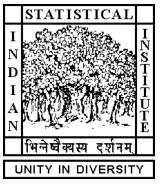
On Some Algebraic and Dynamical Aspects of Families of Polynomials

Prabhakar Ratipal Yadav



Indian Statistical Institute

November 2025

Indian Statistical Institute

Doctoral Thesis

On Some Algebraic and Dynamical Aspects of Families of Polynomials

Author:
Prabhakar Ratipal Yadav

Supervisor:
Shanta Laishram

A thesis submitted to the Indian Statistical Institute
in partial fulfilment of the requirements for
the degree of
Doctor of Philosophy (in Mathematics)

Theoretical Statistics & Mathematics Unit

Indian Statistical Institute, Delhi Centre

November 2025

Dedicated to My Family

Acknowledgements

I would start by thanking Prof. Shanta Laishram because this has been a joint venture and whatever knowledge I have of the subject, I owe it to him. Regular discussions, his calm response to the silliest of my mistakes, his valuable intuitions regarding almost anything I thought of, him working late hours on our work, keeping me involved in other academic activities, his sense of direction while writing a research paper, teaching style, stress upon clarity in understanding, and his giving me the freedom to think in my own way and encouraging collaboration with others have helped me grow as a student of Mathematics.

I express my sincere gratitude to Prof. Kotyada Srinivas for his invaluable guidance and the inspiring discussions that greatly enhanced my understanding. His ever-friendly way, along with his insightful perspectives, made my visits to IMSC, Chennai, truly memorable and productive. I also extend my gratitude to Dr. Anuj Jakhar, for his helpful discussions, brilliant suggestions for challenging problems, and unwavering support throughout my visit. I am deeply grateful for his reliable friendship, which provided invaluable support. I also express my sincere thanks to Dr. Sudhansu Sekhar Rout for all the helpful discussions and hospitality during my visit at NIT Calicut.

My family has always been with me through everything. I am lucky to have parents and Tauji, who has always stood beside me, took great care of me from the very beginning of life. Their efforts are beyond any expression. But a special thanks goes to my brother Vijay. It is him, whom I have always followed and who has silently paved my way to my goals. I am able to do the research with freedom because he is there to take care of the family related responsibilities. My heartfelt thanks to my beloved sister Rajani and sister-in-law Preeti for their incredible kindness and care, and my sweet little nieces, Ishaani and Ishita, for filling my stay at home with so much happiness.

I am truly fortunate to have received constant support from wonderful individuals throughout my academic journey. I thank each and every teacher who encouraged me to pursue Mathematics with passion. My heartfelt thanks go to Meenakshi Akka, who has stood by me since my Class 9 days and continued to support me through my undergraduate years, and to Sujit Anna, for always being there—not just as a friend, but as someone who kept encouraging me and helping me grow by constantly teaching me new skills beyond academics. I am deeply grateful to Indra Sir, Sanket Sir, Ajay Sir, and Mary Ma'am for always believing in my potential and motivating me to pursue research during my early academic years. A special thanks to Prof. Ananthnarayan Sir, who recognised my potential during Mini MTTS and has been a consistent source of inspiration in my journey towards research. I also wish to thank Arun Sir and Mukut Mani Sir,

whose guidance during my master's programme played a crucial role in strengthening my understanding and appreciation of Mathematics.

Life is incomplete without good friends and I've a long list of some of the best people who came across as friends. I am grateful to each of them. First and foremost, I want to thank Shivchand, Roshni and Diksha for being my lifeline—always in my support, believing in me, keeping my spirits high, and helping me become a better version of myself. Sayan and Deepak for your unique skill of blending hilarious, relentless trolling with genuinely insightful life lessons—that made my experience truly transformative and very special, along with PPG you guys made one of the finest memories at ISI Delhi. Vijaypal, Pankaj, Ismail, Ashish (friends for life), Suman (sweet sister), Saransh (the cool guy), Sourav, Saptak, Anirban, Deborshi, Praveen (the gang who kept me alive and happy), Himanshu, Sushil (the Manipur trio), Ravi (a joyful spirit and genuine soul), Saheli (sweet junior). A special thanks to Lalit Bhaiyya, an amazing person, a great cook whose guidance in academia and life has been a true blessing.

I would like to thank the Stat-Math faculty for taking care of the students' convenience. I feel gratitude towards the institute for giving me the opportunity to explore the subject without any inconvenience. A special thanks to the stat-math office staff for making all necessary arrangements whenever required. I also want to thank the thesis referees, whose careful reading and detailed comments have helped to improve the thesis.

Cheers!

Prabhakar Ratipal Yadav

21/11/2025

Contents

Chapter 1

Introduction

Polynomials play a central role in number theory, algebra, arithmetic dynamics and related areas due to their fundamental connection with field extensions, factorization, Diophantine problems, etc. It's algebraic properties like irreducibility, stability, Galois group, monogenity are well studied and there are a lot of interesting problems in the area. Although it is known that almost all the polynomials with integer coefficients are irreducible, proving it even for a certain families remains a challenging problem. In this thesis, we start by considering the irreducibility of a family of truncated binomial polynomials.

1.1 Irreducibility

A non-zero polynomial $f(x)$ with integer coefficients is defined as irreducible over $\mathbb{Z}$ if it is not possible to express it as the product of two non-constant polynomials with integer coefficients. We start this chapter by defining *truncated binomial polynomial*.

Definition 1.1.1. *For positive integers $n \geq m \geq 2$, the truncated binomial polynomial of degree m is defined to be the truncation of $(1+x)^n$ at m^{th} stage i.e.,*

$$P_{n,m}(x) := \sum_{j=0}^{m} \binom{n}{j} x^j = \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \cdots + \binom{n}{m} x^m.$$

In an investigation of the Schubert calculus on Grassmannians, Scherbak [90] proved and used the property that the roots of $P_{n,m}(x)$ are simple. Note that, for $n = m$, we have $P_{m,m}(x) = (1+x)^m$ which is clearly reducible and for $n = m+1$, we have $P_{m+1,m}(x) = (1+x)^{m+1} - x^{m+1}$, which is irreducible over $\mathbb{Q}$ iff $m+1$ is prime (by Eisenstein's criterion).

Theorem 1.1.2 (Eisenstein's Criterion)**.** *For a prime p, let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial such that p does not divide the leading coefficient a_n, $p^2 \nmid a_0$ and for all i in the range $0 \leq i < n$, $p \mid a_i$, then the polynomial $f(x)$ is irreducible over $\mathbb{Q}$. We sometimes call such a polynomial to be p-Eisenstein polynomial.*

In [35], Filaseta, Kumchev and Pasechnik considered the irreducibility of $P_{n,m}(x)$ over rationals. They computationally verified the irreducibility of $P_{n,m}(x)$ for integers n, m with $2 \leq m \leq n-2 \leq 98$ and conjectured that $P_{n,m}(x)$ is irreducible for all positive integers n, m satisfying $2 \leq m \leq n-2$.

For $m = 2$, the discriminant of $P_{n,m}(x)$ is negative whenever $n \geq m = 2$ and hence is irreducible over $\mathbb{Q}$. In [26, Theorem 1.1], Dubickas and Šiurys proved the irreducibility over $\mathbb{Q}$ of above polynomial for $m \leq 6$ and $n \geq m+2$. In [67], Khanduja, Khassa and Laishram proved the irreducibility of $P_{n,m}(x)$ for all n, m such that $2 \leq 2m \leq n < (m+1)^3$.

In a joint work with Laishram [76], we extend the result of [67] and prove the following irreducibility result.

Theorem 1. *[76, Theorem 1.1] Suppose m is a positive integer and n is an integer in the range $2m \leq n < (m+1)^{10}$. Then the polynomial $P_{n,m}(x)$ is irreducible over $\mathbb{Q}$.*

The proof of the above theorem is given in Section 2.2. Thus for m, n, r with $2m \leq n < (m+1)^{r+1}$ and $r \leq 9$, the polynomial $P_{n,m}(x)$ is irreducible. We note here that the proof of Theorem 1 is quite general in nature and with extra computation it can be extended to a higher value of r. However we cannot prove the irreducibility of $P_{n,m}(x)$ for all n, m and hence we stop at $r = 9$. Further for $r \geq 10$, we prove the following finiteness result.

Theorem 2. *[76, Theorem 1.2] Let $m, n, r \in \mathbb{Z}_{>0}$ be such that $2m \leq n < (m+1)^{r+1}$ and $r \geq 10$. If $m \geq \max\{10^6, \frac{r^3}{2}\}$ then the polynomial $P_{n,m}(x)$ is either irreducible over the field of rationals $\mathbb{Q}$ or it contains a factor of whose degree is given by $\frac{im}{j} \left(\leq \frac{m}{2}\right)$ for some $1 \leq i \leq \left[\frac{r+1}{2}\right], j \leq r$. Furthermore, if $m \geq \max\{10^6, 2r^3\}$ then the polynomial $P_{n,m}(x)$ is irreducible over $\mathbb{Q}$.*

The proof of the above theorem is given in Section 2.3. Here we would like to point that the arguments used in the proof of [58, Theorem 1.2] are incomplete the deduction that "there exists a term $n - l_j$ with $0 \leq l_j < k$ such that $v_{p_1}(n - l_j) = e''(\leq e)$ for some prime $p_1 > k$ and $l_j \notin S_t(e'')$ is not correct" and hence the proofs of [58, Theorems 1.1 and 1.2] are not complete.

For a fixed integer $r \geq 10$, Theorem 2 provides an explicit value of m after which $P_{n,m}(x)$ is irreducible. Another aspect one can look at is finding the lower bound on n when m is fixed. In [35], Filaseta et al. showed that for a fixed integer $m \geq 3$, there exists an integer $n_0 = n_0(m)$ depending only on m such that $P_{n,m}(x)$ is irreducible over $\mathbb{Q}$ for all $n \geq n_0$. However their result was ineffective. In Theorem 3, we use Baker's explicit *abc*-conjecture to provide an explicit value of $n_0(m)$ for a fixed integer m.

Theorem 3. *[76, Theorem 1.3] Assume Baker's explicit abc-conjecture (Conjecture 1.1.3). For a fixed integer $m \geq 7$, if $n \geq 2.71851^{3.5m} + 3$ then the polynomial $P_{n,m}(x)$ is irreducible over $\mathbb{Q}$.*

The proof of the above theorem is given in Section 2.4. Here, Baker's explicit *abc*-conjecture, proposed by A. Baker [1] in 2004, is an explicit version of the well known *abc*-conjecture stated as follows:

Conjecture 1.1.3 (Baker's explicit abc-conjecture [1])**.** *Suppose a, b and c are pairwise coprime positive integers such that $a + b = c$. Then*

$$c < \frac{6}{5} R \frac{(\log R)^\omega}{\omega!}$$

where $R = R(abc) = \prod_{p|abc} p$ is the radical of abc and $\omega = \omega(R)$ is the number of distinct prime factors of R.

Definition 1.1.4. *Consider a polynomial $f(x) \in \mathbb{Z}[x]$ with degree n. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be all of its roots in the complex numbers $\mathbb{C}$. The field $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, obtained by adjoining all the roots of $f(x)$ to the field of rational numbers $\mathbb{Q}$, is termed the "splitting field of $f(x)$ over $\mathbb{Q}$". The "Galois group of $f(x)$" is then defined as the set of all automorphisms of this splitting field K that leave every element of $\mathbb{Q}$ unchanged.*

Next we consider the problem of determining the Galois group of the polynomial $P_{n,m}(x)$. Filaseta and Moy in [36, Theorem 1] proved that for any integer $m \geq 2$ with $m \neq 6$, there exists an integer $n_1(m)$ that depends only on m. This integer has the property that for all $n \geq n_1(m)$, the Galois group associated to $P_{n,m}(x)$ over $\mathbb{Q}$ is the symmetric group S_m. In [71], Klahn and Technau established the statement for $m = 6$. However, in both cases the proof was ineffective. Using Baker's explicit abc-conjecture, we provide an explicit value of $n_1(m)$ for a fixed integer m in the following theorem.

Theorem 4. *[76, Theorem 1.4] Assume Baker's explicit abc-conjecture (Conjecture 1.1.3). For a fixed integer $m \geq 10$, if $n \geq 2.71851^{3.5m} + \frac{m}{2} - 1$ then the Galois group of the polynomial $P_{n,m}(x-1)$ (and hence of $P_{n,m}(x)$) is the symmetric group S_m.*

The proof of the above theorem is given in Section 2.4. Proof of Theorems 1, 2, 3 and 4 are published in [76] and are given in Chapter 2 of this thesis. The proofs are based on idea of Newton polygon with respect to prime p and exploitation of large prime divisors of consecutive integers. To define Newton polygon with respect to p, we first need to understand the concept of p-adic valuation.

Fix a prime number p. For a non-zero integer n, $v_p(n)$ will denote the p-adic valuation of n which is defined to be the largest power of p dividing n. We set the convention $v_p(0) = \infty$ for all prime p. This p-adic valuation can be easily extended to the set of rational numbers. Let $\frac{a}{b} \in \mathbb{Q}$ be in it lowest form then we define $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$.

Definition 1.1.5. *Suppose $f(x) = \sum_{i=0}^{e} a_i x^i$ is a polynomial with rational coefficient such that $f(0) \neq 0$. The "Newton polygon of f with respect to a prime p, denoted by $NP_p(f)$, is the polygonal path formed by the lower edges along the convex hull in $\mathbb{R}^2$ of the points $(e-i, v_p(a_i))$ for $0 \leq i \leq e$."*

Newton polygons, named after Isaac Newton, have proven to be an indispensable tool in the study of polynomials. They have numerous applications, including analyzing the factors of a polynomial, studying the Galois group of a polynomial, computing the discriminant of a number field, examining the monogenity and integral basis of number fields, and understanding the splitting of a rational prime in a number field, etc. These applications have attracted significant attention in recent years (cf. [21], [30] [33], [34], [37], [43], [44], [53], [68], [76]–[81]).

Newton initially introduced polygons to study complex curves of two variables, which eventually led to the development of what is now known as the Puiseux series of a curve (cf. [13] for details). This method also applies to polynomials in one variable by looking at their various g-adic expansions. A significant theory in this regard was developed by Ore [85] nearly a century ago. In his 1923 Ph.D. thesis and a series of subsequent papers, Ore extended the arithmetic applications of Newton polygons (*cf.* [84], [85]).

Consider a monic irreducible polynomial $f(x)$ with integer coefficients. Let p be a rational prime and K be the number field obtained by adjoining a root θ of $f(x)$ to $\mathbb{Q}$. Under a certain p-regularity condition, Ore provided a constructive method to determine the prime ideal decomposition of p in K, the p-adic valuation of the index of the subgroup $\mathbb{Z}[\theta]$ in $\mathbb{Z}_K$, and the factorization of f over the field $\mathbb{Q}_p$ of p-adic numbers. The prime ideals are parameterized in terms of combinatorial data associated with different ϕ-Newton polygons, where the polynomials $\phi(x)$ are monic lifts to $\mathbb{Z}[x]$ of the distinct irreducible factors of $f(x)$ modulo p.

To introduce the concept of the ϕ-Newton polygon, we first need to define the *Gauss valuation*. This valuation serves as an extension of the p-adic valuation v_p, which is originally defined on the field of p-adic numbers $\mathbb{Q}_p$, to the field of rational functions in an indeterminate x over $\mathbb{Q}_p$, denoted as $\mathbb{Q}_p(x)$. For a polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Q}_p[x]$, it is given by

$$v_{p,x}(f) = \min_{0\leq j\leq n}\{v_p(a_j)\}.$$

Definition 1.1.6. *Given a rational prime p, let $\phi(x)$ be a monic polynomial within $\mathbb{Z}_p[x]$*

which is not reducible modulo p. Take a monic polynomial $f(x) \in \mathbb{Z}_p[x]$ that is not a multiple of $\phi(x)$. We can express $f(x)$ in terms of powers of $\phi(x)$ as $\sum_{i=0}^{n} a_i(x)\phi(x)^i$, where the degree of each $a_i(x)$ is less than the degree of $\phi(x)$, and $a_n(x)$ is non-zero. For each index i from 0 to n where $a_{n-i}(x)$ is not the zero polynomial, define a point P_i in the plane with coordinates $(i, v_{p,x}(a_{n-i}(x)))$. If both $a_{n-i}(x)$ and $a_{n-j}(x)$ are non-zero, let μ_{ij} represent the slope of the line segment connecting P_i and P_j.

