials have k distinct roots in $\mathbb{Z}$. We also analyze kth-order linear recurrence sequences whose characteristic polynomials have two equal roots and $k-2$ distinct roots in $\mathbb{Z}$. Furthermore, we establish conditions that ensure the denseness of ratio sets of kth-order linear recurrence sequences when the characteristic polynomials have an integer root with multiplicity k and obtain an equivalent condition when $k = 3$.

In Chapter 6, we explore the p-adic valuation of third order linear recurrence sequences by examining a generalization of the conjecture [32, Conjecture 8] proposed by Marques and Lengyel. Consider a third order linear recurrence sequence (x_n) whose characteristic polynomial has a root γ such that $|\gamma| > 1$. We demonstrate that if there exists a prime p for which the conjecture holds for (x_n), then the set of positive integer solutions to the Diophantine equation $x_n = m!$ is finite. Furthermore, we establish that these solutions can be effectively computed when the form of the conjecture is explicitly known. Additionally, we show that the set of twisted integer zeros is equal to the set of zeros for a third order linear recurrence sequence provided the splitting field of the characteristic polynomial satisfies certain conditions.

Finally, in Chapter 7, we generalize the notion of direction sets and define k-generalized direction sets and distinct k-generalized direction sets for subsets of positive integers. We prove a necessary condition for a subset of $\mathcal{S}^{k-1} := \{\underline{x} \in [0,1]^k : ||\underline{x}|| = 1\}$ to be realized as the set of accumulation points of a distinct k-generalized direction set. We provide sufficient conditions for some particular subsets of positive integers so that the corresponding k-generalized direction sets are dense in $\mathcal{S}^{k-1}$. We also consider the denseness properties of certain direction sets and give a partial answer to a question posed by Leonetti and Sanna in [30].

1
Preliminaries

In this chapter, we review the definition of p-adic numbers and recall some topological and algebraic properties of p-adic fields. We also state some theorems that will be used to prove our results in the subsequent chapters.

1.1 p-adic numbers

Let $\mathbb{K}$ be a field.

Definition 1.1. *An absolute value on* $\mathbb{K}$ *is a function* $|\ | : \mathbb{K} \to \mathbb{R}_{\geq 0}$ *that satisfies the following conditions:*

1. $|x| = 0$ *if and only if* $x = 0$

2. $|xy| = |x||y|$ *for all* $x, y \in \mathbb{K}$

3. $|x + y| \leq |x| + |y|$ *for all* $x, y \in \mathbb{K}$. *We say the absolute value on* $\mathbb{K}$ *is non-Archimedian if it satisfies the additional condition:*

4. $|x+y| \leq max\{|x|, |y|\}$ *for all* $x, y \in \mathbb{K}$*; otherwise, the absolute value is said to be Archimedian.*

Definition 1.2. *Fix a prime number* p. *For each integer* $n \in \mathbb{Z}$, $n \neq 0$, *the* p*-adic valuation* $\nu_p(n)$ *is the unique positive integer satisfying* $n = p^{\nu_p(n)}n'$ *with* $p \nmid n'$. *The* p*-adic valuation* ν_p *can be extended to the field of rational numbers as, if* $x = a/b \in \mathbb{Q}^{\times}$ *(non zero rational numbers), then* $\nu_p(x) = \nu_p(a) - \nu_p(b)$. *By convention* $\nu_p(0) = \infty$.

Lemma 1.1. *For all* x *and* $y \in \mathbb{Q}$, *we have*

1. $\nu_p(xy) = \nu_p(x) + \nu_p(y)$

2. $\nu_p(x + y) \geq min\{\nu_p(x), \nu_p(y)\}$.

Definition 1.3. *For any* $x \in \mathbb{Q}$, *the* p*-adic absolute value of* x *is defined as* $\|x\|_p = p^{-\nu_p(x)}$ *if* $x \neq 0$. *For* $x = 0$, *the* p*-adic absolute value is defined as* $\|0\|_p = 0$.

It can be verified that the p-adic absolute value is a non-Archimedian absolute value on the field $\mathbb{Q}$. Using this absolute value, a metric d can be defined on $\mathbb{Q}$ as $d(x, y) = \|x - y\|_p$ for $x, y \in \mathbb{Q}$. The metric satisfies the strong triangle inequality $d(x, z) \leq \max\{d(x, y), d(y, z)\}$. Therefore, the metric is called an ultra-metric. The completion of $\mathbb{Q}$ with respect to this metric gives a field which is called the p-adic numbers, denoted by $\mathbb{Q}_p$. The following theorem says that $\mathbb{Q}_p$ and $\mathbb{R}$ are the only possible completions of $\mathbb{Q}$.

Theorem 1.2. [Ostrowski] *Every non trivial absolute value on* $\mathbb{Q}$ *is equivalent to one of the absolute values* $\| \ \|_p$, *where either* p *is a prime number or* $p = \infty$ *where* $\| \ \|_\infty$ *is the Euclidean norm.*

The p-adic absolute value on $\mathbb{Q}$ can be extended to $\mathbb{Q}_p$ by continuity of the function. The set of values of $\mathbb{Q}_p$ with p-adic absolute value less than or equal to 1 forms a ring and is called the ring of p-adic integers, denoted by $\mathbb{Z}_p$.

1.1.1 Topology of $\mathbb{Q}_p$

The ultra-metric in $\mathbb{Q}_p$ gives it a very interesting geometry.

Proposition 1.3. *If $x, y \in \mathbb{Q}_p$ and $\|x\|_p \neq \|y\|_p$, then $\|x+y\|_p = \max\{\|x\|_p, \|y\|_p\}$.*

As a consequence of the above proposition, all triangles in $\mathbb{Q}_p$ are isosceles. The sphere $S(a, r) = \{x \in \mathbb{Q}_p : \|x - a\|_p = r\}$ is both an open set and a closed set in $\mathbb{Q}_p$ and an open ball in $\mathbb{Q}_p$ is both open and closed. Also, every point of a ball is its center. Two balls in $\mathbb{Q}_p$ have a non empty intersection if and only if one is contained in the other.

Definition 1.4. *A set A is said to be dense in $\mathbb{Q}_p$ if, given any $\epsilon > 0$, $\mathcal{D}(x, \epsilon) \cap A \neq \phi$ for all x in $\mathbb{Q}_p$, where $\mathcal{D}(x, \epsilon) = \{y \in \mathbb{Q}_p : \|x - y\|_p < \epsilon\}$.*

In the p-adic topology, the set $\mathbb{N}$ is dense in $\mathbb{Z}$ which is dense in the set of p-adic integers $\mathbb{Z}_p$.

1.1.2 Hensel's Lemma

Hensel's Lemma is an important algebraic property of the p-adic numbers which helps in deciding whether a polynomial over $\mathbb{Z}_p$ has a root in $\mathbb{Z}_p$.

Theorem 1.4. [Hensel's Lemma] *Let $f(x) \in \mathbb{Z}_p[x]$. Suppose that there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that $f(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p}$ and $f'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p}$, where $f'(x)$ is the derivative of $f(x)$. Then there exists a p-adic integer $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$ and $f(\alpha) = 0$.*

For $a, b \in \mathbb{Z}_p$, $a \equiv b \pmod{p\mathbb{Z}_p}$ means that $a - b \in p\mathbb{Z}_p$. Hensel's lemma has a stronger version which is as follows:

Theorem 1.5. *Let $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ satisfy $\|f(a)\|_p < \|f'(a)\|_p^2$. Then there exists an $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\|\alpha - a\|_p < \|f'(a)\|_p$.*

We state another form of Hensel's lemma which gives factorisation of polynomials over $\mathbb{Z}_p$.

Theorem 1.6. [23, Lemma 3.4.6] *Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial with coefficients in $\mathbb{Z}_p$, and assume that there exist polynomials $g_1(x)$ and $h_1(x)$ in $\mathbb{Z}_p[x]$ such that*

1. *$g_1(x)$ is monic*
2. *$g_1(x)$ and $h_1(x)$ are relatively prime modulo p, and*
3. *$f(x) \equiv g_1(x)h_1(x) \pmod{p}$.*

Then there exist polynomials $g(x), h(x) \in \mathbb{Z}_p[x]$ such that

1. *$g(x)$ is monic,*
2. *$g(x) \equiv g_1(x) \pmod{p}$ and $h(x) \equiv h_1(x) \pmod{p}$, and*
3. *$f(x) = g(x)h(x)$.*

The p-adic absolute value on $\mathbb{Q}_p$ can be extended to a finite normal extension $\mathbb{K}$ over $\mathbb{Q}_p$ of degree n. For $\alpha \in \mathbb{K}$, define $\|\alpha\|_p := \sqrt[n]{\|\det(T_\alpha)\|_p}$ where T_α is the matrix of linear transformation from the vector space $\mathbb{K}$ over $\mathbb{Q}_p$ to itself defined by $x \mapsto \alpha x$ for all $x \in \mathbb{K}$. Also, $\nu_p(\alpha)$ is the unique rational number satisfying $\|\alpha\|_p = p^{-\nu_p(\alpha)}$. The ring of integers of $\mathbb{K}$, denoted by $\mathcal{O}$, is defined as the set of all elements in $\mathbb{K}$ with p-adic absolute value less than or equal to one.

Proposition 1.7. [23, Proposition 5.4.2] *The p-adic valuation ν_p is a homomorphism from the multiplicative group $\mathbb{K}^\times$ to the additive group $\mathbb{Q}$. Its image is of the form $\frac{1}{e}\mathbb{Z}$, where e is a divisor of $n = [\mathbb{K} : \mathbb{Q}_p]$.*

An extension $\mathbb{K}$ is said to an unramified extension of $\mathbb{Q}_p$ if $e = 1$.

1.1.3 p-adic analytic functions

Definition 1.5. *A function $f : \mathcal{O} \to \mathcal{O}$ is called analytic if there exists a sequence $(a_n)_{n\geq 0}$ in $\mathcal{O}$ such that*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n$$

for all $z \in \mathcal{O}$.

Next, we recall the p-adic exponential and logarithmic functions. For $a \in \mathbb{K}$ and $r > 0$, we denote $\mathcal{D}(a, r) := \{z \in \mathbb{K} : \|z - a\|_p < r\}$. Let $\rho = p^{-1/(p-1)}$. If $z \in \mathcal{D}(0, \rho)$, then the p-adic exponential function is defined as

$$\exp_p(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

The derivative is given by $\exp_p'(z) = \exp_p(z)$. On $\mathcal{D}(1, \rho)$, the p-adic logarithmic function is defined as

$$\log_p(z) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(z-1)^n}{n}.$$

For $z \in \mathcal{D}(1, \rho)$, we have $\exp_p(\log_p(z)) = z$. If $\mathbb{K}$ is unramified and $p \neq 2$, then $\mathcal{D}(0, \rho) = \mathcal{D}(0, 1)$ and $\mathcal{D}(1, \rho) = \mathcal{D}(1, 1)$. More properties of these functions can be found in [23].

Hensel's lemma is also true and follows similarly for functions given by power series with coefficients in the ring $\mathcal{O}$.

Theorem 1.8. [23, Hensel's lemma] *Let $f : \mathcal{O} \to \mathcal{O}$ be analytic. Let $b_0 \in \mathcal{O}$ be such that $\|f(b_0)\|_p < 1$ and $\|f'(b_0)\|_p = 1$. Then there exists a unique $b \in \mathcal{O}$ such that $f(b) = 0$ and $\|b - b_0\|_p < \|f(b_0)\|_p$.*

The following theorem of Strassman gives a bound on the number of roots of an analytic function defined in $\mathcal{O}$.

Theorem 1.9. [23, Strassman's Theorem] *Let $f : \mathcal{O} \to \mathcal{O}$ be analytic. Assume that $f(z)$ does not vanish identically on $\mathcal{O}$; equivalently, the coefficients $a_0, a_1, \ldots$ are* *not all* 0*. Define* μ *as the largest* m *with the property*

$$\|a_m\|_p = \max\{\|a_n\|_p : n = 0, 1, \ldots\}.$$

Then $f(z)$ *has at most* μ *zeros on* $\mathcal{O}$*.*

The following result connects the existence of a root of an analytic function in $\mathbb{Z}_p$ to the denseness of quotient set of values assumed.

Theorem 1.10. [36, Theorem 1.2] *Let* $f : \mathbb{Z}_p \to \mathbb{Q}_p$ *be an analytic function and let* $z_1, z_2 \in \mathbb{Z}_p$ *be two (not necessarily distinct) zeros of* f *of multiplicities* μ_1, μ_2*, respectively. If* μ_1, μ_2 *are coprime, then* R_f *is dense in* $\mathbb{Q}_p$*.*

The result below is a straightforward consequence of the theorem.

Theorem 1.11. [36, Corollary 1.3] *Let* $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ *be an analytic function with a simple zero in* $\mathbb{Z}_p$*. Then,* $R(f(\mathbb{N}))$ *is dense in* $\mathbb{Q}_p$*.*

Garcia et al. [19] provided a necessary condition for a set to be dense in $\mathbb{Q}_p$. We present the result below, as it is very useful for proving some results in the subsequent chapters.

Lemma 1.12. [19, Lemma 2.1] *If* S *is dense in* $\mathbb{Q}_p$*, then for each finite value of the* p*-adic valuation, there is an element of* S *with that valuation.*

By Lemma 1.12, it can be easily checked that the ratio set of prime numbers is not dense in $\mathbb{Q}_p$ since the only p-adic valuations possible are $\{-1, 0, 1\}$.

2

p-Adic quotient sets: cubic forms

2.1 Introduction

In this chapter, we prove some results which give conditions under which the ratio set of values assumed by a cubic form is dense in $\mathbb{Q}_p$. A cubic form is a homogeneous polynomial of degree 3 which is of the form

$$C(x_1, x_2, \ldots, x_r) = \sum_{i=1}^{r} \sum_{j=1}^{r} \sum_{k=1}^{r} a_{ijk} x_i x_j x_k.$$

[1]Some contents of this chapter have been published in *Arch. Math. (Basel)* 118 (2022).

We say that C is integral if $a_{ijk} \in \mathbb{Z}$ for all i, j, k and C is primitive if there is no positive integer $d > 1$ such that $d | a_{ijk}$ for all i, j, k. A form C is said to be isotropic over a field $\mathbb{F}$ if there is a nonzero vector $\overline{x} \in \mathbb{F}^r$ such that $C(\overline{x}) = 0$. Otherwise C is said to be anisotropic over $\mathbb{F}$. The ratio set generated by a cubic form C is

$$R(C) = \{C(\overline{x})/C(\overline{y}) : \overline{x}, \overline{y} \in \mathbb{Z}^r, C(\overline{y}) \neq 0\}.$$

2.2 Diagonal cubic form

In this section, we study denseness of $R(C)$ when C is the cubic form $C(x, y) = ax^3 + by^3$, where a and b are nonzero integers. First, we give a necessary condition for the denseness of $R(C)$ in $\mathbb{Q}_p$.

Theorem 2.1. *Let $C(x, y) = ax^3 + by^3$ be primitive and integral. If C is anisotropic modulo p, then $R(C)$ is not dense in $\mathbb{Q}_p$.*

Proof. We claim that $\nu_p(C(x, y))$ is a multiple of 3 for all $x, y \in \mathbb{Z}$. If $C(x, y) \not\equiv 0 \pmod p$, then $\nu_p(C(x, y)) = 0$. Suppose $C(x, y) \equiv 0 \pmod p$. Then $(x, y) \equiv (0, 0) \pmod p$ since C is anisotropic; hence $x = mp^j$ and $y = np^k$ for some $j, k \geq 1$, $p \nmid m$ and $p \nmid n$. Without loss of generality, assume that $j \geq k$. Then,

$$\begin{aligned} \nu_p(C(x, y)) &= \nu_p(am^3p^{3j} + bn^3p^{3k}) \\ &= \nu_p(p^{3k}(am^3p^{3(j-k)} + bn^3)) \\ &= 3k + \nu_p(C(mp^{(j-k)}, n)) \\ &= 3k \end{aligned}$$

since $p \nmid n$ and C is anisotropic. Thus by Lemma 1.12, $R(C)$ is not dense in $\mathbb{Q}_p$. ■

Next, we give some sufficient and necessary conditions for denseness of $R(C)$ in $\mathbb{Q}_p$.

Theorem 2.2. *Let $C(x,y) = ax^3 + by^3$ be primitive and integral.*

1. *If $p \nmid ab$, then $R(C)$ is dense in $\mathbb{Q}_p$ if ba^{-1} is a cubic residue modulo p^α, where $\alpha = 1 + \nu_p(3)$.*

2. *If $a = p^k\ell$ such that $p \nmid \ell$ and $3|k$, then $R(C)$ is dense in $\mathbb{Q}_p$ if $b^{-1}\ell$ is a cubic residue modulo p^α, where $\alpha = 1 + \nu_p(3)$.*

3. *If $p \nmid ab$, then $b^{-1}a$ is a cubic residue modulo p if $R(C)$ is dense in $\mathbb{Q}_p$.*

4. *If $a = p^k\ell$ such that $p \nmid \ell$ and $3|k$, then $b^{-1}\ell$ is a cubic residue modulo p if $R(C)$ is dense in $\mathbb{Q}_p$.*

5. *If $a = p^k\ell$, $p \nmid \ell$ and $3 \nmid k$, then $R(C)$ is not dense in $\mathbb{Q}_p$ if there exists an integer n which is a cubic non-residue modulo p.*

Proof. We first prove part (1) of the theorem. Here $p \nmid ab$. Suppose that $p \neq 3$ and ba^{-1} is a cubic residue modulo p. Then for a $y_0 \in \mathbb{Z}$ with $p \nmid y_0$, there exists $x_0 \in \mathbb{Z}$, $p \nmid x_0$ such that $-ba^{-1}y_0^3 \equiv x_0^3 \pmod{p}$. Consider the polynomial $f(x) = x^3 + ba^{-1}y_0^3$. Then $f(x_0) \equiv 0 \pmod{p}$ and $f'(x_0) = 3x_0^2 \not\equiv 0 \pmod{p}$. Therefore, by Hensel's lemma, f has a root $\alpha \in \mathbb{Z}_p$ which is a simple root since $x_0 \not\equiv 0 \pmod{p}$. By Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(f(\mathbb{N})) \subset R(C)$, hence $R(C)$ is dense in $\mathbb{Q}_p$.

For $p = 3$, consider $C'(x,y) = x^3 + ba^{-1}y^3$. Suppose ba^{-1} is a cubic residue modulo 9. Then by [11, Lemma 3.5], ba^{-1} is a cube in $\mathbb{Z}_3$, that is, there exists a nonzero $x_0 \in \mathbb{Z}_3$ such that $x_0^3 + ba^{-1} = 0$. In particular, x_0 is a simple zero of the polynomial $f(x) = x^3 + ba^{-1}$ in $\mathbb{Z}_3$. Therefore, by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_3$. Since $R(f(\mathbb{N})) \subset R(C')$, $R(C) = R(C')$ is dense in $\mathbb{Q}_3$.

We next prove part (2) of the theorem. Suppose that $b^{-1}\ell$ is a cubic residue modulo p^α. We have $b^{-1}C(x,y) = b^{-1}\ell p^{3k'}x^3 + y^3$. Using part (1) of the theorem, we have that $R(C')$ is dense in $\mathbb{Q}_p$, where $C'(x,y) = b^{-1}\ell x^3 + y^3$. Since

$$\frac{C'(x,y)}{C'(z,w)} = \frac{p^{3k'}C'(x,y)}{p^{3k'}C'(z,w)} = \frac{C'(p^{k'}x, p^{k'}y)}{C'(p^{k'}z, p^{k'}w)} = \frac{C(x, p^{k'}y)}{C(z, p^{k'}w)},$$

therefore, $R(C)$ is dense in $\mathbb{Q}_p$. This completes the proof of part (2) of the theorem.

We next prove part (3) of the theorem. Suppose that $b^{-1}a$ is not a cubic residue modulo p. If $C(x,y) \equiv 0 \pmod p$, that is, $ax^3 + by^3 \equiv 0 \pmod p$ then

$$x^3 \equiv -ba^{-1}y^3 \pmod p.$$

The left side is either a cubic residue or divisible by p and the right side is either a cubic non-residue or divisible by p. Hence $x \equiv y \equiv 0 \pmod p$. Therefore, C is anisotropic modulo p. Hence $R(C)$ is not dense in $\mathbb{Q}_p$ by Theorem 2.1.

We next prove part (4) of the theorem. Here $a = p^k\ell$ such that $p \nmid \ell$ and $3|k$. We write $k = 3k'$. Suppose that $b^{-1}\ell$ is not a cubic residue modulo p. Let $C'(x,y) = b^{-1}\ell x^3 + y^3$. By the third part of the theorem, $R(C')$ is not dense in $\mathbb{Q}_p$. We have

$$b^{-1}C(x,y) = p^k b^{-1}\ell x^3 + y^3 = b^{-1}\ell(p^{k'}x)^3 + y^3 = C'(p^{k'}x, y).$$

Since $R(C) = R(b^{-1}C) \subset R(C')$, $R(C)$ is not dense in $\mathbb{Q}_p$.

Finally, we prove part (5) of the theorem. Here $a = p^k\ell, p \nmid \ell$ and $3 \nmid k$. Suppose that $R(C)$ is dense in $\mathbb{Q}_p$. Let $C'(x,y) = b^{-1}C(x,y)$. Then $R(C')$ is dense in $\mathbb{Q}_p$. Choose a cubic non-residue $n \pmod p$. There exist $x, y, z, w \in \mathbb{Z}$ not all multiples of p such that

$$\left\| \frac{C'(x,y)}{C'(z,w)} - n \right\|_p < \frac{1}{p^k}.$$

This yields

$$\begin{aligned}&\left\|y^3 - nw^3 + p^k b^{-1}\ell(x^3 - nz^3)\right\|_p\\&= \|C'(x,y) - nC'(z,w)\|_p\\&< \frac{\|C'(z,w)\|_p}{p^k}\\&\leq \frac{1}{p^k}.\end{aligned}$$

If $p \nmid y$ or $p \nmid w$, then $y^3 - nw^3 \not\equiv 0 \pmod{p}$ since n is a cubic non-residue. Hence $\|C'(x,y) - nC'(z,w)\|_p = 1$ which is a contradiction. Therefore $p|y$ and $p|w$ which give $\nu_p(y^3 - nw^3) = 3m$ where m is a positive integer. Since $p|y$ and $p|w$, we have either $p \nmid x$ or $p \nmid z$. This yields $\nu_p(x^3 - nz^3) = 0$. Since $3 \nmid k$, therefore $C'(x,y) - nC'(z,w)$ is the sum of a p-adic integer with valuation a multiple of 3 and a p-adic integer with valuation not a multiple of 3. Hence $\|C'(x,y) - nC'(z,w)\|_p \geq p^{-k}$ which gives a contradiction. Thus, $R(C')$ is not dense in $\mathbb{Q}_p$. Hence $R(C)$ is not dense in $\mathbb{Q}_p$. This completes the proof of the theorem. ∎

Remark 2.2.1. *We will be providing generalisations of Theorem 2.1 and Theorem 2.2 in Chapter* 3.

Using Theorem 2.2, we have the following corollary.

Corollary 2.2.1. *Let $C(x_1, x_2, \ldots, x_r) = a_1x_1^3 + a_2x_2^3 + \cdots + a_rx_r^3$ be primitive and integral. Suppose that $p \nmid a_i$ and $p^k|a_j$ for some i, j from 1 to $r, i \neq j$ and $3|k$. Then $R(C)$ is dense in $\mathbb{Q}_p$ if $a_i^{-1}\ell$ is a cubic residue modulo p^α, where $\alpha = 1 + \nu_p(3)$ and $a_j = p^k\ell$, $p \nmid \ell$.*

Proof. It follows from Theorem 2.2 that $R(a_ix_i^3 + a_jx_j^3)$ is dense in $\mathbb{Q}_p$. Since $R(a_ix_i^3 + a_jx_j^3) \subset R(C)$, $R(C)$ is dense in $\mathbb{Q}_p$. ∎

Recall that a vector $\overline{x} \in \mathbb{F}^r$ such that $F(\overline{x}) = 0$ is called a non-singular zero of F if $\frac{\partial F}{\partial x_i}(\overline{x}) \neq 0$ for some $i \in \{1, \ldots, r\}$. We use the following lemma due to

Heath-Brown to prove our next theorem. This lemma guarantees the existence of a non-singular zero for a particular cubic form modulo p.

Lemma 2.3. [24, Lemma 6] *Let $p \neq 3$ and suppose that*

$$f(x, y, z) = ax^3 + bxy^2 + cy^3 + (dx + ey)z^2 + fz^3 \in \mathbb{F}_p[x, y, z],$$

with $acf \neq 0$. Then f has at least one non-singular zero over $\mathbb{F}_p$, where $\mathbb{F}_p$ is the field with p elements.

We give a sufficient condition for the denseness of the ratio set of the values attained by a diagonal cubic form. In [36, Theorem 1.8], Miska et al. proved that the ratio set of $\{x_1^3 + \cdots + x_r^3 : x_1, \ldots, x_r \in \mathbb{Z}_{\geq 0}\}$ is dense in $\mathbb{Q}_p$ for all $r \geq 2$. The following results also generalise this fact.

Theorem 2.4. *Let $C(x, y, z) = ax^3 + by^3 + cz^3$ be integral. If $p \neq 3$ and $p \nmid abc$, then $R(C)$ is dense in $\mathbb{Q}_p$.*

Proof. We have $C(x, y, z) = ax^3 + by^3 + cz^3$. If $p \neq 3$, then by Lemma 2.3, $C(x, y, z)$ has a non-singular solution (x_0, y_0, z_0) modulo p. Suppose that $C(x_0, y_0, z_0) = 0 \pmod{p}$ and $\frac{\partial C}{\partial x}(x_0, y_0, z_0) \neq 0 \pmod{p}$. Then by Hensel's lemma, the polynomial $f(x) = C(x, y_0, z_0)$ has a simple root in $\mathbb{Z}_p$. Therefore, by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Hence, $R(C) \supset R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. ∎

Using Theorem 2.4, we have the following corollary.

Corollary 2.2.2. *Let $C(x_1, x_2, \ldots, x_r) = a_1x_1^3 + a_2x_2^3 + \cdots + a_rx_r^3$ be integral. Suppose that $p \neq 3$ and $\nu_p(a_i) \equiv \nu_p(a_j) \equiv \nu_p(a_k) \pmod{3}$ for some $i, j, k \in \{1, \ldots, r\}$, $i < j < k$. Then $R(C)$ is dense in $\mathbb{Q}_p$.*

Proof. Write $a_i = p^{m_i}\ell_i$, $a_j = p^{m_j}\ell_j$ and $a_k = p^{m_k}\ell_k$, where $m_i \equiv m_j \equiv m_k \pmod{3}$ and $p \nmid \ell_i\ell_j\ell_k$. Without loss of generality assume that $m_i \geq m_j \geq m_k$. Put

$\widetilde{C}(x_i, x_j, x_k) = a_i x_i^3 + a_j x_j^3 + a_k x_k^3$ and $\widehat{C}(x_i, x_j, x_k) = \ell_i x_i^3 + \ell_j x_j^3 + \ell_k x_k^3$. Then

$$\frac{a_i\left(p^{\frac{m_k-m_i}{3}}x_i\right)^3 + a_j\left(p^{\frac{m_k-m_j}{3}}x_j\right)^3 + a_k {x_k}^3}{a_i\left(p^{\frac{m_k-m_i}{3}}y_i\right)^3 + a_j\left(p^{\frac{m_k-m_j}{3}}y_j\right)^3 + a_k {y_k}^3} = \frac{\ell_i x_i^3 + \ell_j x_j^3 + \ell_k x_k^3}{\ell_i y_i^3 + \ell_j y_j^3 + \ell_k y_k^3},$$

which means that $R(\widehat{C}) \subset R(\widetilde{C}(\mathbb{Q}^3)) = R(\widetilde{C}(\mathbb{Z}^3)) = R(\widetilde{C}) \subset R(C)$. From Theorem 2.4, $R(\widehat{C})$ is dense in $\mathbb{Q}_p$. As a result, $R(C)$ is dense in $\mathbb{Q}_p$. ■

We also have the following corollary which follows from Corollary 2.2.2.

Corollary 2.2.3. *For each $p \neq 3$ and every integral diagonal cubic form $C(x_1, x_2, \ldots, x_r) = a_1 x_1^3 + a_2 x_2^3 + \cdots + a_r x_r^3$ with $a_1 a_2 \cdots a_r \neq 0$ and $r \geq 7$ the set $R(C)$ is dense in $\mathbb{Q}_p$.*

Proof. It suffices to note that there are $1 \leq i < j < k \leq 7$ such that $\nu_p(a_i) \equiv \nu_p(a_j) \equiv \nu_p(a_k) \pmod 3$. Then by Corollary 2.2.2, $R(a_i x_i^3 + a_j x_j^3 + a_k x_k^3)$ is dense in $\mathbb{Q}_p$. Since $R(a_i x_i^3 + a_j x_j^3 + a_k x_k^3) \subset R(C)$, we see that $R(C)$ is dense in $\mathbb{Q}_p$. ■

2.3 A general result

Studying denseness of $R(C)$ when C is any cubic form seems to be a difficult problem. We prove a general result on denseness of $R(C)$ when C is a cubic form with more than 9 variables. Before we state our result, we recall some definitions. Two forms F_1 and F_2 over a field K are said to be equivalent if there is a non-singular linear transformation T over K such that $F_1(\overline{x}) = F_2(T\overline{x})$. The order $\mathrm{o}(F)$ of a form F is the smallest integer m such that F is equivalent to a form that contains only m variables explicitly. A form in n variables is called non-degenerate if $\mathrm{o}(F) = n$. In Theorem 2.6, we prove the denseness in $\mathbb{Q}_p$ of the ratio set of the values of a non-degenerate cubic form in more that 9 variables.

We will need the following result to prove the theorem.

Theorem 2.5. [38, Theorem 2] *Every cubic form C over K with $o(C) \geq 10$ has a non-singular zero over K where K is any field complete with respect to a discrete non-archimedean valuation.*

The result is as follows.

Theorem 2.6. *Let C be a non-degenerate, integral and primitive cubic form with more that 9 variables. Then $R(C)$ is dense in $\mathbb{Q}_p$.*

Proof. Let C be a non-degenerate, integral and primitive cubic form with more that 9 variables. Recall that a vector $\overline{x} \in \mathbb{Q}_p^r$ such that $C(\overline{x}) = 0$ is a non-singular zero of C if $\frac{\partial C}{\partial x_i}(\overline{x}) \neq 0$ for some i from 1 to r. In Theorem 2.5, taking $K = \mathbb{Q}_p$, we get a non-singular zero of C over $\mathbb{Q}_p$. By multiplying by an appropriate power of p, we get a non-singular zero $\overline{x_0} = (x_1, x_2, \dots, x_r)$ of C in $\mathbb{Z}_p^r$. We have

$$C(\overline{x_0}) = 0, \frac{\partial C}{\partial x_i}(\overline{x_0}) \neq 0 \tag{2.1}$$

for some i from 1 to r. Consider the polynomial $f(x) = C(x_1, \dots, x, \dots, x_r)$ in one variable x obtained by replacing x_i by x. By (2.1), $f(x)$ has a simple root in $\mathbb{Z}_p$. Therefore by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(f(\mathbb{N})) \subset R(C)$, $R(C)$ is dense in $\mathbb{Q}_p$. This completes the proof of the theorem. ∎

2.4 Binary cubic form

We begin by stating a lemma due to Sun which gives the number of roots modulo a prime $p > 3$ for polynomials of degree 3. We use this lemma to find a sufficient condition for the denseness of ratio sets of a binary cubic form. For a prime p and a polynomial $f(x) \in \mathbb{Z}[x]$, let $N_p(f)$ denote the number of zeros (including multiplicity) of $f(x) \equiv 0 \pmod{p}$. Also, let $(\frac{\cdot}{p})$ denote the Legendre symbol.

Lemma 2.7. [47, Lemma 2.3] *Let $p > 3$ be a prime, $a_1, a_2, a_3 \in \mathbb{Z}, a = (a_1^2 - 3a_2)^3, b = -2a_1^3 + 9a_1a_2 - 27a_3$ and $D = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3$. Then*

1. $b^2 - 4a = -27D$.

2. If $p \nmid a_1^2 - 3a_2$ and $X = (a_1^2 - 3a_2)(3x + a_1)$, then $x^3 + a_1x^2 + a_2x + a_3 = (X^3 - 3aX - ab)/(27a)$ and so $N_p(x^3 + a_1x^2 + a_2x + a_3) = N_p(x^3 - 3ax - ab)$.

3. $N_p(x^3 + a_1x^2 + a_2x + a_3) = 1$ if and only if $(\frac{D}{p}) = -1$.

We now give a sufficient condition for the denseness of the ratio set of a binary cubic form in $\mathbb{Q}_p$.

Theorem 2.8. *Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be an integral binary cubic form. Let $D := a^2b^2c^2 - 4a^3c^3 - 4a^2b^3d - 27a^4d^2 + 18a^3bcd$.*

1. *Let p be a prime. If $(b, c) \neq (0, 0)$ and $a = 0$, then $R(F)$ is dense in $\mathbb{Q}_p$.*

2. *If $a \neq 0, p > 3$ and D is not a quadratic residue modulo p, then $R(F)$ is dense in $\mathbb{Q}_p$.*

Proof. We first prove part (1) of the theorem. We have $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ with $(b, c) \neq (0, 0)$ and $a = 0$. Consider the polynomial

$$f(y) := F(1, y) = by + cy^2 + dy^3 = y(b + cy + dy^2).$$

If $b \neq 0$, then $y = 0$ is a simple root of f in $\mathbb{Z}_p$. Suppose that $b = 0$ and $d \neq 0$. If $c/d \in \mathbb{Z}_p$, then $y = -c/d$ is a simple root of $f(y) := F(1, y) = cy^2 + dy^3$ in $\mathbb{Z}_p$. If $c/d \notin \mathbb{Z}_p$, then $x = -d/c$ is a simple root of the polynomial $f(x) := F(x, 1) = cx + d$ in $\mathbb{Z}_p$. If $b = d = 0$, then $x = 0$ is a simple root of the polynomial $f(x) := F(x, 1) = cx$ in $\mathbb{Z}_p$. In all the cases, by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(f(\mathbb{N})) \subset R(F)$, $R(F)$ is dense in $\mathbb{Q}_p$.

We next prove part (2) of the theorem. Suppose that $a \neq 0$ and $p > 3$. Consider the polynomial

$$f(x) := \frac{F(x, a)}{a} = x^3 + bx^2 + acx + a^2d.$$

If D is not a quadratic residue modulo p, then by part 3 of Lemma 2.7, f has a root x_0 modulo p. Also $f'(x_0) \not\equiv 0 \pmod p$. Therefore, by Hensel's lemma, f has a simple root in $\mathbb{Z}_p$. By Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(F) \supseteq R(f(\mathbb{N}))$, $R(F)$ is dense in $\mathbb{Q}_p$. This completes the proof of the theorem. ■

Remark 2.4.1. *The converse of Theorem 2.8 is not true. For example, consider the cubic form $x^3 + x^2y + xy^2 + y^3$. Using Hensel's lemma, we obtain a simple root for the polynomial $f(x) = x^3 + x^2 + x + 1$ in $\mathbb{Q}_5$ since $f(2) \equiv 0 \pmod 5$ and $f'(2) \not\equiv 0 \pmod 5$. Therefore, by Theorem 1.11, the form has a dense ratio set in $\mathbb{Q}_5$. But $D = -16$ is a quadratic residue modulo 5.*

Though Theorem 2.8(2) does not cover the cases $p = 2, 3$, we can examine these cases separately using some ad-hoc methods. Consider the following examples.

Example 2.4.1. *Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a cubic form such that $a \equiv b \equiv d \equiv 1 \pmod 2$ and $c \equiv 0 \pmod 2$. Then the form F is anisotropic modulo 2. Hence, by Theorem 3.1, $R(F)$ is not dense in $\mathbb{Q}_2$.*

Example 2.4.2. *Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a cubic form such that $a \equiv b \equiv c \equiv d \equiv 1 \pmod 3$. Then $R(F)$ is dense in $\mathbb{Q}_3$. The proof goes as follows. Consider the polynomial $f(x) := F(x, 1) = ax^3 + bx^2 + cx + d$. We have $f(2) \equiv 0 \pmod 3$ and $f'(2) \not\equiv 0 \pmod 3$. By Hensel's lemma, f has a simple root in $\mathbb{Z}_p$. Therefore, by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(F) \supseteq R(f(\mathbb{N}))$, $R(F)$ is dense in $\mathbb{Q}_3$.*

Example 2.4.3. *Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a cubic form such that $a \equiv 2 \pmod 3, b \equiv c \equiv d \equiv 1 \pmod 3$. Then, the form F is anisotropic modulo 3. Hence, by Theorem 3.1, $R(F)$ is not dense in $\mathbb{Q}_3$.*

Using similar arguments, the denseness of any binary cubic forms in $\mathbb{Q}_3$ can be checked. For details, see Table 2.1. However, to study the denseness of the ratio set of a binary cubic form with nonzero odd coefficients in $\mathbb{Q}_2$ seems to be difficult using these methods.

$a \pmod 3$	$b \pmod 3$	$c \pmod 3$	$d \pmod 3$	Denseness in $\mathbb{Q}_3$
1	1	1	1	Dense
1	1	1	2	Not Dense
1	1	2	1	Not Dense
1	1	2	2	Dense
1	2	1	2	Dense
2	1	1	2	Dense
1	2	2	2	Not Dense
2	2	1	2	Not Dense
1	2	2	1	Dense
2	2	2	2	Dense
1	1	0	1	Dense
2	1	0	1	Dense
1	1	0	2	Not Dense
2	1	0	2	Not Dense
2	2	0	1	Not Dense
1	2	0	2	Dense
1	1	0	2	Not Dense
2	2	0	2	Dense

Table 2.1: Denseness of the ratio set of $ax^3 + bx^2y + cxy^2 + dy^3$ in $\mathbb{Q}_3$.

3

p-Adic quotient sets: polynomials and integral forms

3.1 Introduction

In this chapter, we consider forms of degree n and obtain generalisations of some results of Chapter 1. We also consider polynomials in a single variable and produce conditions for the denseness of their ratio sets. First, we recall the definition of a form of degree n.

[1]Some contents of this chapter have been published in *Arch. Math. (Basel) 119* (2022).

A form of degree n is a homogeneous polynomial

$$F(x_1, x_2, \ldots, x_r) = \sum_{1 \le i_1 \le i_2 \le \ldots \le i_n \le r} a_{i_1 i_2 \ldots i_n} x_{i_1} x_{i_2} \cdots x_{i_n}.$$

We say that F is integral if $a_{i_1 i_2 \ldots i_n} \in \mathbb{Z}$ for all $(i_1, i_2, \ldots, i_n)$ and F is primitive if there is no positive integer $d > 1$ such that $d \mid a_{i_1 i_2 \ldots i_n} \in \mathbb{Z}$ for all $(i_1, i_2, \ldots, i_n)$. Recall that a form F is said to be isotropic over a field $\mathbb{F}$ if there is a nonzero vector $\overline{x} \in \mathbb{F}^r$ such that $F(\overline{x}) = 0$. Otherwise F is said to be anisotropic over $\mathbb{F}$. The ratio set generated by an integral form F is

$$R(F) = \{F(\overline{x})/F(\overline{y}) : \overline{x}, \overline{y} \in \mathbb{Z}^r, F(\overline{y}) \neq 0\}.$$

We now prove a result for any form F which is anisotropic modulo p and this extends Theorem 2.1 of Chapter 2.

Theorem 3.1. *Let F be any form of degree $n \ge 2$ that is primitive and integral. If F is anisotropic modulo p, then $R(F)$ is not dense in $\mathbb{Q}_p$.*

Proof. We claim that $\nu_p(F(\overline{x}))$ is a multiple of n for all $\overline{x}$, where $\overline{x} = (x_1, x_2, \ldots, x_r) \in \mathbb{Z}^r$. If $F(\overline{x}) \not\equiv 0 \pmod{p}$, then $\nu_p(F(\overline{x})) = 0$. Suppose that $F(\overline{x}) \equiv 0 \pmod{p}$. Therefore $\overline{x} \equiv \overline{0} \pmod{p}$ as F is anisotropic. Let $k = \min\{\nu_p(x_i) \colon i \in \{1, \ldots, r\}\}$. Then, we get $\nu_p(F(\overline{x})) = nk$ since F is anisotropic. Thus, by Lemma 1.12, $R(F)$ is not dense in $\mathbb{Q}_p$. ∎

3.2 Diagonal forms

In the previous chapter, we provided a result for diagonal cubic form $ax^3 + by^3$. Here, we extend the result to the diagonal binary form $F(x, y) = ax^n + by^n$ for all $n \ge 3$. To be specific, we prove the following result which extends Theorem 2.2. For each logic sentence T we put

$$[T] = \begin{cases} 1 \text{ if } T \text{ is true,} \\ 0 \text{ if } T \text{ is false.} \end{cases}$$

Theorem 3.2. *Let $n \geq 3$. Let $F(x,y) = ax^n + by^n$ be integral.*

1. *If $p \nmid ab$, then $R(F)$ is dense in $\mathbb{Q}_p$ if $-a^{-1}b$ is an nth power residue modulo $p^{\nu_p(n)+\nu_p\left(2^{[2|n]}\right)+1}$.*
2. *If $a = p^k\ell$ such that $p \nmid \ell$ and $n \mid k$, then $R(F)$ is dense in $\mathbb{Q}_p$ if $-b^{-1}\ell$ is an nth power residue modulo $p^{\nu_p(n)+\nu_p\left(2^{[2|n]}\right)+1}$.*
3. *If $p \nmid ab$, then $-b^{-1}a$ is an nth power residue modulo p if $R(F)$ is dense in $\mathbb{Q}_p$.*
4. *If $a = p^k\ell$ such that $p \nmid \ell$ and $n|k$, then $-b^{-1}\ell$ is an nth power residue modulo p if $R(F)$ is dense in $\mathbb{Q}_p$.*
5. *If $a = p^k\ell, p \nmid \ell$ and $n \nmid k$, then $R(F)$ is not dense in $\mathbb{Q}_p$ if there exists an integer m which is not an nth power residue modulo p.*

We first prove a lemma which will be used to prove Theorem 3.2.

Lemma 3.3. *Let p be a prime, $k \geq 1$ and $u \in \mathbb{Z}_p^\times$. Then u is a p^kth power in $\mathbb{Z}_p$ if and only if u is a p^kth power residue modulo $p^{k+\nu_p(2)+1}$.*

Proof. We first prove for any non-negative integer ℓ that if $u \in \mathbb{Z}_p^\times$ is a p^kth power residue modulo $p^{k+\nu_p(2)+\ell+1}$, then u is a p^kth power residue modulo $p^{k+\nu_p(2)+\ell+2}$. Suppose that $u \equiv a^{p^k} \pmod{p^{k+\nu_p(2)+\ell+1}}$ for some $a \in \mathbb{Z}_p$. Then $a \in \mathbb{Z}_p^\times$ and $u/a^{p^k} \equiv 1 \pmod{p^{k+\nu_p(2)+\ell+1}}$. Hence

$$u/a^{p^k} \equiv 1 + cp^{k+\nu_p(2)+\ell+1} \pmod{p^{k+\nu_p(2)+\ell+2}},$$

where $0 \le c \le p-1$. We have

$$\left(1 + cp^{\nu_p(2)+\ell+1}\right)^{p^k} \equiv 1 + cp^{k+\nu_p(2)+\ell+1} \pmod{p^{k+\nu_p(2)+\ell+2}}.$$

Therefore,

$$u \equiv a^{p^k}\left(1 + cp^{\nu_p(2)+\ell+1}\right)^{p^k} \pmod{p^{k+\nu_p(2)+\ell+2}}.$$

Thus, u is a p^kth power residue modulo $p^{k+\nu_p(2)+\ell+2}$.

Let $u \in \mathbb{Z}_p^\times$. Suppose that u is a p^kth power residue modulo $p^{k+\nu_p(2)+1}$. Then, using the above fact repeatedly we find that u is a p^kth power residue modulo p^{2k+1}. Hence, by Hensel's lemma, u is a p^kth power in $\mathbb{Z}_p$. Conversely, suppose that u is a p^kth power in $\mathbb{Z}_p$. Since $u \in \mathbb{Z}_p^\times$, we infer that u is a p^kth power residue modulo $p^{k+\nu_p(2)+1}$. This completes the proof of the lemma. ∎

Having Lemma 3.3 showed, we are ready to prove Theorem 3.2.

Proof of Theorem 3.2. We first prove part (1) of the theorem.
Let $n = p^k m$ where $p \nmid m$. Suppose that $-a^{-1}b$ is an nth power residue modulo $p^{\nu_p(n)+\nu_p\left(2^{[2|n]}\right)+1}$. Then, $-a^{-1}b$ is a p^kth power residue modulo $p^{\nu_p(n)+\nu_p\left(2^{[2|n]}\right)+1}$. By Lemma 3.3, $-a^{-1}b$ is a p^kth power in $\mathbb{Z}_p$. Also, by Hensel's lemma, $-a^{-1}b$ is an mth power in $\mathbb{Z}_p$. Therefore, $-a^{-1}b$ is an nth power in $\mathbb{Z}_p$. Thus $-a^{-1}b = u^n$ for some $u \in \mathbb{Z}_p$. This implies that u is a root of the polynomial $f(x) = x^n + a^{-1}b$. Clearly, $f'(u) = nu^{n-1} \neq 0$, and hence the polynomial $f(x) = x^n + a^{-1}b$ has a simple root in $\mathbb{Z}_p$. Therefore, by Lemma 1.11, $R(f(\mathbb{N})) \subset R(F)$ is dense in $\mathbb{Q}_p$. Hence $R(F)$ is dense in $\mathbb{Q}_p$.

We next prove part (2) of the theorem. Suppose that $-b^{-1}\ell$ is an nth power residue modulo $p^{\nu_p(n)+\nu_p\left(2^{[2|n]}\right)+1}$. We have $b^{-1}F(x,y) = b^{-1}\ell p^{nk'}x^n + y^n$. Using part (1) of the theorem, we have that $R(\widetilde{F})$ is dense in $\mathbb{Q}_p$, where $\widetilde{F}(x,y) = b^{-1}\ell x^n + y^n$.

Since

$$\frac{\widetilde{F}(x,y)}{\widetilde{F}(z,w)} = \frac{p^{nk'}\widetilde{F}(x,y)}{p^{nk'}\widetilde{F}(z,w)} = \frac{\widetilde{F}(p^{k'}x,p^{k'}y)}{\widetilde{F}(p^{k'}z,p^{k'}w)} = \frac{F(x,p^{k'}y)}{F(z,p^{k'}w)},$$

therefore $R(F)$ is dense in $\mathbb{Q}_p$. This completes the proof of part (2) of the theorem.

We next prove part (3) of the theorem. Suppose that $-b^{-1}a$ is not an nth power residue modulo p. If $F(x,y) \equiv 0 \pmod p$, that is, $ax^n + by^n \equiv 0 \pmod p$ then

$$x^n \equiv -ba^{-1}y^n \pmod p.$$

The left side is either an nth power residue or divisible by p and the right side is either not an nth power residue or divisible by p. Hence $x \equiv y \equiv 0 \pmod p$. Therefore F is anisotropic modulo p. Hence $R(F)$ is not dense in $\mathbb{Q}_p$ by Theorem 3.1.

We next prove part (4) of the theorem. Here $a = p^k\ell$ such that $p \nmid \ell$ and $n|k$. We write $k = nk'$. Suppose that $-b^{-1}\ell$ is not an nth power residue modulo p. Let $\widetilde{F}(x,y) = b^{-1}\ell x^n + y^n$. By the third part of the theorem, $R(\widetilde{F})$ is not dense in $\mathbb{Q}_p$. We have

$$b^{-1}F(x,y) = p^k b^{-1}\ell x^n + y^n = b^{-1}\ell(p^{k'}x)^n + y^n = \widetilde{F}(p^{k'}x,y).$$

Since $R(F) = R(b^{-1}F) \subset R(\widetilde{F})$, $R(F)$ is not dense in $\mathbb{Q}_p$.

Finally, we prove part (5) of the theorem. Here $a = p^k\ell, p \nmid \ell$ and $n \nmid k$. Suppose that $R(F)$ is dense in $\mathbb{Q}_p$. Let $\widetilde{F}(x,y) = b^{-1}F(x,y)$. Then $R(\widetilde{F})$ is dense in $\mathbb{Q}_p$. Choose an m which is not an nth power residue modulo p. There exist $x,y,z,w \in \mathbb{Z}$ not all multiples of p such that

$$\left\| \frac{\widetilde{F}(x,y)}{\widetilde{F}(z,w)} - m \right\|_p < \frac{1}{p^k}.$$

This yields

$$\begin{aligned}&\left\|y^n - mw^n + p^k b^{-1}\ell(x^n - mz^n)\right\|_p\\&= \left\|\widetilde{F}(x,y) - m\widetilde{F}(z,w)\right\|_p\\&< \frac{\left\|\widetilde{F}(z,w)\right\|_p}{p^k}\\&\leq \frac{1}{p^k}.\end{aligned}$$

If $p \nmid y$ or $p \nmid w$, then $y^n - mw^n \not\equiv 0 \pmod{p}$ since m is not an nth power residue modulo p. Hence $\left\|\widetilde{F}(x,y) - m\widetilde{F}(z,w)\right\|_p = 1$ which is a contradiction. Therefore $p \mid y$ and $p \mid w$, which gives $\nu_p(y^n - mw^n) = nt$, where t is a positive integer. Since $p \mid y$ and $p \mid w$, we have either $p \nmid x$ or $p \nmid z$. This yields $\nu_p(x^n - mz^n) = 0$. Since $n \nmid k$, we have that $\widetilde{F}(x,y) - m\widetilde{F}(z,w)$ is the sum of a p-adic integer with valuation being a positive multiple of n and a p-adic integer with valuation equal to k. Hence $\left\|\widetilde{F}(x,y) - m\widetilde{F}(z,w)\right\|_p \geq p^{-k}$, which gives a contradiction. Consequently, $R(\widetilde{F})$ is not dense in $\mathbb{Q}_p$. Finally, $R(F)$ is not dense in $\mathbb{Q}_p$. This completes the proof of the theorem. ■

We remark that if n is an odd integer, then $-a^{-1}b$ is an nth power residue modulo $p^{\nu_p(n)+\nu_p\left(2^{[2|n]}\right)+1}$ if and only if $a^{-1}b$ is an nth power residue modulo $p^{\nu_p(n)+1}$.

Let us note that Theorem 3.2 simplifies if $\gcd(n, p(p-1)) = 1$.

Corollary 3.2.1. *Let $n \geq 3$ and p be a prime number such that* $\gcd(n, p(p-1)) = 1$.

1. *Let $F(x,y) = ax^n + by^n$ be integral with $ab \neq 0$ and $\nu_p(a) \equiv \nu_p(b) \pmod{n}$. Then $R(F)$ is dense in $\mathbb{Q}_p$.*

2. *Let $F(x,y) = a_1x_1^n + a_2x_2^n + \cdots + a_rx_r^n$ be integral with $a_1a_2\cdots a_r \neq 0$ and such that $\nu_p(a_i) \equiv \nu_p(a_j) \pmod{n}$ for some $1 \leq i < j \leq r$. Then $R(F)$ is dense in $\mathbb{Q}_p$.*

Proof. We start with the proof of part (1). Let $a = p^{k_1}\ell_1$ and $b = p^{k_2}\ell_2$, where $k_1 \equiv k_2 \pmod{n}$ and $p \nmid \ell_1\ell_2$. Without loss of generality assume that $k_1 \geq k_2$. Let $\widetilde{F}(x, y) = p^{k_1-k_2}\ell_1 x^n + \ell_2 y^n$. Since $\gcd(n, p(p-1)) = 1$, every integer is an nth power residue modulo p. Therefore we can apply Theorem 3.2(2) to conclude that $R(\widetilde{F})$ is dense in $\mathbb{Q}_p$. At last, we see that

$$\frac{\widetilde{F}(x, y)}{\widetilde{F}(z, w)} = \frac{p^{k_2}\widetilde{F}(x, y)}{p^{k_2}\widetilde{F}(z, w)} = \frac{p^{k_1}\ell_1 x^n + p^{k_2}\ell_2 y^n}{p^{k_1}\ell_1 z^n + p^{k_2}\ell_2 w^n} = \frac{F(x, y)}{F(z, w)},$$

which means that $R(F) = R(\widetilde{F})$ is dense in $\mathbb{Q}_p$.

For the proof of (2), we use (1) to claim that $R(a_i x_i^n + a_j x_j^n)$ is dense in $\mathbb{Q}_p$. Since $R(a_i x_i^n + a_j x_j^n) \subset R(F)$, we see that $R(F)$ is dense in $\mathbb{Q}_p$. ■

The second part of the above corollary shows that if $\gcd(n, p(p-1)) = 1$ and F is an integral diagonal form of degree n depending essentially on at least $n+1$ variables, then $R(F)$ is dense in $\mathbb{Q}_p$. However, this result is not optimal in the sense that $n+1$ is not the least number r such that for every integral diagonal form F of degree n depending essentially on at least r variables the set $R(F)$ is dense in $\mathbb{Q}_p$. This is due to Corollary 3.2.1(1) and the result below.

Theorem 3.4. *Let $n \geq 3$ and p be a prime number such that $\gcd(n, p(p-1)) = 1$. Let $F(x, y) = a_1 x_1^n + a_2 x_2^n + \cdots + a_r x_r^n$ be integral and such that $r > \frac{n}{2}$, $a_1 a_2 \cdots a_r \neq 0$ and $\nu_p(a_i) \not\equiv \nu_p(a_j) \pmod{n}$ for any $1 \leq i < j \leq r$ (in particular $r \leq n$). Then $R(F)$ is dense in $\mathbb{Q}_p$.*

Proof. At first, recall that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and F and the operation of division are continuous in $\mathbb{Q}_p$. This implies that $R(F) = R(F(\mathbb{Z}^r))$ is dense in $R(F(\mathbb{Z}_p^r))$. Hence, it suffices to prove that $R(F(\mathbb{Z}_p^r)) = \mathbb{Q}_p$.

Since $\gcd(n, p-1) = 1$, every $c \in \mathbb{Z}_p^\times$ is an n-th power modulo p. In other words, the polynomial $f(x) = x^n - c$ has a root u modulo p. Then $u \in \mathbb{Z}_p^\times$. Since $\gcd(n, p) = 1$, we have $f'(u) = nu^{n-1} \not\equiv 0 \pmod{p}$ and by Hensel's lemma we conclude that f has a root in $\mathbb{Z}_p$, i.e. c is an n-th power in $\mathbb{Z}_p$. Since the set $\mathbb{Z}_p^\times$ is contained in the set of n-th powers in $\mathbb{Z}_p$, the set of n-th powers in $\mathbb{Z}_p$ is exactly the set of p-adic integers with p-adic valuation divisible by n.

Next, let $d \in \mathbb{Q}_p$ be arbitrary. We will show that $d = \frac{a_i}{a_j} p^{kn} u^n$ for some $i, j \in \{1, 2, \ldots, r\}$, $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Consider the sets

$$\{\nu_p(a_i) \pmod n) : i \in \{1, 2, \ldots, r\}\},$$
$$\{(\nu_p(d) + \nu_p(a_j)) \pmod n) : j \in \{1, 2, \ldots, r\}\}.$$

Both of them have cardinality $r > \frac{n}{2}$. Hence, they have non-empty intersection, i.e. $\nu_p(d) + \nu_p(a_j) \equiv \nu_p(a_i) \pmod n$ for some $i, j \in \{1, 2, \ldots, r\}$. Thus $n \mid \nu_p\left(d\frac{a_j}{a_i}\right)$, in other words $d\frac{a_j}{a_i} = p^{kn} c$ for some $k \in \mathbb{Z}$ and $c \in \mathbb{Z}_p^\times$. We already know that $c = u^n$ for some $u \in \mathbb{Z}_p^\times$. As a result, $d\frac{a_j}{a_i} = p^{kn} u^n$, or equivalently, $d = \frac{a_i}{a_j} p^{kn} u^n$. Finally, we can write

$$d = \begin{cases} \frac{a_i (p^k u)^n}{a_j}, & \text{if } k \geq 0, \\ \frac{a_i u^n}{a_j p^{-kn}}, & \text{if } k < 0. \end{cases}$$

This means that $d \in R(F(\mathbb{Z}_p^r))$.

We showed that $R(F(\mathbb{Z}_p^r)) = \mathbb{Q}_p$, which means that $R(F)$ is dense in $\mathbb{Q}_p$. ■

As a consequence of Corollary 3.2.1(2) and Theorem 3.4 we get the following.

Corollary 3.2.2. *Let $n \geq 3$ and p be a prime number such that* $\gcd(n, p(p-1)) = 1$. *The number $\lfloor \frac{n}{2} \rfloor + 1 = \lceil \frac{n+1}{2} \rceil$ is the least number r such that for every integral diagonal form F of degree n depending essentially on at least r variables the set $R(F)$ is dense in $\mathbb{Q}_p$.*

Proof. Corollary 3.2.1 and Theorem 3.4 show that if F is an integral diagonal form of degree n depending essentially on more than $\frac{n}{2}$ variables, then $R(F)$ is dense in

$\mathbb{Q}_p$. It suffices to find an integral diagonal form F_0 of degree n depending on $\lfloor \frac{n}{2} \rfloor$ variables such that $R(F_0)$ is not dense in $\mathbb{Q}_p$.

Consider

$$\begin{aligned}&F_0(x_1, x_2, x_3, \ldots, x_{\lfloor \frac{n}{2} \rfloor})\\&= x_1^n + px_2^n + p^2x_3^n + \cdots + p^{\lfloor \frac{n}{2} \rfloor - 1}x^n_{\lfloor \frac{n}{2} \rfloor}.\end{aligned}$$

Then, for each $x = \left(x_1, x_2, x_3, \ldots, x_{\lfloor \frac{n}{2} \rfloor}\right) \in \mathbb{Z}^{\lfloor \frac{n}{2} \rfloor}$ we have

$$\begin{aligned}\nu_p(F(x)) &= \min_{1 \le i \le \lfloor \frac{n}{2} \rfloor} \nu_p(p^{i-1}x_i^n)\\&= \min_{1 \le i \le \lfloor \frac{n}{2} \rfloor} (i - 1 + n\nu_p(x_i)) \in \left\{0, 1, 2, \ldots, \left\lfloor \frac{n}{2} \right\rfloor - 1\right\} \pmod n.\end{aligned}$$

Hence, $\nu_p\left(\frac{F(x)}{F(y)}\right) \not\equiv \lfloor \frac{n}{2} \rfloor \pmod n$ for any $x, y \in \mathbb{Z}^{\lfloor \frac{n}{2} \rfloor}$. By Lemma 1.12, $R(F_0)$ is not dense in $\mathbb{Q}_p$. ■

Remark 3.2.1. Note that there exists an integral diagonal form F of degree n depending on $\lfloor \frac{n}{2} \rfloor$ variables such that $R(F)$ is dense in $\mathbb{Q}_p$.

Consider

$$\begin{aligned}&F(x_1, x_2, x_3, \ldots, x_{\lfloor \frac{n}{2} \rfloor - 1}, x_{\lfloor \frac{n}{2} \rfloor})\\&= x_1^n + px_2^n + p^2x_3^n + \cdots + p^{\lfloor \frac{n}{2} \rfloor - 2}x^n_{\lfloor \frac{n}{2} \rfloor - 1} + p^{\lfloor \frac{n}{2} \rfloor}x^n_{\lfloor \frac{n}{2} \rfloor}.\end{aligned}$$

Then, for each $x = \left(x_1, x_2, x_3, \ldots, x_{\lfloor \frac{n}{2} \rfloor}\right) \in \mathbb{Z}^{\lfloor \frac{n}{2} \rfloor}$ we have

$$\nu_p(F(x)) \in \left\{0, 1, 2, \ldots, \left\lfloor \frac{n}{2} \right\rfloor - 2, \left\lfloor \frac{n}{2} \right\rfloor\right\} \pmod n.$$

Thus, every finite value can be attained as the p-adic valuation of $\left(\frac{F(x)}{F(y)}\right)$ *for some* $x, y \in \mathbb{Z}^{\lfloor \frac{n}{2} \rfloor}$. *Using similar reasoning to the one from the proof of Theorem 3.4, one* *can show that $R(F)$ is dense in $\mathbb{Q}_p$.*

3.3 Forms in two variables

We provide a sufficient condition for the denseness of $R(F)$ where F is any binary form of degree $d > 1$.

Theorem 3.5. *Let $F(x,y) = a_0x^d + a_1x^{d-1}y + \cdots + a_{d-1}xy^{d-1} + a_dy^d$ be an integral form of degree $d \geq 2$. Let p be a prime number such that $p \mid a_d$ and $p \nmid a_{d-1}$. Then $R(F)$ is dense in $\mathbb{Q}_p$.*

Proof. By the assumption, it follows that 0 is a simple root of the polynomial $F(x,1)$ modulo p. Therefore, by Hensel's lemma, $F(x,1)$ has a simple root in $\mathbb{Z}_p$. Hence, the statement follows by Theorem 1.11. ∎

3.3.1 Quartic form

Before stating the next theorem, we state a result due to Sun which gives the number of roots modulo a prime $p > 3$ for polynomials of degree 4. We use this theorem to find a sufficient condition for the denseness of ratio sets of quartic forms.