Let i_1 be the largest positive integer, not exceeding n, such that the slope μ_{0i_1} is the minimum among all slopes μ_{0j} where $0 < j \leq n$ and $a_{n-j}(x) \neq 0$. If i_1 is less than n, let i_2 be the largest index satisfying $i_1 < i_2 \leq n$ for which $\mu_{i_1 i_2}$ is the minimum of all $\mu_{i_1 j}$ where $i_1 < j \leq n$ and $a_{n-j}(x) \neq 0$. This process continues iteratively. The "ϕ-Newton polygon of $f(x)$" is then defined as the sequence of connected line segments formed by joining the points P_0 to P_n through the sequence of indices $0 = i_0 < i_1 < \cdots < i_k = n$. These segments, known as the edges of the polygon, exhibit strictly increasing, non-negative slopes due to the fact that $f(x)$ is a monic polynomial with coefficients in $\mathbb{Z}_p$.

Ore proved a theorem on product. We use a weaker version of it which relates the ϕ-Newton polygon of a polynomial $f(x) \in \mathbb{Z}_p[x]$ with its factorization over $\mathbb{Z}_p[x]$ (see [20, Theorem 1.5], [68, Theorem 1.1]).

Theorem 1.1.7. *Consider two monic polynomials $f(x)$ and $\phi(x)$ within the polynomial ring $\mathbb{Z}_p[x]$, where p represents a rational prime. Assume that $\phi(x)$ remains irreducible when considered modulo p. Additionally, suppose $f(x)$ is not a multiple of $\phi(x)$, yet its reduction modulo p, denoted as $\overline{f}(x)$, can be expressed as a power of the reduction of $\phi(x)$, $\overline{\phi}(x)$. If the ϕ-Newton polygon of $f(x)$ relative to p exhibits t distinct edges, labeled $S_1, \ldots, S_t$, with strictly increasing slopes $\lambda_1 < \cdots < \lambda_t$, then $f(x)$ can be factored into a product of t monic polynomials in $\mathbb{Z}_p[x]$, say $f_1(x) \cdots f_t(x)$. Each factor $f_i(x)$ will possess a degree equal to $\ell_i \deg(\phi(x))$, and its corresponding ϕ-Newton polygon will consist of a single edge, denoted as S_i', which is a translation of the original edge S_i. Here, ℓ_i signifies the length of the projection of S_i onto the horizontal axis.*

Ore's work has gained renewed interest in recent years (e.g., see [19], [78], [81]). In [29], [43], [44], Guardia, Montes, and Nart extended Ore's ideas and developed the theory

of higher-order Newton polygons as a powerful tool for computing discriminants, prime ideal decomposition, and integral bases of number fields. In 2019, Kim and Miller [70] employed this tool to compute an integral basis and find integral elements of small prime power norm, ultimately establishing an upper bound for the class number. Using further algebraic arguments, they deduced that the class number is 1. Notably, computing the class number without assuming the Generalized Riemann Hypothesis (GRH) remains a highly challenging problem.

In 1906, Dumas [27] considered Newton polygons with respect to a prime p of two polynomials $f(x), g(x) \in \mathbb{Q}[x]$ and gave a beautiful idea to construct the Newton polygon of the polynomial obtained by the product $f(x)g(x)$. This result helped in obtaining various results on the irreducibility of the polynomials. Further, with such a result, one can easily predict the Newton polygon structure of the polynomial $f(x)^n$ (*n-times product*) for any polynomials $f(x) \in \mathbb{Q}[x]$. Dumas proved the following fundamental result:

Theorem 1.1.8. *[27, Dumas' Theorem] Let p be a prime and $g(x), h(x) \in \mathbb{Z}[x]$ be polynomials with non-zero constant terms. Suppose p^r exactly divides the leading coefficient of the product gh. Then $NP_p(gh)$ can be formed by drawing a polygonal path starting at $(0, r)$ and using the translates of the edges of $NP_p(g)$ and $NP_p(h)$ precisely once. The translated edges are arranged to form a polygonal path with increasing slopes.*

It is, therefore, natural to ask the following questions: *Given a polynomial g, how does the Newton polygon of $g \circ f$ change as f varies? Can we describe families of polynomials that, when composed with g, preserve key features (such as segments and slopes) of the Newton polygon?*

In a joint work with Jakhar, Laishram and Srinivas [56], we attempt to answer the above questions. Our main result provides a clear method to construct the Newton polygon of $g \circ f$ from the structure of the Newton polygons of g and f, where both g and f can have Newton polygons with multiple segments. Specifically, this construction works under the condition that the slopes of the Newton polygon of g are not excessively steep, or the p-adic valuation of the constant term of g is bounded relative to the slope of its first edge. Composition with a polynomial f has the effect of "stretching" the

Newton polygon of g horizontally by a factor of $\deg f$. This transformation preserves the number of segments in the Newton polygon and adjusts the slopes in a predictable manner. In particular, we prove Theorems 5 and 7.

We now state our main result in this direction which is proved in Section 3.2.

Theorem 5. *[56, Theorem 1.2] Let p be a prime number and let $g(x) = b_e x^e + b_{e-1}x^{e-1} + \cdots + b_0$, where $b_0 \neq 0$, be a polynomial of degree e with rational coefficients such that $v_p(b_e) = 0$ and p divides b_i for $0 \leq i \leq e-1$. Let $m_0, m_1, \ldots, m_{t-1}, m_t$ be integers such that the successive vertices of the Newton polygon of $g(x)$ with respect to p are given by the set*

$$\{(0,0), (e-m_1, v_p(b_{m_1})), \ldots, (e-m_{t-1}, v_p(b_{m_{t-1}})), (e, v_p(b_0))\},$$

with $m_0 = e$, $m_t = 0$, and $\lambda_i = \frac{v_p(b_{m_i}) - v_p(b_{m_{i-1}})}{m_{i-1} - m_i}$, for $1 \leq i \leq t$.

Let $f(x) = a_d x^d + \cdots + a_0 \in \mathbb{Q}[x]$ be such that $\nu_p(a_d) = 0$. Assume that the slope λ of the first edge of the Newton polygon of $f(x)$ with respect to p is greater than or equal to λ_1. If one of the following conditions holds:

(i) $v_p(b_0) < \lambda_1(d+e-1)$,

(ii) $v_p(b_0) = \lambda_1(d+e-1)$ with $v_p(f(0)) > d\lambda$ or $\lambda > \lambda_1$,

then for any positive integer n, the successive vertices of the Newton polygon of the composition $g(f^n(x))$ with respect to p are given by the set

$$\{(0,0), (d^n(e-m_1), v_p(b_{m_1})), \ldots, (d^n(e-m_{t-1}), v_p(b_{m_{t-1}})), (d^n e, v_p(b_0))\},$$

where $f^n(x)$ denotes the n-th iterate of the polynomial $f(x)$.

The proof of the above theorem is given in Section 3.2.

Remark. As highlighted in [56], we point out that the condition $v_p(b_e) = 0$ in Theorem 5 is redundant. Suppose $v_p(b_e) \neq 0$, and replace assumption (i) of Theorem 5 with the condition $v_p(b_0) - v_p(b_e) < \lambda_1(d+e-1)$. Define the polynomial $g_1(x) = p^{-v_p(b_e)}g(x)$. It is straightforward to verify that $v_p(g_1(0)) = v_p(b_0) - v_p(b_e) < \lambda_1(d+e-1)$, which satisfies

the conditions of Theorem 5. We can then apply Theorem 5 to $g_1(x)$ and determine the Newton polygon structure of the composition $(g_1 \circ f^n)(x)$. This, in turn, provides the Newton polygon of $g(f^n(x)) = p^{v_p(b_e)} g_1(f^n(x))$ for all $n \geq 0$.

For a polynomial $f(x) \in \mathbb{Q}[x]$, the following result about the Newton polygon structure of f^n follows as a immediate consequence of the above theorem.

Theorem 6. *Let p be a prime, and let $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ be a polynomial of degree d with $a_0 \neq 0$ and $\nu_p(a_i) > 0$ for all $0 \leq i < d$. Let $m_1 > \cdots > m_{t-1}$ be positive integers such that the successive vertices of $NP_p(f)$ are given by the set*

$$\{(0,0), (d - m_1, v_p(a_{m_1})), \ldots, (d - m_{t-1}, v_p(a_{m_{t-1}})), (d, v_p(a_0))\}.$$

If $\nu_p(a_0) \leq \frac{v_p(a_{m_1})}{d - m_1}(2d-1)$, then for $n \geq 1$, the successive vertices of $NP_p(f^n)$ are given by the set $\{(0,0), (d^{n-1}(d-m_1), v_p(a_{m_1})), \ldots, (d^{n-1}(d-m_{t-1}), v_p(a_{m_{t-1}})), (d^n, v_p(a_0))\}$.

Let p be a prime and $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0 \in \mathbb{Q}[x]$. For an integer $r \geq 1$, we say $f(x)$ is *p^r-pure*, if $v_p(a_d) = 0$, $v_p(a_0) = r$, and $\frac{v_p(a_i)}{d-i} \geq \frac{r}{d}$ for all $0 < i < d$.

Note that in Theorem 5, if $g(x)$ has a single edge then condition (i) is always satisfied. Consequently, the main result of [22] can be derived as a corollary of Theorem 5 combined with Dumas' Theorem.

Corollary 1.1.9. *[22] Consider a polynomial $f(x) \in \mathbb{Q}[x]$ that is p^r-pure and has degree d. Then, for any positive integer $n \geq 1$, the n-th iteration of f, denoted by $f^n(x)$, possesses at most $\gcd(d^n, r)$ irreducible factors over the field of rational numbers $\mathbb{Q}$. Moreover, each of these irreducible factors has a degree that is at least $\frac{d^n}{\gcd(d^n, r)}$.*

A p^r-pure polynomial f of degree d is said to be *p^r-Dumas* if $\gcd(r, d) = 1$. The following corollary regarding p^r-Dumas polynomials is an immediate consequence of Corollary 1.1.9.

Corollary 1.1.10. *[22] Let $f(x) \in \mathbb{Q}[x]$ be a p^r-Dumas polynomial of degree d. Then, for every positive integer $n \geq 1$, the n-th iteration of f, denoted by $f^n(x)$, remains irreducible over the field of rational numbers $\mathbb{Q}$.*

Note that the application of Theorem 5 relies on the condition that all edges of $NP_p(g)$ have positive slopes. Our next result extends this stretching property of the Newton polygon to cases where the edges can have negative slopes, provided some distinct restrictions are imposed on the polynomial f. We prove the following result.

Theorem 7. *[56, Theorem 1.5] Let p be a prime number, and let $g(x) = b_e x^e + b_{e-1}x^{e-1} + \cdots + b_0$ with $b_0 \neq 0$ be a polynomial of degree e with rational coefficients. Let $m_0, m_1, \ldots, m_{t-1}, m_t$ be integers such that the successive vertices of the Newton polygon of $g(x)$ with respect to p are given by the set*

$$\{(0, v_p(b_e)), (e - m_1, v_p(b_{m_1})), \ldots, (e - m_{t-1}, v_p(b_{m_{t-1}})), (e, v_p(b_0))\},$$

with $m_0 = e$, $m_t = 0$, and $\lambda_i = \frac{v_p(b_{m_i}) - v_p(b_{m_{i-1}})}{m_{i-1} - m_i}$, for $1 \leq i \leq t$.

Let u be an integer such that $u > |\lambda_j|$ for all $j \in \{1, 2, \ldots, t\}$. Suppose $f(x) = a_d x^d + \cdots + a_1 x + a_0$ is a polynomial of degree d such that $v_p(a_d) = 0$ and $v_p(a_i) \geq \frac{u}{\beta}(d - i)$ for all $i \in \{0, 1, 2, \ldots, d\}$, where $\beta \leq d$ is a positive integer coprime to u. Then, the successive vertices of the Newton polygon of the composition $g(f(x))$ with respect to p are given by the set

$$\{(0, v_p(b_e)), (d(e - m_1), v_p(b_{m_1})), \ldots, (d(e - m_{t-1}), v_p(b_{m_{t-1}})), (de, v_p(b_0))\}.$$

The proof of the above theorem is given in Section 3.3. The following corollary follows as a direct consequence of Theorem 7.

Corollary 1.1.11. *[56] Under the notations and assumptions of Theorem 7, the successive vertices of the Newton polygon of $(g \circ f^n)(x)$ with respect to p are given by the set*

$$\{(0, v_p(b_e)), (d^n(e - m_1), v_p(b_{m_1})), \ldots, (d^n(e - m_{t-1}), v_p(b_{m_{t-1}})), (d^n e, v_p(b_0))\}.$$

Let m be a positive integer, and let $b_0, b_1, \ldots, b_m$ denote arbitrary integers such that $|b_0| = |b_m| = 1$. A *Schur polynomial* of degree m, denoted by G_m, is defined as:

$$G_m(x) = b_0 + b_1 x + b_2 \frac{x^2}{2!} + \cdots + b_m \frac{x^m}{m!}.$$

It is well known that G_m is irreducible for all m (see [92], [33, Theorem 2]).

In the special case where $b_i = 1$ for all $i, 0 \leq i \leq m$, G_m becomes the *truncated exponential polynomial* E_m. An independent proof of the irreducibility of truncated exponential polynomials using Newton polygons was given by Coleman in 1987 (cf. [21]).

In Section 3.5.1, we prove the following result, which demonstrates how Theorem 7 can be utilized to construct a large family of polynomials f that are dynamically irreducible at *Schur polynomials*, and consequently, at *truncated exponential polynomials*, irrespective of whether these polynomials are irreducible themselves.

Theorem 8. *[56, Theorem 1.9] Fix $m \geq 1$ and let $G_m(x)$ be the Schur polynomial of degree m. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree d with leading coefficient a_d such that $v_p(a_d) = 0$ and $f(x) \equiv a_d x^d \pmod{p}$. If d is coprime to $m!$ and $\gcd(b_i, m) = 1$ for all $0 < i < m$, then f is dynamically irreducible at G_m.*

The proof of the above theorem is given in Section 3.5.1. The subsequent corollary arises directly as a result of Theorem 8.

Corollary 1.1.12. *Suppose $f(x)$ is as given in Theorem 8, and let E_m denote the truncated exponential polynomial of degree m. If d is coprime to $m!$, then f is dynamically irreducible at E_m.*

In Section 3.5.2, we use Theorem 5 to construct an iterative family of non-monogenic polynomials. The Section 3.5.3 applies Theorems 5 and 7 to analyze the number of irreducible factors and their degrees in the iterates of certain polynomials. Finally, in Section 3.5.4, we present a family of examples that satisfy Sookdeo's Conjecture, showcasing an application of Theorems 5 and 7.

In 2024, Gajek-Leonard and Tomer [41] proved an interesting result regarding the Newton polygon of composition of polynomials, which can be deduced as an easy corollary of Theorem 7.

Corollary 1.1.13. *[41, Theorem 1.1] Let $f(x) \in \mathbb{Q}[x]$ be a polynomial. Consider a polynomial $g(x)$ and its Newton polygon constructed with respect to a prime number p. Assume that this Newton polygon is composed of t distinct segments, and the slopes of these segments are ordered such that $\lambda_1 < \cdots < \lambda_t$. If $f(x)$ is p^r-pure and $|\lambda_i| < r$ for all $1 \leq i \leq t$, then the Newton polygon of $(g \circ f)(x)$ has t segments with slopes $\frac{\lambda_1}{\deg f} < \cdots < \frac{\lambda_t}{\deg f}$.*

A degree d polynomial $f(x)$ with rational coefficients, is termed *stable* (or *dynamically irreducible*) over $\mathbb{Q}$ if $f^n(x)$ (n-th iteration of f) is irreducible over $\mathbb{Q}$ for all $n \geq 1$. It is said to be *eventually stable* if there exists a constant C_f that depends only on the polynomial f itself, such that the number of irreducible factors of $f^n(x)$ is bounded by C_f. One can easily note that a stable polynomial f is eventually stable with $C_f = 1$. The advantage eventual stability has over stability is that, the property easily carriers over to any finite extension of $\mathbb{Q}$ as illustrated in example below.