Theorem 3.6. [47, Theorem 5.3] *Let $p > 3$ be a prime, and $a, b, c \in \mathbb{Z}$.*

1. *If $a^2+12c \not\equiv 0 \pmod p$, then the congruence $x^4+ax^2+bx+c \equiv 0 \pmod p$ has one and only one solution if and only if $s_{p+1} \equiv a^2-4c \pmod p$, where $\{s_n\}$ is given by $s_0 = 3, s_1 = -2a, s_2 = 2a^2+8c, s_{n+3} = -2as_{n+2}+(4c-a^2)s_{n+1}+b^2s_n$ $(n = 0,1,2,\dots)$.*

2. *If $a^2+12c \equiv 0 \pmod p$, then the congruence $x^4+ax^2+bx+c \equiv 0 \pmod p$ has one and only one solution if and only if $p \equiv 1 \pmod 3$ and $8a^3+27b^2$ is a cubic non-residue $\pmod p$.*

Theorem 3.7. *Let $F(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be an integral binary quartic form with $a, b \neq 0$. Suppose that $p > 3$ is a prime with $\nu_p(b) > 0$. Then $R(F)$ is dense in $\mathbb{Q}_p$ if one of the following two conditions holds:*

1. *$p \equiv 1 \pmod 3$, $a^2c^2 + 12a^3e \equiv 0 \pmod p$, and $8a^3c^3 + 27a^4d^2$ is a cubic non-residue modulo p.*

2. *$a^2c^2 + 12a^3e \not\equiv 0 \pmod p$ and $s_{p+1} \equiv a^2c^2 - 4a^3e \pmod p$, where $\{s_n\}$ is given by $s_0 = 3, s_1 = -2ac, s_2 = 2a^2c^2 + 8a^3e$ and $s_{n+3} = -2acs_{n+2} + (4a^3e - a^2c^2)s_{n+1} + a^4d^2s_n$ for $n \geq 0$.*

Proof. We have $F(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ with $a, b \neq 0$ and $p|b$. Consider the polynomial

$$f(x) := \frac{F(x,a)}{a} = x^4 + bx^3 + acx^2 + a^2dx + a^3e.$$

Suppose that condition (1) of the theorem is true. Then, by Theorem 3.6,

$$f(x) \equiv x^4 + acx^2 + a^2dx + a^3e \equiv 0 \pmod p$$

has a simple root modulo p, i.e, there exists an $x_0 \in \mathbb{Z}$ such that

$$f(x_0) \equiv 0 \pmod p \quad \text{and} \quad f'(x_0) \not\equiv 0 \pmod p.$$

Therefore, by Hensel's lemma, f has a simple root in $\mathbb{Z}_p$. Hence, by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(f(\mathbb{N})) \subset R(F)$, $R(F)$ is dense in $\mathbb{Q}_p$.

Next, we assume that condition (2) of the theorem is true. Then again, by Theorem 3.6, f has a simple root modulo p. Therefore, by Hensel's lemma, f has a simple root in $\mathbb{Z}_p$. Hence, by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(f(\mathbb{N})) \subset R(F)$, $R(F)$ is dense in $\mathbb{Q}_p$. ■

For example, consider the form $F(x,y) = 5x^4 + x^3y + xy^3 + 19y^4$ in $\mathbb{Q}_{19}$. Here,

$a^2c^2 + 12a^3e \equiv 0 \pmod{p}$, $p \equiv 1 \pmod{3}$ and $8a^3c^3 + 27a^4d^2 \equiv 3 \pmod{19}$ is a cubic non-residue modulo 19. Therefore, $R(F)$ is dense in $\mathbb{Q}_{19}$.

Remark 3.3.1. *The converse of Theorem 3.7 is not true. For example, consider the binary quartic form $x^4 + 17x^3y + y^4$ in $\mathbb{Q}_{17}$. Using Hensel's lemma and Theorem 1.11, it can be seen that the ratio set of the quartic form is dense in $\mathbb{Q}_{17}$ since 2 is a simple root of the polynomial $x^4 + 17x^3 + 1$ modulo 17. However, $a^2c^2 + 12a^3e \not\equiv 0 \pmod{17}$, but $s_{18} \not\equiv a^2c^2 - 4a^3e \pmod{17}$.*

Remark 3.3.2. *In Theorem 3.7, if we remove the condition $a \neq 0$, it can be easily seen that $R(F)$ is dense in $\mathbb{Q}_p$ for any prime p. If $a = 0$, we consider the polynomial $f(y) := F(1, y) = y(b + cy + dy^2 + ey^3)$. Since $y = 0$ is a simple zero of f in $\mathbb{Z}_p$, by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(F) \supseteq R(f(\mathbb{N}))$, $R(F)$ is dense in $\mathbb{Q}_p$.*

3.4 Forms dense in infinitely many $\mathbb{Q}_p$

Before stating the next result, let us recall the definition of the discriminant of a polynomial over a field K. The discriminant of a polynomial $f(x) = a_nx^n + \cdots + a_0 \in K[x]$ is defined as

$$D(f) := a_n^{2n-2} \prod_{1 \le i < j \le n} (r_i - r_j)^2,$$

where $r_1, \ldots, r_n$ are the roots of f in the algebraically closed field containing K. The discriminant of an integral polynomial is always an integer. It can be observed that the discriminant of a polynomial over a field is zero if and only if the polynomial has repeated roots. The following theorem gives a sufficient condition for an integral form F to have a dense ratio set in $\mathbb{Q}_p$ for infinitely many primes p.

Theorem 3.8. *Let F be an integral form in n variables of degree greater than one. Suppose that there exist integers $a_1, a_2, \ldots, a_{n-1}$ for which the polynomial*

$F(x, a_1, a_2, \ldots, a_{n-1})$ in x has nonzero discriminant. Then $R(F)$ is dense in $\mathbb{Q}_p$ for infinitely many primes p.

Before proving the theorem, let us recall a theorem of Schur that guarantees the existence of infinitely many prime divisors for a polynomial. For a polynomial $f \in \mathbb{Z}[x]$, a prime number p is said to be a prime divisor of f if $p|f(n)$ for some $n \in \mathbb{Z}$. Let $P(f)$ be the set of all the prime divisors of f. Then the following theorem holds.

Theorem 3.9. [22, Theorem 1] *If $f(x) \in \mathbb{Z}[x]$ is non-constant, then $P(f)$ is infinite.*

Proof of Theorem 3.8. Suppose that the polynomial defined as

$$f(x) := F(x, a_1, a_2, \ldots, a_{n-1})$$

has nonzero discriminant $D(f)$. Consider primes p such that $p \nmid D(f)$. By Schur's theorem, there exists $n_p \in \mathbb{Z}$ such that $p|f(n_p)$ for infinitely many primes $p \nmid D(f)$ i.e, $f(n_p) \equiv 0 \pmod{p}$. Since $D \not\equiv 0 \pmod{p}$, f has distinct roots modulo p. Hence, $f'(n_p) \not\equiv 0 \pmod{p}$. Therefore, by Hensel's lemma, f has a simple root in $\mathbb{Z}_p$. Hence, by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(F) \supseteq R(f(\mathbb{N}))$, $R(F)$ is dense in $\mathbb{Q}_p$. This completes the proof as there are infinitely many such primes. ■

We discuss two examples as applications of Theorem 3.8. We have calculated discriminants of polynomials in the following examples with the help of Wolfram Alpha.

Example 3.4.1. *Consider the form $F(x, y, z) = x^5 + x^3yz + yz^4 + x^4z + xy^4 + y^5$. The polynomial $f(x) := F(x, 1, 0) = x^5 + x + 1$ has discriminant equal to $3381 = 3 \cdot 7^2 \cdot 23$. Also, $f(2) = 35 \equiv 0 \pmod{5}$ but $f'(2) \not\equiv 0 \pmod{5}$. Hence by Hensel's lemma, f has a simple root in $\mathbb{Z}_5$. Therefore, by Theorem 1.11, $R(F) \supseteq R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_5$. Moreover, Schur's theorem guarantees the existence of infinitely many such* *primes* $p \neq 3, 7, 23$ *for which* $R(F)$ *is dense in* $\mathbb{Q}_p$. *For example,* $f(3) = 247 = 13 \cdot 19$. *Hence,* $R(F)$ *is dense in* $\mathbb{Q}_{13}$ *and* $\mathbb{Q}_{19}$. *Similarly, it can be shown that* $R(F)$ *is dense in* $\mathbb{Q}_p$ *for* $p = 31, 43, 101, 181$ *etc.*

Example 3.4.2. *Consider the form* $F(x, y, z) = x^6+x^5y+x^4y^2+x^2y^4+y^6+x^2z^4+z^6$. *The discriminant of the polynomial* $f(z) := F(1, 0, z) = 1 + z^4 + z^6$ *is nonzero and it can be shown that* $R(F)$ *is dense in* $\mathbb{Q}_p$ *for* $p = 3, 607, 1451, 5417, 88747$ *etc.*

3.4.1 Quintic form

Now, we consider the particular case of a fifth degree form. We provide a result that gives the denseness of the ratio set of values assumed by certain quintic forms in $\mathbb{Q}_p$ for infinitely many primes p. Before stating the result, we state a theorem which gives existence of non-singular roots for quintic forms over finite fields. For a prime p, let $q = p^r, r \geq 1$. Let $\mathbb{F}_q$ denote the finite field with q elements.

Theorem 3.10. [27, Corollary 4.5] *Let* f *be a non-degenerate quintic form of order at least* 6 *over* $\mathbb{F}_q$. *If* $q > 101$, *then* f *has a non-singular* $\mathbb{F}_q$*-rational zero.*

The following theorem gives a sufficient condition for the denseness of ratio sets of quintic forms.

Theorem 3.11. *Let* p *be a prime. Let* F *be an integral non-degenerate quintic form of order at least* 6 *over the field* $\mathbb{F}_p$. *If* $p > 101$, *then* $R(F)$ *is dense in* $\mathbb{Q}_p$.

Proof. By Theorem 3.10, F has a non-singular root in $\mathbb{Z}/p\mathbb{Z}$ i.e,

$$F(a_1, a_2, \ldots, a_n) = 0, \frac{\partial F}{\partial x_j}(a_1, a_2, \ldots, a_n) \neq 0$$

for $a_i \in \mathbb{Z}/p\mathbb{Z}$, $1 \leq i \leq n$ and for some j satisfying $1 \leq j \leq n$. Consider the polynomial $f(x) := F(a_1, a_2, \ldots, x, \ldots, a_n)$ formed by replacing a_j by x. We have $f(a_j) \equiv 0 \pmod{p}$ and $f'(a_j) \not\equiv 0 \pmod{p}$. Therefore, by Hensel's lemma, there exists a simple root of f in $\mathbb{Z}_p$. Hence, by Theorem 1.11, $R(f(\mathbb{N}))$ is dense in $\mathbb{Q}_p$. Since $R(f(\mathbb{N})) \subset R(F)$, $R(F)$ is dense in $\mathbb{Q}_p$. ■

3.5 Forms dense in finitely many $\mathbb{Q}_p$

The previous results could make us think whether the existence of one p such that $R(F)$ is dense in $\mathbb{Q}_p$ must imply that $R(F)$ is dense in infinitely many different fields $\mathbb{Q}_q$. However, that is not the case. We construct forms defined over $\mathbb{Z}$ in any number of variables which prove that the answer to the previous question is no. To do so, first we obtain polynomials for which the ratio set is dense in (fixed) $\mathbb{Q}_p$, but they do not satisfy the conditions of [36, Theorem 1.2] and then using these polynomials we construct forms. Now, we state the result.

Theorem 3.12. *Let p be a prime number. Consider three prime numbers $q_1 < q_2 < q_3$ such that $q_1q_2q_3$ is coprime to $p(p-1)$. Define the polynomial*

$$f(x) = x^{q_1q_2}(x + p^{q_1+1})^{q_2q_3} \prod_{i=1}^{q_1} (x + p^i)^{q_1q_3}.$$

Then

1. *$R(f)$ is dense in $\mathbb{Q}_p$.*

2. *For almost all primes q, including those greater than p^{q_1+1}, $R(f)$ is not dense in $\mathbb{Q}_q$.*

Proof. (1) It is sufficient to prove that for any $u \in \mathbb{Z}_p$, there are $x, y \in \mathbb{Z}_p$ such that $\frac{f(x)}{f(y)} = u$. Let $u = p^{nq_1+s}v$, where $n, s \in \mathbb{Z}_{\geq 0}$ with $s < q_1$, and $p \nmid v$. There is exactly one $m \in \{1, \ldots, q_1\}$ such that $q_2q_3(1-m) \equiv s \pmod{q_1}$. We will find $x, y \in \mathbb{Z}_p$ in the shape $x = p^k x_1$ and $y = p^l y_1 - p^m$, where $k, l > q_1 + 1$ and $x_1, y_1 \in \mathbb{Z}_p^*$. For such

x and y, we have

$$\nu_p(f(x)) = kq_1q_2 + q_1q_3\frac{q_1(q_1+1)}{2} + (q_1+1)q_2q_3;$$
$$\nu_p(f(y)) = mq_1q_2 + q_1q_3(\frac{(m-1)m}{2} + l + m(q_1-m)) + mq_2q_3;$$
$$\frac{f(x)}{f(y)} = p^{\nu_p(f(x))-\nu_p(f(y))}\frac{x_1^{q_1q_2}(pf_1(x_1)+1)}{y_1^{q_1q_3}(pf_2(y_1)\pm 1)},$$

for some polynomials f_1, f_2 with coefficients in $\mathbb{Z}_p$, and for the unique choice of $+$ or $-$ in the denominator.

The choice of m implies that there are $k, l > q_1+1$ such that $\nu_p(f(x)) - \nu_p(f(y)) = nq_1 + s$ because we can divide by q_1 and obtain an equation $q_2k - q_3l = N$ for some $N \in \mathbb{Z}$. This equation has infinitely many solutions (and greater than q_1+1) because q_2 and q_3 are coprime. Now we need to prove that there are $x_1, y_1 \in \mathbb{Z}_p^*$ such that

$$\frac{x_1^{q_1q_2}(pf_1(x_1)+1)}{y_1^{q_1q_3}(pf_2(y_1)\pm 1)} = v. \tag{3.1}$$

This directly follows from Hensel's lemma after multiplying the denominator on both sides of the equation, fixing any $y_1 \in \mathbb{Z}_p^*$, and reducing the equation modulo p. We obtain an equation $x_1^{q_1q_2} \equiv \pm v y_1^{q_2q_3} \pmod p$, which has a simple solution because $x \mapsto x^{q_1q_2}$ is a bijective map $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$. We use that q_1q_2 is coprime to $(p-1)p$.

(2) Let q be a prime such that $q \nmid p^i - p$, for any $1 \leq i \leq q_1+1$. Then, for every $x \in \mathbb{Z}_q$, at most one of the following values is positive $\nu_q(x), \nu_q(x+p), \ldots, \nu_q(x+p^{q_1+1})$. Hence, for each $x \in \mathbb{Z}_q$, $\nu_q(f(x))$ is divisible by q_1q_2, or q_2q_3 or q_1q_3, so we cannot find $x, y \in \mathbb{Z}_q$ such that $\nu_q(f(x)/f(y)) = 1$, and $R(f)$ is not dense in $\mathbb{Q}_q$. In particular, this holds for all q greater than p^{q_1+1}. ■

Next, we present a multivariable version of the above theorem.

Theorem 3.13. *Let p be a prime number. Consider three prime numbers $q_1 < q_2 <$*

q_3 such that $q_1q_2q_3$ is coprime to $p(p-1)$. Define the form

$$g_2(x_1,x_2) = x_1^{q_1q_2}(x_1+p^{q_1+1}x_2)^{q_2q_3}\prod_{i=1}^{q_1}(x_1+p^ix_2)^{q_1q_3}\prod_{i=1}^{q_3-1}(p^ix_1+x_2)^{q_1q_2} \times \prod_{i=q_3}^{q_3+q_2-q_1-1}(p^ix_1+x_2)^{q_1q_3}\prod_{i=q_3+q_2-q_1}^{q_3+q_2-2}(p^ix_1+x_2)^{q_2q_3}.$$

Then

1. *$R(g_2)$ is dense in $\mathbb{Q}_p$.*

2. *For almost all primes q, including those greater than $p^{q_3+q_2+q_1-1}$, $R(g_2)$ is not dense in $\mathbb{Q}_q$.*

3. *Let $n>2$ and $g_n(x_1,\ldots,x_n) = g_2(x_1,x_2)(x_3\cdots x_n)^{q_1q_2q_3}$. Then, $R(g_n)$ is dense in $\mathbb{Q}_p$, but for almost all primes q, $R(g_n)$ is not dense in $\mathbb{Q}_q$.*

Proof. (1) We will prove that for any $u = p^{\nu_p(u)}v$, where $v\in\mathbb{Z}_p^*$, we can find $x_1,y_1\in\mathbb{Z}_p$ such that $\frac{g_2(x_1,1)}{g_2(y_1,1)} = u$. We note that $g_2(x_1,1) = f(x_1)(ph(x_1)+1)$, where f is from Theorem 3.12 and $h\in\mathbb{Z}_p[x]$ is some polynomial. Hence, $\nu_p(g_2(x_1,1)) = \nu_p(f(x_1))$ for all $x_1\in\mathbb{Z}_p$. Hence, we can use the same strategy as in Theorem 3.12 (i.e., look for $x_1,y_1\in\mathbb{Z}_p$ in the shape $x_1 = p^kx_2$ and $y_1 = p^ly_2-p^m$) to arrange that $\nu_p(\frac{g_2(x_1,1)}{g_2(y_1,1)}) = \nu_p(u)$. Then, after dividing by powers of p, we end up in the notation of (3.1) in

$$\frac{x_2^{q_1q_2}(pf_1(x_2)+1)(ph(p^kx_2)+1)}{y_2^{q_1q_3}(pf_2(y_2)\pm 1)(ph(p^ly_2-p^m)+1)} = v.$$

Now, as in Theorem 3.12, by Hensel's lemma, we can find such x_2 and y_2, and hence $R(g_2)$ is dense in $\mathbb{Q}_p$.

(2) First note that $g_2(x_1,x_2)$ has degree

$$q_1q_2+q_1^2q_3+q_2q_3+(q_3-1)q_1q_2+(q_2-q_1)q_1q_3+(q_1-1)q_2q_3 = 3q_1q_2q_3.$$

We will now prove that for q big enough, we cannot find $x_1, x_2, y_1, y_2 \in \mathbb{Z}_p$ such that

$$\nu_q\left(\frac{g_2(x_1,x_2)}{g_2(y_1,y_2)}\right) = 1.$$

More precisely, we will prove that at least one of q_1, q_2, or q_3 divides $\nu_q\left(\frac{g_2(x_1,x_2)}{g_2(y_1,y_2)}\right)$, and for that it suffices to prove that for any $x_1, x_2 \in \mathbb{Z}_p$, two of q_1, q_2, and q_3 divide $\nu_q(g_2(x_1,x_2))$, so we now focus on proving the latter statement.

We may assume that $q \nmid x_1$ or $q \nmid x_2$, because $g_2(qx_1, qx_2) = q^{3q_1q_2q_3} g_2(x_1, x_2)$.

If $\nu_q(g_2(x_1,x_2)) \neq 0$ (otherwise, the statement is true), then q divides at least one of the terms x_1, $x_1 + p^i x_2$ for $1 \leq i \leq q_1 + 1$, or $p^j x_1 + x_2$ for $1 \leq j \leq q_2 + q_3 - 2$. We now prove that q cannot divide more than one of these terms. If q divides at least two of them, then we distinguish between the cases. If $q \mid x_1$, then the second division implies that $q \mid p^i x_2$, for some i, hence $q \mid x_2$, which we assume it is not the case. If q divides two terms of the same shape, then $q \mid (p^i - p^j)x_k$, for $i, j < q_2 + q_3 - 1$, which again implies that q divides both x_1 and x_2. Similarly, if $q \mid x_1 + p^i x_2$ and $q \mid p^j x_1 + x_2$ for some $i \leq q_1 + 1$ and $j \leq q_2 + q_3 - 2$, but then $q \mid (p^{i+j} - 1)x_1$, which again implies that $q \mid x_1$ because $q > p^{q_1+q_2+q_3-1}$ and $q \mid x_2$. Thus, $R(g_2)$ is not dense in $\mathbb{Q}_q$.

(3) Since $g_n(x_1, x_2, 1, \ldots, 1) = g_2(x_1, x_2)$, by (1), $R(g_n)$ is dense in $\mathbb{Z}_p$. Also, since $\nu_q(g_n(x_1, \ldots, x_n)) \equiv \nu_q(g_2(x_1, x_2)) \pmod{q_1q_2q_3}$ for any prime number q, the same argument as in (2) shows that $R(g_n)$ is not dense for $q > p^{q_3+q_2+q_1-1}$. ■

3.6 More polynomials and forms not satisfying condition of Theorem 1.10

In this section we show that condition of Theorem 1.10 is not necessary for the denseness of ratio sets of values assumed by polynomials. First, we recall the definition of a difference set.

Definition 3.1. *Let q be a positive integer.*

1. *For a set $S \subseteq \mathbb{Z}/q\mathbb{Z}$, let $S - S := \{s_1 - s_2 \mid s_1, s_2 \in S\}$.*

2. *A subset $S \subseteq \mathbb{Z}/q\mathbb{Z}$ is called a difference set if the set $S - S = \mathbb{Z}/q\mathbb{Z}$.*

We present a theorem that generates polynomials with dense ratio sets, where the roots of each polynomial have equal multiplicities.

Theorem 3.14. *Let q be a positive integer greater than 1 and let $S = \{0, s_1, \dots, s_k\}$ (and write $s_0 = 0$) be a difference set for $\mathbb{Z}/q\mathbb{Z}$. Define the polynomial f with $2k+1$ distinct factors:*

$$f = x^q(x-1)^q \cdots (x-k)^q((x-1)^q + p^{s_1}) \cdots ((x-k)^q + p^{s_k}).$$

Then $R(f)$ is dense in $\mathbb{Q}_p$ for primes p satisfying $\gcd(q, p(p-1)) = 1$.

Proof. We first prove that for any non-negative integer r, we can find $x, y \in \mathbb{Z}_p$ such that $\nu_p(f(x)/f(y)) = r$. For $g \in \mathbb{Z}_p[x]$, we use the notation $\widetilde{g} = g \pmod p$ to denote the reduction modulo p. Also, $x^* = x/p^{\nu_p(x)}$ denotes the coprime to p part of x.

Write $r = r_0 q + r_1$, such that $0 \le r_0, r_1$ and $r_1 < q$. There are $s_i, s_j \in S$ such that $s_i - s_j \equiv r_1 \pmod q$. Let us consider $x = p^a x_1 + i$ with $x_1 \in \mathbb{Z}_p^*$ and $y = p + j$, where $a = r_0 + 1$ if $s_i \ge s_j$ or $a = r_0 + 2$ otherwise. Then,

$$\frac{f(x)}{f(y)} = p^r \left(\frac{f(x)}{f(y)}\right)^*, \quad \text{and} \quad \widetilde{\left(\frac{f(x)}{f(y)}\right)^*} = x_1^q C,$$

where $C \in \mathbb{Z}_p^*$ is some number independent of x_1, a and b. So, if $u = p^r v$, with $v \in \mathbb{Z}_p^*$, we can solve $\left(\frac{f(x)}{f(y)}\right)^* = v$ by Hensel's lemma since there is a unique solution modulo p of $x_1^q \equiv C^{-1} v \pmod p$ (recall that $\gcd(q, p-1) = 1$, so $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$, $x \mapsto x^q$ is a bijection). This proves that $R(f)$ is dense in $\mathbb{Q}_p$. ∎

We now demonstrate the existence of polynomials of degrees 5 and higher than 6 that do not satisfy the condition in Theorem 1.10, yet have a dense ratio set in all $\mathbb{Q}_p$.

Theorem 3.15. *Let $d = 5$ or $d \geq 7$. There is a monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree $\deg(f) = d$ with only one root of multiplicity greater than 1 such that $R(f)$ is dense in $\mathbb{Q}_p$ for all primes p.*

Proof. Consider $f(x) = x^{d_1}((x+1)^{d_2}+p^{d_1 d_2+1})$ where $d_1, d_2 > 1$ such that $d_1+d_2 = d$ and $\gcd(d_1, d_2) = 1$. We prove that $R(f)$ is dense in $\mathbb{Q}_p$. First, we note that $(x+1)^{d_2} + p^{d_1 d_2+1}$ is irreducible, which we can read of its Newton polygon.

Consider any $p^{d_1 k+l}u \in \mathbb{Z}_p$ for $0 \leq l < d_1$. There is $0 < m \leq d_1$ such that $d_2 m \equiv -l \pmod{d_1}$. Consider $y = p^m y_1 - 1$, where $y_1 \in \mathbb{Z}_p^*$. Then $\nu_p(f(y)) = d_2 m = d_1 n - l$, for some $n \in \mathbb{N}$. Then, take $x = p^{k+n}x_1$ with $x_1 \in \mathbb{Z}_p^*$. We compute $\nu_p(f(x)/f(y)) = d_1 k + l$. Then, by Hensel's lemma, we can find $x_1, y_1 \in \mathbb{Z}_p^*$ such that

$$\frac{x_1^{d_1}((px_1+1)^{d_2}+p^{d_1 d_2+1})}{(p^m y_1 - 1)^{d_1}(y_1^{d_2}+p^{(d_1-m)d_2+1})} = u,$$

because we can get any nonzero residue v mod p as $x_1^{d_1}/y_1^{d_2}$ mod p, as there are $a, b \in \mathbb{N}$ such that $d_1 a - d_2 b = 1$, so just take $x_1 = u^a$ and $y_1 = u^b$ mod p. ∎

We state an analogous result for binary forms.

Theorem 3.16. *We have:*

1. *Let $p \equiv 3 \pmod 8$. Then*

$$F(x, y) = (x^2 + p^4 y^2)((x-y)^2 + py^2) \in \mathbb{Z}_p[x, y]$$

is a binary form of degree 4 such that $R(F)$ is dense in $\mathbb{Q}_p$ and F has no linear factors over $\mathbb{Q}_p$.

2. *Let* $p \equiv 11 \pmod{24}$. *Then*

$$F(x,y) = (x^2 + p^6 y^2)((x+y)^2 + p^3 y^2)((x-y)^2 + py^2) \in \mathbb{Z}_p[x,y]$$

is a binary form of degree 6 *such that* $R(F)$ *is dense in* $\mathbb{Q}_p$ *and* F *has no linear factors over* $\mathbb{Q}_p$.

3. *Let* p *be a prime number and* $d = 5$ *or* $d \geq 7$. *Let* $f \in \mathbb{Z}_p[x]$ *be the polynomial from Theorem 3.15 for the chosen* d. *Then* $F(x,y) = y^d f(\frac{x}{y}) \in \mathbb{Z}_p[x,y]$ *is a binary form of degree* d *such that* $R(F)$ *is dense in* $\mathbb{Q}_p$ *and* F *has no simple linear factors over* $\mathbb{Q}_p$.

Proof. Firstly, we prove part (1) of the theorem. We assume $p \equiv 3 \pmod 8$, so that -1 and 2 are not quadratic residues modulo p. Furthermore, in this case, $y \mapsto y^4 \colon \mathbb{F}_p^* \to \mathbb{F}_p^*$ has the same image as $y \mapsto y^2 \colon \mathbb{F}_p^* \to \mathbb{F}_p^*$, i.e., all squares in $\mathbb{F}_p^*$.

We find it easier to use $z = \frac{x}{y}$, so that $F(y,z) = y^4(z^2 + p^4)((z-1)^2 + p)$. For each $r \in \mathbb{Z}_p$, we want to find $y_1, y_2, z_1, z_2 \in \mathbb{Z}_p$ such that $\frac{F(y_1,z_1)}{F(y_2,z_2)} = r$. All elements of $\mathbb{Z}_p$ are of the shape $p^{4k+i} a u^2$, where $k \in \mathbb{Z}_{\geq 0}$, $i \in \{0,1,2,3\}$, $a \in \{1,2\}$, and $u \in \mathbb{Z}_p^*$. We do two cases in more detail, and the others are analogous.

Consider first $r = p^{4k} u^2$, for some $k \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}_p^*$. Then, let $y_1 = p^k y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = -1$, $y_2 = 1$, $z_2 = -1$. Then

$$p^{4k} u^2 = \frac{F(y_1, -1)}{F(1, -1)} = p^{4k} {y_1'}^4,$$

and we need to solve ${y_1'}^4 = u^2$, and this has a solution in $\mathbb{Z}_p^*$ by Hensel's lemma.

Now, consider $r = 2p^{4k} u^2$, for some $k \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}_p^*$. Let $y_1 = p^k y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p^2$, $y_2 = p$, $z_2 = -1$. Then

$$2p^{4k} u^2 = \frac{F(y_1, p^2)}{F(p, -1)} = 2p^{4k} {y_1'}^4 \frac{(p^2-1)^2 + p}{(1+p^4)(4+p)}.$$

After dividing by p^{4k}, we can solve ${y_1'}^4 \equiv 4u^2 \pmod{p}$, so, by Hensel's lemma, we can find the required y_1'.

Similarly, we prove that in the following cases, we can use

- $r = p^{4k+1}u^2$: $y_1 = p^k y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = 1$, $y_2 = 1$, $z_2 = -1$;
- $r = 2p^{4k+1}u^2$: $y_1 = p^{k+1} y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = 1$, $y_2 = 1$, $z_2 = p^2$;
- $r = p^{4k+2}u^2$: $y_1 = p^{k+1} y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = -1$, $y_2 = 1$, $z_2 = p$;
- $r = 2p^{4k+2}u^2$: $y_1 = p^k y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p^2$, $y_2 = 1$, $z_2 = p$;
- $r = p^{4k+3}u^2$: $y_1 = p^{k+1} y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = -1$, $y_2 = 1$, $z_2 = 1$;
- $r = 2p^{4k+3}u^2$: $y_1 = p^k y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p^2$, $y_2 = 1$, $z_2 = 1$.

Now we prove part (2) similarly to part (1). We assume $p \equiv 11 \pmod{24}$, so that -1 and 2 are not quadratic residues modulo p and that $y \mapsto y^6 \colon \mathbb{F}_p^* \to \mathbb{F}_p^*$ has the same image as $y \mapsto y^2 \colon \mathbb{F}_p^* \to \mathbb{F}_p^*$, i.e., all squares in $\mathbb{F}_p^*$. Again, we find it easier to use $z = \frac{x}{y}$, so that $F(y, z) = y^6(z^2 + p^6)((z+1)^2 + p^3)((z-1)^2 + p)$.

For each possibility $r = p^{6k+i}au^2 \in \mathbb{Z}_p$, where $k \in \mathbb{Z}_{\geq 0}$, $0 \leq i \leq 5$, $a \in \{1, 2\}$, $u \in \mathbb{Z}_p^*$, we can find corresponding $y_1, y_2, z_1, z_2 \in \mathbb{Z}_p$ such that $\frac{F(y_1,z_1)}{F(y_2,z_2)} = r$ has a solution, again, by specifying z_1, y_2, z_2 and $\nu_p(y_1)$, and then solving for y_1^* using Hensel's lemma.

- $r = p^{6k}u^2$: $y_1 = p^k y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = 1$, $y_2 = 1$, $z_2 = 1$;
- $r = p^{6k+1}u^2$: $y_1 = p^k y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p$, $y_2 = 1$, $z_2 = 1$;
- $r = p^{6k+2}u^2$: $y_1 = p^k y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = -1$, $y_2 = 1$, $z_2 = 1$;
- $r = p^{6k+3}u^2$: $y_1 = p^k y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p^2$, $y_2 = 1$, $z_2 = 1$;

- $r = p^{6k+4}u^2$: $y_1 = p^{k+1}y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p$, $y_2 = 1$, $z_2 = p^2$;
- $r = p^{6k+5}u^2$: $y_1 = p^{k+1}y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = -1$, $y_2 = 1$, $z_2 = p^2$;
- $r = 2p^{6k}u^2$: $y_1 = p^{k}y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p^3$, $y_2 = p$, $z_2 = p-2$;
- $r = 2p^{6k+1}u^2$: $y_1 = p^{k+1}y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = 1$, $y_2 = 1$, $z_2 = p^3$;
- $r = 2p^{6k+2}u^2$: $y_1 = p^{k}y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p^3$, $y_2 = 1$, $z_2 = p^2$;
- $r = 2p^{6k+3}u^2$: $y_1 = p^{k}y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p^3$, $y_2 = 1$, $z_2 = -1$;
- $r = 2p^{6k+4}u^2$: $y_1 = p^{k}y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p^3$, $y_2 = 1$, $z_2 = p$;
- $r = 2p^{6k+5}u^2$: $y_1 = p^{k}y_1'$, for $y_1' \in \mathbb{Z}_p^*$, $z_1 = p^3$, $y_2 = 1$, $z_2 = 1$;

The proof of (3) is immediate as we have that $R(f)$ is dense in $\mathbb{Q}_p$, then $R(F)$ is dense too, as $R(F(x,1))$ is dense. ∎

3.7 Polynomials with factors having degree divisible by $q > 1$

In this section, we examine specific types of polynomials and describe their image. Even though we have in mind a concrete application to the denseness result, the result is exciting on its own. We first introduce the notation that will be used in this section. Let $g \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree $\deg(g) = d > 1$. We will use the following notation:

$\tilde{g} = g \pmod p$ denotes the reduction modulo p;

$x^* = x/p^{\nu_p(x)}$ denotes the coprime to p part of x.

Assume that $\tilde{g}$ has a root in $\mathbb{F}_p$. Since g is irreducible, Hensel's lemma for polynomials implies that $\tilde{g}$ is a dth power of a linear polynomial because it cannot have coprime factors in $\mathbb{F}_p[x]$. We can assume that g is monic because p does not divide its leading coefficient (otherwise, $\tilde{g} = 1$, which contradicts the assumption that $\tilde{g}$ has a zero in $\mathbb{F}_p$). Furthermore, we can assume (by applying a linear change of variables if necessary) that $\tilde{g} = x^d$. Thus,

$$g(x) = x^d + p^{k_{d-1}} a_{d-1} x^{d-1} + \cdots + p^{k_1} a_1 x + p^{k_0} a_0,$$

where $k_0, \ldots, k_{d-1} \in \mathbb{Z}_{>0} \cup \{+\infty\}$, $a_0, \ldots, a_{d-1} \in \mathbb{Z}_p^*$. We allow $k_i = +\infty$ for $0 < i < d$ if the coefficient of x^i is 0, but note that $k_0 < +\infty$.

Now, we are ready to define the quantity $\tau(g)$.

Definition 3.2. *Let $g \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree* $\deg(g) = d$.

- *If $\tilde{g}$ does not have a zero in $\mathbb{F}_p$, define $\tau(g) := 0$.*
- *If $\tilde{g}$ has a root in $\mathbb{F}_p$, assuming the notation from above, define $\tau(g) := \frac{k_0}{d}$.*

We want to use the quantity $\tau(g)$ to study $\nu_p(g(x))$ for $x \in \mathbb{Z}_p$. Irreducibility of g implies that all of its roots have the same valuation at p, so the Newton polygon of g is a straight line connecting $(0, k_0)$ and $(d, 0)$. We also denote $a_d = 1$, $k_d = 0$. Then, for each $0 \leq i \leq d$, we have

$$k_i \geq \left\lceil \frac{d-i}{d} k_0 \right\rceil = \lceil (d-i)\tau(g) \rceil, \tag{3.2}$$

where $\lceil x \rceil$ denotes the smallest $y \in \mathbb{Z}$ such that $y \geq x$.

If $p \nmid x$, then $\nu_p(g(x)) = 0$, so consider $p \mid x$.

If $\nu_p(x) < \tau(g)$, then for all $0 \leq i < d$, we have

$$k_i \geq \lceil (d-i)\tau(g) \rceil \geq (d-i)\tau(g) > (d-i)\nu_p(x) \implies k_i + \nu_p(x) i > d\nu_p(x).$$

Hence, $\nu_p(x^d) < \nu_p(p^{k_i} a_i x^i)$, so $\nu_p(g(x)) = d\nu_p(x)$.

If $\nu_p(x) > \tau(g)$, then for all $0 < i \leq d$, we have

$$k_i + \nu_p(x)i > \lceil (d-i)\tau(g) \rceil + i\tau(g) \geq d\tau(g) = k_0.$$

Then $\nu_p(a_0) < \nu_p(p^{k_i} a_i x^i)$, so $\nu_p(g(x)) = k_0$.

Thus, if $\tau(g) \notin \mathbb{Z}_{>0}$, we have completely described $\nu_p(g(x))$.

It remains to consider the case when $\tau(g) \in \mathbb{Z}_{>0}$ and $\nu_p(x) = \tau(g)$. Denote

$$g_1(x) := x^d + p^{k_{d-1}+(d-1)\tau(g)-k_0} a_{d-1} x^{d-1} + \cdots + p^{k_1+\tau(g)-k_0} a_1 x + a_0.$$

Inequality (3.2) implies that $g_1 \in \mathbb{Z}_p[x]$. Let $x = p^{\tau(g)} x_1$, then

$$g(x) = p^{d\tau(g)} g_1(x_1).$$

Since we used a linear change of variables, g_1 is also irreducible in $\mathbb{Z}_p[x]$. It is now sufficient to consider $g_1 \in \mathbb{Z}_p[x]$ and $x_1 \in \mathbb{Z}_p$, so we can repeat the whole process.

Since this transformation plays an important role for us, we give it a name T.

Definition 3.3. *We denote the above transformation by* $T\colon \mathbb{Z}_p[x] \longrightarrow \mathbb{Z}_p[x]$, $T(g) = g_1$.

The valuations of the discriminants of g and $g_1 = T(g)$ are related by

$$\nu_p(D(T(g))) = \nu_p(D(g)) - d(d-1)\tau(g),$$

because if $\alpha_1, \ldots, \alpha_d$ are roots of $T(g)$, then $p^{\tau(g)}\alpha_1, \ldots, p^{\tau(g)}\alpha_d$ are roots of g. Note that since g is irreducible, we have $D(g) \neq 0$ as $\mathbb{Q}_p$ has characteristic zero, so we can apply the transformation T only finitely many times.

Now, we are ready to introduce the last important notion for this section.

Definition 3.4. *Let* $g \in \mathbb{Z}_p[x]$ *be an irreducible polynomial of degree* d.

- *If* $\tau(g) = 0$*, we call* g *of type 2.*
- *If* $\tau(g) \notin \mathbb{Z}_{\geq 0}$*, we call* g *of type 1.*
- *If* $\tau(g) \in \mathbb{Z}_{>0}$*, we can apply the transformation* $g_1 = T(g) \in \mathbb{Z}_p[x]$ *from Definition 3.3. We define recursively the type of* g *to be the type of* g_1*.*

As we will see soon, the quantity $\tau(g)$ is useful to study $\nu_p(g(x))$. For better understanding, we give some examples:

Example 3.7.1.

- *For the polynomial* $g_1(x) = x^2 + p$*, we have* $\tau(g_1) = \frac{1}{2}$*, so* g_1 *is of type 1. For* $g_2(x) = (x-1)^3 + p^2(x-1)^2 + p^4$*, after a linear change of variables, we can consider* $h_2(x) = x^3 + p^2x^2 + p^4$*, and we have* $\tau(h_2) = \frac{4}{3}$ *and* g_2 *is of type 1. Also, let* $g_3(x) = x^2 + 2px + p^2(p+1)$*. Then,* $\tau(g_3) = 1$*, so, we can apply the* T *transformation (in this case, replace* x *by* px *and divide by* p^2*). Then* $h_3 = T(g_3)$*, for* $h_3(x) = x^2 + 2x + p + 1 = (x+1)^2 + p$*, and after a linear change of variables, we consider* $g_1(x) = x^2 + p$*, so we conclude that* g_3 *is of type 1.*
- *Let* $p \equiv 3 \pmod 4$*. Let* $g_4(x) = x^2 + 1$*. Since* g_4 *does not vanish modulo* p*, it is of type 2. Let* $g_5(x) = x^2 - 2px + 5p^2$*, then* $\tau(g_5) = 1$*. After applying* T*, we get* $h_5 = T(g_5)$*, for* $h_5 = x^2 - 2x + 5 = (x-1)^2 + 4$*. As* h_5 *does not vanish modulo* p*,* g_5 *is also of type 2.*

Let q be a positive integer. From now on, we will study the polynomials $f(x) = g_1(x) \cdots g_s(x)$ such that all $g_i \in \mathbb{Z}_p[x]$ are irreducible polynomials of degree $\deg(g_i) := d_i = m_i q$ for some $m_i \in \mathbb{Z}_{>0}$, for all $1 \leq i \leq s$. Our goal is to prove that their number limits the possible values of $\nu_p(f(x)) \pmod q \in \mathbb{Z}/q\mathbb{Z}$ and $\widetilde{f(x)}^* \in \mathbb{F}_p^*/\mathbb{F}_p^{*q}$. The result is as follows.

Theorem 3.17. *Let p be a prime number, $q > 1$ a positive integer, and $k \in \mathbb{Z}_{>0}$. Let $g_1, \ldots, g_k \in \mathbb{Z}_p[x]$ be monic of type 1, whose degrees $\deg(g_i) = d_i$ are divisible by q. Denote $f(x) = g_1(x) \cdots g_k(x) \in \mathbb{Z}_p[x]$. Then*

$$\{[(\nu_p(f(x)), f(x)^*)] \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q} \,:\, x \in \mathbb{Z}_p\}$$

can take at most $k+1$ values, including $(0,1)$.

Proof. We prove the theorem by induction.

Base case $k = 1$. Let $g = g_1$ and $d = d_1$. Assume that

$$g(x) = x^d + p^{k_{d-1}} a_{d-1} x^{d-1} + \cdots + p^{k_1} a_1 x + p^{k_0} a_0,$$

where $a_0, \ldots, a_{d-1} \in \mathbb{Z}_p^*$, $k_0, \ldots, k_{d-1} > 0$ (possibly $+\infty$ except from k_0).

If $p \nmid x$, then $[(\nu_p(g(x)), g(x)^*)] = (0,1) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$.

Otherwise, let $x = p^{\nu_p(x)} x_1$, where $x_1 \in \mathbb{Z}_p^*$. If $0 < \nu_p(x) < \tau(g) = \frac{k_0}{d}$, then

$$g(x) = p^{d\nu_p(x)}(x_1^d + px_2)$$

for some $x_2 \in \mathbb{Z}_p$, so $[(\nu_p(g(x)), g(x)^*)] = (0,1)$.

If $\nu_p(x) > \tau(g)$, then

$$g(x) = p^{k_0}(a_0 + px_2)$$

for some $x_2 \in \mathbb{Z}_p$, so $[(\nu_p(g(x)), g(x)^*)] = (k_0, a_0)$. Therefore, if $\tau(g) \notin \mathbb{Z}_{>0}$, then the proof is finished.

If $\tau(g) \in \mathbb{Z}_{>0}$, we can make a T transformation $g \mapsto T(g) \in \mathbb{Z}_p[x]$ so that $p^{k_0} T(g)(x) = g(p^{\tau(g)} x)$. Since g is of type 1, $T(g)$ vanishes modulo p. Hence, as $T(g)$ is irreducible in $\mathbb{Z}_p[x]$, we have $T(g) \equiv (x-a)^d \pmod{p}$, for some $a \in \mathbb{Z}_p^*$. This implies that $a_0 \equiv a^d \pmod{p}$. Since $q \mid d \mid k_0$, we have $(k_0, a_0) = (0,1) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$, so for any x such that $\nu_p(x) \neq \tau(g)$, we have $[(\nu_p(g(x)), g(x)^*)] = (0,1)$.

As $\nu_p(g(p^{\tau(g)}x)) \equiv \nu_p(T(g)(x))$ modulo q and $g(p^{\tau(g)}x)^* = T(g)(x)^*$, we can focus entirely on $T(g)$ and repeat the process. The process of applying transformations T eventually stops (when $\tau(T \circ \cdots \circ T(g)) \notin \mathbb{Z}_{>0}$), and for this polynomial, we already have proven the statement.

Induction step. Assume that the statement is true for all numbers up to k, and we prove that it is true for $k+1$.

Let $g_1 \equiv (x-\sigma_1)^{d_1} \pmod{p}, \ldots, g_k \equiv (x-\sigma_k)^{d_k} \pmod{p}$ be the polynomials of type 1 and $\sigma_1 \leq \ldots \leq \sigma_k \in \{0, \ldots, p-1\}$. If $\sigma_1 \neq \sigma_k$, then we split the polynomials g_i into two groups: $g_1, \ldots, g_s$ whose zero modulo p is σ_1 and the remaining $g_{s+1}, \ldots, g_k$ whose zeros modulo p are different from σ_1; note that $s < k$.

If $x \equiv \sigma_1 \pmod{p}$, then we have

$$[(\nu_p(g_{s+1}(x)\cdots g_k(x)), (g_{s+1}(x)\cdots g_k(x))^*)] = (0,1) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q},$$

and by applying the inductive hypothesis to $g_1 \cdots g_s$, we have that

$$[(\nu_p(g_1(x)\cdots g_s(x)\cdot g_{s+1}(x)\cdots g_k(x)), (g_1(x)\cdots g_s(x)\cdot g_{s+1}(x)\cdots g_k(x))^*)]$$

can take at most $s+1$ pairs in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$, including $(0,1)$.

Similarly, when $x \not\equiv \sigma_1 \pmod{p}$, then

$$[(\nu_p(g_1(x)\cdots g_s(x)), (g_1(x)\cdots g_s(x))^*)] = (0,1),$$

and by applying the inductive hypothesis to $g_{s+1}\cdots g_k$, we have that

$$[(\nu_p(g_1(x)\cdots g_s(x)\cdot g_{s+1}(x)\cdots g_k(x)), (g_1(x)\cdots g_s(x)\cdot g_{s+1}(x)\cdots g_k(x))^*)]$$

can take at most $(k-s)+1$ pairs in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$, including $(0,1)$.

Thus, in total, there are at most $s + 1 + (k - s) + 1 - 1 = k + 1$ possible pairs in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$, including $(0, 1)$, which appears in both cases, so it is the reason why we could subtract 1 in the estimate.

It remains to consider the case $\sigma := \sigma_1 = \cdots = \sigma_k$. Now reorder the polynomials such that $\tau(g_1) \leq \cdots \leq \tau(g_k)$. First, suppose that $\tau(g_1) < \tau(g_k)$, and similarly, split the polynomials g_i into two groups, where the τ value is the same for the first s of them: $\tau(g_1) = \ldots = \tau(g_s) < \tau(g_{s+1}) \leq \ldots \leq \tau(g_k)$.

It suffices to consider $x \equiv \sigma \pmod{p}$ and $\nu_p(x) \geq \tau(g_1)$ (otherwise, all other x lead to the pair $(0, 1) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$). If $\nu_p(x) = \tau(g_1)$, then

$$[(\nu_p(g_{s+1}(x) \cdots g_k(x)), (g_{s+1}(x) \cdots g_k(x))^*)] = (0, 1) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q},$$

and by the inductive hypothesis, we have that

$$[(\nu_p(g_1(x) \cdots g_s(x) \cdot g_{s+1}(x) \cdots g_k(x)), (g_1(x) \cdots g_s(x) \cdot g_{s+1}(x) \cdots g_k(x))^*)]$$

can take at most $s + 1$ pairs in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$, including $(0, 1)$.

On the other hand, if $\nu_p(x) > \tau(g_1)$, then

$$[(\nu_p(g_1(x) \cdots g_s(x)), (g_1(x) \cdots g_s(x))^*)]$$

has a constant value in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$, and that pair belongs to the set of potential pairs from the previous case. We apply the inductive hypothesis to conclude that

$$[(\nu_p(g_{s+1}(x) \cdots g_k(x)), (g_{s+1}(x) \cdots g_k(x))^*)]$$

can take at most $k - s + 1$ pairs in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$, including $(0, 1)$.

Therefore, in total

$$[(\nu_p(g_1(x) \cdots g_s(x) \cdot g_{s+1}(x) \cdots g_k(x)), (g_1(x) \cdots g_s(x) \cdot g_{s+1}(x) \cdots g_k(x))^*)]$$

can again take at most $s+1+k-s+1-1 = k+1$ pairs in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$, including $(0,1)$, and we subtract 1 because the latter two sets have at least one pair in the intersection. Note that if $\tau(g_1) \notin \mathbb{Z}_{>0}$, then we only need to consider the second case, and we can apply the inductive hypothesis directly to $g_{s+1} \cdots g_k$. Hence, this completes the proof in this case as well.

The only remaining case is when $\tau := \tau(g_1) = \cdots = \tau(g_k)$. If $\tau(g_1) \notin \mathbb{Z}_{\geq 0}$, then we already know that $[(\nu_p(g_1(x) \cdots g_k(x)), (g_1(x) \cdots g_k(x))^*)]$ can take at most two pairs in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$. This follows as the only possible pair different than $(0,1)$ can appear for $\nu_p(x) > \tau$, but then for each i, $[(\nu_p(g_i(x)), g_i(x)^*)]$ is constant in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$.

If $\tau \in \mathbb{Z}_{>0}$, we apply a T transformation to all polynomials g_i, and proceed the proof with $T(g_1), \ldots, T(g_k) \in \mathbb{Z}_p[x]$ instead (as we already know that all x such that $\nu_p(x) \neq \tau$ lead to the pair $(0,1)$ in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*q}$). Since we can only apply finitely many transformations T, this process eventually stops, and then we end up in some case for which we have already proven the statement, which finishes the proof of this case. ■

Theorem 3.18. *Let p be a prime number, and $q, s \in \mathbb{Z}_{>0}$. Let $g_1, \ldots, g_s \in \mathbb{Z}_p[x]$ be irreducible polynomials of degree $\deg(g_i) := d_i = m_i q$ for some $m_i \in \mathbb{Z}_{>0}$, for all $1 \leq i \leq s$. Then*

$$\{\nu_p(g_1(x) \cdots g_s(x)) : x \in \mathbb{Z}_p\} \pmod{q}$$

can take at most $s+1$ values, including 0.

Proof. The proof readily follows using Theorem 3.17 and the fact that for polynomials g of type 2, we have $\nu_p(g(x)) \equiv 0 \pmod{q}$ for all $x \in \mathbb{Z}_p$. ■

3.8 Sufficient condition such that $R(f)$ is not dense in $\mathbb{Q}_p$

In this section, we present some criteria when $R(f)$ is not dense in $\mathbb{Q}_p$. First, we start with a useful lemma, which will be used in the proof.

Lemma 3.19. *Let $z \in \mathbb{Z}_p$ and $g \in \mathbb{Z}_p[x]$ such that $g(z) \neq 0$. Then, there is a neighbourhood U of z such that $\nu_p(g(x))$ and $g(x)^* \pmod p$ are constant for $x \in U$ and equal $\nu_p(g(z))$ and $g(z)^* \pmod p$, respectively.*

Proof. Using Taylor's expansion $g(z+\varepsilon) = g(z) + \varepsilon g'(z) + \cdots$, or simply noting that $g(z+\varepsilon) = g(z) + \varepsilon h(z,\varepsilon)$, for some $h \in \mathbb{Z}_p[z,\varepsilon]$, it suffices to take ε such that $\nu_p(\varepsilon) > \nu_p(g(z))$, and then

$$g(z+\varepsilon) = p^{\nu_p(g(z))}(g(z)^* + p^{\nu_p(\varepsilon)-\nu_p(g(z))}h(z,\varepsilon)),$$

which directly implies the statement. ∎

We are ready to give our criterion about when $R(f)$ is not dense in $\mathbb{Q}_p$.

Theorem 3.20. *Let p be a prime number, and $q \in \mathbb{Z}_{>1}$. Let $k, l \in \mathbb{Z}_{>0}$, $e_1, \ldots, e_l \in \mathbb{Z}_{>0}$, and $a_1, \ldots, a_l \in \mathbb{Z}_p$. Further, let $h_1, h_2 \in \mathbb{Z}_p[x]$ be such that h_1 has no zeros in $\mathbb{Z}_p$, and $\tilde{h_2}$ has no zeros in $\mathbb{F}_p$. Finally, let $g_1, \ldots, g_k \in \mathbb{Z}_p[x]$ be irreducible polynomials such that $d_i := \deg(g_i) = qm_i$ for each $1 \leq i \leq k$ and some $m_i \in \mathbb{Z}_{>0}$. Define*

$$f(x) = ((x-a_1)^{e_1} \cdots (x-a_l)^{e_l} \cdot h_1(x))^q \cdot g_1(x) \cdots g_k(x) \cdot h_2(x). \tag{3.3}$$

If $1 + kl < q$, then $R(f)$ is not dense in $\mathbb{Q}_p$.

Proof. We will prove that there is $r \in \mathbb{Z}_p$ such that $\nu_p(r) \notin \{\nu_p(f(x)/f(y)) \colon x, y \in \mathbb{Z}_p\}$. Denote

$$G(x) := g_1(x) \cdots g_k(x) \cdot h_2(x).$$

Consider $z \in \{a_1, \dots, a_l\}$. Then, by Theorem 3.19, there is a neighbourhood U_z of z such that $\nu_p(G(x))$ is constant (and equal $\nu_p(G(z))$) for $x \in U_z$.

Consider $r \in \mathbb{Z}_p$, which is close to 0, i.e., divisible by a high power of p. Since, f is continuous, and since $\nu_p(rf(y)) \geq \nu_p(r)$, which can be arbitrarily large, if $\nu_p(f(x)/f(y)) = \nu_p(r)$, then x has to be close to a zero of f. We can choose r such that x has to be in the set $U_{a_1} \cup \cdots \cup U_{a_l}$. For $x \in U_{a_1} \cup \cdots \cup U_{a_l}$, we have

$$\nu_p(f(x)) \equiv \nu_p(G(x)) \in \{\nu_p(G(a_1)), \dots, \nu_p(G(a_l))\} \pmod q,$$

so $\nu_p(f(x)) \pmod q$ can take at most l different values.

By the assumption, $p \nmid h_2(y)$ for any $y \in \mathbb{Z}_p$, so, by applying Theorem 3.18, we have that $\nu_p(f(y)) \pmod q$ can take at most $k+1$ values. We note that the set of these at most $k+1$ possible values of $\nu_p(f(y)) \pmod q$ contains the set of at most l possible values of $\nu_p(f(x)) \pmod q$. Hence, the set of possible values of $\nu_p(f(x)/f(y)) \pmod q$ can contain at most $l(k+1)-(l-1) = lk+1$ (because at least l values coincide in both sets, so we get the zero difference at least l times, so we overcount it at least $l-1$ times).

Since we assume that $1+lk < q$, there is a class modulo q which does not belong to the set of possible classes of $\nu_p(f(x)/f(y)) \pmod q$, so for r in this class, there do not exist $x, y \in \mathbb{Z}_p$ such that $\nu_p(f(x)/f(y)) = \nu_p(r)$. ■

Corollary 3.8.1. *In the situation of Theorem 3.20, if* $k+l < 2\sqrt{q-1}$, *then* $R(f)$ *is not dense in* $\mathbb{Q}_p$.

Proof. By the inequality of arithmetic and geometric means and the assumption,

$$1 + kl \leq 1 + \frac{(k+l)^2}{4} < 1 + \frac{4(q-1)}{4} = q.$$

The conclusion follows directly from Theorem 3.20. ■

3.8.1 Sharpness of the inequality in Theorem 3.20

Assume that p is such that $p > q$ and $\gcd(q, p-1) = 1$. The latter condition implies that the qth power function $\cdot^q \colon \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$, $x \mapsto x^q$ is a bijection, and since $q < p$, all the elements of $\mathbb{Z}_p^*$ are qth powers by Hensel's lemma. We mention two examples for which $R(f)$ is dense in $\mathbb{Q}_p$:

1. If $l = 1$ and $k = q-1$, consider

$$f(x) = x^q((x-1)^q + p)((x-2)^q + p^2)\cdots((x-(q-1))^q + p^{q-1}).$$

2. If q is odd, and $l = 2$, $k = \frac{q-1}{2}$, consider

$$f(x) = x^q(x-k)^q((x-1)^q + p^{q+1})((x-2)^q + p^{q+2})\cdots((x-k)^q + p^{q+k}).$$

In both of these cases, we have $1+kl = q$, so this shows the sharpness of Theorem 3.20. We note that the second polynomial has less degree than the first one. It is an interesting problem to find the smallest sum $k+l$ for which there is a polynomial of the shape of Theorem 3.20 whose ratio set is dense. We know by Corollary 3.8.1 that $k + l \geq 2\sqrt{q-1}$.

Remark 3.8.1. *We see from the proof of Theorem 3.20, that we may assume that $l \leq k+1$, because $k+1$ is the maximum of possible values of $\nu_p(f(x)) \pmod q$ for $x \in \mathbb{Z}_p$.*

4

p-Adic quotient sets: linear recurrence sequences- I

4.1 Introduction

Let $(F_n)_{n\geq 0}$ be the sequence of Fibonacci numbers, defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all integers $n \geq 2$. In [20], Garcia and Luca showed that the ratio set of Fibonacci numbers is dense in $\mathbb{Q}_p$ for all primes p. Later, Sanna [42, Theorem 1.2] showed that, for any $k \geq 2$ and any prime p, the ratio set of the k-generalized Fibonacci numbers is dense in $\mathbb{Q}_p$. Sanna remarked that his result

[1] The contents of this chapter have been published in *Bull. Aust. Math. Soc.* 108 (2023).

could be extended to other linear recurrence sequences over the integers. However, he used some specific properties of the k-generalized Fibonacci numbers in the proof. Therefore, he made the following open question.

Question 4.1.1. [42, Question 1.3] *Let $(S_n)_{n\geq 0}$ be a linear recurrence of order $k \geq 2$ satisfying*

$$S_n = a_1 S_{n-1} + a_2 S_{n-2} + \cdots + a_k S_{n-k},$$

for all integers $n \geq k$, where $a_1, \ldots, a_k, S_0, \ldots, S_{k-1} \in \mathbb{Z}$, with $a_k \neq 0$. For which prime numbers p is the quotient set of $(S_n)_{n\geq 0}$ dense in $\mathbb{Q}_p$?

In [19], Garcia et al. studied the quotient sets of certain second order recurrences. To be specific, given two fixed integers r and s, let $(a_n)_{n\geq 0}$ be defined by $a_n = ra_{n-1} + sa_{n-2}$ for $n \geq 2$ with initial values $a_0 = 0$ and $a_1 = 1$; and let $(b_n)_{n\geq 0}$ be defined by $b_n = rb_{n-1} + sb_{n-2}$ for $n \geq 2$ with initial values $b_0 = 2$ and $b_1 = r$. Garcia et al. proved the following result.

Theorem 4.1. [19, Theorem 5.2] *Let $A = \{a_n : n \geq 0\}$ and $B = \{b_n : n \geq 0\}$.*

(a) If $p \mid s$ and $p \nmid r$, then $R(A)$ is not dense in $\mathbb{Q}_p$.

(b) If $p \nmid s$, then $R(A)$ is dense in $\mathbb{Q}_p$.

(c) For all odd primes p, $R(B)$ is dense in $\mathbb{Q}_p$ if and only if there exists a positive integer n such that $p \mid b_n$.

In this chapter, we give some answers to Question 4.1.1.

4.2 Linear recurrence sequence with irreducible characteristic polynomial

Our first result gives the denseness of the ratio set of kth-order linear recurrence sequences with irreducible characteristic polynomials over $\mathbb{Q}_p$ provided certain conditions hold.

We state a lemma and a theorem which is used in the proof of our result.

Lemma 4.2. [19, Lemma 2.3] *Let $A \subset \mathbb{N}$.*

1. *If A is p-adically dense in $\mathbb{N}$, then $R(A)$ is dense in $\mathbb{Q}_p$.*
2. *If $R(A)$ is p-adically dense in $\mathbb{N}$, then $R(A)$ is dense in $\mathbb{Q}_p$.*

Theorem 4.3. [6, Theorem 1] *Let $\alpha_1, \ldots, \alpha_n$ be units in Ω_p, the completion of algebraic closure of $\mathbb{Q}_p$, which are algebraic over the rationals $\mathbb{Q}$ and whose p-adic logarithms are linearly independent over $\mathbb{Q}$. These logarithms are then linearly independent over the algebraic closure of $\mathbb{Q}$ in Ω_p.*

Recall that a *Pisot number* is a positive algebraic integer greater than 1 all of whose conjugate elements have absolute value less than 1.

Theorem 4.4. *Let $(x_n)_{n\geq 0}$ be a kth-order linear recurrence satisfying*

$$x_n = a_1x_{n-1} + a_2x_{n-2} + \cdots + a_{k-1}x_{n-k+1} + x_{n-k}$$

for all integers $n \geq k$ with initial values $x_0 = x_1 = \cdots = x_{k-2} = 0, x_{k-1} = 1$ and $a_1, \ldots, a_{k-1} \in \mathbb{Z}$. Suppose that the characteristic polynomial of the reccurence sequence has a root $\pm\alpha$, where α is a Pisot number. If p is a prime such that the characteristic polynomial of the recurrence sequence is irreducible in $\mathbb{Q}_p$, then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$.