Example 1.1.14. *Let $f(x) = x^2 - 2$, then it is well known that all the iterates $f^n(x)$ are irreducible over $\mathbb{Q}$ (cf. Corollary 1.1.10) i.e., f is stable over $\mathbb{Q}$. But f is not stable over $\mathbb{Q}(\sqrt{2})$. Further, f is eventually stable over both $\mathbb{Q}$ as well as $\mathbb{Q}(\sqrt{2})$.*

The structures of Newton polygons obtained in Theorems 5 and 7 establishes stability and eventual stability for a large class of polynomials, which is a central theme in the arithmetic of dynamical systems. Eventual stability has been pivotal in proving Sookdeo's conjecture [97], finite-index results for arboreal representations (see [12, 11]). It also has a lot of applications in preimage curves and arboreal Galois representations, as detailed in [65, Section 3].

Our next result which we prove in Section 3.4, establishes eventual stability to a broader class of polynomials compared to Theorems 5 and 7, although it does not provide explicit details about the Newton polygon structure or the number and degrees of irreducible factors of $f^n(x)$ that Theorems 5, 7 offer.

Theorem 9. *[56, Theorem 1.8] Let p be a prime, and let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, $a_0 \neq 0$ be a polynomial of degree d with rational coefficients such that $v_p(a_i) > 0$ for all i, $0 \leq i < d$, and $v_p(a_d) = 0$. Then $f^n(x)$ is eventually stable over $\mathbb{Q}$.*

The proof of the above theorem is given in Section 3.4. Proof of Theorems 5, 6, 7, 8 and 9 are published in [56] and are given in Chapter 3 of this thesis. For a polynomial $g(x) \in \mathbb{Q}[x]$, we say f is *dynamically irreducible at* g if $g \circ f^n$ is irreducible for all $n \geq 0$. Jones [64] proved an interesting result connecting stability with the sequence in forward orbit.

Lemma 1.1.15. *[64, Proposition 4.2] Let K be a field whose characteristic is not equal to 2. Consider two monic polynomials $f(x)$ and $g(x)$ that are elements of the polynomial ring $K[x]$, and assume that $f(x)$ has degree 2. Let γ be a critical point of f. If none of the element*

$$\{(-1)^{deg\ g} g(f(\gamma))\} \cup \{g(f^n(\gamma)) : \ n \geq 2\}$$

is a square in K, then f is dynamically irreducible at g.

From the above result, it is clear that a better understading of the sequence $(g(f^n(\gamma)))$ can lead to the stability of the sequence of polynomial $g \circ f^n$. Let $\mathcal{A} = (a_1, a_2, \ldots)$ be a sequence of integers. For a sequence $\mathcal{A}$, we define a term a_n to have a *primitive prime divisor* if there exists a prime number p that divides a_n (i.e., $p \mid a_n$) but does not divide any preceding term a_m in the sequence, where $1 \leq m < n$ (i.e., $p \nmid a_m$).

Definition 1.1.16. *Consider the sequence of integers $\mathcal{A} = (a_1, a_2, \ldots)$. The set*

$$\mathcal{Z}(\mathcal{A}) = \{n \geq 1 : a_n \textit{ does not have a primitive prime divisor}\},$$

is called the Zsigmondy set of the integer sequence $\mathcal{A}$.

The first question that one asks about the Zsigmondy set of a sequence is whether it is finite and this question has received a lot of attention. Bang [2] (for $b = 1$) and Zsigmondy [100] proved that for any co-prime integers $a > b > 0$, $\mathcal{Z}(a^n - b^n)$ is a finite set. Further, this result was extended to more general binary linear recurrence

sequences. In fact, following the works of Carmichael [15], Schinzel [91], Stewart [98] and Voutier [99], finally Bilu, Hanrot and Voutier [6] proved that $\mathcal{Z}(\mathcal{A})$ is a finite set for any non-trivial Lucas or Lehmer sequence of integers $\mathcal{A}$.

Assuming that the Zsigmondy sets under consideration are finite, it is natural to ask for explicit bounds for $\#\mathcal{Z}(\mathcal{A})$ and $\max \mathcal{Z}(\mathcal{A})$. For instance, Zsigmondy's original theorem shows that for integers $a > b > 0$, we have $\max \mathcal{Z}(a^n - b^n) \leq 6$ and in particular $\max \mathcal{Z}(2^n - 1) = 6$. Also, the deep result of Bilu et al., [6] shows that $\max \mathcal{Z}(\mathcal{U}) \leq 30$ for any non-trivial Lucas or Lehmer sequence of integers $\mathcal{U}$.

The questions related to Zsigmondy set have been also studied for non-linear recurrences sequences. For example, Silverman [93] first showed that Zsigmondy set is finite for a elliptic divisibility sequence, but gave no effective bound for the largest element in the Zsigmondy set. Later for some special elliptic curves, a uniform bound for the largest element in the Zsigmondy set was obtained (see [31, 50]).

Recently, several authors explored the subject of primitive divisors in recurrence sequences generated by the iteration of nonlinear polynomials and rational functions. For a set S endowed with self map f and for $\alpha \in S$, we define the *forward orbit* by

$$\mathcal{O}_f^+(\alpha) := \{f^m(\alpha) \mid m \in \mathbb{N}\}.$$

We say that a point α in S is *preperiodic* if $f^{m+n}(\alpha) = f^m(\alpha)$ for some $n \geq 1$ and $m \geq 0$. In an equivalent manner, an element α is termed preperiodic iff its forward orbit under the action of f, denoted by $\mathcal{O}_f^+(\alpha)$, constitutes a finite set. A non preperiodic point, i.e., point with infinite f-orbit, is called a *wandering point*. For a polynomial f, the Zsigmondy set of the sequence $(f^n(\alpha))_{n\geq 1}$ is defined by

$$\mathcal{Z}(f, \alpha) = \{n \geq 1 : f^n(\alpha) \text{ does not have a primitive prime divisor}\}.$$

In this direction, Rice [88] first proved that for a monic polynomial $f(x) \in \mathbb{Z}[x]$, $f(x) \neq x^d$, if 0 is a preperiodic of f and $\alpha \in \mathbb{Z}$ has infinite orbit, then $\mathcal{Z}(f, \alpha)$ is finite. Ingram and Silverman [52] later generalized this result to arbitrary rational maps over number

fields. In fact, they proved that for any rational function $f(x) \in \mathbb{Q}(x)$ of degree $d \geq 2$ with $f(0) = 0$ and order of vanishing of f at $x = 0$ is not d, if α has infinite orbit, writing $f^n(\alpha) = \frac{A_n}{B_n} \in \mathbb{Q}$ in lowest terms, the Zsigmondy set $\mathcal{Z}((A_n)_{n\geq 0})$ is finite. Their proof, relies on Roth's theorem and does not provide an effective upper bound for $\max \mathcal{Z}((A_n)_{n\geq 0})$.

Hereafter, by $\mathcal{Z}(f, 0)$ we denote the Zsigmondy set for the sequence defined by the numerators of $f^n(0)$. In [25], Doerksen and Haensch explicitly characterized the Zsigmondy set $\mathcal{Z}(f, 0)$ for the polynomial $f(x) = x^d + c$ of degree $d \geq 2$ with $c \in \mathbb{Z}$ and $\mathcal{O}_f(0)$ infinite. In fact, they proved that $\max \mathcal{Z}(f, 0) \leq 2$ if $c = \pm 1$ and $\mathcal{Z}(f, 0)$ is empty for all other $c \in \mathbb{Z}$. Krieger [72] considered the Zsigmondy set for such f when $c \in \mathbb{Q}$ and showed that $\#\mathcal{Z}(f, 0) \leq 23$. Recently, Ren [87] further generalized the result of Krieger for more general polynomials which are not necessarily monic nor integer polynomial. The main result of [87] asserts that for every polynomial $f \in \mathbb{Q}[x]$ of degree $d \geq 2$ with a critical point $u \in \mathbb{Q}$ there is a constant $M_f > 0$, depending only on f (and not on $c \in \mathbb{Q}$), such that $\#\mathcal{Z}(f_c, u) \leq M_f$ for every c satisfying certain condition where $f_c(x) = f(x) + c$. For other related results in this direction, we refer to [80, 17, 42].

In a joint work with Rout and Laishram [74], we study the question of the existence of an effective bound on the largest element of $\mathcal{Z}(f, 0)$, and also finding a uniform bound on the largest element of the Zsigmondy set for some class of rational polynomials. To state our result, let

$$f(x) = a_d x^d + \cdots + a_1 x + a_0, \text{ with } a_i \in \mathbb{Q}, a_d \neq 0, \text{and } a_1 = 0. \tag{1.1}$$

As defined in [74], let $P^{\pm}, N^{\pm}$ and $n^{\pm}$ be defined as:

$$\begin{aligned} P^{+} &= \{0 \leq i \leq d : a_i = 0 \text{ or } \operatorname{sgn}(a_i) = \operatorname{sgn}(a_d)\} \\ P^{-} &= \{0 \leq i \leq d : a_i = 0 \text{ or } \operatorname{sgn}((-1)^i a_i) = \operatorname{sgn}((-1)^d a_d)\} \\ N^{\pm} &= (P^{\pm})^c \quad \text{(complement of } P^{\pm} \text{ in } \{0,1,2,\ldots,d\}) \\ n^{\pm} &= \begin{cases} \max\{1, \max\{i : i \in N^{\pm}\}\} & \text{if } N^{\pm} \neq \emptyset \\ 1 & \text{if } N^{\pm} = \emptyset \end{cases} \end{aligned} \tag{1.2}$$

where $\operatorname{sgn}(a) = a/|a|$ for any real number $a \neq 0$. Let x be such that $|x| \geq 1$ and satisfies

$$\sum_{n^{+}<i\leq d} |a_i||x|^{i-n^{+}} \geq \left(\sum_{i\in N^{+}} |a_i|\right) + 1 \quad \text{and} \quad \sum_{n^{-}<i\leq d} |a_i||x|^{i-n^{-}} \geq \left(\sum_{i\in N^{-}} |a_i|\right) + 1 \tag{1.3}$$

for both the sets N^{+} and N^{-}. Then our main result is the following.

Theorem 10. *[74, Theorem 1.1] Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree $d \geq 2$ as in (1.1) with $|a_0| \geq 1$. Let $\hat{h}_f$ be the associated canonical height. Further assume that a_0 satisfies inequality (1.3). If $n \in \mathcal{Z}(f, 0)$, then*

$$n \leq \frac{2}{\log d} \log\left(\frac{dC}{(d-1)\hat{h}_f(a_0)}\right) + 2 \tag{1.4}$$

where $C \geq \sum_{v\in V_K} \log C_v$ and C_v is the associated constant in Remark 4.1.9.

The proof of the above theorem is given in Section 4.2. The method used in proving the theorem are inspired by the work of Krieger [72]. We would like to point out that the upper bound on $\mathcal{Z}(f, 0)$ for polynomials of type (1.1) is enough for the upper bound on Zsigmondy set $\mathcal{Z}(g, \gamma)$ of the sequence $(g^n(\gamma) - \gamma)_{n\geq 1}$ for any polynomial $g(x) \in \mathbb{Q}[x]$ with a critical point $\gamma \in \mathbb{Q}$. Define a polynomial $f(x) = g(x+\gamma) - \gamma$, a simple calculation will yield that linear term of f is zero and $g^n(\gamma) - \gamma = f^n(0)$, for all $n \in \mathbb{N}$. The following result of Krieger [72, Proposition 5.3] can be easily seen as a corollary of Theorem 10 (see Subsection 4.2.1).

Corollary 1.1.17. *[72] For $d \geq 3$, suppose $f(x) = x^d + c \in \mathbb{Q}[x]$ is such that $c \in \mathbb{Q}\backslash\mathbb{Z}$ and $|c| > 2^{\frac{d}{d-1}}$, then $\mathcal{Z}(f, 0) = \emptyset$.*

Proof of the above corollary is given in Section 4.2.1. Next, we apply Theorem 10 to provide an explicit and uniform bound on the Zsigmondy set for the orbit of 0 of polynomials $f(x) = x^d + x^e + c \in \mathbb{Q}[x]$ where $d > e \geq 2$. In particular, we prove the following result.

Theorem 11. *[74, Theorem 1.3] For $d > e \geq 2$, suppose $f(x) = x^d + x^e + c \in \mathbb{Q}[x]$ is such that $c = \frac{a}{b} \in \mathbb{Q}$ and $|c| > 2$. If $n \in \mathcal{Z}(f, 0)$, then $n \leq 6$.*

The proof of the above theorem is given in Section 4.3. In Theorem 10, we have taken c to be rational which are not integers, because the case for an integer c has been solved by Shokri [80]. In Section 4.4, we use the method similar to those used by Krieger [72] to obtain the upper bound of $\mathcal{Z}(f, 0)$ when $|c| < 2$ with certain assumptions on parity of d and e.

Zsigmondy questions of this type also connect to broader problems in number theory and arithmetic dynamics. In 2013, assuming the *abc*-conjecture, Gratton, Nguyen and Tucker [42] proved the finiteness of Zsigmondy set for the numerator sequence of infinite orbit under rational iteration. Silverman and Voloch [96] used Zsigmondy results of Ingram and Silverman [52] to prove that there is no dynamical Brauer-Manin obstruction for dimension 0 subvarieties under morphisms ϕ between projective number field of degree at least 2, whereas Faber and Voloch [32], have used the Zsigmondy results of [52] in studying the nonarchimedean convergence of Newton's method.

1.2 Monogenity

Consider a number field K, and let $\mathbb{Z}_K$ denote the ring of algebraic integers in K. A classical question in algebraic number theory is to determine whether K is monogenic—that is, whether there exists an element $\xi \in \mathbb{Z}_K$ such that the set $\{1, \xi, \ldots, \xi^{n-1}\}$ forms an integral basis of $\mathbb{Z}_K$. The problem of an arithmetic characterization of monogenic number fields was raised by Hasse [48] in 1960. Extensive literature exists on monogenic fields.

Dedekind [23] provided the first example of a non-monogenic number field. Gaál's [38] book provides some classification of monogenity in lower degree number fields using index form equation (cf. [38]). Recently, Bhargava, Shankar, and Wang [5] established that the density of monic irreducible polynomials $f(x) \in \mathbb{Z}[x]$, such that a root θ of $f(x)$ yields a power basis for the ring of algebraic integers of $\mathbb{Q}(\theta)$, is approximately 30.71%. The aim over here, is to provide an infinite family of monogenic number fields of any degree.

Consider an algebraic number field $K = \mathbb{Q}(\theta)$, where θ is a root of a monic irreducible polynomial $f(x)$ of degree n over the field of rational numbers $\mathbb{Q}$.Let d_K denote the discriminant of K and D_f denote the discriminant of the polynomial $f(x)$, then it is well-known that d_K and D_f are related by the following formula (see [69, 18])

$$D_f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 d_K. \tag{1.5}$$

In the above formula, if $[\mathbb{Z}_K : \mathbb{Z}[\theta]] = 1$, then we have $\mathbb{Z}_K : \mathbb{Z}[\theta]$, i.e., one of the integral basis of K is $\{1, \theta, \cdots, \theta^{n-1}\}$; in this situation we say that $f(x)$ is monogenic. Clearly if $f(x)$ is monogenic, then K is also monogenic. In 1878, Dedekind gave a necessary and sufficient criterion to be satisfied by the minimal polynomial $f(x)$ of θ so that p does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ (cf. [18, Theorem 6.1.4], [24]). Dedekind criterion has generated a lot of interest among the mathematicians. Its several equivalent versions and generalizations are known (cf. [16], [54], [73]). In 2016-17, using Dedekind criterion, Jakhar, Khanduja and Sangwan [55] gave necessary and sufficient conditions for $\mathbb{Z}_K = \mathbb{Z}[\theta]$ when θ is a root of an irreducible trinomial $x^n + ax^m + b \in \mathbb{Z}[x]$ having degree n. As an application, they deduced infinitely many monogenic trinomials. In 2021, Harrington and Jones [47] determined formula for the discriminant of the polynomial $f(x) = x^{n-km}(x^k + a)^m + b$ assuming $k \mid n$. In a joint work with Jakhar and Laishram [57], we extend this result to provide the formula for the discriminant of $f(x)$ without the restriction $k \mid n$. Recently, several results on the monogenity of certain classes of polynomials and the number fields have been developed (cf. [38], [40], [54] –[62]).