Proof. Let $p(x) = x^k - a_1x^{k-1} - a_2x^{k-2} - \cdots - a_{k-1}x - 1$ be the characteristic polynomial. Let $\alpha_1, \ldots, \alpha_k$ be the k distinct roots of the characteristic polynomial in its splitting field, say, K over $\mathbb{Q}_p$. The generating function of the sequence is

$$t(x) = \frac{x^{k-1}}{1 - a_1x - a_2x^2 - \cdots - x^k} = \sum_{i=1}^{k} \frac{1}{q(\alpha_i)} \sum_{n=0}^{\infty} \alpha_i^n x^n,$$

where $q(x) := p'(x)$, the derivative of the polynomial $p(x)$. Hence, the nth term of the sequence is given by

$$x_n = \sum_{i=1}^{k} \frac{1}{q(\alpha_i)} \alpha_i^n, n \geq 0.$$

Since $p(0) = -1$, the roots of $p(x)$ are units in the ring formed by elements in K with p-adic absolute value less than or equal to one. Following Sanna's proof of [42, Theorem 1.2], we can choose an even $t \in \mathbb{N}$ such that the function defined as

$$G(z) := \sum_{i=1}^{k} \frac{1}{q(\alpha_i)} \exp_p(z \log_p(\alpha_i^t))$$

is analytic over $\mathbb{Z}_p$ and the Taylor series of $G(z)$ around 0 converges for all $z \in \mathbb{Z}_p$. Also, note that $x_{nt} = G(n)$ for $n \geq 0$.

We now use a variant of the following lemma which gives the multiplicative independence of any $k-1$ roots among the k roots $\alpha_1, \ldots, \alpha_k$ of the characteristic polynomial $x^k - x^{k-1} - \cdots - x - 1$ of the k-generalized Fibonacci sequence in the field of complex numbers.

Lemma 4.5. [16, Lemma 1] *Each set of $k-1$ different roots $\alpha_1, \ldots, \alpha_{k-1}$ is multiplicatively independent, that is, $\alpha_1^{e_1} \ldots \alpha_{k-1}^{e_{k-1}} = 1$ for some integers $e_1, \ldots, e_{k-1}$ if and only if $e_1 = \cdots = e_{k-1} = 0$.*

Let $\sigma(\alpha_1) = \pm\alpha$, where α is a Pisot number with absolute value greater than 1 and other roots, $\sigma(\alpha_2), \ldots, \sigma(\alpha_k)$ with absolute values less than 1, where, σ is an isomorphism from $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ to the splitting field of $p(x)$ over $\mathbb{Q}$ in the field of complex numbers. Therefore, the proof of Lemma 4.5 holds true for the roots of $p(x)$, which are $\sigma(\alpha_1), \ldots, \sigma(\alpha_k)$, since $\log|\sigma(\alpha_1)|$ is positive and $\log|\sigma(\alpha_2)|, \ldots, \log|\sigma(\alpha_k)|$ are negative. Hence, $\sigma(\alpha_1), \ldots, \sigma(\alpha_{k-1})$ are multiplicatively independent, implying that $\alpha_1^t, \ldots, \alpha_{k-1}^t$ are multiplicatively independent. Thus, $\log_p(\alpha_1^t), \ldots, \log_p(\alpha_{k-1}^t)$ are linearly independent over $\mathbb{Z}$ and hence linearly independent over algebraic numbers by Theorem 4.3.

If $G'(0) = \sum_{i=0}^{k} \frac{1}{q(\alpha_i)} \log_p(\alpha_i^t) = 0$, we obtain

$$\sum_{i=1}^{k-1} \Big(\frac{1}{q(\alpha_i)} - \frac{1}{q(\alpha_k)} \Big) \log_p(\alpha_i^t) = 0$$

since $\log_p(\alpha_k^t) = -\log_p(\alpha_1^t) - \cdots - \log_p(\alpha_k^t)$ as product of the roots is -1 and t is even. By linear independence of $\log_p(\alpha_1^t), \ldots, \log_p(\alpha_{k-1}^t)$, $\frac{1}{q(\alpha_1)} = \cdots = \frac{1}{q(\alpha_k)} = c$, for some p-adic number c. This gives k distinct roots $\alpha_1, \ldots, \alpha_k$ of the $k-1$ degree polynomial $q(x) - \frac{1}{c}$, which is not possible. Therefore, $G'(0) \neq 0$. Since

$$G(z) = \sum_{j=0}^{\infty} \frac{G^{(j)}(0)}{j!} z^j$$

converges at $z = 1$, so $\| \frac{G^{(j)}(0)}{j!} \|_p \to 0$. Hence, there exists an integer ℓ such that $\nu_p(G^{(j)}(0)/j!) \geq -\ell$ for all j. Thus, we obtain $G(mp^h) = G'(0)mp^h + d$ such that $\nu_p(d) \geq 2h - \ell$ for all $m, h \geq 0$. For $h > h_0 := \ell + \nu_p(G'(0))$, we have

$$\nu_p\Big(\frac{G(mp^h)}{G(p^h)} - m \Big) \geq h - h_0.$$

This yields

$$\lim_{h\to\infty} \left\| \frac{G(mp^h)}{G(p^h)} - m \right\|_p = 0,$$

and hence $R(G(n)_{n\geq 0})$ is p-adically dense in $\mathbb{N}$. Since $x_{nt} = G(n), n \geq 0$, we find that $R((x_n)_{n\geq 0})$ is also p-adically dense in $\mathbb{N}$. Therefore, by Lemma 4.2, $R((x_n)_{n\geq 0})$

is dense in $\mathbb{Q}_p$. ■

If we take $k = 3$ in Theorem 4.4, then we have the following corollary.

Corollary 4.2.1. *Let $(x_n)_{n\geq 0}$ be a third-order linear recurrence satisfying*

$$x_n = ax_{n-1} + bx_{n-2} + x_{n-3}$$

for all integers $n \geq 3$ with initial values $x_0 = x_1 = 0, x_2 = 1$, and the integers a and b are such that $(a+b)(b-a-2) < 0$. If p is a prime such that the characteristic polynomial of the recurrence sequence is irreducible in $\mathbb{Q}_p$, then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$.

Proof. Since $p(1)p(-1) = (-a-b)(b-a-2) > 0$ and $p(0) = -1$, by continuity of the polynomial function in $\mathbb{R}$, $p(x)$ has one real root with absolute value greater than 1 and other two roots with absolute values less than 1. Hence, the characteristic polynomial has a root $\pm\alpha$ with α a Pisot number. Now, the corollary follows from Theorem 4.4. ■

We discuss two examples as applications of Corollary 4.2.1.

Example 4.2.1. *For $a \in \mathbb{N}$, let ℓ be an odd positive integer less than $2a$. Let $(x_n)_{n\geq 0}$ be a linear recurrence satisfying*

$$x_n = ax_{n-1} + (a-\ell)x_{n-2} + x_{n-3}$$

for all integers $n \geq 3$ with initial values $x_0 = x_1 = 0, x_2 = 1$. Then, a and $b := a - \ell$ satisfy $(a+b)(b-a-2) < 0$. The characteristic polynomial is $p(x) = x^3 - ax^2 - (a-\ell)x - 1$. Since $p(0) = -1$ and $p(1) = -2a + \ell \not\equiv 0 \pmod 2$, hence $p(x)$ is irreducible in $\mathbb{Q}_2$. Therefore, by Corollary 4.2.1, $R((x_n)_{n\geq 0})$ is dense in $\mathbb{Q}_2$.

Example 4.2.2. *For $a \in \mathbb{N}$ such that $3 \nmid a$, let ℓ be an odd positive integer less than $2a$ and $3 \mid \ell$. Let $(x_n)_{n\geq 0}$ be a linear recurrence satisfying*

$$x_n = ax_{n-1} + (a-\ell)x_{n-2} + x_{n-3}$$

for all integers $n \geq 3$ with initial values $x_0 = x_1 = 0, x_2 = 1$. Then, a and $b = a - \ell$ satisfy $(a+b)(b-a-2) < 0$. The characteristic polynomial is $p(x) = x^3 - ax^2 - (a-\ell)x - 1$. Since $p(0) = -1$, $p(1) = -2a + \ell \not\equiv 0 \pmod 3$ and $p(2) = -6a + 2\ell + 7 \not\equiv 0 \pmod 3$, hence $p(x)$ is irreducible in $\mathbb{Q}_3$. Therefore, by Corollary 4.2.1, $R((x_n)_{n\geq 0})$ is dense in $\mathbb{Q}_3$.

4.3 Some special linear recurrence sequences

First, we consider linear recurrence sequences whose nth term depends on all the previous $n-1$ terms.

Theorem 4.6. *Let $(x_n)_{n\geq 0}$ be a linear recurrence satisfying*

$$x_n = x_{n-1} + 2x_{n-2} + \cdots + (n-1)x_1 + nx_0$$

for all integers $n \geq 1$ with initial value $x_0 = 1$. Then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$ for all primes p.

We need the following corollary to prove Theorem 4.6.

Corollary 4.3.1. [12, Corollary 2.2] *The linear recurrence relation $x_{n+1} = x_n + 2x_{n-1} + \cdots + nx_1 + (n+1)x_0, n \geq 0$ with the initial data $x_0 = 1$ has the solution $x_n = \frac{1}{\sqrt{5}}\left((\frac{3+\sqrt{5}}{2})^n - (\frac{3-\sqrt{5}}{2})^n\right), n \geq 1$.*

Proof of Theorem 4.6. By Corollary 4.3.1, we have

$$x_n = \frac{1}{\sqrt{5}}\left(\left(\frac{3+\sqrt{5}}{2}\right)^n - \left(\frac{3-\sqrt{5}}{2}\right)^n\right), n \geq 1$$

$$= \frac{\alpha^{2n} - \beta^{2n}}{\sqrt{5}}$$
$$= F_{2n},$$

where $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$, and F_n denotes the nth Fibonacci number which is obtained by the Binet formula. From the work of Garcia et. al [20], we know that the ratio set of Fibonacci numbers is dense in $\mathbb{Q}_p$ for all primes p. Therefore, by Lemma 1.12, $\nu_p(F_n)$ is not bounded. Hence, for any $j \in \mathbb{N}$, there exists F_m such that $\nu_p(F_m) \geq j$, that is, $\frac{\alpha^m - \beta^m}{\sqrt{5}} \equiv 0 \pmod{p^j}$ which gives $\alpha^m \equiv \beta^m \pmod{p^j}$. This yields

$$\alpha^{2mp^{j-1}(p-1)} = (\alpha^m \alpha^m)^{p^{j-1}(p-1)} \equiv (\alpha^m \beta^m)^{p^{j-1}(p-1)} \pmod{p^j}.$$

Since $\alpha\beta = -1$, by using Euler's theorem, we find that

$$\alpha^{2mp^{j-1}(p-1)} \equiv (\alpha^m \beta^m)^{p^{j-1}(p-1)} \equiv 1 \pmod{p^j}.$$

This gives $\alpha^{2k} \equiv \beta^{2k} \equiv 1 \pmod{p^j}$, where $k = mp^{j-1}(p-1)$. Hence,

$$\frac{x_{kn}}{x_k} = \frac{F_{2kn}}{F_{2k}} = \frac{(\alpha^{2k})^n - (\beta^{2k})^n}{\alpha^{2k} - \beta^{2k}} = (\alpha^{2k})^{(n-1)} + (\alpha^{2k})^{n-2}\beta^{2k} + \cdots + (\beta^{2k})^{n-1},$$

which is congruent to n modulo p^j. Since for $n \in \mathbb{N}$, there exists $k \in \mathbb{N}$ such that $\| \frac{x_{kn}}{x_k} - n \|_p \leq p^{-j}$, $R((x_n)_{n\geq 0})$ is p-adically dense in $\mathbb{N}$. Therefore, by Lemma 4.2, $R((x_n)_{n\geq 0})$ is dense in $\mathbb{Q}_p$. ■

Theorem 4.7. *Let $(x_n)_{n\geq 0}$ be a linear recurrence satisfying*

$$x_n = ax_{n-1} + arx_{n-2} + \cdots + ar^{n-1}x_0$$

for all integers $n \geq 1$, and $x_0, a, r \in \mathbb{Z}$. Then the quotient set of $(x_n)_{n\geq 0}$ is not dense in $\mathbb{Q}_p$ for all primes p.

We need the following results to prove Theorem 4.7.

Theorem 4.8. [12, Theorem 3.1] *The numbers x_n are solutions of the linear recurrence relation with constant coefficients in geometric progression $x_{n+1} = ax_n + aqx_{n-1} + \cdots + aq^{n-1}x_1 + aq^n x_0, n \geq 0$ with initial data x_0, if and only if they form the geometric progression given by the formula $x_n = ax_0(a+q)^{n-1}, n \geq 1$.*

Lemma 4.9. [19, Lemma 2.2] *If A is a geometric progression in $\mathbb{Z}$, then $R(A)$ is not dense in any $\mathbb{Q}_p$.*

Proof of Theorem 4.7. By Theorem 4.8, $(x_n)_{n\geq 1}$ forms a geometric progression where nth term is $ax_0(a+r)^{n-1}$ for $n \geq 1$. Hence, by Lemma 4.9, $R((x_n)_{n\geq 0})$ is not dense in $\mathbb{Q}_p$ for any prime p. ■

4.3.1 Second order linear recurrence sequences

In Theorem 4.1, Garcia et al. studied second order linear recurrence relations with specific initial values. In the following result, we consider a particular form of second order linear recurrence sequence with arbitrary initial values x_0 and x_1 in the set of integers.

Theorem 4.10. *Let $(x_n)_{n\geq 0}$ be a second-order linear recurrence satisfying $x_n = 2ax_{n-1} - a^2x_{n-2}$ for all integers $n \geq 2$, where $a, x_0, x_1 \in \mathbb{Z}$. Then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$ for all primes p satisfying $p \nmid a(x_1 - ax_0)$.*

We need few results on uniform distribution of sequence of integers to prove Theorem 4.10. Recall that a sequence $(x_n)_{n\geq 0}$ is said to be uniformly distributed modulo m if each residue occurs equally often, that is,

$$\lim_{N\to\infty} \frac{\#\{n \leq N | x_n \equiv t \pmod{m}\}}{N} = \frac{1}{m}$$

for all $t \in \mathbb{Z}$. The following theorems will be used to prove Theorem 4.10.

Proposition 4.11. [10, Proposition 1] *Suppose* $\langle G_n \rangle$ *be the sequence of integers determined by the recurrence relation* $G_{n+1} = AG_n - BG_{n-1}$ *with initial values* G_0, G_1 *where* $A, B, G_0, G_1 \in \mathbb{Z}$. *If* $A = 2a, B = a^2$, *then* $\langle G_n \rangle$ *is uniformly distributed modulo a prime* p *if and only if* $p \nmid a(G_1 - aG_0)$.

Theorem 4.12. [10, Theorem] *Suppose* $\langle G_n \rangle$ *be the sequence of integers determined by the recurrence relation* $G_{n+1} = AG_n - BG_{n-1}$ *with initial values* G_0, G_1 *where* $A, B, G_0, G_1 \in \mathbb{Z}$. *If* $\langle G_n \rangle$ *is uniformly distributed modulo* p, *then* $\langle G_n \rangle$ *is uniformly distributed modulo* p^h *with* $h > 1$ *iff:*

1. $p > 3$;
2. $p = 3$ *and* $A^2 \not\equiv B \pmod 9$; *or*
3. $p = 2, A \equiv 2 \pmod 4, B \equiv 1 \pmod 4$.

Now, we are ready to prove Theorem 4.10.

Proof of Theorem 4.10. Let p be a prime. The given recurrence sequence $(x_n)_{n\geq 0}$ satisfies the hypotheses of Proposition 4.11, and hence $(x_n)_{n\geq 0}$ is uniformly distributed modulo p. If $p > 3$, then by part (1) of Theorem 4.12, $(x_n)_{n\geq 0}$ is uniformly distributed modulo p^k with $k > 1$, that is,

$$\lim_{N\to\infty} \frac{\#\{n \leq N | x_n \equiv t \pmod{p^k}\}}{N} = \frac{1}{p^k} > 0.$$

Therefore, for all $t \in \mathbb{N}$ and for all $k > 1$, there exists x_n such that $\| x_n - t \|_p \leq p^{-k}$. Hence, $R((x_n)_{n\geq 0})$ is p-adically dense in $\mathbb{N}$. Therefore, by Lemma 4.2, $R((x_n)_{n\geq 0})$ is dense in $\mathbb{Q}_p$.

We next consider the remaining primes $p = 2, 3$. From the condition $p \nmid a(x_1 - ax_0)$, we have $p \nmid a$. It is easy to check that $p = 3$ satisfies the condition given in part (2) of Theorem 4.12 and $p = 2$ satisfies the condition given in part (3) of Theorem 4.12. The rest of the proof follows similarly as shown in the case of $p > 3$. This completes the proof of the theorem. ■

4.4 Sequences with ratio sets not dense in $\mathbb{Q}_p$

The following theorem gives a set of linear recurrence sequences of order k whose ratio sets are not dense in $\mathbb{Q}_p$.

Theorem 4.13. *Let $(x_n)_{n\geq 0}$ be a linear recurrence of order $k \geq 2$ satisfying*

$$x_n = a_1 x_{n-1} + \cdots + a_k x_{n-k}$$

for all integers $n \geq k$, where $x_0, \ldots, x_{k-1}, a_1, \ldots, a_k \in \mathbb{Z}$. If p is a prime such that $p \nmid a_k$ and $\min\{\nu_p(a_j) : 1 \leq j < k\} > \max\{\nu_p(x_m) - \nu_p(x_n) : 0 \leq m, n < k\}$, then the quotient set of $(x_n)_{n\geq 0}$ is not dense in $\mathbb{Q}_p$.

We need the following lemma to prove Theorem 4.13.

Lemma 4.14. [41, Lemma 3.3] *Let $(r_n)_{n\geq 0}$ be a linearly recurring sequence of order $k \geq 2$ given by $r_n = a_1 r_{n-1} + \cdots + a_k r_{n-k}$ for each integer $n \geq k$, where $r_0, \ldots, r_{k-1}$ and $a_1, \ldots, a_k$ are all integers. Suppose that there exists a prime number p such that $p \nmid a_k$ and $\min\{\nu_p(a_j) : 1 \leq j < k\} > \max\{\nu_p(r_m) - \nu_p(r_n) : 0 \leq m, n < k\}$. Then $\nu_p(r_n) = \nu_p(r_{n \pmod k})$ for each nonnegative integer n.*

Proof of Theorem 4.13. By Lemma 4.14, we have

$$\nu_p(x_n/x_m) = \nu_p(x_{n \pmod k}) - \nu_p(x_{m \pmod k}) \leq M$$

for all $n, m \in \mathbb{N} \cup \{0\}$, where $M = \max\{\nu_p(x_i) : i = 0, 1, \ldots, k-1\}$. Therefore, by Lemma 1.12, $R((x_n)_{n\geq 0})$ is not dense in $\mathbb{Q}_p$. ■

Next, we discuss one example as an application of Theorem 4.13. Given a prime p, this example gives infinitely many recurrence sequences of order $k \geq 2$ so that their quotient sets are not dense in $\mathbb{Q}_p$.

Example 4.4.1. *Let* $(x_n)_{n\geq 0}$ *be a linear recurrence of order* $k \geq 2$ *satisfying*

$$x_n = a_1 x_{n-1} + \cdots + a_k x_{n-k}$$

for all integers $n \geq k$*, where* $x_0 = x_1 = \cdots = x_{k-1} = 1$ *and* $a_1, \ldots, a_k \in \mathbb{Z}$*. If* p *is a prime such that* $p | a_j, 1 \leq j \leq k-1$ *and* $p \nmid a_k$*, then by Theorem 4.13, the quotient set of* $(x_n)_{n\geq 0}$ *is not dense in* $\mathbb{Q}_p$*.*

5

p-Adic quotient sets: linear recurrence sequences- II

5.1 Introduction

In the previous chapter, we obtained that kth order linear recurrence sequences whose characteristics polynomials have pisot roots and are irreducible over $\mathbb{Q}_p$ have a dense ratio set in $\mathbb{Q}_p$. In this chapter, we focus on linear recurrence sequences with reducible characteristic polynomials. Also, we extend Theorem 4.10, which gives condition for the denseness of ratio sets of second order linear recurrence sequences

[1]The contents of this chapter have been published in *Can. Math. Bull.* 68 (2024).

$(x_n)_{n\geq 0}$ whose characteristic polynomials are of the form $(x-a)^2$, to kth order linear recurrence sequences with characteristic polynomials of the form $(x-a)^k$ in the case when the initial values are given as $x_0 = x_1 = \cdots = x_{k-2} = 0, x_{k-1} = 1$.

5.2 Linear recurrence sequences with reducible characteristic polynomial

Suppose that the characteristic polynomial of a linear recurrence sequence be of the form $(x-a_1)(x-a_2)\dots(x-a_k)$, where $a_i \in \mathbb{Z}$. We consider the cases when all a_i's are distinct, exactly two a_i's are equal and the case when all the a_i's are equal.

5.2.1 k distinct roots in $\mathbb{Z}$

In our first theorem, we consider linear recurrence sequences whose characteristic polynomials have distinct integer roots. In the proofs, we will use certain representation of the nth term of linear recurrence sequence in terms of the roots of the characteristic polynomial. More details on such representations can be found in [40].

Theorem 5.1. *Let $(x_n)_{n\geq 0}$ be a linear recurrence of order $k \geq 2$ satisfying*

$$x_n = b_1 x_{n-1} + b_2 x_{n-2} + \cdots + b_k x_{n-k},$$

for all integers $n \geq k$, where $b_1, \dots, b_k, x_0, \dots, x_{k-1} \in \mathbb{Z}$, with $b_k \neq 0$ and $x_0, x_1, \dots, x_{k-1}$ not all zeros. Suppose that the characteristic polynomial of $(x_n)_{n\geq 0}$ is given by

$$(x-a_1)(x-a_2)\dots(x-a_k),$$

where $a_i \in \mathbb{Z}$, $a_i \neq a_j$ for $1 \leq i \neq j \leq k$, and $\gcd(a_i, a_j) = 1$ for all $i \neq j$. Let p be a prime such that $p \nmid a_1 a_2 \cdots a_k$. If $x_0 = 0$, then the quotient set of $(x_n)_{n\geq 0}$ is dense *in* $\mathbb{Q}_p$.

Proof. For $n \geq 0$, the nth term of the sequence (x_n) is given by

$$x_n = c_0 a_1^n + c_1 a_2^n + \cdots + c_{k-1} a_k^n,$$

where

$$C = \begin{bmatrix} c_0 & c_1 & \ldots & c_{k-1} \end{bmatrix}^t$$

is given by $C = \frac{1}{\det(A)} \mathrm{adj}(A) \cdot X_0$, where

$$X_0 = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{k-1} \end{bmatrix}, A = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_k \\ a_1^2 & a_2^2 & \ldots & a_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \ldots & a_k^{k-1} \end{bmatrix}.$$

Let $p > 2$. We define a function f as

$$f(z) := \det(A) \left[c_0 \exp_p \left(z \log_p a_1^{p-1} \right) + \cdots + c_{k-1} \exp_p \left(z \log_p a_k^{p-1} \right) \right].$$

Since $p \nmid a_1 a_2 \ldots a_k$, f is defined for all $z \in \mathbb{Z}_p$ and $f(n) = \det(A) x_{n(p-1)}$ for all $n \in \mathbb{Z}_{\geq 0}$. Moreover, $\mathbb{Z}_{\geq 0}$ is dense in $\mathbb{Z}_p$. Therefore, f is an analytic function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. We have,

$$f(0) = \det(A)(c_0 + c_1 + \cdots + c_{k-1}) = \det(A) x_0 = 0$$

and

$$f'(0) = \det(A)(c_0 \log_p a_1^{p-1} + c_1 \log_p a_2^{p-1} + \cdots + c_{k-1} \log_p a_k^{p-1}).$$

Suppose that $f'(0) = 0$. Since $\gcd(a_i, a_j) = 1$ for all $i \neq j$, therefore, $a_1^{p-1}, \ldots, a_k^{p-1}$

are multiplicatively independent i.e, $(a_1^{p-1})^{u_1}(a_2^{p-1})^{u_2}\dots(a_k^{p-1})^{u_k} = 1$ for some integers $u_1, u_2, \dots, u_k$ only if $u_1 = u_2 = \cdots = u_k = 0$. Hence,

$$\log_p a_1^{p-1}, \log_p a_2^{p-1}, \dots, \log_p a_k^{p-1}$$

are linearly independent over $\mathbb{Z}$. Thus, if $f'(0) = 0$ then $c_0 = c_1 = \cdots = c_{k-1} = 0$ which is not possible. Hence, $f'(0)$ is nonzero. Therefore, 0 is a simple zero of f in $\mathbb{Z}_p$. By Theorem 1.11, $R(f(\mathbb{N})) = R((x_{n(p-1)}))$ is dense in $\mathbb{Q}_p$. Hence, the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$.

Suppose that $p = 2$. Then, we can consider an analytic function f from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ defined as $f(z) := \det(A)\left[c_0 \exp_p\left(z \log_p a_1^2\right) + \cdots + c_{k-1} \exp_p\left(z \log_p a_k^2\right)\right]$ and show that $R(f(\mathbb{N})) = R((x_{2n}))$ is dense in $\mathbb{Q}_p$. ■

Example 5.2.1. *Suppose that p_1, p_2, and p_3 are distinct primes. Let $(x_n)_{n\geq 0}$ be a linear recurrence sequence defined by the recurrence relation*

$$x_n = (p_1 + p_2 + p_3)x_{n-1} - (p_1p_2 + p_1p_3 + p_2p_3)x_{n-2} + (p_1p_2p_3)x_{n-3}$$

for $n \geq 3$, where $x_0 = 0$, and x_1 and x_2 are any integers not both zero. The characteristic polynomial is equal to $(x - p_1)(x - p_2)(x - p_3)$. Hence, by Theorem 5.1, the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$ for all primes $p \neq p_1, p_2, p_3$.

5.2.2 Exactly two equal roots

In the following theorem, we consider kth order linear recurrence sequences whose characteristic polynomials have exactly two equal roots.

Theorem 5.2. *Let $(x_n)_{n\geq 0}$ be a linear recurrence of order $k \geq 3$ satisfying*

$$x_n = b_1x_{n-1} + b_2x_{n-2} + \cdots + b_kx_{n-k},$$

for all integers $n \geq k$, where $b_1, \ldots, b_k, x_0, \ldots, x_{k-1} \in \mathbb{Z}$, with $b_k \neq 0$. Suppose that the characteristic polynomial of $(x_n)_{n\geq 0}$ is given by

$$(x-a_1)^2(x-a_2)(x-a_3)\ldots(x-a_{k-1}),$$

where $a_i \in \mathbb{Z}, a_i \neq a_j$ for $1 \leq i \neq j \leq k-1$, and $x_0 = x_1 = \cdots = x_{k-2} = 0, x_{k-1} = 1$. Let p be a prime such that $p \nmid a_1 a_2 \cdots a_{k-1}$. If $a_i \not\equiv a_j \pmod p$ for all $i \neq j$, then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$.

Proof. The nth term of the sequence is given by

$$\begin{aligned} x_n &= a_1^n(c_0 + c_1 n) + c_2 a_2^n + c_3 a_3^n + \cdots + c_{k-1} a_{k-1}^n \\ &= a_1^n(c_0 + c_1 n + c_2(a_2 a_1^{-1})^n + c_3(a_3 a_1^{-1})^n + \cdots + c_{k-1}(a_{k-1} a_1^{-1})^n), \end{aligned}$$

where

$$C = \begin{bmatrix} c_0 & c_1 & \ldots & c_{k-1} \end{bmatrix}^t$$

is given by $C = \frac{1}{\det(A)}\text{adj}(A) \cdot X_0$, where

$$X_0 = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}, A = \begin{bmatrix} 1 & 0 & 1 & \ldots & 1 \\ a_1 & a_1 & a_2 & \ldots & a_{k-1} \\ a_1^2 & 2a_1^2 & a_2^2 & \ldots & a_{k-1}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & (k-1)a_1^{k-1} & a_2^{k-1} & \ldots & a_{k-1}^{k-1} \end{bmatrix}.$$

Let $p > 2$. We define an analytic function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ as

$$\begin{aligned} f(z) := \det(A) \exp_p(z \log_p(a_1)^{p-1})(c_0 + c_1 z(p-1) + c_2 \exp_p(z \log_p(a_2 a_1^{-1})^{p-1}) \\ + \cdots + c_{k-1} \exp_p(z \log_p(a_{k-1} a_1^{-1})^{p-1})). \end{aligned}$$

Then, $f(n) = \det(A)x_{n(p-1)}$ for all $n \in \mathbb{Z}_{\geq 0}$. Also, we have

$$f(0) = \det(A)(c_0 + c_2 + \cdots + c_{k-1}) = \det(A)x_0 = 0$$

and

$$\begin{aligned} f'(0) &= \det(A)(c_1(p-1) + c_2 \log_p (a_2 a_1^{-1})^{p-1} + \cdots + c_{k-1} \log_p (a_{k-1} a_1^{-1})^{p-1} \\ &\quad + (c_0 + c_2 + \cdots + c_{k-1}) \log_p (a_1)^{p-1}) \\ &= \det(A)(c_1(p-1) + c_2 \log_p (a_2 a_1^{-1})^{p-1} + \cdots + c_{k-1} \log_p (a_{k-1} a_1^{-1})^{p-1}). \end{aligned}$$

We find that $\det(A)c_1 = (-1)^{k+1} \prod_{1 \leq i < j \leq (k-1)} (a_i - a_j)$. By the hypothesis, we have $p \nmid \det(A)c_1$. Using the definition of $\log_p(z)$, we obtain that p divides $\log_p (a_i a_1^{-1})^{p-1}$ for $2 \leq i \leq k-1$. Therefore, $p \nmid f'(0)$ which implies $f'(0)$ is nonzero. Hence, 0 is a simple zero of f in $\mathbb{Z}_p$. By Theorem 1.11, $R(f(\mathbb{N})) = R(x_{n(p-1)})$ is dense in $\mathbb{Q}_p$. Hence, the quotient set of $(x_n)_{n \geq 0}$ is dense in $\mathbb{Q}_p$.

Suppose that $p = 2$. Then, we can consider an analytic function f from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ defined as

$$\begin{aligned} f(z) := \det(A) \exp_p (z \log_p (a_1)^2)(c_0 + 2c_1 z + c_2 \exp_p (z \log_p (a_2 a_1^{-1})^2) \\ + \cdots + c_{k-1} \exp_p (z \log_p (a_{k-1} a_1^{-1})^2)). \end{aligned}$$

and show that $R(f(\mathbb{N})) = R((x_{2n}))$ is dense in $\mathbb{Q}_p$. ■

Example 5.2.2. *Given an integer a, let $(x_n)_{n \geq 0}$ be a linear recurrence sequence defined by the recurrence relation*

$$x_n = 4ax_{n-1} - 5a^2 x_{n-2} + 2a^3 x_{n-3}$$

for $n \geq 3$, where $x_0 = x_1 = 0$ and $x_2 = 1$. The characteristic polynomial is equal to $(x-a)^2(x-2a)$. By Theorem 5.2, the quotient set of $(x_n)_{n \geq 0}$ is dense in $\mathbb{Q}_p$ for all *primes* $p \nmid 2a$.