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ having minimal polynomial $f(x) = x^{n-km}(x^k + a)^m + b$ over $\mathbb{Q}$, $1 \leq km < n$. In [57], we explicitly compute the discriminant

of $f(x)$ and characterize all the primes dividing the index of the subgroup $\mathbb{Z}[\theta]$ in $\mathbb{Z}_K$. We use this discriminant to provide the critrions when these primes will divide the index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. To better understand our results, we will later present several illustrative examples. In few of these examples, we will also explicitly compute the index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$.

In what follows throughout this section, the notation D_f will represent the discriminant of the polynomial $f(x) = x^{n-km}(x^k + a)^m + b$, where the integers n, m, k satisfy $1 \leq km < n$. Additionally, t will denote the greatest common divisor of n and k, and we will use n_1 and k_1 to represent $\frac{n}{t}$ and $\frac{k}{t}$, respectively. Precisely stated, we prove the following results.

Theorem 12. *[57, Theorem 1.1] For integers n, m, k with $n > km \geq 1$, consider an irreducible polynomial $f(x) = x^{n-km}(x^k + a)^m + b \in \mathbb{Z}[x]$. Then the discriminant D_f of the polynomial $f(x)$ is given by the formula,*

$$D_f = (-1)^{\frac{n(n-1)}{2}}\ b^{n-k-1}\big[b^{k_1}n^{n_1} + (-1)^{n_1-k_1m+k_1+1}\ a^{n_1}k^{k_1m}m^{k_1m}(n-km)^{n_1-k_1m}\big]^t, \tag{1.6}$$

where $t = \gcd(n, k)$ and $n = n_1t, k = k_1t$.

The proof of the above theorem is given in Section 5.2. We shall denote U and V to be the integers defined by

$$U = b^{k_1}\ n^{n_1} \text{ and } V = (-1)^{n_1-k_1m+k_1+1}a^{n_1}k^{k_1m}m^{k_1m}(n-km)^{n_1-k_1m}, \tag{1.7}$$

then in view of the above theorem $D_f = (-1)^{\frac{n(n-1)}{2}}\ b^{n-k-1}\ (U+V)^t$.

Theorem 13. *[57, Theorem 1.2] Consider $f(x) = x^{n-km}(x^k + a)^m + b$ where $a, b \in \mathbb{Z}$ and $n > km \geq 1$. Suppose $f(x)$ is irreducible and has a root θ. Denote $K = \mathbb{Q}(\theta)$ and $\mathbb{Z}_K$ be the ring of integers of K. Let $\gcd(n, k) = t$ and $n = n_1t, k = k_1t$. Let p be a prime dividing D_f, then $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ iff one of the following condition is satisfied:*

(i) if $p \mid b$, assume either $p|a$ or $p \nmid a$ with $m \geq 2$, then $p^2 \nmid b$;

(ii) if $p \mid b$, $m = 1$, $p \nmid a$ with $j = v_p(k) \geq 0$, then either p divides a_1 but not b_1 or $p \nmid b_1^{n-k-1}a_1[(-a)^{n_1-k_1}a_1^{k_1} - (-b_1)^{k_1}]$, where $a_1 = \frac{a+(-a)^{p^j}}{p}$ and $b_1 = \frac{b}{p}$;

(iii) *if* $p \mid a$ *and* $p \nmid b$ *with* $j = v_p(n) \geq 1$, *then either* p *divides* a_2 *but not* b_2 *or* $p \nmid a_2 \left[a_2^{n_1} b^{n_1-k_1} - (-1)^{k_1} b_2^{n_1}\right]$, *where* $a_2 = \frac{ma}{p}$ *and* $b_2 = \frac{b+(-b)^{p^j}}{p}$;

(iv) *if* $p \nmid ab$ *and* $p \mid k$ *with* $k = p^j s, n = p^j s'$, $p \nmid \gcd(s, s')$, *then polynomials* $\frac{1}{p}\left[(-1)^{p^j}\left(\sum_{i=1}^{m} \binom{m}{i} x^{s'-si} a^i + b\right)^{p^j} + \sum_{i=1}^{m} \binom{m}{i} x^{p^j(s'-si)} a^i + b\right]$ *and* $x^{s'-sm}(x^s + a)^m + b$ *are co-prime modulo* p;

(v) *if* $p \nmid abk$ *and* $p \mid m$, *then* $p^2 \nmid [(-b)^p + b]$;

(vi) *if* $p \nmid abkm$, *then* $p^2 \nmid (U + V)$ *where* U *and* V *are as in* (1.7).

Above theorem is proved in Section 5.2. The following corollaries are immediate consequence of Theorem 13.

Corollary 1.2.1. *[57] Consider the polynomial* $f(x)$ *and the field* K *as defined in Theorem 13. Then the ring of integers of* K, *denoted by* $\mathbb{Z}_K$, *is equal to* $\mathbb{Z}[\theta]$ *iff every prime number* p *that divides the discriminant* D_f *satisfies at least one of the conditions* $(i) - (vi)$ *stated in Theorem 13.*

Corollary 1.2.2. *[57] Consider the polynomial* $f(x)$ *and the field* K *as defined in Theorem 13. Given that* $m \geq 2$ *and* $\gcd(n, akm) = 1$, *the equality* $\mathbb{Z}_K = \mathbb{Z}[\theta]$ *holds precisely when every prime* p *that is a divisor of* D_f *fulfills one of these conditions:* (i) $v_p(b) = 1$, *or* (ii) p *does not divide* b *and* p^2 *does not divide* $(U + V)$, *where* U *and* V *are defined as in* (1.7).

Suppose $f(x) = x^{n-km}(x^k + a)^m + b \in \mathbb{Z}[x]$ with $\gcd(a, b) > 1$. Let q be a prime dividing $\gcd(a, b)$ with $q^2 \nmid b$. For $j \geq 0$, denote $f_{q,j}(x) = f(x^{q^j})$. Then $f_{q,j}(x)$ is q-Eisenstein for all $j \geq 0$ and the discriminant $D_{f_{q,j}}$ of polynomial $f_{q,j}(x)$ satisfies $|D_{f_{q,j}}| = |b^{q^j(n-k)-1} q^{jnq^j} (U+V)^{tq^j}|$ where $t = \gcd(n, k)$, U and V are as in (1.7). Using the formula for $|D_{f_{q,j}}|$, Corollary 1.2.2 and Theorem 13, we deduce that the composition of a certain type of polynomial is also monogenic polynomial.

Corollary 1.2.3. *[57] Let* $f(x) = x^{n-km}(x^k + a)^m + b$ *be as in Corollary 1.2.2 with* $\gcd(a, b) > 1$. *Let* q *be a prime number dividing* $\gcd(a, b)$ *with* $q^2 \nmid b$. *For* $j \geq 0$, *denote* $f_{q,j}(x) = f(x^{q^j})$. *Then* $f_{q,j}(x)$ *is* q*-Eisenstein for all* $j \geq 0$. *Further* $f_{q,j}(x)$ *becomes monogenic for every* $j \geq 0$ *iff every prime* p *that is a divisor of* D_f *fulfills one of these*

conditions: (i) $v_p(b) = 1$, *or* (ii) p *does not divide* b *and* p^2 *does not divide* $(U + V)$, *where* U *and* V *are defined as in* (1.7).

The classical inverse Galois problem asks whether, for a given finite group G, there exists a polynomial $f(x)$ over $\mathbb{Q}$ whose Galois group is isomorphic to G. In a foundational result from 1892, Hilbert demonstrated that for any positive integer n, there are infinitely many irreducible polynomials of degree n over $\mathbb{Q}$ whose Galois group is either the symmetric group S_n or the alternating group A_n. After that, several mathematicians have used many techniques such as class field theory, elliptic curves, Newton polygons, resolvents to obtain similar results for various groups (cf. [7], [46], [49], [62]). Our next result gives a class of polynomials of prime degree q such that their discriminant are not square-free and their Galois group G_f is isomorphic to S_q.

Theorem 14. *[57, Theorem 1.6] Suppose* q, k, m *are integers such that* $q > km \geq 1$ *and* q *is prime. Let* $f(x) = x^{q-km}(x^k + a)^m + b \in \mathbb{Z}[x]$ *be irreducible. Suppose there exists a prime* p *such that* $p \mid D_f, p \nmid abkm$ *and* $p^2 \nmid D_f$, *then the Galois group of* $f(x)$ *over* $\mathbb{Q}$ *is isomorphic to the full symmetric group* S_q.

The proof of the above theorem is given in Section 5.3. As an application of Theorem 14, we provide examples of monogenic polynomials of prime degree p having Galois group S_p using Corollaries 1.2.2, 1.2.3. For the example below, θ will denote a root of the polynmial $f(x)$ and K will denote the number field generated by θ over $\mathbb{Q}$.

Example 1.2.4. *[57] Suppose* $p \geq 5$ *is an odd prime number. Set* $k = 2$, $m = \frac{p-1}{2}$, $a = 2, b = 2p$ *and* $n = p$ *in Corollary 1.2.2. Note that* $p \geq 5$ *implies* $m \geq 2$. *So we have* $f(x) = x(x^2+2)^m + 2p$ *is* $2-$*Eisenstein. Note that* $|D_f| = (2p)^{p-3}(4p^{2+p} + 2^p(p-1)^{p-1})$. *Applying Corollary 1.2.2, we get* $\mathbb{Z}_K = \mathbb{Z}[\theta]$ *iff the part* $U + V = p^{2+p} + 2^{p-2}(p-1)^{p-1}$ *in the discriminant* D_f *is square-free. For all primes* p *satisfying* $5 \geq p \leq 17$, *we verify that* $p^{2+p} + 2^{p-2}(p-1)^{p-1}$ *is square-free. Further, Theorem 14 implies that Galois group of* $f(x)$ *is* S_p. *Further, using Corollary 1.2.3 and keeping in mind that* $2 \mid \gcd(a, b)$ *and* $2^2 \nmid b$, *we conclude that* $f(x^{2^j})$ *are monogenic for all* $j \geq 0$ *and primes* $5 \leq p \leq 17$.

Now for $p = 19$, $p^{2+p} + 2^{p-2}(p-1)^{p-1} = 17^2 u$ *where* u *is a square-free integer. Then Corollary 1.2.2 implies that* $17 \mid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$. *Further, using Corollary 1.2.3 and keeping*

in mind that $2 \mid \gcd(a,b)$ *and* $2^2 \nmid b$*, we conclude that* $f(x^{2^j})$ *are non-monogenic for all* $j \geq 0$ *and* $p = 19$*. The computations to obtain factorisation of the discriminant were carried out using sage.*

Observing (1.5), it is evident that any irreducible polynomial $f(x)$ with a squarefree discriminant is monogenic. This is precisely the method used in [66, 10]. However, when D_f is not squarefree, establishing the monogenity of $f(x)$ becomes non-trivial.

Recently, Jones [60] found infinitely many monogenic polynomials of given prime degree p whose discriminant is not squarefree. Part of this result relied on generalized *abc*-conjecture for number fields. Jones and White [63] gave asymptotic formula for some special types of monogenic trinomials. In 2021, Jones [61] gave an infinite family of monogenic polynomials of general degree but no asymptotic formula was provided. In a joint work with Jakhar and Srinivas, we provide an asymptotic formula for the number of monogenic polynomials of the type $x^{n-km}(x^k+a)^m + b \in \mathbb{Z}[x]$.

Theorem 15. *[59, Theorem 1.1] Let* n, m, k *be positive integers with* $n > km$ *and* $k \mid n$*. Let* $t = n/k$ *and* $\kappa = \ell \operatorname{rad}(km)$*, where* ℓ *is a prime number not dividing* km*. Then for a fixed integer* a *coprime to* t *and divisible by* κ*, there are*

$$\frac{X}{\kappa\zeta(2)} \prod_{p\mid\kappa} \left(1+\frac{1}{p}\right)^{-1} \prod_{p\nmid atm(t-m)} \left(1-\frac{1}{p^2-1}\right) + O(X^{3/4}). \tag{1.8}$$

monogenic polynomials $f(x) = x^{n-km}(x^k+a)^m + b$ *satisfying* $b \leq X$ *and* $b \equiv 0 \pmod{\kappa}$*. The* O*-constant in* (1.8) *may depend on* n, k, m *and* a*.*

The proof of the above theorem is given in Section 5.4. A necessary condition for $f(x) = x^{n-km}(x^k+a)+b$ to be monogenic is that b must be squarefree, as can be seen in 12. Our next result proves that there are infinitely many monogenic polynomial $f(x)$ with both a and b squarefree. Part of the proof relies on *abc*-conjecture for number fields (see [86, Conjecture 4.1]).

Theorem 16. *[59, Theorem 1.2] Let* n, m, k, t, ℓ *and* κ *be as in Theorem 15 with* $\gcd(t, \kappa) = 1$*. Let* b *be a squarefree integer divisible by* κ*. Assume abc-conjecture for number fields, then there exists infinitely many primes* p *such that* $f(x) = x^{n-km}(x^k +$

$\kappa p)^m + b$ *is monogenic. However, for* $t = 2, 3$*, the result is true without assuming abc-conjecture.*

The proof of the above theorem is given in Section 5.5.

Remark 1.2.5. *We wish to point out here that in the above theorems, if* $k > 1$ *and* $n - k > 2$*, then the polynomials will have a squarefull discriminant as can be seen from* (1.7)*. Further we also note that, if* $n - k > k \geq 3$*, then the discriminant of these polynomials are* k*-full.*

It is worth noting that each monogenic polynomial derived from the aforementioned theorems helps to construct infinite families of monogenic polynomials of higher degrees. This is achievable through the application of Corollary 1.2.3, which facilitates the generation of such families by composing $f(x)$ with x^{q^j}, where q satisfies the conditions outlined in the corollary. Proof of Theorems 12, 13, 14, 15 and 16 are published in [59, 57] and are given in Chapter 5 of this thesis.

Chapter 2

Truncated Binomial Polynomials

For positive integers $n \geq m$, let $P_{n,m}(x) := \sum_{j=0}^{m} \binom{n}{j} x^j = \binom{n}{0} + \binom{n}{1}x + \ldots + \binom{n}{m}x^m$ be the truncated binomial expansion of $(1+x)^n$ consisting of all terms of degree $\leq m$. It is conjectured that for $n > m+1$, the polynomial $P_{n,m}(x)$ is irreducible. In this Chapter, We confirm this conjecture when $2m \leq n < (m+1)^{10}$. Also we show that for any $r \geq 10$ and $2m \leq n < (m+1)^{r+1}$, the polynomial $P_{n,m}(x)$ is irreducible when $m \geq \max\{10^6, 2r^3\}$. Under the explicit abc-conjecture, for a fixed m, we give an explicit n_0, n_1 depending only on m such that $\forall n \geq n_0$, the polynomial $P_{n,m}(x)$ is irreducible. Further $\forall n \geq n_1$, the Galois group associated to $P_{n,m}(x)$ is the symmetric group S_m. The results of this chapter has been published in [76].

2.1 Preliminaries

Recall that, for positive integers $n \geq m$, the truncated binomial polynomial which is the truncation of $(1+x)^n$ at m^{th} stage is defined as:

$$P_{n,m}(x) := \sum_{j=0}^{m} \binom{n}{j} x^j = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{m}x^m.$$

In this chapter, we prove Theorems 1, 2, 3 and 4 which are about the irreducibility and Galois group of $P_{n,m}(x)$. The ideas of the proofs are quite general in nature. For

the proofs of theorems, we consider the Newton polygons of $F_{n,m}(x)$ and $P_{n,m}(x-1)$ where

$$F_{n,m}(x) := \sum_{j=0}^{m} \binom{n-m-1+j}{j} x^{m-j} \quad \text{and} \quad P_{n,m}(x-1) = \sum_{j=0}^{m} c_j x^j$$

with $c_j = \sum_{i=j}^{m} \binom{n}{i}\binom{i}{j}(-1)^{i-j}$ (see [35]). Note that the irreducibility of $P_{n,m}(x)$, $P_{n,m}(x-1)$ and $F_{n,m}(x)$ are all same since $F_{n,m}(x+1) = x^n P_{n,m}(1/x)$ (see [9, Lemma 3]). A simple calculation yields that

$$c_j = (-1)^{m-j}\binom{n}{j}\binom{n-j-1}{m-j} = \frac{(-1)^{m-j}n(n-1)\cdots(n-m)}{j!(m-j)!}\frac{1}{n-j}. \tag{2.1}$$

The proof of Theorem 1 spreads over Sections 2.2.1, 2.2.2 and 2.2. The proof of Theorem 2 is given in Section 2.3. Theorems 3 and 4 are proved in Section 2.4. The calculations presented in this paper were performed using the software system SAGE. These SAGE codes has been listed in the Section 2.5.

From this point onward, the symbol p will invariably represent a prime number, and the letters n, m, k, t will consistently denote positive integers. For any positive integer v, let $P(v)$ stand for its greatest prime divisor, with the understanding that $P(1) = 1$. Let $\pi(v)$ denote the number of primes upto v. We begin this section with some bounds on prime counting functions due to Dusart.

Lemma 2.1.1. *[28, pp. 14; Prop 1.7] For $v > 1$, we have*

1. $\pi(v) \leq \dfrac{v}{\log v}\left(1 + \dfrac{1.2762}{\log v}\right)$.
2. $\displaystyle\prod_{p \leq v} p < 2.71851^v$.

Definition 2.1.2. *Fix $m \geq 2$. For positive integers $t \leq m/2$ and e, define*

$$U_t(e) := \left\{ l \in [0,m] : t = a\frac{l}{e} + b\frac{m-l}{e} \text{ with } a\frac{l}{e}, b\frac{m-l}{e} \in \mathbb{Z} \right\},$$
$$V_t(e) := \left\{ l \in [0,m] : t = a\frac{l}{e} + b\frac{m-l}{e} \text{ with } a\frac{l}{e}, b\frac{m-l}{e} \in \mathbb{Z} \text{ and } a \neq b \right\} \setminus \{0, m\}$$
$$\text{and} \quad W_t(e) := \left\{ l \in [0,m] : t = a\frac{l}{e} + b\frac{m-l}{e} \text{ with } a\frac{l}{e}, b\frac{m-l}{e} \in \mathbb{Z} \text{ and } a = b \right\}$$

where $0 \leq a, b \leq e$. *Throughout the paper, the integer* l *will lie between* 0 *and* m *both inclusive and the integer* t *will lie between* 1 *and* $\frac{m}{2}$ *both inclusive.*

Note that for any positive integer k, $U_t(e) \subseteq U_t(ke)$ and $V_t(e) \subseteq V_t(ke)$. Clearly, $U_t(e) = W_t(e) \cup V_t(e)$. Suppose that $W_t(e)$ is non-empty, say $l_0 \in W_t(e)$. Then $t = a\frac{l_0}{e} + a\frac{m-l_0}{e} \implies t = \frac{am}{e}$. In fact, if we assume $t = \frac{im}{j}$ for some $i, j \in \mathbb{Z}_{>0}$ with $i \leq \frac{j}{2}$ then for any e divisible by j, $j \in W_t(e)$. Hence, we deduce that $W_t(e)$ is non-empty iff $t = \frac{im}{j}$ for some $j \mid e$. Further we can assume that i and j are relatively prime whenever $t = \frac{im}{j}$ and hence $j \mid m$. For $t = \frac{im}{j}$ and $j \mid e$, we notice that $a = b \implies \frac{im}{j} = a\frac{l}{e} + a\frac{m-l}{e} = \frac{am}{e}$ implying $a = \frac{ie}{j}$. Substituting this value of a in set $W_t(e)$, we obtain

$$\begin{aligned} W_t(e) =& \left\{ l : \frac{im}{j} = \frac{il}{j} + \frac{i(m-l)}{j} \text{ with } \frac{il}{j}, \frac{i(m-l)}{j} \in \mathbb{Z} \right\} \\ =& \{ l : j \mid l \} \qquad [\because \gcd(i, j) = 1] \end{aligned}$$

Summarizing all the above, we obtain.

$$W_t(e) = \begin{cases} \{ l : j \mid l \} & \text{if } t = \frac{im}{j}, \text{ where } j \mid (e, m) \text{ and } (i, j) = 1, \\ \emptyset & \text{otherwise.} \end{cases}$$

Now for the set $V_t(e)$ notice that if $\left\lceil \frac{e+1}{2} \right\rceil \leq a, b$ with at least one inequality strict (as $a \neq b$ in $V_t(e)$) then $t = a\frac{l}{e} + b\frac{m-l}{e} > \left\lceil \frac{e+1}{2} \right\rceil \frac{m}{e} \geq \frac{m}{2}$ which is not possible. Also note that,

$$V_t(e) \subseteq \left\{ l \in [0, m] : \frac{te - bm}{a - b} = l \text{ for some } 0 \leq a \neq b \leq e \right\}.$$

Therefore, we conclude $V_t(e) \subseteq S_t(e)$ and hence $|V_t(e)| \leq M_e$ where $S_t(e)$ and M_e are as defined by Jakhar and Sangwan [58].

Definition 2.1.3. *For a positive integer* e, M_e *is defined as*

$$M_e = \begin{cases} \frac{(e+1)(3e+1)}{4} & \text{if } e \text{ is odd,} \\ \frac{e(3e+2)}{4} & \text{if } e \text{ is even.} \end{cases}$$

The motivation for defining the set $U_t(e)$ comes from the Dumas' Theorem 1.1.8.

Definition 2.1.4. *For $n > m$, we define*

$$\mathfrak{Z}_m := \{i : 0 \leq i < m, P(n-i) > m\}, \quad \mathfrak{z}_m := |\mathfrak{Z}_m|$$
$$\text{and } g_{n,m} := \#\{0 \leq i < m : \exists p > m \text{ with } v_p(n+i) \text{ odd}\}.$$

We prove the following lemma, which will be crucial for the proofs of Theorems 1, 2, 3 and 4.

Lemma 2.1.5. *Let $2 \leq 2m \leq n < (m+1)^{r+1}$ for some positive integer r. Let $1 \leq t \leq \frac{m}{2}$. If $\mathfrak{Z}_m \setminus \bigcup_{e=1}^{r} U_t(e)$ is non-empty then $P_{n,m}(x)$ does not have a factor of degree t over $\mathbb{Q}$. Further, for $t \notin D = \{im/e : e \leq r; 1 \leq i \leq \left[\frac{e+1}{2}\right]\}$, if $\mathfrak{Z}_m \setminus \bigcup_{e=1}^{r} V_t(e)$ is non-empty then $P_{n,m}(x)$ does not have a factor of degree t over $\mathbb{Q}$.*

Proof. Let $2 \leq 2m \leq n < (m+1)^{r+1}$ for some positive integer r and $l \in \mathfrak{Z}_m$. Then there exists a prime $p > m$ such that $p^e \mid\mid (n-l)$ with $e \leq r$. Suppose $P_{n,m}(x)$ has a factor of degree $t \in \left[1, \frac{m}{2}\right]$. Then $P_{n,m}(x-1)$ has a factor of degree t and the Newton polygon of $P_{n,m}(x-1)$ with respect to p consists of two line segments one joining $(0, e)$ with $(m-l, 0)$ and another joining $(m-l, 0)$ with (m, e). Applying Dumas' Theorem (Theorem 1.1.8), we obtain

$$t = a\frac{l}{e} + b\frac{m-l}{e} \quad \text{for some integers } 0 \leq a, b \leq e \text{ and } a\frac{l}{e}, b\frac{m-l}{e} \in \mathbb{Z} \tag{2.2}$$

implying $l \in U_t(e)$. Hence $\mathfrak{Z}_m \subseteq \bigcup_{e=1}^{r} U_t(e)$.

Therefore, if $\mathfrak{Z}_m \setminus \bigcup_{e=1}^{r} U_t(e)$ is non-empty, then $P_{n,m}(x)$ cannot have a factor of degree t.

Further for $t \notin D$ clearly $U_t(e) = V_t(e)$ implying $\mathfrak{Z}_m \subseteq \bigcup_{e=1}^{r} V_t(e)$ whenever $P_{n,m}(x)$ has a factor of degree t. Therefore, if $\mathfrak{Z}_m \setminus \bigcup_{e=1}^{r} V_t(e)$ is non-empty, then $P_{n,m}(x)$ cannot have a factor of degree t. □

The following consequence is immediate.

Corollary 2.1.6. *Let $2 \leq 2m \leq n < (m+1)^{r+1}$ for some positive integer r. Suppose $P_{n,m}(x)$ has a factor of degree t. Let*

$$\mathcal{L}_{m,t} = \left\{ l \in [0,m] : l \notin \bigcup_{e=1}^{r} U_t(e) \right\}.$$

Then $P(n-l) \leq m$ for all $l \in \mathcal{L}_{m,t}$.

Lemma 2.1.7. *If $n > m$, then*

$$\mathfrak{z}_m \geq m - \pi(m) - \frac{\log(m-1)!}{\log(n-m)} \geq m - \pi(m) - \frac{(m-1)\log(m-1)}{\log(n-m)}.$$

Proof. Let $T = \{n-i : 0 \leq i < m, P(n-i) \leq m\}$ and $t = |T|$. Then $t = m - \mathfrak{z}_m$. For each prime $p \leq m$, choose $n - i_p \in T$ such that $v_p(n-i_p)$ is maximal. Let $T' = T \backslash \{n - i_p : p \leq m\}$. For $i \neq i_p$, from $n-i = n-i_p+i_p-i$, we have $v_p(n-i) \leq v_p(i_p-i)$. Hence,

$$v_p\left(\prod_{\substack{i=1 \\ i\neq i_p}}^{t}(n-i)\right) \leq v_p\left(\prod_{\substack{i=1 \\ i\neq i_p}}^{t}(i_p-i)\right) \leq v_p\left(i_p!(m-1-i_p)!\right) \leq v_p((m-1)!).$$

Therefore, from $t = m - \mathfrak{z}_m$,

$$(n-m)^{m-\mathfrak{z}_m-\pi(m)} = (n-m)^{t-\pi(m)} \leq \prod_{n-i\in T'}(n-i) \leq (m-1)!$$
$$\Longrightarrow \mathfrak{z}_m \geq m - \pi(m) - \frac{\log((m-1)!)}{\log(n-m)}$$

implying the first assertion of the lemma. The second inequality of the lemma follows by observing that $(m-1)! \leq (m-1)^{m-1}$. □

The following result is the generalization of an observation made by Borisov et al. in [9, pp. 4].

Lemma 2.1.8. *Suppose $F_{n,m}(x)$ has a factor of degree $t \leq m/2$. Fix $l \in \{0,1,2,\ldots,t-1\}$ and a factor q of $m-l$. Let $g_0 = \max_{1\leq s\leq l}\{\gcd(q,s)\}$. If $p > m$ is such that $p^e || (n-m+l)$ or $p^e || (n-l)$, then $e \geq q/g_0$.*

Proof. Let $p > m$ be such that $p^e || (n-m+l)$. For $l+1 \leq j \leq m$, we deduce from

$$\binom{n-m-1+j}{j} = \frac{(n-m-1+j)(n-m+j-2)\dots(n-m-1+1)}{j!}$$

that p divides the numerator but not the denominator of the last expression. In fact, p^e exactly divides the numerator. As $p > m > t$ and $p \mid (n-m+l)$, we can conclude that $p \nmid \binom{n-m-1+l}{l}$. The Newton polygon of $F_{n,m}(x)$ with respect to this prime p, will have its rightmost edge the line segment joining $(l,0)$ and (m,e). Recall $t \geq l+1$. Since $F_{n,m}(x)$ has a factor of degree t, it follows that there are two lattice points, say (a,b) and (c,d) with $c > a$ on rightmost edge with $c-a \leq t$. Comparing slope of this line with the slope of rightmost edge, we observe that

$$\frac{|d-b|}{c-a} = \frac{e}{m-l} \Rightarrow (m-l)|d-b| = (c-a)e$$

Now $q \mid (m-l) \Rightarrow q \mid ((c-a)e)$. Hence we conclude that q/g divides e, where $g = \gcd(q, c-a)$. Since $q/g > 0$ and $e > 0$, we conclude that $e \geq q/g \geq q/g_0$.

Let $p > m$ be such that $p^e || (n-l)$. If $F_{n,m}(x)$ has a factor of degree t then $F_{n,m}(x+1)$ has a factor of degree t, where $F_{n,m}(x+1)$ is given by (see [9, Lemma 3])

$$F_{n,m}(x+1) = \sum_{j=0}^{m} \binom{n}{j} x^{m-j} (= x^m P_{n,m}(1/x)).$$

Since $l \leq t-1 \leq m/2-1$, we have $n-l \neq n-m+l$ and hence we deduce that for any j with $l+1 \leq j \leq m$, $p^e || \binom{n}{j}$ and $p \nmid \binom{n}{l}$. Therefore, the rightmost edge of the Newton Polygon of $F_{n,m}(x+1)$ with respect to this p contains the line segment with endpoints $(l,0)$ and (m,e). The same argument as above gives q/g divides e. Hence we conclude $e \geq q/g_0$. □

Remark: Observe that if q is prime and $q > l$, then $g_0 = 1$. Further $q \mid e$ from the proof of Lemma 2.1.8.

The next two results follows from the solutions of $P(x^2-1) < 100$ given explicitly by Luca and Najman [79].

Lemma 2.1.9. *If* $n > 814997916 (\approx 8.1 \times 10^8)$*, then* $P(n(n+2)(n+4)) > 100$*. In fact if* $n > 8818136 (\approx 9 \times 10^6)$ *and* $P(n(n+2)(n+4)) < 100$ *then*

$$n \in \{12334686, 13143546, 14993286, 15068480, 30947616, 86368800, 814997916\}.$$

Proof. Suppose $P(n(n+2)(n+4)) < 100$. Then $P(n(n+2)) < 100$ and $P((n+2)(n+4)) < 100$ implying $P((n+1)^2-1) < 100$ and $P((n+3)^2-1) < 100$. Hence $(n+1)$ and $(n+3)$ both should be a solution of $P(x^2-1) < 100$. From Luca and Najman [79], we find that $n \leq 814997916$ and further there are only 7 values of n satisfying the above contraints and are bigger than 8818136. These values are precisely those listed in the statement of the lemma. □

Lemma 2.1.10. *[79, Corollary 6] If* $P(n(n+1)(n+2)(n+3)) < 100$*, then* $n \leq 97524$*. If* $P(n(n+1)(n+2)) < 100$*, then* $n < 4.1 \times 10^8$*.*

For the application of explicit *abc*-conjecture in the proof of Theorems 3 and 4, we use the following result proved by Laishram and Shorey [75].

Lemma 2.1.11. *[75] Assume Baker's explicit abc-conjecture (Conjecture 1.1.3). Let* a, b *and* c *be pairwise coprime positive integers satisfying* $a + b = c$ *and* $R = R(abc)$*. Then*

$$c < R^{1+\frac{3}{4}}.$$

2.2 Proof of Theorem 1

In this section, we prove that the polynomial $P_{n,m}(x)$ is irreducible over $\mathbb{Q}$ for positive integers n, m satisfying $2m \leq n < (m+1)^{10}$. For the ease of calculations and using some better known estimates, we will split the proof the Theorem 1 into two parts. Assuming $m \geq 14$, first we will prove the irreducibility of $P_{n,m}(x)$ for n with $(m+1)^3 \leq n < (m+1)^5$ in Section 2.2.1, then for n with $(m+1)^5 \leq n < (m+1)^{10}$ in Section 2.2.2.