5.2.3 A root repeated k times

We present sufficient conditions under which a kth order linear recurrence sequence, with a characteristic polynomial that has a root of multiplicity k, is dense in $\mathbb{Q}_p$.

Theorem 5.3. *Let* $(x_n)_{n\geq 0}$ *be a linear recurrence of order* $k \geq 2$ *satisfying*

$$x_n = b_1 x_{n-1} + b_2 x_{n-2} + \cdots + b_k x_{n-k},$$

for all integers $n \geq k$*, where* $b_1, \ldots, b_k, x_0, \ldots, x_{k-1} \in \mathbb{Z}$*, with* $b_k \neq 0$*. Suppose that the characteristic polynomial of* $(x_n)_{n\geq 0}$ *is given by* $(x-a)^k$*, where* $a \in \mathbb{Z}$*, and* $x_0 = x_1 = \cdots = x_{k-2} = 0, x_{k-1} = 1$*. If* p *is a prime such that* $p \nmid a$*, then the quotient set of* $(x_n)_{n\geq 0}$ *is dense in* $\mathbb{Q}_p$*.*

Proof. The nth term of the sequence is given by

$$x_n = a^n(c_0 + c_1 n + \cdots + c_{k-1} n^{k-1}),$$

where

$$C = \begin{bmatrix} c_0 & c_1 & \ldots & c_{k-1} \end{bmatrix}^t$$

is given by $C = \frac{1}{\det(A)} \mathrm{adj}(A) \cdot X_0$, where

$$X_0 = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}, A = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ a & a & a & \ldots & a \\ a^2 & 2a^2 & 2^2a^2 & \ldots & 2^{k-1}a^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a^{k-1} & (k-1)a^{k-1} & (k-1)^2a^{k-1} & \ldots & (k-1)^{k-1}a^{k-1} \end{bmatrix}.$$

We simplify $C = \frac{1}{\det(A)}\text{adj}(A) \cdot X_0$ and obtain

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{k-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & 2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & (k-1) & \dots & (k-1)^{k-1} \end{bmatrix}^{-1} \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1/a^{k-1} \end{bmatrix}.$$

Let $p > 2$. We consider an analytic function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ defined as

$$f(z) := \det(A) \exp_p\left(z \log_p\left(a^{p-1}\right)\right)(c_0 + c_1(p-1)z + c_2(p-1)^2 z^2 + \\ + \cdots + c_{k-1}(p-1)^{k-1} z^{k-1}).$$

Let

$$h(z) := \exp_p\left(z \log_p\left(a^{p-1}\right)\right)$$

and

$$g(z) := \det(A)(c_0 + c_1(p-1)z + c_2(p-1)^2 z^2 + \cdots + c_{k-1}(p-1)^{k-1} z^{k-1}).$$

We have $\|a^n\|_p = 1$ and $h(n) = a^{n(p-1)}$ for all positive integers n. Hence, $\|h(z)\|_p = 1$ for all $z \in \mathbb{Z}_p$. Therefore, $f(z) = 0$ if and only if $g(z) = 0$ for some $z \in \mathbb{Z}_p$. We have, $g(0) = \det(A)c_0 = \det(A)x_0 = 0$ and $g'(0) = \det(A)c_1(p-1)$. Using Lemma 2.2 of [39], we find that

$$c_1 = \frac{(-1)^k}{a^{k-1}(k-1)}.$$

Thus, $c_1 \neq 0$ for all $k \geq 2$. Therefore, 0 is a simple zero of f in $\mathbb{Z}_p$. By Theorem 1.11, $R(f(\mathbb{N})) = R(x_{n(p-1)})$ is dense in $\mathbb{Q}_p$, which yields that the quotient set of

$(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$.

Suppose that $p = 2$. Then, we can consider an analytic function f from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ defined as

$$f(z) := \det(A)\exp_p\left(z\log_p\left(a^2\right)\right)(c_0 + 2c_1 z + (2)^2 c_2 z^2 + \\ + \cdots + (2)^{k-1} c_{k-1} z^{k-1}).$$

and show that $R(f(\mathbb{N})) = R((x_{2n}))$ is dense in $\mathbb{Q}_p$. ■

Remark 5.2.1. *Let $a \in \mathbb{Z}$. Consider the kth order linear recurrence sequence $(x_n)_{n\geq 0}$ generated by the recurrence relation*

$$x_n = \binom{k}{1} a x_{n-1} - \binom{k}{2} a^2 x_{n-2} + \cdots + (-1)^{k-1}\binom{k}{k} a^k x_{n-k}$$

for $n \geq k$, where $x_0 = \cdots = x_{k-2} = 0, x_{k-1} = 1$. Then, the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$ for all primes p not dividing a. This generalises Theorem 4.10 for the case $k = 2$.
Note that a linear recurrence sequence generated by a relation of the above form may not always have a dense quotient set in $\mathbb{Q}_p$. For example, consider the p-th order linear recurrence sequence (x_n) generated by the recurrence relation

$$x_n = \binom{p}{1} a x_{n-1} - \binom{p}{2} a^2 x_{n-2} + \cdots + (-1)^{p-1}\binom{p}{p} a^p x_{n-p}$$

for $n \geq p$, where the initial values $x_0, \ldots, x_{p-1} \in \mathbb{Z}\backslash\{0\}$ have the same p-adic valuation. Then, the quotient set of (x_n) is not dense in $\mathbb{Q}_p$ which follows from Theorem 4.13 of the previous chapter.

5.3 Third order linear recurrence sequences

In case of third order recurrence sequences, we obtain a more general result where we do not need to fix all the initial values.

Theorem 5.4. *Let $(x_n)_{n\geq 0}$ be a third order linear recurrence sequence given by*

$$x_n = b_1 x_{n-1} + b_2 x_{n-2} + b_3 x_{n-3},$$

for all integers $n \geq 3$, where $b_1, b_2, b_3, x_0, x_1, x_2 \in \mathbb{Z}$, with $b_3 \neq 0$. Suppose that the characteristic polynomial of $(x_n)_{n\geq 0}$ is given by $(x-a)(x-b)(x-c)$, where $a, b, c \in \mathbb{Z}$. Let p be a prime such that $p \nmid abc$. Then, the following hold.

(a) Suppose that $a = b = c$. Let $\alpha = 2^{\nu_2(p)}$. If $p^\alpha | x_0$ and $p \nmid 4ax_1 - x_2 - 3a^2 x_0$, then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$. Moreover, if $x_0 = 0$, then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$ if and only if $4ax_1 \neq x_2$.

(b) Suppose that $a = c \neq b$. Let $\beta = 3^{\nu_2(p)}$. If $p^\beta | x_0$ and $p \nmid (a-b)\left(x_2 - x_1(a+b) + x_0 ab\right)$, then the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$.

Proof. We first prove part (a) of the theorem. For $n \geq 0$, the nth term of the sequence is given by the formula

$$x_n = a^n(c_0 + c_1 n + c_2 n^2),$$

where

$$c_0 = x_0,$$
$$c_1 = \frac{4ax_1 - x_2 - 3a^2 x_0}{2a^2},$$
$$c_2 = \frac{x_2 - 2ax_1 + a^2 x_0}{2a^2}.$$

Let $p > 2$. Then, $\alpha = 1$. We define a function f as

$$f(z) := 2a^2 \exp_p(z \log_p a^{p-1})(c_0 + c_1(p-1)z + c_2(p-1)^2 z^2).$$

Since $p \nmid a$, f is defined for all $z \in \mathbb{Z}_p$ and $f(n) = 2a^2 x_{n(p-1)}$ for all $n \in \mathbb{Z}_{\geq 0}$. Moreover, $\mathbb{Z}_{\geq 0}$ is dense in $\mathbb{Z}_p$. Therefore, f is an analytic function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. We have,

$$f(0) = 2a^2 c_0 = 2a^2 x_0 \equiv 0 \pmod{p}$$

and

$$f'(0) \equiv 2a^2 c_1(p-1) = (4ax_1 - x_2 - 3a^2 x_0)(p-1) \not\equiv 0 \pmod{p}.$$

Therefore, by Hensel's lemma, f has a zero z_0 in $\mathbb{Z}_p$ such that $z_0 \equiv 0 \pmod{p}$. Since f has a power series expansion with p-adic integral coefficients, we have $f'(z_0) \equiv f'(0) \pmod{p}$. Hence, z_0 is a simple zero of f in $\mathbb{Z}_p$. Therefore, by Theorem 1.11, $R(f(\mathbb{N})) = R((x_{n(p-1)}))$ is dense in $\mathbb{Q}_p$. Hence, the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$.

Suppose that $p = 2$. Then, $\alpha = 2$. We define a function f from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ as

$$f(z) := 2a^2 \exp_p(z \log_p a^2)(c_0 + 2c_1 z + (2)^2 c_2 z^2).$$

It can be shown that $R(f(\mathbb{N})) = R((x_{2n}))$ is dense in $\mathbb{Q}_p$ which follows same as the $p > 2$ case.

Next, if $x_0 = 0$, then $c_0 = 0$ and $c_1 = \frac{4ax_1 - x_2}{2a^2}$. We have $f(0) = 0$. Suppose that $4ax_1 \neq x_2$. Then, $f'(0) \neq 0$ which implies that 0 is a simple zero of f. Therefore, by Theorem 1.11, the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$. Conversely, suppose that $4ax_1 = x_2$. This gives $c_1 = 0$, and hence $x_n = a^n c_2 n^2$. If $c_2 = 0$, then $x_n = 0$ for all n. If $c_2 \neq 0$, then the quotient set of $(x_n)_{n\geq 0}$ is equal to the quotient set of $\{a^n n^2 : n \in \mathbb{Z}_{\geq 0}\}$. Since $\nu_p(a^n n^2) = 2\nu_p(n)$, the p-adic valuation of these elements is even for all $n \in \mathbb{Z}_{>0}$. Therefore, by Lemma 1.12, the quotient set of $(x_n)_{n\geq 0}$ is not dense in $\mathbb{Q}_p$. This completes the proof of part (a) of the theorem.

Next, we prove part (b) of the theorem. For $n \geq 0$, the nth term of the sequence is given by

$$x_n = c_0 a^n + c_1 n a^n + c_2 b^n = a^n(c_0 + c_1 n + c_2 (ba^{-1})^n),$$

where

$$c_0 = \frac{b^2 x_0 - 2abx_0 - x_2 + 2ax_1}{(b-a)^2},$$
$$c_1 = \frac{x_2 - x_1(a+b) + x_0 ab}{a(a-b)},$$
$$c_2 = \frac{x_2 - 2ax_1 + a^2 x_0}{(b-a)^2}.$$

Let $p > 2$. Then, $\beta = 1$. Since $p \nmid ab(a-b)$, we can define an analytic function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ as

$$f(z) := \exp_p(z \log_p a^{p-1})(c_0 + c_1 z(p-1) + c_2 \exp_p(z \log_p (ba^{-1})^{p-1})),$$

which satisfies the equation $f(n) = x_{n(p-1)}$ for all $n \geq 0$.
Now, we have

$$f(0) = c_0 + c_2 = x_0 \equiv 0 \pmod p$$

and

$$f'(0) = c_1(p-1) + c_2 \log_p (ba^{-1})^{p-1} + (c_0 + c_2) \log_p a^{p-1} \not\equiv 0 \pmod p.$$

Therefore, by Hensel's lemma, f has a zero z_0 in $\mathbb{Z}_p$ such that $z_0 \equiv 0 \pmod p$. Since f has a power series expansion with p-adic integral coefficients, we have $f'(z_0) \equiv f'(0) \pmod p$. Hence, z_0 is a simple zero of f in $\mathbb{Z}_p$. Therefore, by Theorem 1.11,

$R(f(\mathbb{N})) = R(x_{n(p-1)})$ is dense in $\mathbb{Q}_p$. Hence, the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$.

Suppose that $p = 2$. Then, $\beta = 3$. We define a function f from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ as

$$f(z) := \exp_p(z \log_p a^2)(c_0 + 2c_1 z + c_2 \exp_p(z \log_p (ba^{-1})^2)).$$

It can be shown that $R(f(\mathbb{N})) = R((x_{2n}))$ is dense in $\mathbb{Q}_p$ which follows same as the $p > 2$ case. ∎

Example 5.3.1. *Let $a \in \mathbb{Z}$ be such that $p \nmid a$, and let $(x_n)_{n\geq 0}$ be a linear recurrence sequence defined by the recurrence relation*

$$x_{n+1} = 3ax_n - 3a^2 x_{n-1} + a^3 x_{n-2}$$

for $n \geq 2$, where $x_0 = 0$, and x_1 and x_2 are any integers satisfying $\gcd(4a, x_2) = 1$*. Then, by Theorem 5.4 (a), the quotient set of $(x_n)_{n\geq 0}$ is dense in $\mathbb{Q}_p$.*

6

p-Adic valuation of third order linear recurrence sequences

6.1 Introduction

Understanding the p-adic valuation of sets is crucial for studying their denseness in $\mathbb{Q}_p$. In this chapter, we will focus on the p-adic valuation of third order linear recurrence sequences.

[1]The contents of this chapter have been published in *Results Math.* 79 (2024).

6.1.1 Tribonacci sequence

There are several generalizations of Fibonacci numbers. One of the most well-known is the Tribonacci sequence (T_n), which is defined by the recurrence $T_{n+1} = T_n + T_{n-1} + T_{n-2}$, with initial values $T_0 = 0$ and $T_1 = T_2 = 1$. In [32], Marques and Lengyel calculated the 2-adic valuation of the Tribonacci numbers T_n, and used their result to solve the Diophantine equation $T_n = m!$ in positive integers n, m. Later, the 2-adic valuations of some other generalizations of Fibonacci numbers where calculated, see for example [29, 50, 44]. Tripell sequences were also considered by Bravo et al. in [4].

In [32, Conjecture 8], Marques and Lengyel conjectured that the p-adic valuation of a Tribonacci number T_n is either constant or is linearly dependent on the p-adic valuation of the index n of the terms of the sequence for n in some congruence class. However, in [2, Theorem 1.5] Bilu et al. showed that the conjecture fails for a specific infinite set of primes of relative density $1/12$. Our aim is to consider the conjecture for any third order linear recurrence sequence.

6.2 A generalisation of the Marques and Lengyel conjecture

For any third order linear recurrence sequence (x_n), we restate the conjecture as follows. We restate [2, Conjecture 1.2] which is equivalent to [32, Conjecture 8].

Conjecture 6.1. [2, Conjecture 1.2] *Let (x_n) be a third order linear recurrence sequence. Let p be a prime number. There exists a positive integer Q such that for every $i \in \{0, 1, \ldots, Q-1\}$ we have one of the following two options.*

(C) *There exists $\kappa_i \in \mathbb{Z}_{\geq 0}$ such that for all but finitely many $n \in \mathbb{Z}$ satisfying $n \equiv i \pmod{Q}$ we have $\nu_p(x_n) = \kappa_i$.*

(L) *There exist*

$$a_i \in \mathbb{Z}, \qquad \kappa_i \in \mathbb{Z}, \qquad \mu_i \in \mathbb{Z}_{>0}$$

satisfying

$$\nu_p(a_i - i) \geq \nu_p(Q),$$

such that for all but finitely many $n \in \mathbb{Z}$ *satisfying* $n \equiv i \pmod{Q}$ *we have*

$$\nu_p(x_n) = \kappa_i + \mu_i \nu_p(n - a_i).$$

For $a, b, c \in \mathbb{Z}$, and a prime p, we consider a third order linear recurrence sequence (x_n) for $n \in \mathbb{Z}$ defined as

$$x_n = ax_{n-1} + bx_{n-2} + cx_{n-3} \text{ with } x_0, x_1, x_2 \in \mathbb{Z} \text{ and } p \nmid c. \tag{6.1}$$

The characteristic polynomial of the linear recurrence sequence (6.1) is given by the polynomial $P(x) = x^3 - ax^2 - bx - c$. A linear recurrence sequence is said to be degenerate if its characteristic polynomial has a pair of distinct roots whose ratio is a root of unity. Otherwise it is said to be non-degenerate. Suppose that (x_n) is a simple sequence, i.e, $P(x)$ has distinct roots. Let $\mathbb{K} = \mathbb{Q}_p(\lambda_1, \lambda_2, \lambda_3)$ be the splitting field of $P(x)$ over $\mathbb{Q}_p$, where $\lambda_1, \lambda_2, \lambda_3$ are the distinct roots of $P(x)$. Let $\mathcal{O}$ be the ring of integers of $\mathbb{K}$. Throughout the chapter, we consider primes p which do not divide the discriminant of the characteristic polynomial so that $\mathbb{K}$ is unramified over $\mathbb{Q}_p$.

For $n \geq 0$, the nth term of the sequence (x_n) is given by the formula

$$x_n = \sum_{i=1}^{3} c_{\lambda_i} \lambda_i^n, \text{ where } c_{\lambda_i} = q(\lambda_i)/P'(\lambda_i), \tag{6.2}$$

where $q(x) := x_0x^2 + (x_1 - x_0a)x + (x_2 - x_1a - x_0b)$. Since p does not divide the discriminant of the polynomial, we have, $c_{\lambda_i} \in \mathcal{O}$. By our assumption, p does not divide c which implies that the roots $\{\lambda_1, \lambda_2, \lambda_3\} \subset \mathcal{O}^\times$.

6.2.1 Twisted integral zero of a sequence

We consider non-degenerate third order linear recurrence sequences (x_n) given by (6.1) whose nth term satisfies the equation

$$x_n = \sum_{i=1}^{3} c_{\lambda_i} \lambda_i^n \quad \text{for all} \quad n \in \mathbb{Z}. \tag{6.3}$$

For $n \in \mathbb{Z}$, we say that n is a zero of (x_n) if

$$\sum_{i=1}^{3} c_{\lambda_i} \lambda_i^n = 0.$$

Bilu et al. introduced the notion of a *Twisted Integral Zero* (TIZ), denoted by $\mathcal{Z}$, which is defined as the set of integers n such that

$$\sum_{i=1}^{3} \xi_i c_{\lambda_i} \lambda_i^n = 0$$

for some roots of unity ξ_1, ξ_2, ξ_3. A systematic study of Twisted Zeros of the Tribonacci sequence can be found in [3].

For a positive integer n, let N_{p^n} be the order of the subgroup $\langle \lambda_1, \lambda_2, \lambda_3 \rangle$ in the multiplicative group $(\mathcal{O}/p^n)^\times$. For $\ell \in \{0, 1, \ldots, N_{p^n} - 1\}$, consider the analytic function $f_\ell : \mathbb{Z}_p \to \mathbb{Z}_p$ defined by

$$f_\ell(x) = \sum_{i=1}^{3} c_{\lambda_i} \lambda_i^\ell \exp_p(x \log_p(\lambda_i^N)), \text{ where } N = N_{p^n}. \tag{6.4}$$

Here, $\mathbb{Z}_p$ denotes the ring of p-adic integers in $\mathbb{Q}_p$. We have,

$$f_\ell(m) = x_{\ell + mN} \text{ for all } m \in \mathbb{Z}$$

and it can be seen that N_{p^n} is the period of the sequence modulo p^n.

It can be verified that the proof of the set of equivalent conditions of Conjecture 6.1 in [2] in terms of the zeros of the functions $f_\ell(x)$ holds true in the case of a third order linear recurrence sequence (6.1) satisfying condition (6.3) as well. The equivalent conditions are as follows.

Theorem 6.2. [2, Theorem 6.1] *The following three statements are equivalent.*

1. *Conjecture 6.1 holds for the given p.*
2. *For every $\ell \in \{0, \ldots, N-1\}$, the zeros of the function $f_\ell(z)$ belong to $N^{-1}\mathbb{Z}$.*
3. *For every ℓ the following holds: if $b \in \mathbb{Z}_p$ is a zero of $f_\ell(z)$ then $\ell + Nb \in \mathcal{Z}$.*

Note that the equivalent statements hold for any $N = N_{p^n}$.

6.2.2 Tests to verify the validity of the conjecture

Using the equivalent conditions, we obtain two results that can be used to find primes p for which the conjecture is true or false for sequences of the form (6.1).

Theorem 6.3. *Let $x_n = ax_{n-1} + bx_{n-2} + cx_{n-3}$ be a third order linear recurrence sequence with initial values x_0, x_1, x_2 satisfying equation (6.3). Suppose that the characteristic polynomial $P(x) := x^3 - ax^2 - bx - c$ of (x_n) is irreducible over $\mathbb{Q}$ and $\lambda_1, \lambda_2, \lambda_3$ are the roots of $P(x)$ in some extension of $\mathbb{Q}_p$. Also, assume that p divides neither c nor the discriminant of $P(x)$. Then the following holds:*

1. *If $p = 2$, then if there exists an $\ell \in \{0, 1, \ldots, N_{p^2} - 1\}$ such that $p^2 | x_\ell$, $x_{\ell+N_{p^2}} - x_\ell \not\equiv 0 \pmod{p^3}$ and*

$$\ell - \frac{x_\ell}{p^2}\left(\frac{x_{\ell+N_{p^2}} - x_\ell}{p^2}\right)^{-1} N_{p^2} \not\equiv r \pmod{p}$$

for all $r \in \mathcal{Z}$, then Conjecture 6.1 does not hold for p.

2. *If $p \neq 2$, then if there exists an $\ell \in \{0, 1, \ldots, N_p - 1\}$ such that $p | x_\ell$, $x_{\ell+N_p} - x_\ell \not\equiv 0 \pmod{p^2}$ and*

$$\ell - \frac{x_\ell}{p}\left(\frac{x_{\ell+N_p} - x_\ell}{p}\right)^{-1} N_p \not\equiv r \pmod{p}$$

for all $r \in \mathcal{Z}$, then Conjecture 6.1 does not hold for p.

We prove a lemma which will be used in the proof of the theorem.

Lemma 6.4. *Let (x_n) be a linear recurrence sequence defined by (6.1) satisfying equation (6.3). Suppose that $N = N_{p^2}$. For f_ℓ defined by (6.4), if $p^2 \nmid x_\ell$, then $f_\ell(z) \neq 0$ for all $z \in \mathbb{Z}_p$.*

Proof. Suppose that $p^2 \nmid x_\ell$. Since $x_n \equiv x_\ell \pmod{p^2}$ for $n \equiv \ell \pmod{N}$, we have $\nu_p(x_n) < 2$ for all $n \equiv \ell \pmod{N}$. Therefore, $|f_\ell(m)|_p > p^{-2}$ for all integers m. Hence, $|f_\ell(z)|_p \geq p^{-2}$ for all $z \in \mathbb{Z}_p$. This completes the proof. ■

Having Lemma 6.4 showed, we are ready to prove Theorem 6.3.

Proof of Theorem 6.3. Suppose that $p = 2$, $N = N_{p^2}$ and $\ell \in \{0, \ldots, N_{p^2} - 1\}$. If $p^2 \nmid x_\ell$, then by Lemma 6.4, $f_\ell(x)$ has no zero in $\mathbb{Z}_p$. Hence, we consider ℓ such that $p^2 | x_\ell$. We define an analytic function

$$g(x) := f_\ell(x)/p^2 = \sum_{k=0}^{\infty} \beta_k x^k.$$

Then, we have

$$\beta_0 = g(0) = \frac{f_\ell(0)}{p^2} = \frac{x_\ell}{p^2} \in \mathbb{Z},$$
$$\beta_k = \frac{p^{2(k-1)}}{k!} \sum_{i=1}^{3} c_{\lambda_i} \lambda_i^\ell \left(\frac{\log_p \lambda_i^N}{p^2}\right)^k$$

for $k \geq 1$. Note that $\nu_p(\beta_k) > 0$ for $k \geq 2$. Also,

$$g'(x) = \beta_1 + \sum_{k=2}^{\infty} k\beta_k x^{k-1} \equiv \beta_1 \pmod{p}.$$

Now,

$$\begin{aligned} g'(0) = \beta_1 &= \sum_{i=1}^{3} c_{\lambda_i} \lambda_i^{\ell} \frac{\log_p \lambda_i^N}{p^2} \\ &\equiv \sum_{i=1}^{3} c_{\lambda_i} \lambda_i^{\ell} \frac{\lambda_i^N - 1}{p^2} \pmod{p} \\ &\equiv \frac{x_{\ell+N} - x_\ell}{p^2} \pmod{p}. \end{aligned}$$

Therefore, $x_{\ell+N} - x_\ell \not\equiv 0 \pmod{p^3}$ implies $g'(0) = \beta_1 \not\equiv 0 \pmod{p}$.

For $b_0 \equiv -\beta_0\beta_1^{-1} \pmod{p}$, we get,

$$g(b_0) \equiv 0 \pmod{p}, g'(b_0) \equiv \beta_1 \not\equiv 0 \pmod{p}.$$

Therefore, by Strassman's Theorem and Hensel's Lemma, g has a unique zero $b \equiv b_0 \pmod{p}$ in $\mathbb{Z}_p$. Hence, $f_\ell(x)$ has a unique zero b in $\mathbb{Z}_p$.

If $\ell + b_0 N \not\equiv r \pmod{p}$ for all $r \in \mathcal{Z}$, then $\ell + bN \notin \mathcal{Z}$. But we have,

$$\ell + b_0 N \equiv \ell - \frac{x_\ell}{p^2} \left(\frac{x_{\ell+N} - x_\ell}{p^2} \right)^{-1} N \not\equiv r \pmod{p} \text{ for all } r \in \mathcal{Z}.$$

Therefore, by Theorem 6.2, the conjecture fails for p.

For $p \neq 2$, the proof proceeds along similar lines to the proof of [2, Theorem 8.1]. ■

We now present the second result, which gives specific conditions under which the conjecture holds true.

Theorem 6.5. *Let $x_n = ax_{n-1} + bx_{n-2} + cx_{n-3}$ be a third order linear recurrence* *sequence with initial values* x_0, x_1, x_2 *satisfying equation* (6.3). *Suppose that the characteristic polynomial* $P(x) := x^3 - ax^2 - bx - c$ *of* (x_n) *is irreducible over* $\mathbb{Q}$ *and* $\lambda_1, \lambda_2, \lambda_3$ *are the roots of* $P(x)$ *in some extension of* $\mathbb{Q}_p$. *Also, assume that* p *divides neither* c *nor the discriminant of* $P(x)$. *Then the following holds:*

1. *If* $p = 2$, *then if for all* $\ell \in \{0, 1, \dots, N_{p^2} - 1\}$, $p^2 | x_\ell$ *implies* $x_{\ell+N_{p^2}} - x_\ell \not\equiv 0 \pmod{p^3}$ *then, Conjecture* 6.1 *holds for* p *if* $\ell \equiv r \pmod{N_{p^2}}$ *for some* $r \in \mathcal{Z}$.

2. *If* $p \neq 2$, *then if for all* $\ell \in \{0, 1, \dots, N_p - 1\}$, $p | x_\ell$ *implies* $x_{\ell+N_p} - x_\ell \not\equiv 0 \pmod{p^2}$ *then, Conjecture* 6.1 *holds for* p *if* $\ell \equiv r \pmod{N_p}$ *for some* $r \in \mathcal{Z}$.

Proof. The proof proceeds along similar lines to the proof of Theorem 8.2 in [2, Theorem 8.2], so we omit the details for reasons of brevity. ■

6.3 Twisted integral zeros of some third order linear recurrence sequences

As evident from the previous theorems, it is beneficial to have a way to find out the twisted integral zeros of sequences. The result below gives certain conditions which ensure that for certain linear recurrence sequences, zeros are the only possible twisted integral zeros. Using the Skolem tool [1], zeros of non-degenerate linear recurrence sequences can be easily calculated. Before stating the result, we state a lemma by Bilu et al. which is used to prove the result.

Lemma 6.6. [2, Lemma 2.5] *Let* α *be an algebraic number of degree* 3. *Assume that* $\mathbb{Q}(\alpha)$ *is not a Galois extension of* $\mathbb{Q}$. *Let* $\alpha_1 (= \alpha), \alpha_2, \alpha_3$ *be the conjugates of* α *over* $\mathbb{Q}$. *Assume further that the field* $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ *does not contain primitive cubic roots of unity. Let* ξ_1, ξ_2, ξ_3 *be roots of unity such that*

$$\alpha_1 \xi_1 + \alpha_2 \xi_2 + \alpha_3 \xi_3 = 0.$$

Then $\xi_1 = \xi_2 = \xi_3$ *and hence* $\alpha_1 + \alpha_2 + \alpha_3 = 0$.

Theorem 6.7. *Let* $x_n = ax_{n-1} + bx_{n-2} + cx_{n-3}$ *be a third order linear recurrence sequence with initial values* x_0, x_1, x_2 *satisfying equation* (6.3). *Suppose that the characteristic polynomial* $P(x) := x^3 - ax^2 - bx - c$ *of* (x_n) *is irreducible over* $\mathbb{Q}$ *and* $\lambda_1, \lambda_2, \lambda_3$ *are the roots of* $P(x)$ *in* $\mathbb{C}$. *Then, the set of Twisted Integral Zeros of* (x_n) *is equal to the set of zeros of* (x_n) *if the following three conditions hold:*

1. $\mathbb{Q}(\lambda_i)$ *is not Galois for some* $1 \leq i \leq 3$.
2. *For the* i *satisfying condition (1),* $\log\left|\frac{c(\lambda_i)}{c(\lambda_j)}\right| / \log\left|\frac{\lambda_j}{\lambda_i}\right| \notin \mathbb{Z}$ *for some* $1 \leq j \leq 3, j \neq i$.
3. $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$ *does not contain primitive cubic roots of unity.*

Proof. We define $\alpha_i := \frac{q(\lambda_i)}{P'(\lambda_i)}\lambda_i^n$. Then, an integer n is a Twisted Integral Zero of (x_n) if $\sum_{i=1}^{3} \xi_i \alpha_i = 0$ for some roots of unity ξ_1, ξ_2, ξ_3.

Suppose that $\mathbb{Q}(\lambda_i)$ is not Galois for some $1 \leq i \leq 3$. Clearly, $\alpha_i \in \mathbb{Q}(\lambda_i)$. If $\mathbb{Q}(\alpha_i) \neq \mathbb{Q}(\lambda_i)$, then $\alpha_i \in \mathbb{Q}$ since $[\mathbb{Q}(\lambda_i) : \mathbb{Q}] = 3$. Since $\mathbb{Q}(\lambda_i)$ is not Galois, we have $\mathrm{Gal}(\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)/\mathbb{Q})$ is isomorphic to the symmetric group S_3. For $\sigma = (i, j) \in S_3$, we have $\sigma(\alpha_i) = \alpha_j$. Since σ fixes $\alpha_i \in \mathbb{Q}$, we have

$$\frac{q(\lambda_i)}{P'(\lambda_i)}\lambda_i^n = \frac{q(\lambda_j)}{P'(\lambda_j)}\lambda_j^n$$

which yields

$$n = \log\left|\frac{q(\lambda_i)P'(\lambda_j)}{q(\lambda_j)P'(\lambda_i)}\right| / \log\left|\frac{\lambda_j}{\lambda_i}\right| \notin \mathbb{Z},$$

and this gives a contradiction. Therefore, $\mathbb{Q}(\alpha_i)$ is equal to $\mathbb{Q}(\lambda_i)$ which shows that $\mathbb{Q}(\alpha_i)$ is not Galois. Also, since $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subset \mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$, by condition (3), $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ does not contain primitive cubic roots of unity. Therefore, by Lemma 6.6, we have

$$\sum_{i=1}^{3} \xi_i \alpha_i = 0 \text{ implies } \sum_{i=1}^{3} \alpha_i = 0.$$

Hence, n has to be a zero of (x_n). ■

We give some examples as applications of Theorem 6.7.

Example 6.3.1. *The Tribonacci sequence is defined as*

$$x_n = x_{n-1} + x_{n-2} + x_{n-3}, x_0 = 0, x_1 = x_2 = 1.$$

In [2], Bilu et al. proved that the set of Twisted Integral Zeros of (x_n) *is equal to* $\{0, -1, -4, -17\}$ *which is also the set of zeros of the sequence.*

Example 6.3.2. *The Tripell sequence is defined as*

$$x_n = 2x_{n-1} + x_{n-2} + x_{n-3}, x_0 = 0, x_1 = 1, x_2 = 2.$$

Let λ_1 *be the real root of the characteristic polynomial* $P(x) = x^3 - 2x^2 - x - 1$. *We have,* $\mathbb{Q}(\lambda_1)$ *is not Galois. Here* $q(x) = x$. *The condition* (2) *of Theorem 6.7 reduces to*

$$\log|\frac{q(\lambda_i)P'(\lambda_j)}{q(\lambda_j)P'(\lambda_i)}|/\log|\frac{\lambda_j}{\lambda_i}| \approx 0.668 \notin \mathbb{Z}.$$

Now, to show that $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$ *does not contain primitive cubic roots of unity, observe that* $P(x) = x^3 - 2x^2 - x - 1 \equiv (x+25)(x+27)(x+28) \pmod{41}$. *Therefore, by Hensel's lemma,* $P(x)$ *has three distinct roots, say,* $\lambda_1', \lambda_2', \lambda_3'$ *in* $\mathbb{Q}_{41}$ *i.e,* $\mathbb{Q}(\lambda_1', \lambda_2', \lambda_3') \subset \mathbb{Q}_{41}$ *but* $x^3 - 1$ *does not split modulo* 41. *Hence,* $\mathbb{Q}_{41}$ *does not contain primitive cubic roots of unity. Therefore,* $\mathbb{Q}(\lambda_1', \lambda_2', \lambda_3')$ *does not contain primitive cubic roots of unity. Since* $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$ *is isomorphic to* $\mathbb{Q}(\lambda_1', \lambda_2', \lambda_3')$, $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$ *does not contain primitive cubic roots of unity. Also, the Tripell sequence satisfies the equation* (6.3). *Hence, the set of Twisted Integral Zeros of* (x_n) *is equal to the set of zeros of* $(x_n) = \{-1, 0\}$. *The set of zeros is calculated by using Skolem tool [1].*

Example 6.3.3. *A slightly modified Tripell sequence is defined as*

$$x_n = 2x_{n-1} + 2x_{n-2} + x_{n-3}, x_0 = 0, x_1 = 1, x_2 = 2.$$

Let λ_1 be the real root of the characteristic polynomial $P(x) = x^3 - 2x^2 - 2x - 1$. We have, $\mathbb{Q}(\lambda_1)$ is not Galois. Here $q(x) = x$. The condition (2) of Theorem 6.7 reduces to

$$\log|\frac{q(\lambda_i)P'(\lambda_j)}{q(\lambda_j)P'(\lambda_i)}|/\log|\frac{\lambda_j}{\lambda_i}| \approx 0.861 \notin \mathbb{Z}.$$

Since $P(x) \equiv (x+19)(x+30)(x+31) \pmod{41}$, following the same argument as given in Example 6.3.2, we find that $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$ does not contain primitive cubic roots of unity. Hence, by Theorem 6.7, the set of Twisted Integral Zeros of (x_n) is equal to the set of zeros of $(x_n) = \{-1, 0\}$. We again calculate the zeros of (x_n) by using Skolem tool [1].

Using the above results, we run a program for primes upto 1000 for the recurrence sequences defined in Examples 6.3.2 and 6.3.3 respectively, and obtain the following.

Theorem 6.8. *(1) For the Tripell sequence as defined in Example 6.3.2, Conjecture 6.1 fails for*

$$p \in [5, 1000]\backslash\{5, 19, 29, 41, 103, 137, 151, 191, 283, 397, 487, 491, 571, 709, 773, 787, 877, 883, 971, 983\}$$

and Conjecture 6.1 holds for

$$p \in \{103, 137, 191, 397, 487, 491, 709, 773, 787, 883, 971, 983\}$$

in the form

$$\nu_p(x_n) = \begin{cases} \nu_p(n+c)+1, & \text{if } n \equiv -c \pmod{Q_p}, -c \in \{0,-1\}; \\ 0, & \text{otherwise}, \end{cases}$$

where Q_p is given below.

p	103	137	191	397	487	491	709	773	787	883	971	983
Q_p	102	136	95	198	486	245	708	772	262	882	970	491

(2) For the modified Tripell sequence as defined in Example 6.3.3, Conjecture 6.1 fails for

$$p \in [5, 1000] \backslash \{5, 7, 23, 41, 83, 131, 193, 227, 293, 397, 401, 659, 701, 787, 983\}$$

and Conjecture 6.1 holds for

$$p \in \{5, 23, 41, 131, 193, 227, 293, 401, 659, 701, 787, 983\}$$

in the form

$$\nu_p(x_n) = \begin{cases} \nu_p(n+c)+1, & \text{if } n \equiv -c \pmod{Q_p}, -c \in \{0,-1\}; \\ 0, & \text{otherwise}, \end{cases}$$

where Q_p is given below.

p	5	23	41	131	193	227	293	401	659	701	787	983
Q_p	8	22	40	130	192	113	292	400	658	350	786	982

Proof. In view of Theorem 6.7, we obtain $\mathcal{Z} = \{-1, 0\}$ for the Tripell and modified Tripell sequences. For both the sequences, we run a Python program for primes $p \leq 1000$ and search for ℓ which satisfy the conditions of Theorem 6.3. This gives primes for which the conjecture fails. Similarly, by running a Python program for primes $p \leq 1000$, we check the conditions of Theorem 6.5 and obtain primes for which the conjecture is true. In the cases where the conjecture holds, the p-adic valuation can be calculated and the proof follows similar to the proof of Theorem 1.7 in [2, Theorem 1.7]. ■

6.4 The Diophantine equation $x_n = m!$

To illustrate an application of p-adic valuation, we begin by explicitly calculating the 2-adic valuation of the modified Tripell sequence, as defined in Example 6.3.3.

Theorem 6.9. *Let (x_n) be the modified Tripell sequence. For $n \geq 1$, we have*

$$\nu_2(x_n) = \begin{cases} 0, & \text{if } n \equiv 1,4 \pmod 6, \\ 1, & \text{if } n \equiv 2,3 \pmod 6, \\ 2 + \nu_2(n), & \text{if } n \equiv 0 \pmod 6, \\ 3 + \nu_2(n+1), & \text{if } n \equiv 5 \pmod 6. \end{cases}$$

Proof. The period of the sequence modulo 2^2 is $N_{2^2} = 6$. It can be calculated that $\nu_2(x_n)$ is constant 0 for $n \equiv 1,4$ modulo 6 and is constant 1 for $n \equiv 2,3$ modulo 6. Now, we consider $f_\ell(x)$ for $\ell = 0$ and -1.

For $n \equiv \ell \pmod 6$, $x_n = f_\ell(x)$ where $x = \frac{n-\ell}{6}$. Define

$$g_\ell(x) = \frac{f_\ell(x)}{2^2} = \sum_{k=0}^{\infty} \beta_k x^k,$$

where

$$\beta_k = \frac{f_\ell^k(0)}{2^2 k!} = \frac{\sum_{i=1}^{3} c_{\lambda_i} \lambda_i^\ell (\log_p(\lambda_i^6))^k}{2^2 k!} = \frac{2^{2(k-1)}}{k!} \sum_{i=1}^{3} c_{\lambda_i} \lambda_i^\ell \left(\frac{\log_p(\lambda_i^6)}{2^2} \right)^k, \tag{6.5}$$

where $\sum_{i=1}^{3} c_{\lambda_i}\lambda_i^{\ell}\left(\frac{\log_p(\lambda_i^6)}{2^2}\right)^k \in \mathbb{Z}_2$. We have $\beta_0 = 0$ for $\ell = 0, -1$ and

$$\begin{aligned}\beta_1 &= \frac{f_\ell'(0)}{2^2} = \frac{\sum_{i=1}^{3} c_{\lambda_i}\lambda_i^{\ell}\log_p(\lambda_i^6)}{2^2}\\ &\equiv \frac{1}{2^2}\sum_{i=1}^{3} c_{\lambda_i}{\lambda_i}^{\ell}\left(\lambda_i^6 - 1 - \frac{(\lambda_i^6-1)^2}{2}\right) \pmod{2^4}\\ &\equiv \frac{1}{2^2}\left(x_{\ell+6} - x_\ell - \frac{(x_{\ell+2\times 6} - 2x_{\ell+6} + x_\ell)}{2}\right) \pmod{2^4}.\end{aligned}$$

It can be calculated that for $\ell = 0$, $\beta_1 \equiv 2 \pmod{2^4}$. Hence, $\nu_2(\beta_1) = 1$. Similarly, for $\ell = -1$, we have $\beta_1 \equiv 4 \pmod{2^4}$. Hence, $\nu_2(\beta_1) = 2$.

Now,

$$\beta_2 \equiv \frac{1}{2^2}\left(x_{\ell+2\times 6} - 2x_{\ell+6} + x_\ell\right) \equiv 0 \pmod{2^3}$$

for both $\ell = 0$ and $\ell = -1$. Also, we have

$$\beta_3 \equiv \frac{1}{2^2\times 3!}\left(x_{\ell+3\times 6} - 3x_{\ell+2\times 6} - x_\ell + 3x_{\ell+6}\right) \equiv 0 \pmod{2^3}$$

for $\ell = -1$. Moreover, by equation (6.5), we obtain

$$\nu_2(\beta_k) \geq \nu_2\left(\frac{2^{2(k-1)}}{k!}\right) = 2(k-1) - \nu_2(k!) > 2(k-1) - k = k-2.$$

Therefore, $\nu_2(\beta_k) > 1$ for $k \geq 3$ and $\nu_2(\beta_k) > 2$ for $k \geq 4$. Hence, for $\ell = 0$, we have

$$\begin{aligned}\nu_2(x_n) = \nu_2(f_0(x)) &= \nu_2\left(2^2\left(\sum_{k\geq 0}\beta_k x^k\right)\right)\\ &= \nu_2(2^2\beta_1 x)\\ &= 3 + \nu_2\left(\frac{n}{6}\right)\\ &= 2 + \nu_2(n).\end{aligned}$$

Similarly, $\nu_2(x_n) = 3 + \nu_2(n+1)$ for $\ell = -1$. This completes the proof of the theorem. ■

We state a lemma which gives bounds for the p-adic valuation of $m!$ for any positive integer m.

Lemma 6.10. [4, Lemma 2.1] *For any integer $m \geq 1$ and prime p, we have*

$$\frac{m}{p-1} - \left\lfloor \frac{\log m}{\log p} \right\rfloor - 1 \leq \nu_p(m!) \leq \frac{m-1}{p-1},$$

where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x.

Theorem 6.11. *For the linear recurrence sequence defined as $x_n = 2x_{n-1} + 2x_{n-2} + x_{n-3}, x_0 = 0, x_1 = 1, x_2 = 2$, the only solutions of the Diophantine equation $x_n = m!$ in positive integers n, m are $(n, m) \in \{(1,1), (2,2), (3,3)\}$.*

Next, we prove a lemma which will be used in the proof of Theorem 6.11.

Lemma 6.12. *Let (x_n) be a linear recurrence sequence defined by $x_n = ax_{n-1} + bx_{n-2} + cx_{n-3}, a, b, c > 0$ such that the characteristic polynomial has a real root $\gamma > 1$. Suppose that the initial values of the sequence satisfy the condition*

$$\gamma^{-1} \leq x_1 \leq \gamma^0 \leq x_2 \leq \gamma^1 \leq x_3 \leq \gamma^2.$$

Then we have, for $n \geq 1$,

$$\gamma^{n-2} \leq x_n \leq \gamma^{n-1}.$$

Proof. We prove the lemma using induction on n. The result holds for $n = 1, 2, 3$ by the hypothesis. Let $n \geq 4$. Suppose that $\gamma^{m-2} \leq x_m \leq \gamma^{m-1}$ holds for all m where $3 \leq m \leq n-1$. Then,

$$a\gamma^{m-2} + b\gamma^{m-3} + c\gamma^{m-4} \leq ax_m + bx_{m-1} + cx_{m-2} \leq a\gamma^{m-1} + b\gamma^{m-2} + c\gamma^{m-3}$$

which implies

$$\gamma^{m-4}(a\gamma^2 + b\gamma + c) \leq x_{m+1} \leq \gamma^{m-3}(a\gamma^2 + b\gamma + c). \tag{6.6}$$

Since γ is a root of the polynomial $x^3 - ax^2 - bx - c$, so (6.6) gives

$$\gamma^{m-1} \leq x_{m+1} \leq \gamma^m.$$

This completes the proof. ■

Having Lemma 6.12 showed, we are ready to prove Theorem 6.11.

Proof of Theorem 6.11. Suppose that $x_n = m!$ for some positive integers n and m. For $m \leq 5$, it can be checked that the only solutions are $(n, m) \in \{(1, 1), (2, 2), (3, 3)\}$. By Theorem 6.9, we have $\nu_2(x_n) = \nu_2(m!) \leq 3 + \max\{\nu_2(n), \nu_2(n+1)\}$. By Lemma 6.10, we have

$$m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 1 \leq \nu_2(m!) \leq 3 + 2\max\{\nu_2(n), \nu_2(n+1),$$

which yields

$$\frac{m}{2} - \frac{\log m}{2\log 2} - \frac{5}{2} \leq \max\{\nu_2(n), \nu_2(n+1)\}.$$

Therefore,

$$2^{\frac{m}{2} - \frac{\log m}{2\log 2} - \frac{5}{2}} \leq 2^{\max\{\nu_2(n), \nu_2(n+1)\}} \leq n + 1,$$

and hence

$$\frac{m}{2} - \frac{\log m}{2\log 2} - \frac{5}{2} \leq \frac{\log(n+1)}{\log 2}. \tag{6.7}$$

By Lemma 6.12, since $\gamma \approx 2.83$ is a root which satisfies the conditions of Lemma

6.12, we have $2.83^{n-2} \leq x_n = m! < \left(\frac{m}{2}\right)^m$, for $m > 5$ which gives

$$(n-2)\log(2.83) < m \log \frac{m}{2}.$$

Hence,

$$n < \frac{m \log \frac{m}{2}}{\log 2.83} + 2.$$

Inserting this bound in equation (6.7), we get

$$\frac{m}{2} - \frac{\log m}{2\log 2} - \frac{5}{2} \leq \frac{\log\left(\frac{m \log \frac{m}{2}}{\log 2.83} + 2 + 1\right)}{\log 2}$$

which gives, $m \leq 21$ and hence $n < 52$. By a computational search, it can be checked that $\{(1,1),(2,2),(3,3)\}$ are the only solutions. ■

In [44, Theorem 2], Sobolewski examined the Diophantine equation $\prod_{i=1}^{d} x_{n_i} = m!$ for a general linear recurrence sequence (x_n). He observed some properties for (x_n) which guarantees that the equation has only finitely many solutions in positive integers $m, n_1, \ldots, n_d$. In the following theorem, we demonstrate that the Diophantine equation $x_n = m!$, with (x_n) satisfying a certain third order linear recurrence, has only finitely many solutions if there exist a prime p for which Conjecture 6.1 holds.

Theorem 6.13. *Let (x_n) be a linear recurrence sequence defined by $x_n = ax_{n-1} + bx_{n-2} + cx_{n-3}$, with initial values x_0, x_1, x_2 not all zeroes such that the characteristic polynomial has a root γ with $|\gamma| > 1$. If there exists a prime p for which Conjecture 6.1 holds for (x_n), then the Diophantine equation $x_n = m!$ has finitely many solutions in positive integers (n, m) and the solutions can be effectively computed when the form of Conjecture 6.1 is explicitly known.*

We state a theorem which will be used in the proof of Theorem 6.13.

Theorem 6.14. [15, Theorem 2.4] *For any integer non-degenerate linear recurrence sequence a of order n with $r \leq 3$ dominating characteristic roots (roots of the characteristic polynomial with maximum absolute value),*

$$|a(x)| \geq |\alpha_1|^x x^{-k(a)}, x \geq c(a)$$

where $k(a)$ and $c(a)$ are effective constants depending on the sequence and α_1 is a dominating characteristic root.

Proof of Theorem 6.13. Suppose that $x_n = m!$ for some positive integers n and m. If Conjecture 6.1 holds for p, there exists Q such that for $i \in \{0, 1, \ldots, Q-1\}$, either $\nu_p(x_n) = \kappa_i + \mu_i(\nu_p(n - a_i))$ i.e, (L) holds or $\nu_p(x_n) = \kappa_i$ i.e, (C) holds for $n \equiv i \pmod{Q}$ except for finitely many n. Suppose that $\kappa = \max_i\{|\kappa_i|\}$. Define $L = \mu \max_i\{\nu_p(n - a_i)\}$ where $\mu = \max_i\{\mu_i\}$ if the set of i such that (L) holds is nonempty and $L = 0$ otherwise. Then,

$$\nu_p(x_n) = \nu_p(m!) \leq \kappa + L.$$

By Lemma 6.10,

$$\frac{m}{p-1} - \left\lfloor \frac{\log m}{\log p} \right\rfloor - 1 \leq \nu_p(m!) \leq \kappa + \mu \max_i\{\nu_p(n - a_i)\}, \text{ when } L \neq 0$$

and

$$\frac{m}{p-1} - \left\lfloor \frac{\log m}{\log p} \right\rfloor - 1 \leq \nu_p(m!) \leq \kappa, \text{ when } L = 0.$$

For $L \neq 0$, we have

$$\frac{m}{\mu(p-1)} - \left\lfloor \frac{\log m}{\log p} \right\rfloor \frac{1}{\mu} - \frac{1+\kappa}{\mu} \leq \max_i\{\nu_p(n - a_i)\}.$$

Therefore,

$$p^{\frac{m}{\mu(p-1)}-\left\lfloor\frac{\log m}{\log p}\right\rfloor\frac{1}{\mu}-\frac{1+\kappa}{\mu}} \leq p^{\max_i\{\nu_p(n-a_i)\}} \leq n+a, \text{ where } a = |\max_i\{-a_i\}|$$

which gives

$$\frac{m}{\mu(p-1)} - \left\lfloor\frac{\log m}{\log p}\right\rfloor\frac{1}{\mu} - \frac{1+\kappa}{\mu} \leq \frac{\log(n+a)}{\log p}, \text{ where } a = |\max_i\{-a_i\}|. \tag{6.8}$$

By Theorem 6.14,

$$|\gamma|^n n^{-k(x)} \leq |x_n| \text{ for } n > c(x) \tag{6.9}$$

where x denotes the sequence (x_n) and γ is a dominating characteristic root such that $|\gamma| > 1$. From inequality (6.9), we can calculate a bound for values of n for which $x_n = m!$ for $m \leq 5$. Suppose that $m > 5$. We have

$$\frac{|\gamma|^n}{n^{k(x)}} \leq |x_n| = x_n = m! < \left(\frac{m}{2}\right)^m$$

which gives

$$n\log|\gamma| - k(x)\log n < m\log\frac{m}{2}. \tag{6.10}$$

Combining (6.8) and (6.10), we get an effective bound for m and n. Similarly, it can be shown that m and n are bounded effectively in the case when $L = 0$ as well. This completes the proof. ■

6.5 An Example

In [2], Bilu et al. studied Conjecture 6.1 for Tribonacci sequences, and they showed that the conjecture fails for a specific infinite set of primes of relative density

1/12. Following the same approach, we now give an example of a set of third order linear recurrence sequences for which Conjecture 6.1 does not hold.

Example 6.5.1. *Consider linear recurrence sequences defined as*

$$x_n = 3x_{n-1} + ax_{n-2} + x_{n-3}, x_0 = 0, x_1 = 1, x_2 = 3,$$

where $a \in \mathbb{Z}$ *is such that the characterisitic polynomial* $P(x) = x^3 - 3x^2 - ax - 1$ *is irreducible over* $\mathbb{Q}$ *and has a root* $\lambda \in \mathbb{C}$ *such that* $\frac{\lambda}{P'(\lambda)^3} \notin \mathbb{R}$. *It can be shown that Conjecture 6.1 fails for an infinite set of primes with relative density* $1/12$. *Suppose that* $\Lambda = \{\lambda_1, \lambda_2, \lambda_3\}$ *is the set of roots of* P *in some extension of* $\mathbb{Q}_p$ *where* λ_2 *and* λ_3 *are complex conjugates. Now, consider primes* $p \equiv 2 \pmod 3$ *for which* $\Lambda \subset \mathbb{Q}_p$ *and* p *does not divide the discriminant of* $P(x)$. *By the Chebotarev density theorem and Dirichlet's theorem, we obtain that such primes have relative density* $1/12$. *We have,* $f_\ell(m) = x_{\ell+mN}$ *for* $m \in \mathbb{Z}_{\geq 0}$, *where* $N = N_p$ *and* $\ell \in \{0, 1, \ldots, N-1\}$. *Consider the function*

$$\begin{aligned} F(x, y, z) &= x^3 + y^3 + z^3 - 3xyz \\ &= (x + y + z)(x + \zeta y + \overline{\zeta} z)(x + \overline{\zeta} y + \zeta z), \end{aligned}$$

where ζ *and* $\overline{\zeta}$ *are primitive cube roots of unity. Since* $p \equiv 2 \pmod 3$, $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$ *does not contain any primitive cube roots of unity. Moreover, every element of* $\mathbb{Z}_p^\times$ *has only a single cube root in* $\mathbb{Z}_p$. *Let* $\alpha_i = c_i\lambda_i^{-2/3}$, *where* $\lambda_i^{1/3}$ *is the cube root of* $\lambda_i \in \mathbb{Z}_p$. *Since* $\lambda_1 + \lambda_2 + \lambda_3 = 3$, *we have,*

$$F(\alpha_1, \alpha_2, \alpha_3) = \frac{-3 + \lambda_1 + \lambda_2 + \lambda_3}{(\lambda_1 - \lambda_2)^2(\lambda_2 - \lambda_3)^2(\lambda_1 - \lambda_3)^2} = 0.$$

Therefore, one of the following holds.

$$c_1\lambda_1^{-2/3} + c_2\lambda_2^{-2/3} + c_3\lambda_3^{-2/3} = 0, \tag{6.11}$$

$$c_1\lambda_1^{-2/3} + \zeta c_2\lambda_2^{-2/3} + \overline{\zeta} c_3\lambda_3^{-2/3} = 0, \tag{6.12}$$

$$c_1\lambda_1^{-2/3} + \overline{\zeta} c_2\lambda_2^{-2/3} + \zeta c_3\lambda_3^{-2/3} = 0. \tag{6.13}$$

If (6.12) *holds, then applying* $\sigma \in Gal(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ *where* $\sigma(\zeta) = \overline{\zeta}$, *we obtain* (6.13). *Hence, we get* $(\zeta - \overline{\zeta})(c_2\lambda_2^{-2/3} - c_3\lambda_3^{-2/3}) = 0$, *which yields* $\frac{\lambda_2}{P'(\lambda_2)^3} = \frac{\lambda_3}{P'(\lambda_3)^3}$. *This is not possible since* $\lambda/P'(\lambda)^3 \notin \mathbb{R}$. *Therefore, we have,* $c_1\lambda_1^{-2/3} + c_2\lambda_2^{-2/3} + c_3\lambda_3^{-2/3} = 0$. *Now, let* ℓ *be such that* $-2/3 \equiv \ell \pmod{N}$. *Then, there exists* $b \in \mathbb{Z}_p \cap \mathbb{Q}$ *such that* $\frac{-2}{3} = \ell + bN$. *Similar to the proof of Theorem 1.5 in [2], we can show that* $f_\ell(b) = 0$. *Consider* $n \in \mathbb{Z}_{\geq 0}$ *such that* $n \equiv -2/3 \pmod{p-1}$. *Then,* $n \equiv \ell \equiv -2/3 \pmod{N}$. *Therefore,* $n = \ell + Nm$ *for* $m \in \mathbb{Z}_{\geq 0}$. *Since* $f_\ell(b) = 0$, *we have*

$$\nu_p(x(n)) = \nu_p(f_\ell(m)) = \nu_p(f_\ell(m) - f_\ell(b)).$$

By Proposition 3.1 *in [2], we have*

$$\nu_p(f_\ell(m) - f_\ell(b)) \geq \nu_p(m - b) = \nu_p(n + 2/3).$$

Therefore, for $n \in \mathbb{Z}_{\geq 0}$, $n \equiv -2/3 \pmod{p-1}$, *we have* $\nu_p(x_n) \geq \nu_p(n + \frac{2}{3})$. *Let* (n_k) *be a sequence of positive integers satisfying* $n_k \equiv -2/3 \pmod{(p-1)p^k}$. *If Conjecture 6.1 is true for* p, *then for some* $i \in \{0, \dots, Q-1\}$, *the residue class* $i \pmod{Q}$ *contains infinitely many* n_k. *Since* $\nu_p(n_k + 2/3) \to \infty$, *we have* $\nu_p(x(n)) \to \infty$. *Hence, for this* i *we must have option* (L) *of Conjecture 6.1 i.e,* $\nu_p(x_{n_k}) = \kappa_i + \mu_i\nu_p(n_k - a_i)$ *for some* $a_i \in \mathbb{Z}$. *Therefore* $\nu_p(n_k - a_i) \to \infty$. *But we also have that* $\nu_p(n_k + 2/3) \to \infty$ *which gives a contradiction since* $a_i \neq -2/3$.

Note that, in Example 6.5.1, for almost all positive integers a, $P(x)$ has 3 real roots, providing a method that mostly works for negative a. One could consider flipping the sign of a.

Remark 6.5.1. *In [2, Theorem 1.8], it was shown that the conjecture can be partially, but not completely, rescued by allowing rational twisted zeros in addition to integral twisted zeros. It would be interesting to explore the same for the Tripell and modified Tripell sequence. Also, in view of Theorem 6.13, it would be interesting to know, given any third order linear recurrence sequence, does there exist a prime p for which the conjecture holds?*

7
Direction Sets

7.1 Introduction

Very recently, Leonetti and Sanna [30] introduced the notion of *direction sets*, which generalizes the notion of ratio sets in $\mathbb{R}_{\geq 0}$. For an integer $k \geq 2$ and $\emptyset \neq A \subseteq \mathbb{N}$, they considered the following sets:

$$\mathcal{S}^{k-1} := \{\underline{x} \in [0,1]^k : ||\underline{x}|| = 1\}, \ \mathcal{D}^k(A) := \{\rho(\underline{a}) : \underline{a} \in A^k\}$$

[1]The contents of this chapter have been published in *Integers* 22 (2022).

and

$$\mathcal{D}^{\underline{k}}(A) := \{\rho(\underline{a}) : \underline{a} \in A^{\underline{k}}\},$$

where $\rho : \mathbb{R}^k \setminus \{\underline{0}\} \to \mathcal{S}^{k-1}$ is the map defined by $\rho(\underline{x}) = \frac{\underline{x}}{||\underline{x}||}$ and $A^{\underline{k}} = \{\underline{a} \in A^k : a_i \neq a_j \text{ for all } i \neq j\}$. The sets $\mathcal{D}^k(A)$ and $\mathcal{D}^{\underline{k}}(A)$ are called the k-direction sets of A. We note that, for $k = 2$, we can identify $\mathcal{S}^1$ with $[0, +\infty]$ via a bijective map and thus the question of denseness in $\mathbb{R}_{>0}$ can be translated into that in $\mathcal{S}^1$. Therefore, direction sets are indeed generalizations of ratio sets. Leonetti and Sanna [30, Theorem 1.2] proved a necessary and sufficient criterion that determines whether a set $X \subseteq \mathcal{S}^{k-1}$ can be realized as the set of accumulation points of $\mathcal{D}^{\underline{k}}(A)$ for some $A \subseteq \mathbb{N}$. Moreover, they proved a sufficient condition (cf. [30, Theorem 1.5]) that asserts whether $\mathcal{D}^k(A)$ is dense in $\mathcal{S}^{k-1}$. In this chapter, we further generalize the notion of direction sets and introduce generalized k-direction sets as follows.

7.2 k-generalized direction set

Definition 7.1. *Let $k \geq 2$ be an integer and let $U_1, \ldots, U_k$ be non-empty subsets of $\mathbb{N}$. We define the k-generalized direction set for the k-tuple $(U_1, \ldots, U_k)$ to be $\mathcal{D}^k(U_1, \ldots, U_k) := \{\rho(u_1, \ldots, u_k) : u_j \in U_j \text{ for } j = 1, \ldots, k\}$. Also, we define the distinct k-generalized direction set to be $\mathcal{D}^{\underline{k}}(U_1, \ldots, U_k) := \{\rho(u_1, \ldots, u_k) : u_j \in U_j \text{ for } j = 1, \ldots, k \text{ and } u_i \neq u_j \text{ for all } i \neq j\}$.*

Our first theorem is an analogue of Theorem 1.2 of [30] for distinct k-generalized direction sets. For any set $X \subseteq \mathcal{S}^{k-1}$, we denote by X' the set of accumulation points of X. Also, we denote by S_k the symmetric group on k elements $\{1, \ldots, k\}$. For a permutation $\pi \in S_k$, we define $\pi(x_1, \ldots, x_k) := (x_{\pi(1)}, \ldots, x_{\pi(k)})$ for all $\underline{x} = (x_1, \ldots, x_k)$ in $\mathcal{S}^{k-1}$. Also, for any subset I of $\{1, \ldots, k\}$, we define $\rho_I(\underline{x}) := \rho(\underline{y})$ where $\underline{y} = (y_1, \ldots, y_k)$ is defined as $y_i := x_i$ if $i \in I$ and $y_i := 0$ if $i \notin I$. We say that I *meets* $\underline{x}$ if $x_i \neq 0$ for some $i \in I$.