2.2.1 Proof for $m \geq 14$ and $(m+1)^3 \leq n < (m+1)^5$

Lemma 2.2.1. *For $m \geq 14$ and $(m+1)^3 \leq n < (m+1)^5$, the polynomial $P_{n,m}(x)$ is irreducible.*

Proof. Let $m \geq 14$ and $(m+1)^3 \leq n < (m+1)^5$. Suppose the polynomial $P_{n,m}(x)$ has a factor of degree $t \leq m/2$. By using the lower bound $3\log m$ of $\log(n-m)$ in Lemma 2.1.7 and using Lemma 2.1.1, we obtain

$$\mathfrak{z}_m \geq \begin{cases} m - \pi(m) - \frac{\log(m-1)!}{3\log m} & \text{if } m < 67. \\ m - \frac{m}{\log m}\left(1 + \frac{1.2762}{\log m}\right) - \frac{(m-1)\log(m-1)}{3\log m} & \text{if } m \geq 67. \end{cases} \tag{2.3}$$

We compute M_e (see Definition 2.1.3) for $2 < e \leq 4$ to obtain $M_3 = 10$ and $M_4 = 14$. Further using $|V_t(e)| \leq M_e$ and $V_t(e) \subseteq V_t(ke)$ for any $k \in \mathbb{Z}$, we get $|\bigcup_{e=1}^{4} V_t(e)| \leq |\bigcup_{2<e\leq 4} V_t(e)| \leq M_3 + M_4 = 24$. From (2.3), for $m \geq 67$, we obtain $\mathfrak{z}_m > 24 (\geq |\bigcup_{e=1}^{4} V_t(e)|)$ and for $32 \leq m < 67$, we obtain $\mathfrak{z}_m > |\bigcup_{e=1}^{4} V_t(e)|$. By Lemma 2.1.5, we have $t \in \{m/2, m/3, m/4\}$ for $m \geq 32$.

Since $n \geq (m+1)^3$, by [82, Theorem 1], we have $g_{n-m,m} \geq 8$ for $m \geq 14$ where $g_{n-m,m}$ is given in Definition 2.1.4. For t not of the type $im/3$ or $im/1$, if $|V_t(1) \cup V_t(3)| < 8$ then there exist $l \notin V_t(1) \cup V_t(3)$ and a prime $p > m$ such that either $p \mid\mid (n-l)$ or $p^3 \mid\mid (n-l)$ since $g_{n-m,m} \geq 8$. From Lemma 2.1.5, $P_{n,m}(x)$ cannot have a factor of degree t for $m \geq 14$. For $t = m/2$ and $m/4$, we obtain that $|V_t(1) \cup V_t(3)| < 8$ and hence for $m \geq 14$, $P_{n,m}(x)$ cannot have a factor of degree $m/2$ or $m/4$.

Let $t = m/3$. Then we have $|\bigcup_{e=1}^{4} U_t(e)| \leq 9 + m/3$. However from (2.3), we obtain $\mathfrak{z}_m > 9 + m/3$ for $m \geq 68$. The SAGE code used to calculate the values of $\mathfrak{z}_m$ is given in Listing 2.1.

Therefore, summarizing above, $P_{n,m}(x)$ is irreducible for $m \geq 68$. For $32 \leq m < 68$, $P_{n,m}(x)$ may have a factor of degree $m/3$ and further for $14 \leq m < 32$, $P_{n,m}(x)$ may have a factor of any degree $t < m/2$, $t \neq m/4$.

Let $14 \leq m < 68$ and $P_{n,m}(x)$ has a factor of degree $t = m/3$. Then $3 \mid m$. We give arguments for $m = 66$ and similar arguments work for the other values of m. Let $m = 66$. Then $t = m/3 = 22$. Using $61 \mid (m-5)$ and Lemma 2.1.8 with $l = 5(< t)$ and $q = 61$, we obtain $61 \mid v_p((n-5)(n-66+5))$ for any prime $p > 66$. Since $n < (m+1)^5 < 67^{61}$, we must have $v_p((n-5)(n-66+5)) = 0$ for all primes $p > 66$ i.e. $P((n-5)(n-61)) \leq 66$. Again using $59 \mid (m-7)$ and Lemma 2.1.8 with $l = 7(< t)$ and $q = 59$ yields $P((n-7)(n-59)) \leq 66$. Hence, $P((n-5)(n-7)(n-59)(n-61)) \leq 66$ implying $P((n-6)^2 - 1) \leq 66 < 100$ and $P((n-60)^2 - 1) \leq 66 < 100$. Therefore, $n-6$ and $n-60$ are solutions of $P(x^2-1) < 100$. From Luca and Najman [79], this is possible for 13 values of n. For each such n, there exist $p > 66$ with $v_p(n-1) = 1$. For eg. $n = 108763$, there exist $p = 18127 > 66$ with $v_p(n-1) = 1 \implies t \in \{1, 65\}$ contradicting $t = 22$. Similarly, we exclude factors of degree $m/3$ for other values of m with $14 \leq m < 68$.

Let $14 \leq m \leq 31$ and assume that $P_{n,m}(x)$ has a factor of degree $t \notin \{m/2, m/3, m/4\}$. Recall that if $|V_t(1) \cup V_t(3)| < 8$ then $P_{n,m}(x)$ cannot have a factor of degree t. From now on we will consider those t with $|V_t(1) \cup V_t(3)| \geq 8$. For such a t, using explicit computation we find $l_1, l_2 \in \mathcal{L}_{m,t}$ (with $r = 4$) and $i_1, i_2 \in \{1, 2, 4\}$ such that $l_1 + i_1, l_2 + i_2 \in \mathcal{L}_{m,t}$. The values of l_1, l_2 and i_1, i_2 were calculated using the algorithm given in Listing 2.3. Given $l \in \{l_1, l_1 + i_1, l_2, l_2 + i_2\} \subseteq \mathcal{L}_{m,t}$, we have $P(n-l) \leq m$ by Corollary 2.1.6. Using Lehmer [77], there are only few values of $n - l_1$ and $n - l_2$ which are explicitly given. We have excluded these values of n using the prime divisors of $n - i$ for $0 \leq i \leq m$. □

2.2.2 Proof for $m \geq 14$ and $(m+1)^5 \leq n < (m+1)^{10}$

We start this section with the following result.

Lemma 2.2.2. *For $m \geq 68$ and $(m+1)^5 \leq n < (m+1)^{10}$, the polynomial $P_{n,m}(x)$ is either irreducible over $\mathbb{Q}$ or it has a factor of degree in*

$$D = \left\{ \frac{im}{j} : 2 \leq j \leq 9, 2i \leq j, \gcd(i,j) = 1 \right\}.$$

Proof. Let $m \geq 68$ and $(m+1)^5 \leq n < (m+1)^{10}$. Suppose the polynomial $P_{n,m}(x)$ has a factor of degree $t \leq m/2$, with $t \notin D$. By using the lower bound $5 \log m$ of $\log(n-m)$ in Lemma 2.1.7 and using Lemma 2.1.1, we obtain

$$\mathfrak{z}_m \geq \mathcal{Z}_m := \begin{cases} m - \pi(m) - \frac{\log(m-1)!}{5 \log m} & \text{if } m < 200. \\ m - \pi(m) - \frac{(m-1)\log(m-1)}{5 \log m} & \text{if } 200 \leq m < 370. \\ m - \frac{m}{\log m}\left(1 + \frac{1.2762}{\log m}\right) - \frac{(m-1)\log(m-1)}{5 \log m} & \text{if } m \geq 370. \end{cases} \tag{2.4}$$

It suffices to show $\mathcal{Z}_m > |\bigcup_{e=1}^{9} V_t(e)|$ by Lemma 2.1.5.

Using $|V_t(e)| \leq M_e$ (given by Definition 2.1.3) and $V_t(e) \subseteq V_t(ke)$ for any $k \in \mathbb{Z}$, we have $|\bigcup_{e=1}^{9} V_t(e)| \leq \sum_{e=5}^{9} M_e = 220$. From (2.4), we obtain $\mathcal{Z}_m > 220$ for $m \geq 370$.

Hence we consider $m < 370$. For $m < 370$, the computation performed using the algorithm given in Listing 2.2 yields:

$$\max_{t,m} |V_t(9)| \leq 38; \quad \max_{t,m} |V_t(8)| \leq 32; \quad \max_{t,m} |V_t(7)| \leq 28$$

$$\implies |\bigcup_{e=1}^{9} V_t(e)| \leq \sum_{e=5}^{6} M_e + 28 + 32 + 38 = 152.$$

For $291 \leq m < 370$, we obtain $\mathcal{Z}_m > 152$. Hence $m < 291$. Exact computation for $m < 291$ yields

$$|\bigcup_{e=1}^{9} V_t(e)| < \mathcal{Z}_m \text{ for } 103 \leq m < 291 \text{ and } m \in T = \{85, 89, 91, 95, 97, 99, 100, 101\}.$$

Hence, we consider $68 \leq m < 103$ and $m \notin T$. For such an m, we find maximum $5 \leq E \leq 8$ such that $|\bigcup_{e=1}^{E} V_t(e)| < \mathcal{Z}_m$. From Lemma 2.1.5, we obtain that $P_{n,m}(x)$ can only have a factor of degree im/j for $n < (m+1)^{E+1}$. Thus we may assume that $n \geq (m+1)^{E+1}$. Further, using the lower bound $(E+1)\log m$ of $\log(n-m)$ in Lemma 2.1.7, we obtain $|\bigcup_{e=1}^{9} V_t(e)| < \mathfrak{z}_m$. Hence the assertion follows. □

Lemma 2.2.3. *For $m \geq 68$ and $(m+1)^5 \leq n < (m+1)^{10}$, the polynomial $P_{n,m}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. By Lemma 2.2.2, it suffices to check that the polynomial $P_{n,m}(x)$ does not have factor of degree $t = im/j \in D$. Throughout the proof l will be chosen between 0 to m.

Using $t = im/j$ in the set $V_t(e)$, we observe that

$$\bigcup_{e=1}^{9} V_t(e) \subseteq \left\{ l : \frac{im}{j} = a\frac{l}{e} + b\frac{m-l}{e} \text{ for some } e \leq 9 \text{ and } 0 \leq a \neq b \leq e \right\} \setminus \{0, m\}$$
$$= \left\{ l : \frac{l}{m} = \frac{ei - bj}{j(a-b)} \text{ for some } e \leq 9 \text{ and } 0 \leq a \neq b \leq e \right\} \setminus \{0, m\}.$$

As $0 < l < m$, we have $0 < \frac{l}{m} < 1$ implying

$$|\bigcup_{e=1}^{9} V_t(e)| \leq \# \left\{ 0 < \frac{ei - bj}{j(a-b)} < 1 : e \leq 9 \text{ and } 0 \leq a \neq b \leq e \right\} =: v_t.$$

Using lower bound for $\mathfrak{z}_m$ in (2.4) and exact computations using Listings 2.1 and 2.2 yields the following

Degree $t = \frac{im}{j}$	v_t	$\mathfrak{z}_m > v_t + \frac{m}{j} + 1$ for
$m/2$	27	$m \geq 235$
$m/3$	45	$m \geq 168$
$m/4$	59	$m \geq 168$
$m/5$	57	$m \geq 144$
$m/6$	63	$m \geq 146$
$m/7$	59	$m \geq 132$
$m/8$	57	$m \geq 123$
$m/9$	45	$m \geq 96$
$2m/5$	63	$m \geq 158$
$2m/7$	71	$m \geq 155$
$2m/9$	67	$m \geq 140$
$3m/7$	67	$m \geq 147$
$3m/8$	75	$m \geq 159$
$4m/9$	79	$m \geq 161$

For $m \geq 235$,

$$\mathfrak{z}_m > v_t + \frac{m}{j} + 1 \geq |\bigcup_{e=1}^{9} V_t(e)| + |\bigcup_{e=1}^{9} W_t(e)| \geq |\bigcup_{e=1}^{9} U_t(e)|.$$

Hence, $P_{n,m}(x)$ is irreducible for $m \geq 235$ by Lemma 2.1.5.

For $m < 235$, exact computation using Listings 2.1 and 2.3 yields $\mathfrak{z}_m > |\bigcup_{e=1}^{9} U_t(e)|$ is true for each $68 \leq m < 235$ except when $t = \frac{m}{2}$ and $m = 70, 90$. Let $(m,t) \in \{(70,35),(90,45)\}$. We find that $1,3,5 \in \mathcal{L}_{m,t}$ with $r = 9$. Corollary 2.1.6 implies $P((n-1)(n-3)(n-5)) \leq m < 100$. From Lemma 2.1.9, we obtain $n - 5 < 814997916$ contradicting $n \geq (m+1)^5 \geq 71^5 > 814997921$. □

Lemma 2.2.4. *For $41 < m < 68$ and $(m+1)^5 \leq n < (m+1)^{10}$, the polynomial $P_{n,m}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Let $41 < m < 68$ and assume that $P_{n,m}(x)$ has a factor of degree t. Recall that if $|\bigcup_{e=1}^{9} U_t(e)| < \mathfrak{z}_m$, then Lemma 2.1.5 implies that $P_{n,m}(x)$ cannot have a factor of degree t. From now on we will consider $t \in T_0(m)$ where

$$T_0(m) := \left\{ t : 0 < t \leq \frac{m}{2} \text{ and } |\bigcup_{e=1}^{9} U_t(e)| \geq \mathfrak{z}_m \right\}.$$

For $t \in T_0(m)$, consider the set $\mathcal{L}_{m,t}$ defined in Corollary 2.1.6 with $r = 9$. Using Corollary 2.1.6, we obtain $P(n-l) \leq m$ for all $l \in \mathcal{L}_{m,t}$. Let

$$T_1(m) := \left\{ t \in T_0(m) : \exists l \in \mathcal{L}_{m,t} \text{ with } l+2, l+4 \in \mathcal{L}_{m,t} \text{ or } l+1, l+2, l+3 \in \mathcal{L}_{m,t} \right\}.$$

Let $t \in T_1(m)$. Then there exist $l \in \mathcal{L}_{m,t}$ such that either $P((n-l)(n-l-2)(n-l-4)) \leq m < 100$ or $P((n-l)(n-l-1)(n-l-2)(n-l-3)) \leq m < 100$. Here $n \geq (m+1)^5 \geq 42^5 > 8818136$ and we use Lemma 2.1.9 or Lemma 2.1.10, respectively to obtain

$$n - l - 4 \in \{12334686, 13143546, 14993286, 15068480, 30947616, 86368800, 814997916\}.$$

For these values of n, we find that there exist $0 \leq i \leq m$ such that $P(n-i) > m$ and $i \notin \bigcup_{e=1}^{9} U_t(e)$. Hence, $P_{n,m}(x)$ cannot have a factor of degree t for $t \in T_1(m)$.

For $t \in T_0(m) \backslash T_1(m)$, define

$$T_2(m) := \left\{ t \in T_0(m) : \exists l_1 \neq l_2 \in \mathcal{L}_{m,t} \text{ and } \exists i \in \{1,2\} \text{ such that } l_1 + i, l_2 + i \in \mathcal{L}_{m,t} \right\}.$$

For $t \in T_2(m)$, suppose $l_1, l_2, l_1 + i, l_2 + i \in \mathcal{L}_{m,t}$ for some $i \in \{1,2\}$. Clearly for each $l \in \{l_1, l_1 + i, l_2, l_2 + i\}$, we have $P(n-l) \leq m < 100$. Suppose $i = 1$. Then we have $P((n-l_1)(n-l_1-1)) < 100$ implying $P((2(n-l_1))(2(n-l_1)-2)) < 100$ i.e. $P((2(n-l_1)-1)^2 - 1) < 100$ a solution to $P(x^2-1) < 100$. If $i = 2$ then $P((n-l_1-1)^2 - 1) = P((n-l_1)(n-l_1-2)) < 100$ which is again a solution to $P(x^2-1) < 100$. Applying similar arguments to l_2 we obtain another solution of $P(x^2-1) < 100$. The solutions to $P(x^2-1) < 100$ is given in Luca and Najman [79], there are only few choices of solutions x_1, x_2 satisfying $x_1 - x_2 = (n-l_1-1) - (n-l_2-1) = l_2 - l_1$ when $i = 2$ similarly $x_1 - x_2 = (2(n-l_1)-1) - (2(n-l_2)-1) = 2(l_2 - l_1)$ when $i = 1$. We use algorithm in Listing 2.3 to find these values of l_1, l_2 and $i \in \{1,2\}$. We have excluded these values of n using the prime divisors of $n-i$ for $0 \leq i \leq m$. Hence, $P_{n,m}(x)$ cannot have a factor of degree t for any $t \in T_1(m) \cup T_2(m)$. After this we are left with the following few cases:

$$(m,t) \in T = \{(42,16), (43,15), (43,18), (47,18), (50,22), (52,18), (54,14), (57,22)\}.$$

For $(m,t) \in T$, we follow the arguments similar to that shown for $m = 66,\ t = 22$ in the proof of Lemma 2.2.1 to exclude each $(m,t) \in T$. Hence, the assertion follows. □

Lemma 2.2.5. *For* $14 \leq m \leq 41$ *and* $(m+1)^5 \leq n < (m+1)^{10}$, *the polynomial* $P_{n,m}(x)$ *is irreducible over* $\mathbb{Q}$.

Proof. We apply the same method as in Lemma 2.2.4 except here we use the table given by Lehmer [77] instead of solutions to $P(x^2-1) < 100$ in the process of obtaining the few values of n. Then the assertions follows using the arguments in Lemma 2.2.4. □

Proof of Theorem 1. Combining the Lemmas from Section 2.2.1 and Section 2.2.2, we have obtained the irreducibility for $m \geq 14$. Using SAGE we find the solutions to the diophantine equations given in [35, pp. 462 (4)] for $6 < m < 14$. For these solutions, we have verified the irreducibility using the prime divisors of $n - i$ for $0 \leq i \leq m$. We already know the irreducibility for $m \leq 6$ due to [26]. Hence, the assertion follows. □

2.3 Proof of Theorem 2

For positive integers m and $r \geq 10$, let n be an integer in the range $2m \leq n < (m+1)^{r+1}$. For the above values of n, m and r, we prove that the polynomial $P_{n,m}(x)$ is irreducible over $\mathbb{Q}$ whenever $m \geq \max\{10^6, 2r^3\}$.

Proof of Theorem 2. Consider an integer t such that $0 \leq t \leq m/2$. Our objective is to determine the smallest integer value of m for which the polynomial $P_{n,m}(x)$ does not possess any factor of degree t. Then one simple observation to note is that for any positive integer k, $U_t(e) \subseteq U_t(ke)$. Using this observation, we note that

$$|\bigcup_{e=1}^{r} U_t(e)| \leq |\bigcup_{r/2<e\leq r} U_t(e)| \leq \begin{cases} \sum_{r/2<e\leq r} M_e + \frac{m}{j} & \text{if } t = \frac{im}{j} \in D, \\ \sum_{r/2<e\leq r} M_e & \text{otherwise.} \end{cases} \tag{2.5}$$

Computation yields that $\sum_{r/2<e\leq r} M_e < \frac{r^3}{3}$ for $r = 10$. Using induction one can easily prove that $\sum_{r/2<e\leq r} M_e < \frac{r^3}{3}$ for all $r \geq 10$.

As we have already proved the irreducibility for $2m \leq n < (m+1)^{10}$, we can assume that $n \geq (m+1)^{10}$. Substituting this lower bound for n along with upper bound for $\pi(m)$ (Lemma 2.1.1) in Lemma 2.1.7, we deduce

$$\mathfrak{z}_m \geq m - \frac{m}{\log m}\left(1 + \frac{1.2762}{\log m}\right) - \frac{(m-1)\log(m-1)}{10\log m} \geq \frac{2m}{3}$$

since $m \geq 10^6$. For $0 < t \leq \frac{m}{2}$, suppose that $t \notin D$ where the set D is as defined in Lemma 2.1.5. By Lemma 2.1.5, $P_{n,m}(x)$ does not have a factor of degree t if $\mathfrak{z}_m > |\bigcup_{e=1}^{r} V_t(e)|$ which is true if $\frac{2m}{3} \geq \frac{r^3}{3}$ i.e. $m \geq \frac{r^3}{2}$.

Now suppose $t = \frac{im}{j}$. Again by Lemma 2.1.5, $P_{n,m}(x)$ does not have a factor of degree t if $\mathfrak{z}_m > |\bigcup_{e=1}^{r} U_t(e)|$ which is true if $\frac{2m}{3} \geq \frac{r^3}{3} + \frac{m}{2}$ as $\frac{m}{j} \leq \frac{m}{2}$. This holds if $m \geq 2r^3$. Hence the assertion. □

2.4 Bounds using abc-conjecture

Filaseta et al. [35] proved that for a fixed m, there exist n_0 such that for all $n \geq n_0$, the polynomial $P_{n,m}(x)$ is irreducible. However their method is ineffective viz. we do not have any upper bound on the value of n_0. In this section using Baker's explicit abc-conjecture, we provide an explicit n_0.

Lemma 2.4.1. *Assume Baker's explicit abc-conjecture (Conjecture 1.1.3). Fix positive integers m, d, f with $f \geq d \geq 5$. Let a, b, c be positive integers with $P(abc) \leq m$. If the equation $ax^d - by^f = c$ has a solution $(x, y) \in \mathbb{N} \times \mathbb{N}$ then $a^{\frac{3}{5}} x^{d-3.5} < 2.71851^{\frac{7m}{4}}$. In particular, for $d \geq 7$ we have $ax^d < 2.71851^{3.5m}$.*

Proof. Let $(x, y) \in \mathbb{N} \times \mathbb{N}$ be a solution of the equation $ax^d - by^f = c$. We use Lemma 2.1.11 with $\varepsilon = \frac{3}{4}$ for the equation $ax^d = by^f + c$ to obtain $ax^d < R(axbyc)^{1+\varepsilon}$ implying

$$\begin{aligned} & ax^d < R(abc)^{1+\varepsilon} R(x)^{1+\varepsilon} R(y)^{1+\varepsilon} \\ \implies & ax^d < 2.71851^{(1+\varepsilon)m} x^{1+\varepsilon} R(y)^{1+\varepsilon} && [\textit{using Lemma 2.1.1}] \\ \implies & \frac{a^{\frac{3}{5}} x^{d-2-2\varepsilon}}{2.71851^{(1+\varepsilon)m}} a^{\frac{2}{5}} x^{1+\varepsilon} < y^{1+\varepsilon}. \end{aligned}$$

For $d \geq 5$, we want ε such that $d - 2 - 2\varepsilon > 0$ which is true for $\varepsilon = \frac{3}{4}$ chosen above. Assume that $a^{\frac{3}{5}} x^{d-2-2\varepsilon} \geq 2.71851^{7m/4}$ we obtain

$$a^{\frac{2}{5}} x^{7/4} < y^{7/4} \implies ax^d \leq (a^{\frac{2}{5}} x^{7/4})^{4d/7} < (y^{7/4})^{4d/7} \leq by^d \leq by^f,$$

since $d \leq f$ which is a contradiction to $ax^d > by^f$. Hence $a^{\frac{3}{5}} x^{d-3.5} < 2.71851^{\frac{7m}{4}}$. □

The following two lemmas are due to Filaseta et al. in [35, Lemma 2 and Lemma 3] with k replaced by m in their statement.

Lemma 2.4.2. *[35, Lemma 2] Let n' be the largest divisor of $n(n-m)$ that is relatively prime to $m!$. Write $n' = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where the p_j denote distinct primes and the e_j are positive integers. Let*

$$d = \gcd(m, e_1, e_2, \ldots, e_r). \tag{2.6}$$

Then the degree of each irreducible factor of $P_{n,m}(x)$ is a multiple of m/d.

Lemma 2.4.3. *[35, Lemma 3] Suppose $d = 2$ in the statement of Lemma 2.4.2. Let n'' be the largest divisor of $(n-1)(n-m+1)$ that is relatively prime to $m!$. Let p be a prime $> m$ such that $v_p(n'') = e \geq 1$. If $P_{n,m}(x)$ is reducible, then $(m-1) \mid e$.*

Next lemma will be helpful in the proof of Theorem 3.

Lemma 2.4.4. *Let $m \geq 7$ and $P_{n,m}(x)$ be reducible. Then there exists $i \in \{0,1,2,3\}$ and $r \geq 7$ such that*

$$n - i = ax^r \text{ and } n - m + i = by^r \text{ for some } a, b, x, y \in \mathbb{N} \text{ with } P(ab) \leq m. \tag{2.7}$$

Proof. Suppose $P_{n,m}(x)$ is reducible and d be as defined in Lemma 2.4.2. Then by Lemma 2.4.2, $P_{n,m}(x)$ has an irreducible factor of degree a multiple of m/d implying $d \geq 2$.

If $d = 2$ then Lemma 2.4.3 implies that (2.7) is satisfied for $i = 1$ and $r = m - 1$. Clearly $r = m - 1 \geq 7$ since $m \geq 7$ and $2 \mid m$.

If $d = 3$ then $P_{n,m}(x)$ has factors of degree $\frac{m}{3}$ and $\frac{2m}{3}$. Let $i \in \{1,2\}$ be such that $m - i$ is odd. Let $p > m$ be prime such that $p^e \mid\mid (n-i)$ and $r = \gcd(m-i, e)$. Then the Newton polygon of $P_{n,m}(x-1)$ with respect to p will consist of two line segments one joining $(0, e)$ to $(m-i, 0)$ and other joining $(m-i, 0)$ to (m, e). Applying Dumas' Theorem, we obtain $\frac{m-1}{r}$ divides ($\frac{m}{3}$ and $\frac{2m}{3} - 1$) or it divides ($\frac{m}{3} - 1$ and $\frac{2m}{3}$) when $i = 1$ and $\frac{m-2}{r}$ divides ($\frac{m}{3}$ and $\frac{2m}{3} - 2$) or it divides ($\frac{m}{3} - 2$ and $\frac{2m}{3}$) or it divides ($\frac{m}{3} - 1$ and $\frac{2m}{3} - 1$) when $i = 2$. In each of the cases, we obtain $\frac{m-i}{r}$ divides 4 implying $\frac{m-i}{r} = 1$ since $m - i$ is odd. Hence, we obtain $i \in \{1,2\}$ and $r = m - i$ such that $p^{r\alpha} \mid\mid (n-i)$ for all prime $p > m$ dividing $n - i$ and some positive integer α implying (2.7) is satisfied by $n - i$ for some $i \in \{1,2\}$ and $r = m - i$. Clearly $r = m - i \geq 7$ as $m \geq 7$ and $3 \mid m$.

Similar arguments also give that (2.7) is satisfied by $n-m+i$ for the same i, r as that for $n-i$.

If $d=4$ then $P_{n,m}(x)$ has factors of degree $\left(\frac{m}{2} \text{ and } \frac{m}{2}\right)$ or $\left(\frac{m}{4} \text{ and } \frac{3m}{4}\right)$. If $P_{n,m}(x)$ has factors of degree $\frac{m}{2}$ and $\frac{m}{2}$ then the assertion of the Lemma follows from the arguments used for $d=2$. Now suppose that $P_{n,m}(x)$ have factors of degree $\frac{m}{4}$ and $\frac{3m}{4}$. Let $p>m$ be prime such that $p^e \mid\mid (n-1)$ and $r=\gcd(m-1,e)$. Then the Newton polygon of $P_{n,m}(x-1)$ with respect to p will consist of two line segments, one joining $(0,e)$ to $(m-1,0)$ and other joining $(m-1,0)$ to (m,e). Applying Dumas' Theorem, we obtain $\frac{m-1}{r}$ divides ($\frac{m}{4}$ and $\frac{3m}{4}-1$) or it divides ($\frac{m}{4}-1$ and $\frac{3m}{4}$). In both the cases, we obtain $\frac{m-1}{r}$ divides 3 implying $r=\frac{m-1}{3}$ or $m-1$. If $r=m-1$ then $r \geq 7$ since $m \geq 7$ and $4 \mid m$. Let $r=\frac{m-1}{3}$. Then $r \geq 7$ for $m \geq 22$. Further from $4 \mid m$, $3 \mid (m-1)$ and $m \geq 7$, we only need to consider $m=16$.

Let $m=16$. Assume that $P_{n,16}(x)$ has factors of degree $\frac{m}{4}=4$ and $\frac{3m}{4}=12$. Let $p>m$ be a prime such that $p^e \mid\mid (n-2)$ and $r=\gcd(m-2,e)$. Then the Newton polygon of $P_{n,16}(x-1)$ with respect to p will consist of two line segments one joining $(0,e)$ to $(14,0)$ and other joining $(14,0)$ to $(16,e)$. Applying Dumas' Theorem, we obtain $\frac{14}{r}$ divides either both 4 and $12-2$ or both $4-1$ and $12-1$ or both $4-2$ and 12. In each of the cases, we obtain $\frac{14}{r} \mid 2$ implying $r=14$ or 7. Hence, we obtain $i \in \{1,2\}$ and $r \geq 7$ such that $p^{r\alpha} \mid\mid (n-i)$ for all $p>m$ dividing $n-i$ and some positive integer α, i.e. $n-i$ satisfies (2.7). Similar arguments also give $n-m+i$ satisfies (2.7).

If $d=5$ then $P_{n,m}(x)$ has factors of degree $\left(\frac{m}{5} \text{ and } \frac{4m}{5}\right)$ or $\left(\frac{2m}{5} \text{ and } \frac{3m}{5}\right)$. If $P_{n,m}(x)$ have factors of degree $\frac{m}{5}$ and $\frac{4m}{5}$ using arguments as above, we obtain (2.7) with $i=1$ and $r=\frac{m-1}{\gcd(m-1,4)}$. Then $r \geq 7$ for $m \geq 29$. Further from $5 \mid m$, $2 \mid (m-1)$ and $m \geq 7$, we only need to consider $m \in \{15,25\}$. For $m \in \{15,25\}$, we obtain (2.7) with $i=2$ and $r=m-2 \geq 7$.

Now, if $P_{n,m}(x)$ has factors of degree $\frac{2m}{5}$ and $\frac{3m}{5}$, we obtain (2.7) with $i=1$ and $r=\frac{m-1}{\gcd(m-1,3)}$. Clearly $r \geq 7$ for $m \geq 22$. Further from $5 \mid m$, $3 \mid (m-1)$ and $m \geq 7$, we have $r \geq 7$ except for $m=10$. For $m=10$, similar arguments can be used to obtain (2.7) with $i=3$ and $r=m-3=7$.

If $d = 6$ then $P_{n,m}(x)$ has factors of degree $\left(\frac{m}{6} \text{ and } \frac{5m}{6}\right)$ or $\left(\frac{m}{2} \text{ and } \frac{m}{2}\right)$ or $\left(\frac{m}{3} \text{ and } \frac{2m}{3}\right)$. If $P_{n,m}(x)$ has factors of degree $\frac{m}{2}$ and $\frac{m}{2}$ then the assertion of the Lemma follows from the arguments used for $d = 2$. If $P_{n,m}(x)$ has factors of degree $\frac{m}{3}$ and $\frac{2m}{3}$ then the assertion of the Lemma follows from the arguments used for $d = 3$.

If $P_{n,m}(x)$ has factors of degree $\frac{m}{6}$ and $\frac{5m}{6}$, we obtain (2.7) with $i = 1$ and $r = \frac{m-1}{\gcd(m-1,5)}$. From $6 \mid m$, observe that $r = m - 1 \geq 7$ if $5 \nmid (m-1)$ and $r = \frac{m-1}{5} \geq 7$ if $5 \mid (m-1)$.

If $d \geq 7$ then $p^{d\alpha} \mid\mid (n(n-m))$ for all primes $p > m$ dividing $n(n-m)$ and some $\alpha \in \mathbb{N}$. Hence we obtain (2.7) with $i = 0$ and $r = d \geq 7$. □

Now we will prove Theorem 3 by providing the value of n_0 such that for all $n \geq n_0$, $P_{n,m}(x)$ is irreducible.

Proof of Theorem 3. Fix $m \geq 7$ and assume that $P_{n,m}(x)$ is reducible. Applying Lemma 2.4.4, we deduce that there exists $i \in \{0, 1, 2, 3\}$ and an integer $r \geq 7$ satisfying (2.7). Note that $P(ax^r - by^r) = P(m - 2i) \leq m$ also $P(ab) \leq m$. Applying Lemma 2.4.1, we obtain $n - i = ax^r < 2.71851^{3.5m} \implies n < 2.71851^{3.5m} + 3$. Therefore, for $m \geq 7$ and $n \geq 2.71851^{3.5m} + 3$ the polynomial $P_{n,m}(x)$ is irreducible over $\mathbb{Q}$. □

The proof of Theorem 4 is based on the following result, see [45, Theorem 2.2].