Our theorem provides a necessary condition for a set $X \subseteq \mathcal{S}^{k-1}$ to be realized as the set of accumulation points of $\mathcal{D}^{\underline{k}}(U_1, \ldots, U_k)$. This indeed extends the necessary conditions of Theorem 1.2 of [30] when all the U_i's are equal. It would be interesting to investigate whether the necessary conditions of the following theorem are also sufficient. We state our first theorem as follows.

Theorem 7.1. *Let $k \geq 2$ be an integer. For subsets $U_1, \ldots, U_k$ of $\mathbb{N}$, let $X = \mathcal{D}^{\underline{k}}(U_1, \ldots, U_k)'$. Then, we have:*

(i) X is a closed subset of $\mathcal{S}^{k-1}$.

(ii) If $U_{i_1} = \cdots = U_{i_m}$ for some $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, k\}$, then for $\pi \in S_k$ with $\pi(j) = j$ for all $j \notin \{i_1, \ldots, i_m\}$, we have $\pi(\underline{x}) \in X$ for every $\underline{x} \in X$.

(iii) If $|U_i| \geq k$ for each $i \in \{1, \ldots, k\}$, then for every $I \subseteq \{1, \ldots, k\}$ that meets $\underline{x}$, we have $\rho_I(\underline{x}) \in X$.

Proof. Since X is the set of accumulation points of a subset of $\mathcal{S}^{k-1}$, we immediately conclude that X is closed and (i) is satisfied.

To prove (ii), let $U_{i_1} = \cdots = U_{i_m}$ for some $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, k\}$ and let $\underline{x} = (x_1, x_2, \ldots, x_k) \in X = \mathcal{D}^{\underline{k}}(U_1, \ldots, U_k)'$. Then there exists a sequence $\rho(\underline{a}^{(n)}) \in \mathcal{D}^{\underline{k}}(U_1, \ldots, U_k)$ converging to $\underline{x}$ such that $\rho(\underline{a}^{(n)}) \neq \underline{x}$ for infinitely many n, where $\underline{a}^{(n)} \in \prod_{i=1}^{k} U_i$. For $\pi \in S_k$ with $\pi(j) = j$ for all $j \notin \{i_1, \ldots i_m\}$, we consider $\underline{b}^{(n)} := \pi(\underline{a}^{(n)}) \in \prod_{i=1}^{k} U_i$. Then $\rho(\underline{b}^{(n)})$ converges to $\pi(\underline{x})$. Consequently, we have $\pi(\underline{x}) \in X$ for every $\underline{x} \in X$ and thus (ii) is satisfied.

Now, assume that I is a non-empty subset of $\{1, \ldots, k\}$ that meets $\underline{x}$. We can consider a subsequence of $\underline{a}^{(n)}$ such that each $a_i^{(n)}$ is non-decreasing for each $i \in \{1, \ldots, k\}$. If $j \in \{1, \ldots, k\} \setminus I$, then we can choose distinct $c_j \in U_j$ such that for sufficiently large positive integer n_0, a sequence $\underline{d}^{(n)} \in U_1 \times \cdots \times U_k$ with distinct coordinates can be defined for all $n \geq n_0$ with $d_i^{(n)} := a_i^{(n)}$ for $i \in I$ and $d_i^{(n)} := c_i$

for $i \notin I$. This choice is possible because of the assumption $|U_i| \geq k$ for each i. It then follows that $\rho(\underline{d}^{(n)})$ converges to $\rho_I(\underline{x})$. Thus (iii) holds. This completes the proof of Theorem 7.1. ■

We recall that for a non-empty set $A \subseteq \mathbb{N}$, the natural density of A is defined as $d(A) := \lim_{X\to\infty} \dfrac{\#\{n \in A : n \leq X\}}{X}$, provided the limit exists. The next theorem provides a sufficient condition for $\mathcal{D}^k(U_1, \ldots, U_k)$ to be dense in $\mathcal{S}^{k-1}$.

Theorem 7.2. *Let $k \geq 2$ be an integer and let $U_1, \ldots, U_k \subseteq \mathbb{N}$ be such that $d(U_i)$ exists and equals $\delta_i > 0$ for all $i = 1, \ldots, k$. Assume that $\bigcap_{i=1}^{k} U_i$ is an infinite set. Then $\mathcal{D}^k(U_1, \ldots, U_k)$ is dense in $\mathcal{S}^{k-1}$.*

Proof. Let $\underline{x} \in (x_1, \ldots, x_k) \in \mathcal{S}^{k-1}$ and let $I_i = (a_i, b_i)$ be open intervals such that $x_i \in I_i$ for each $i \in \{1, \ldots, k\}$. Then $\prod_{i=1}^{k}(a_i, b_i) \cap \mathcal{S}^{k-1}$ is a basic open set in $\mathcal{S}^{k-1}$ containing $\underline{x}$. For a real number $X > 1$, let $U_i(X) := \#\{u_i \in U_i | u_i \leq X\}$. By the hypothesis, we have that $\lim_{X\to\infty} \frac{U_i(X)}{X} = \delta_i > 0$. This implies that $U_i(X) = \delta_i X + o(X)$. Therefore,

$$\lim_{X\to\infty} \frac{U_i(a_i X)}{U_i(b_i X)} = \lim_{X\to\infty} \frac{\delta_i a_i X + o(a_i X)}{\delta_i b_i X + o(b_i X)} = \frac{a_i}{b_i} < 1.$$

Thus for every sufficiently large real number X, there exists $u_i \in U_i$ such that $a_i X < u_i \leq b_i X$. That is, $a_i < \frac{u_i}{X} \leq b_i$. Since $\bigcap_{i=1}^{k} U_i$ is an infinite set, we can choose a large enough element $u \in \bigcap_{i=1}^{k} U_i$ such that $a_i u < u_i \leq b_i u$ for all $i = 1, \ldots, k$. This, in turn, implies that $\frac{u_i}{u} \in (a_i, b_i)$. Using the fact that $\rho(\underline{\alpha}) = \frac{\underline{\alpha}}{\|\underline{\alpha}\|}$ is continuous function, we see that $\rho(u_1, \ldots, u_k) \in \prod_{i=1}^{k} I_i \cap \mathcal{S}^{k-1}$. In other words, $\mathcal{D}^k(U_1, \ldots, U_k)$ is dense in $\mathcal{S}^{k-1}$. ■

The next theorem extends Theorem 1.5 of [30], which asserts that if for a set $A \subseteq \mathbb{N}$, there exists an increasing sequence $\{a_n\}_{n=1}^{\infty} \subseteq A$ with $\lim_{n\to\infty} \dfrac{a_n}{a_{n+1}} = 1$, then

$\mathcal{D}^k(A)$ is dense in $\mathcal{S}^{k-1}$. We generalize this for $\mathcal{D}^k(U_1,\ldots,U_k)$ as follows.

Theorem 7.3. *Let $k \geq 2$ be an integer and let $U_1, U_2, \ldots, U_k$ be non-empty subsets of $\mathbb{N}$. If there exist increasing sequences $u_i^{(n)} \subseteq U_i$ for all $i \in \{1,\ldots,k\}$ such that $\lim_{n\to\infty} \frac{u_i^{(n-1)}}{u_i^{(n)}} = 1$, then $\mathcal{D}^k(U_1,\ldots,U_k)$ is dense in $\mathcal{S}^{k-1}$.*

Proof. Let $\underline{x} = (x_1,\ldots,x_k) \in \mathcal{S}^{k-1}$ with $x_i > 0$ for all $i \in \{1,\ldots,k\}$. We pick an integer m such that $m > \frac{u_i^{(1)}}{\min\{x_1,\ldots,x_k\}}$ for all $i \in \{1,\ldots,k\}$. By the choice of m, we have $\frac{u_i^{(1)}}{x_i} < m$. Since $u_i^{(n)}$ is an increasing sequence of positive integers, for each i, there exists a smallest integer m_i such that $\frac{u_i^{(m_i)}}{x_i} > m$. Therefore, for all $i \in \{1,\ldots,k\}$, there exist m_i such that $\frac{u_i^{(m_i-1)}}{x_i} \leq m < \frac{u_i^{(m_i)}}{x_i}$. That is, $x_i < \frac{u_i^{(m_i)}}{m} \leq \frac{u_i^{(m_i)}}{u_i^{(m_i-1)}} x_i$. Since $m_i \to \infty$ as $m \to \infty$, it follows that $\lim_{m\to\infty} \frac{u_i^{(m_i)}}{m} = x_i$. Consequently, $\frac{1}{m}\underline{u} = (\frac{1}{m}u_1^{(m_1)},\ldots,\frac{1}{m}u_k^{(m_k)})$ converges to $\underline{x}$. Since ρ is a continuous map, we conclude that $\rho(\underline{u}) = \rho(\frac{1}{m}\underline{u})$ converges to $\underline{x}$. Consequently, $\mathcal{D}^k(U_1,\ldots,U_k)$ is dense in $\mathcal{S}^{k-1}$. ■

Remark 7.2.1. *For an integer $k \geq 2$ and for each $i \in \{1,\ldots,k\}$, let a_i and m_i be integers with $\gcd(a_i, m_i) = 1$. Let $\mathbb{P}_{m_i} := \{p \in \mathbb{P} : p \equiv a_i \pmod{m_i}\}$. For $U_i = \mathbb{P}_{m_i}$, using Dirichlet's theorem for primes in arithmetic progressions, we see that the hypotheses of Theorem 7.3 are satisfied. Therefore, $\mathcal{D}^k(\mathbb{P}_{m_1},\ldots,\mathbb{P}_{m_k})$ is dense in $\mathcal{S}^{k-1}$.*

Theorem 7.4. *Let $k \geq 2$ be an integer. For each $i \in \{1,\ldots,k\}$, let $f_i(X_1,\ldots,X_m) \in \mathbb{Z}[X_1,\ldots,X_m]$ be polynomials of total degree d_i such that the sum of the coefficients of degree d_i terms is positive. Let $U_i := \{f_i(n_1,\ldots,n_m) | (n_1,\ldots,n_m) \in \mathbb{N}^m\} \cap \mathbb{N}$. Then $\mathcal{D}^k(U_1,\ldots,U_k)$ is dense in $\mathcal{S}^{k-1}$.*

Proof. For a fixed integer $i \in \{1,\ldots,k\}$, we consider the polynomial $g_i(X)$ obtained by replacing all the variables of g_i by the variable X. We get, $g_i(X) = a_{d_i}X^{d_i} + a_{d_i-1}X^{d_i-1} + \cdots + a_0 \in \mathbb{Z}[X]$. Since $a_{d_i} > 0$, we conclude that for a sufficiently large positive real number X, we have $g_i(X) > 0$. Let $B_i := \{g_i(n) | n \in \mathbb{N}\} \cap \mathbb{N}$. We have $\frac{g_i(X-1)}{g_i(X)} = \frac{a_{d_i}(X-1)^{d_i}+\cdots+a_0}{a_{d_i}X^{d_i}+\cdots+a_o}$ which tends to 1 as X tends to ∞. Also, since $g_i(X)$ is a polynomial in one variable, the sequence $\{g_i(n)\}_{n=1}^{\infty}$ is eventually increasing. Therefore, by using Theorem 7.3, we obtain that $\mathcal{D}^k(B_i)$ is dense in $\mathcal{S}^{k-1}$. Since $B_i \subseteq U_i$, we conclude that $\mathcal{D}^k(U_1, \ldots, U_k)$ is dense in $\mathcal{S}^{k-1}$. ■

In [8], it is proven that there is a 3-partition of $\mathbb{N} = A \cup B \cup C$, such that none of $R(A), R(B)$ and $R(C)$ is dense in $\mathbb{R}_{>0}$. That is, none of $\mathcal{D}^2(A), \mathcal{D}^2(B)$ and $\mathcal{D}^2(C)$ is dense in $\mathcal{S}^1$. In [30], Leonetti and Sanna asked for a possible generalization of this result for $k \geq 3$ [30, Question 1.9]. We give a partial answer to their question in the next theorem.

Theorem 7.5. *Let $k \geq 3$ be an integer. Then there exists a 3-partition $\mathbb{N} = A \cup B \cup C$ of $\mathbb{N}$ such that none of $\mathcal{D}^k(A), \mathcal{D}^k(B)$ or $\mathcal{D}^k(C)$ is dense in $\mathcal{S}^{k-1}$.*

Proof. We consider the following three sets as in [8] (see also [5]).

$$A := \bigcup_{k=0}^{\infty} [5^k, 2 \cdot 5^k) \cap \mathbb{N},$$
$$B := \bigcup_{k=0}^{\infty} [2 \cdot 5^k, 3 \cdot 5^k) \cap \mathbb{N},$$
$$C := \bigcup_{k=0}^{\infty} [3 \cdot 5^k, 5 \cdot 5^k) \cap \mathbb{N}.$$

It is clear that A, B and C indeed give a partition of $\mathbb{N}$. If $\mathcal{D}^k(A)$, $\mathcal{D}^k(B)$ or $\mathcal{D}^k(C)$ is dense in $\mathcal{S}^{k-1}$, then by Theorem 1.4 of [30], which states that if $\mathcal{D}^k(A)$ is dense in $\mathcal{S}^{k-1}$ for some $A \subseteq \mathbb{N}$, then $\mathcal{D}^{k-1}(A)$ is dense in $\mathcal{S}^{k-2}$, we see inductively that $\mathcal{D}^2(A)$ (or $\mathcal{D}^2(B)$ or $\mathcal{D}^2(C)$) is dense in $\mathcal{S}^1$, which is false (cf. [5, Proposition 3]). Therefore, we get a 3-partition of $\mathbb{N}$ such that none of $\mathcal{D}^k(A)$, $\mathcal{D}^k(B)$ or $\mathcal{D}^k(C)$ is dense in $\mathcal{S}^{k-1}$. This completes the proof of Theorem 7.5. ■

Remark 7.2.2. *In view of Theorem 7.5, it remains to be seen whether for a 2-partition $\mathbb{N} = A \cup B$, either $\mathcal{D}^k(A)$ or $\mathcal{D}^k(B)$ is dense in $\mathcal{S}^{k-1}$ or not. We note* *that Theorem 7.3 cannot be directly applied to resolve this issue. In other words, we exhibit a 2-partition of* $\mathbb{N}$*, none of which contains a sequence with the ratio of consecutive terms converging to* 1*. This can be seen by considering* $A = \bigcup_{k=0}^{\infty}[3^k, 2\cdot 3^k)\cap\mathbb{N}$ *and* $B = \bigcup_{k=0}^{\infty}[2\cdot 3^k, 3^{k+1})\cap\mathbb{N}$*. For, if* $\{a_n\}_{n=1}^{\infty} \subseteq A$ *is an infinite sequence, then there are infinitely many indices* i *for which* $a_i \in [3^k, 2\cdot 3^k)$ *and* $a_{i+1} \in [3^\ell, 2\cdot 3^\ell)$ *for* $k < \ell$*. Then it follows that* $\frac{a_i}{a_{i+1}} < \frac{2\cdot 3^k}{3^\ell} \leq \frac{2}{3}$*. Therefore, the elements of the sequence* $\{\frac{a_n}{a_{n+1}}\}_{n=1}^{\infty}$ *cannot get arbitrarily close to* 1*. Similar argument works for* B *as well. This itself is an interesting question to decide whether* $\mathcal{D}^k(A)$ *or* $\mathcal{D}^k(B)$ *is dense in* $\mathcal{S}^{k-1}$*.*

One of the interesting questions in the literature of fractionally dense sets is to look for sets $A \subseteq \mathbb{N}$ such that the ratio set $R(A)$ is dense in $\mathbb{R}_{>0}$ but A contains no 3-term arithmetic progressions. One such set is $A = \{2^m : m \geq 2\} \cup \{3^n : n \geq 2\}$, which is known to be fractionally dense in $\mathbb{R}_{>0}$ but A contains no 3-term arithmetic progressions (cf. [5, Proposition 6]).

We shall see in the following theorem that we can obtain infinitely many sets $A \subseteq \mathbb{N}$ having no arithmetic progression of length 3 such that $\mathcal{D}^k(A)$ is dense in $\mathcal{S}^{k-1}$.

Theorem 7.6. *There exists a set* $A \subseteq \mathbb{N}$ *such that* A *contains no* 3*-term arithmetic progressions and* $\mathcal{D}^k(A)$ *is dense in* $\mathcal{S}^{k-1}$*.*

Proof. In [13], it has been proven that the equation $x^n + y^n = 2z^n$ has no non-trivial solution in $\mathbb{Z}$ if $n \geq 3$. In other words, the set $A := \{m^r : r, m \in \mathbb{Z}, r \geq 3\}$ does not contain any 3-term arithmetic progressions. Since for a fixed value of $r \geq 3$, we have $\frac{m^r}{(m+1)^r} \to 1$ as $m \to \infty$, by Theorem 1.5 of [30], we conclude that $\mathcal{D}^k(A)$ is dense in $\mathcal{S}^{k-1}$. ■

7.2.1 Examples of dense direction sets

We discuss the denseness of some particular type of sets whose properties have been recently considered in [17]. For an arithmetic function $f : \mathbb{N} \to \mathbb{N}$ and a positive real number X, let $f_X := \#\{n \leq X : n = kf(k) \text{ for some } k \in \mathbb{N}\}$. Keeping this notation, we state the results of [17] as follows.

Theorem 7.7. *[17] (i) Let* $\omega(n) = \sum_{\substack{p|n \\ p\in\mathbb{P}}} 1$ *be the prime divisor function. Then*

$$\omega_X = \frac{X}{\log\log X} + o\left(\frac{X}{\log\log X}\right).$$

(ii) Let $\phi(n) = \#\{1 \leq k \leq n : \gcd(k,n) = 1\}$ *be the Euler's totient function. Then*

$$\phi_X = cX^{\frac{1}{2}} + o(X^{\frac{1}{2}}),$$

where $c = \prod_p \left(1 + \frac{1}{p(p-1+\sqrt{p^2-p})}\right) \sim 1.365\ldots$.

Now, we state our result as follows.

Theorem 7.8. *Let* $A = \{n\omega(n) : n \in \mathbb{N}\}$ *and* $B = \{n\phi(n) : n \in \mathbb{N}\}$*. Then for any integer* $k \geq 2$*, we have that both* $\mathcal{D}^k(A)$ *and* $\mathcal{D}^k(B)$ *are dense in* $\mathcal{S}^{k-1}$*.*

Proof. Let $\underline{x} = (x_1, \ldots, x_k) \in \mathcal{S}^{k-1}$ and let $\prod_{i=1}^{k}(a_i, b_i)$ be a basic neighborhood of $\underline{x}$. Then by Theorem 7.7, we see that

$$\lim_{X\to\infty} \frac{\omega_{a_iX}}{\omega_{b_iX}} = \lim_{X\to\infty} \frac{a_iX}{\log\log a_iX} \cdot \frac{\log\log b_iX}{b_iX} = \frac{a_i}{b_i} < 1 \text{ for all } i \text{ with } 1 \leq i \leq k.$$

Therefore, for sufficiently large X, there exists $\alpha_i \in A$ such that $a_iX < \alpha_i < b_iX$ for all i. That is, $\left(\frac{\alpha_1}{X}, \ldots, \frac{\alpha_k}{X}\right) \in \prod_{i=1}^{k}(a_i, b_i)$. Hence $\rho(\alpha_1, \ldots, \alpha_k) = \rho\left(\frac{\alpha_1}{X}, \ldots, \frac{\alpha_k}{X}\right) \in \prod_{i=1}^{k}(a_i, b_i)$. Consequently, $\mathcal{D}^k(A)$ is dense in $\mathcal{S}^{k-1}$.

Similarly, for $\mathcal{D}^k(B)$, we note that

$$\lim_{X\to\infty} \frac{\phi_{a_i X}}{\phi_{b_i X}} = \frac{\sqrt{a_i}}{\sqrt{b_i}} < 1 \text{ for all } i \text{ with } 1 \le i \le k$$

and thereafter it follows a similar line of argument. ■

Remark 7.2.3. *It is interesting to extend the notion of direction sets in the set up of number fields and formulate analogous questions for the same. Let* $K \subsetneq \mathbb{R}$ *be a number field of degree* $d \ge 2$ *and let* $\mathcal{O}_K$ *be its ring of integers. Let* $\mathcal{O}_K^0 := \{\alpha \in \mathcal{O}_K : \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0\}$ *be the set of elements in* $\mathcal{O}_K$ *with trace* 0*. Since* $\mathcal{O}_K$ *is a free* $\mathbb{Z}$*-module of rank* d *and* Tr *is an additive group homomorphism from* $\mathcal{O}_K$ *to* $\mathbb{Z}$*, we see that* $\mathcal{O}_K \cong \mathcal{O}_K^0 \oplus \mathbb{Z}$*. In particular,* $\mathcal{O}_K^0$ *is a free* $\mathbb{Z}$*-module of rank* $d-1$*. Therefore,* $\mathcal{O}_K^0$ *itself is dense in* $\mathbb{R}$ *whenever* $d \ge 3$*. Also, for* $d = 2$*, we see that the ratio set of* $\mathcal{O}_K^0$ *is* $\mathbb{Q}$*. Consequently, the direction set of* $\mathcal{O}_K^0$ *is dense in* $\mathcal{S}^{k-1}$ *for any integer* $k \ge 2$*. We note that* $\mathcal{O}_K^0 \cap \mathbb{N} = \emptyset$*. In view of this, we ask the following question.*

Question 7.2.1. *Let* $d \ge 2$ *and* $k \ge 2$ *be integers and let* K *be a number field of degree* d*. Characterize the sets* $\mathcal{A} \subseteq \mathcal{O}_K$ *such that* $\mathcal{A} \cap \mathbb{N}$ *is finite and* $\mathcal{D}^{k-1}(\mathcal{A})$ *is dense in* $\mathcal{S}^{k-1}$*.*

Bibliography

[1] Y. F. Bilu, F. Luca, J. Nieuwveld, J. Ouaknine, D. Purser, and J. Worrell, The skolem tool, *https://skolem.mpi- sws.org* (2022) .

[2] Y. F. Bilu, F. Luca, J. Nieuwveld, J. Ouaknine, and J. Worrell, On the p-adic zeros of the Tribonacci sequence, *Math. Comp.* **93** no. 347, (2024) 1333–1353.

[3] Y. F. Bilu, F. Luca, J. Nieuwveld, J. Ouaknine, and J. Worrell, Twisted rational zeros of linear recurrence sequences, *preprint, https://arxiv.org/abs/2401.06537* (2024) .

[4] J. J. Bravo, M. Díaz, and J. L. Ramírez, The 2-adic and 3-adic valuation of the Tripell sequence and an application, *Turkish J. Math.* **44** no. 1, (2020) 131–141.

[5] B. Brown, M. Dairyko, S. R. Garcia, B. Lutz, and M. Someck, Four quotient set gems, *Amer. Math. Monthly* **121** no. 7, (2014) 590–599.

[6] A. Brumer, On the units of algebraic number fields, *Mathematika* **14** (1967) 121–124.

[7] J. Bukor and P. Csiba, On estimations of dispersion of ratio block sequences, *Math. Slovaca* **59** no. 3, (2009) 283–290.

[8] J. Bukor, P. Erdös, T. Šalát, and J. T. Tóth, Remarks on the $\mathbb{R}$-density of sets of numbers. ii, *Mathematica Slovaca* **47** (1997) 517–526.

[9] J. Bukor and J. T. Tóth, On accumulation points of ratio sets of positive integers, *Amer. Math. Monthly* **103** no. 6, (1996) 502–504.

[10] R. T. Bumby, A distribution property for linear recurrence of the second order, *Proc. Amer. Math. Soc.* **50** (1975) 101–106.

[11] J. W. S. Cassels, *Local fields*, vol. 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

[12] M. I. Cîrnu, Linear recurrence relations with the coefficients in progression, *Ann. Math. Inform.* **42** (2013) 119–127.

[13] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's last theorem, *J. Reine Angew. Math.* **490** (1997) 81–100.

[14] C. Donnay, S. R. Garcia, and J. Rouse, p-adic quotient sets II: Quadratic forms, *J. Number Theory* **201** (2019) 23–39.

[15] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence sequences*, vol. 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.

[16] C. Fuchs, C. Hutle, F. Luca, and L. Szalay, Diophantine triples and k-generalized Fibonacci sequences, *Bull. Malays. Math. Sci. Soc.* **41** no. 3, (2018) 1449–1465.

[17] M. R. Gabdullin, V. V. Iudelevich, and F. Luca, Numbers of the form $kf(k)$, *Int. J. Number Theory* **19** no. 5, (2023) 1191–1204.

[18] S. R. Garcia, Quotients of Gaussian primes, *Amer. Math. Monthly* **120** no. 9, (2013) 851–853.

[19] S. R. Garcia, Y. X. Hong, F. Luca, E. Pinsker, C. Sanna, E. Schechter, and A. Starr, p-adic quotient sets, *Acta Arith.* **179** no. 2, (2017) 163–184.

[20] S. R. Garcia and F. Luca, Quotients of Fibonacci numbers, *Amer. Math. Monthly* **123** no. 10, (2016) 1039–1044.

[21] S. R. Garcia, V. Selhorst-Jones, D. E. Poore, and N. Simon, Quotient sets and Diophantine equations, *Amer. Math. Monthly* **118** no. 8, (2011) 704–711.

[22] I. Gerst and J. Brillhart, On the prime divisors of polynomials, *Amer. Math. Monthly* **78** (1971) 250–266.

[23] F. Q. Gouvêa, *p-adic numbers: An introduction.* Universitext. Springer, Cham, third ed., 2020.

[24] D. R. Heath-Brown, Zeros of p-adic forms, *Proc. Lond. Math. Soc. (3)* **100** no. 2, (2010) 560–584.

[25] S. Hedman and D. Rose, Light subsets of $\mathbb{N}$ with dense quotient sets, *Amer. Math. Monthly* **116** no. 7, (2009) 635–641.

[26] D. Hobby and D. M. Silberger, Quotients of primes, *Amer. Math. Monthly* **100** no. 1, (1993) 50–52.

[27] D. B. Leep and C. C. Yeomans, Nonsingular zeros of quintic forms over finite fields, *Rocky Mountain J. Math.* **26** no. 3, (1996) 1043–1055.

[28] T. Lengyel, The order of the Fibonacci and Lucas numbers, *Fibonacci Quart.* **33** no. 3, (1995) 234–239.

[29] T. Lengyel and D. Marques, The 2-adic order of some generalized Fibonacci numbers, *Integers* **17** (2017) Paper No. A5, 10.

[30] P. Leonetti and C. Sanna, Directions sets: a generalisation of ratio sets, *Bull. Aust. Math. Soc.* **101** no. 3, (2020) 389–395.

[31] F. Luca, C. Pomerance, and v. Porubský, Sets with prescribed arithmetic densities, *Unif. Distrib. Theory* **3** no. 2, (2008) 67–80.

[32] D. Marques and T. Lengyel, The 2-adic order of the Tribonacci numbers and the equation $T_n = m!$, *J. Integer Seq.* **17** no. 10, (2014) Article 14.10.1, 8.

[33] A. Micholson, Quotients of primes in arithmetic progressions, *Notes Number Theory Discrete Math* **18** no. 2, (2012) 56–57.

[34] P. Miska, On p-adic valuations of Stirling numbers, *Acta Arith.* **186** no. 4, (2018) 337–348.

[35] P. Miska, A note on p-adic denseness of quotients of values of quadratic forms, *Indag. Math. (N.S.)* **32** no. 3, (2021) 639–645.

[36] P. Miska, N. Murru, and C. Sanna, On the p-adic denseness of the quotient set of a polynomial image, *J. Number Theory* **197** (2019) 218–227.

[37] L. Mišík, Sets of positive integers with prescribed values of densities, *Math. Slovaca* **52** no. 3, (2002) 289–296.

[38] P. A. B. Pleasants, Forms over p-adic fields, *Acta Arith.* **18** (1971) 289–296.

[39] E. A. Rawashdeh, A simple method for finding the inverse matrix of Vandermonde matrix, *Mat. Vesnik* **71** no. 3, (2019) 207–213.

[40] K. Rosen, *Discrete Mathematics and Its Applications.* McGraw-Hill Education, 2011.

[41] C. Sanna, The p-adic valuation of Lucas sequences, *Fibonacci Quart.* **54** no. 2, (2016) 118–124.

[42] C. Sanna, The quotient set of k-generalised Fibonacci numbers is dense in $\mathbb{Q}_p$, *Bull. Aust. Math. Soc.* **96** no. 1, (2017) 24–29.

[43] B. D. Sittinger, Quotients of primes in an algebraic number ring, *Notes Number Theory Discrete Math.* **24** no. 2, (June, 2018) 55–62.

[44] B. Sobolewski, The 2-adic valuation of generalized Fibonacci sequences with an application to certain Diophantine equations, *J. Number Theory* **180** (2017) 730–742.

[45] P. Starni, Answers to two questions concerning quotients of primes, *Amer. Math. Monthly* **102** no. 4, (1995) 347–349.

[46] O. Strauch and J. T. Tóth, Asymptotic density of $A \subset \mathbb{N}$ and density of the ratio set $R(A)$, *Acta Arith.* **87** no. 1, (1998) 67–78.

[47] Z.-H. Sun, Cubic and quartic congruences modulo a prime, *J. Number Theory* **102** no. 1, (2003) 41–89.

[48] T. Šalát, On ratio sets of sets of natural numbers, *Acta Arith.* **15** (1968/69) 273–278.

[49] T. Šalát, Corrigendum to the paper "On ratio sets of sets of natural numbers", *Acta Arith.* **16** (1969/70) 103.

[50] P. T. Young, 2-adic valuations of generalized Fibonacci numbers of odd order, *Integers* **18** (2018) Paper No. A1, 13.

Publications

Publications from Thesis work

1. D. Antony and R. Barman, *p-adic quotient sets: cubic forms*, Arch. Math. (Basel) 118 (2) (2022), 143–149.

2. D. Antony, R. Barman, and P. Miska, *p-adic quotient sets: diagonal forms*, Arch. Math. (Basel) 119 (5) (2022), 461–470.

3. D. Antony and R. Barman, *p-adic quotient sets: linear recurrence sequences*, Bull. Aust. Math. Soc. 108 (2023), 19–28.

4. D. Antony and R. Barman, *p-adic quotient sets: linear recurrence sequences with reducible characteristic polynomials*, Can. Math. Bull. 68 (2025), 177–186.

5. D. Antony and R. Barman, *On the p-adic valuation of third order linear recurrence sequences*, Results Math. 79 (2024), 14 pages.

6. D. Antony, R. Barman, and J. Chattopadhyay, *On denseness of certain direction and generalized direction sets*, Integers 22 (2022), Article No. 88.

7. D. Antony, R. Barman, and S. Gajović, *On p-adic denseness of quotient set of values of integral forms* (submitted).

8. D. Antony, R. Barman, and S. Gajović, *On p-adic denseness of quotient set of values of polynomials* (under preparation).