Lemma 2.4.5. *[45, Theorem 2.2] Let $f(x)$ be an irreducible polynomial of degree m and suppose q is prime in the interval $(m/2, m-2)$ such that the Newton polygon with respect to some prime p has an edge with slope a/b where a and b are relatively prime integers and $q \mid b$. Let Δ be the discriminant of $f(x)$. Then the Galois group of $f(x)$ over $\mathbb{Q}$ is the alternating group A_m if Δ is a square and is the symmetric group S_m if Δ is not a square.*

Filaseta and Moy [36, Lemma 3] showed that the discriminant of $P_{n,m}(x-1)$ is given by

$$\Delta = (-1)^{\frac{m(m-1)}{2}} (n(n-m))^{m-1} \left(\frac{(n-m+1)(n-m+2)\cdots(n-1)}{m!}\right)^{m-2}.$$

Using the above observation we prove the following result.

Lemma 2.4.6. *Let $m \geq 5$. Let Δ be the discriminant of $P_{n,m}(x-1)$. Then Δ is not a square for $n \geq \max\{\frac{m(m-1)^2}{4} + m + 1, (m-1)^2 + m - 1\}$.*

Proof. It was proved in [36, Lemma 4] that for even m, and $n \geq \frac{m(m-1)^2}{4} + m + 1$, Δ is not a square. Let m be odd. Then Δ is a square if there exists $y \in \mathbb{Z}$ such that

$$(n-m+1)(n-m+2)\cdots(n-1) = m!y^2. \tag{2.8}$$

Using [89, Corollary 2] with (k, n) replaced by $(m-1, n-m+1)$, we obtain that the equation (2.8) has no solution for $m-1 \geq 4$ and $n-m+1 > (m-1)^2$. Hence the assertion. Further note that $m^3 \geq \max\{\frac{m(m-1)^2}{4} + m + 1, (m-1)^2 + m - 1\}$. □

Let n, m be positive integers. In Theorem 4, we find the value of $n_1(m)$ such that for all $n \geq n_1(m)$, the polynomial $P_{n,m}(x)$ has Galois group S_m.

Proof of Theorem 4. By Bertrand's postulate, there is a prime number q with $\frac{m}{2} < q < m-2$ for $m \geq 8$. Further such $q \geq 7$ if $m \geq 10$ also $n - q \neq n - m + q$.

Let $p^e \mid\mid (n-q)$ with $p > m$. Then the Newton polygon of $P_{n,m}(x-1)$ with respect to p consists of two edges, one joining $(0, e)$ to $(m-q, 0)$ and the other joining $(m-q, 0)$ to (m, e). The rightmost edge of the Newton polygon has slope $\frac{e}{q}$. If $P_{n,m}(x-1)$ is irreducible, using Lemmas 2.4.5 and 2.4.6, we deduce that for $m \geq 5$ and $n > m^3$, the Galois group of $P_{n,m}(x-1)$ is S_m unless $q \mid e$. Using similar arguments for primes $p > m$ dividing $n - m + q$, we obtain that the Galois group is S_m unless $q \mid v_p(n-m+q)$ i.e. (2.7) is satisfied with $i = m - q$ and $r = q$.

As $P((n-m+q) - (n-q)) = P(2q-m) \leq m$, we obtain $ax^q - by^q = 2q - m$ where $P(ab(2q-m)) \leq m$. Since $q \geq 7$ for $m \geq 10$, applying Lemma 2.4.1 we obtain $n-m+q = ax^q < (2.71851)^{3.5m} \implies n < (2.71851)^{3.5m} + m - q \leq (2.71851)^{3.5m} + \frac{m}{2} - 1$.

Therefore, for $m \geq 10$ and $n \geq (2.71851)^{3.5m} + \frac{m}{2} - 1$, the irreducibility of $P_{n,m}(x-1)$ follows from Theorem 3 and hence the Galois group is S_m. □

2.5 SAGE codes

```
def factorial(k):
fac=0;
R=range(1,k);
for i in R:
fac=fac+log(i);
return(fac)

for m in range(200,300):
fac=factorial(m);
alpha= ceil(float(m- prime_pi(m) - ((m-1)*log(m-1))/(5*log(m))));
beta= ceil(float(m- prime_pi(m) - (fac)/(5*log(m+1)) - m/2))
print("For m=",m,"\t",alpha," ",beta);
```

Listing 2.1: Value of $\mathfrak{z}_m$

```
E=range(7,8);
s=0;
Vte=set(); Xte=set();
for m in range(291,370):
for t in range(1,ceil((m+1)/2)):
Vte.clear(); Xte.clear(); f=0;
for e in E:
Xte.clear();
for a in range(0,e+1):
for b in range(0,e+1):
if(a!=b):
r=simplify((t*e-m*b)/(a-b));
if(r>=0 and r in ZZ and r<=m):
Xte.add(r);
Vte=Vte.union(Xte);
s=max(s,len(Vte));

print("\t Max length of V_t(e)=",s);
```

Listing 2.2: The set $V_t(e)$ and its upper bound

```
m=42;
print("For m=",m);
E=range(1,10);
s=0; j=0;
T=range(1,ceil((m+1)/2));
Vte=set(); Xte=set(); Ute=set(); Yte=set();
for t in T:
print("\n\nFor t=",t,"\t",t/m);
j=(t/m).denominator();
Vte.clear(); Xte.clear(); f=0; Ute.clear(); Yte.clear();
for e in E:
Xte.clear();
for a in range(0,e+1):
for b in range(0,e+1):
if(a!=b):
r=simplify((t*e-m*b)/(a-b));
if(r>=0 and r in ZZ and r<=m):
Xte.add(r);
Vte=Vte.union(Xte);
s=max(s,len(Vte));
if(j in E):
for l in range(0,m+1):
if(l%j==0):
Yte.add(l);
Ute=Vte.union(Yte);
print("U_t(e) is a subset of ",sorted(Ute));

print("\nPairs (l,l+1) both not in U_t(e)")
for i in range(0,m):
if(i in Ute or (i+1) in Ute): f=2;
else: print(i,(i+1),end="\t");

print("\n\nPairs (l,l+2) both not in U_t(e)");
for i in range(0,m-1):
if(i in Ute or (i+2) in Ute): f=2;
else: print(i,i+2,end="\t");

print("\n\nPairs (l,l+4) both not in U_t(e)");
for i in range(0,m-3):
if(i in Ute or (i+4) in Ute): f=2;
else: print(i,i+4,end="\t");
```

Listing 2.3: The set $U_t(e)$ and $\mathcal{L}_{m,t}$

Chapter 3

Behaviour of Newton Polygon over polynomial composition

In this chapter, we study the structure of Newton polygons for compositions of polynomials over the rationals. For $f(x), g(x) \in \mathbb{Q}[x]$, we establish sufficient conditions under which the successive vertices of the Newton polygon of the composition $g(f^n(x))$ with respect to a prime p can be explicitly described in terms of the Newton polygon of the polynomial $g(x)$. Our results provide deeper insights into how the Newton polygon of a polynomial evolves under iteration and composition, with applications to the study of dynamical irreducibility, eventual stability, non-monogenity of tower of number fields, etc. All the proofs and results in this chapter are taken from [56].

3.1 Preliminaries

Throughout this chapter, p will always denote a prime number and we use the notation $NP_p(h)$ to denote the Newton polygon of $h(x) \in \mathbb{Q}[x]$ with respect to p. To prove Theorems 5 and 7, we will need the following four lemmas.

Lemma 3.1.1. *Let $g(x) = b_e x^e + b_{e-1}x^{e-1} + \cdots + b_0$, with $b_0 \neq 0$, be a polynomial of degree e with rational coefficients such that $v_p(b_e) = 0$ and p divides b_s for $0 \leq s \leq e-1$. Let $m_0, m_1, \ldots, m_{t-1}, m_t$ be integers such that the successive vertices of the Newton polygon of $g(x)$ with respect to p are given by the set*

$$\{(0,0), (e - m_1, v_p(b_{m_1})), \ldots, (e - m_{t-1}, v_p(b_{m_{t-1}})), (e, v_p(b_0))\},$$

where $m_0 = e$ and $m_t = 0$. If α is a positive integer such that $v_p(b_0) \leq \frac{v_p(b_{m_1})}{e-m_1}\alpha$, then for any s with $0 \leq s \leq t$, we have

$$v_p(b_{m_s}) \leq \frac{v_p(b_{m_1})}{e-m_1}(\alpha - m_s). \tag{3.1}$$

Proof. Denote $v_p(b_{m_s})$ by r_s for $0 \leq s \leq t$. Using the fact that $m_t = 0$ and the hypothesis $v_p(b_0) \leq \frac{r_1}{e-m_1}\alpha$, it is clear that (3.1) holds for $s = t$.

Now, let us fix an integer s with $0 \leq s < t$. As the slopes of the edges of the Newton polygon of $g(x)$ with respect to p are in increasing order, we can easily verify that

$$\frac{r_1}{e-m_1} \leq \frac{r_{s+1} - r_s}{m_s - m_{s+1}} \leq \frac{r_t - r_s}{e-(e-m_s)}.$$

Using the above inequality along with the hypothesis $r_t \leq \frac{r_1}{e-m_1}\alpha$, we obtain

$$r_s \leq r_t - \frac{r_1}{e-m_1}m_s \leq \frac{r_1}{e-m_1}\alpha - \frac{r_1}{e-m_1}m_s.$$

This completes the proof of the lemma. □

Lemma 3.1.2. *Let $g(x) = b_e x^e + b_{e-1}x^{e-1} + \cdots + b_0 \in \mathbb{Q}[x]$, with $b_0 \neq 0$, be a polynomial of degree e. Let $m_0, m_1, \ldots, m_{t-1}, m_t$ be integers such that the successive vertices of the Newton polygon of $g(x)$ with respect to p are given by the set*

$$\{(0, v_p(b_e)), (e-m_1, v_p(b_{m_1})), \ldots, (e-m_{t-1}, v_p(b_{m_{t-1}})), (e, v_p(b_0))\},$$

where $m_0 = e$, $m_t = 0$, and the slopes of the segments of the Newton polygon of g are given by

$$\lambda_i = \frac{v_p(b_{m_i}) - v_p(b_{m_{i-1}})}{m_{i-1} - m_i} \quad \text{for } 1 \leq i \leq t.$$

Let s and α be non-negative integers. Then we have the following:

(i) If $s+1 < \alpha \leq t$, then

$$v_p(b_{m_{s+1}}) + \lambda_{s+1}(m_{s+1} - j) < v_p(b_{m_\alpha}) + \lambda_\alpha(m_\alpha - j), \quad \text{for all } j \leq m_\alpha.$$

(ii) If $0 \leq \alpha \leq s+1 \leq t$, then

$$v_p(b_{m_{s+1}}) = v_p(b_{m_\alpha}) + \sum_{i=\alpha+1}^{s+1} \lambda_i(m_{i-1} - m_i).$$

Proof. Denote $v_p(b_{m_i})$ by r_i for $0 \leq i \leq t$. We will prove the two cases separately.

Case (i): Suppose $s+1 < \alpha$. Since the slopes of the edges of the Newton polygon of $g(x)$ with respect to p are in increasing order, we have

$$\lambda_{s+1} < \frac{r_\alpha - r_{s+1}}{m_{s+1} - m_\alpha} \quad \text{and} \quad \lambda_{s+1} < \lambda_\alpha.$$

Using these inequalities and the identity $\lambda_{s+1}(m_{s+1}-j) = \lambda_{s+1}(m_{s+1}-m_\alpha)+\lambda_{s+1}(m_\alpha - j)$ for $j \leq m_\alpha$, it follows that

$$\lambda_{s+1}(m_{s+1} - j) < r_\alpha - r_{s+1} + \lambda_\alpha(m_\alpha - j),$$

which can be rearranged as

$$r_{s+1} + \lambda_{s+1}(m_{s+1} - j) < r_\alpha + \lambda_\alpha(m_\alpha - j).$$

This completes the proof of Case (i).

Case (ii): Suppose $0 \leq \alpha \leq s+1 \leq t$. Using the definition of λ_i, we have $r_{s+1} = r_s + \lambda_{s+1}(m_s - m_{s+1})$. With iterative similar equalities, we obtain

$$v_p(b_{m_{s+1}}) = v_p(b_{m_\alpha}) + \sum_{i=\alpha+1}^{s+1} \lambda_i(m_{i-1} - m_i).$$

This completes the proof of the lemma. □

Lemma 3.1.3. *With the notations and assumptions of Theorem 5, denote $v_p(b_{m_i})$ by r_i for $0 \leq i \leq t$. Assume that the successive vertices of the Newton polygon of $(g \circ f^n)(x)$ with respect to p are given by the set*

$$\{(0,0), (d^n(e-m_1), r_1), \ldots, (d^n(e-m_{t-1}), r_{t-1}), (d^n e, r_t)\}.$$

If the polynomial $(g \circ f^{n+1})(x)$ is given by $(g \circ f^{n+1})(x) = \sum_{k=0}^{d^{n+1}e} C_k x^k$, then for $k = d^{n+1}m_s$ with $0 \leq s \leq t$, we have $v_p(C_k) = r_s$.

Proof. Let $f(x) = \sum_{i=0}^{d} A_i x^i$ and $(g \circ f^n)(x) = \sum_{j=0}^{d^n e} B_j x^j$. Composition of $(g \circ f^n)(x)$ and f is given by

$$(g \circ f^{n+1})(x) = \sum_{j=0}^{d^n e} B_j \left(\sum_{i=0}^{d} A_i x^i \right)^j = \sum_{k=0}^{d^{n+1}e} C_k x^k,$$

For given $k = d^{n+1}m_s$, we determine $v_p(C_k)$ by analyzing the p-adic valuation of the coefficient of x^k in the expansion of the term:

$$B_j \left(\sum_{i=0}^{d} A_i x^i \right)^j \tag{3.2}$$

for each j in the range $0 \leq j \leq d^n e$.

By hypothesis, the successive vertices of the Newton polygon of $(g \circ f^n)(x)$ are given by the set

$$\{(0,0), (d^n(e-m_1), r_1), \ldots, (d^n(e-m_{t-1}), r_{t-1}), (d^n e, r_t)\}.$$

This means that $NP_p(g \circ f^n)$ will appear as shown in Figure 3.1 below.

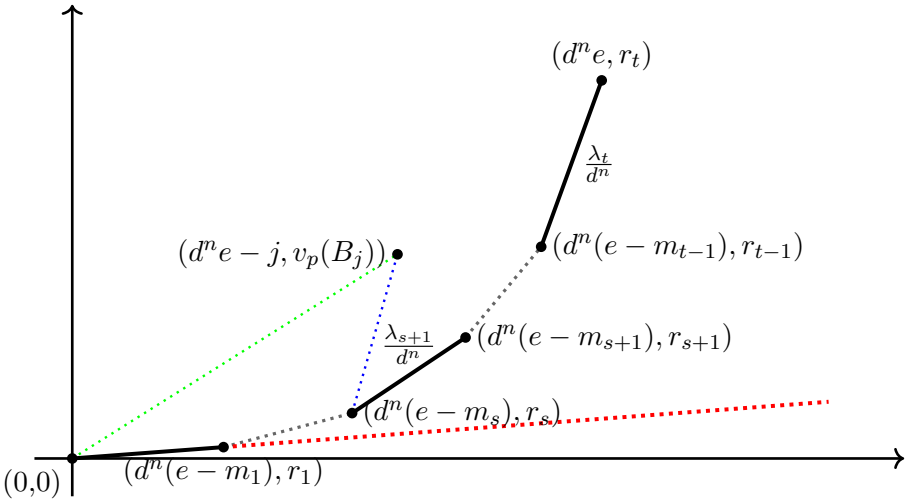


Figure 3.1: Newton polygon of $g \circ f^n(x)$ with respect to p

Recall that the Newton polygon of $g \circ f^n$ is the lower convex hull formed using the points $\{(d^n e - j, v_p(B_j)) : 0 \leq j \leq d^n e\}$. Therefore, for any $0 < j \leq d^n e$, the point $(d^n e - j, v_p(B_j))$ will lie on or above the Newton polygon, i.e.,

$$\frac{v_p(B_j) - 0}{d^n e - j - 0} \geq \frac{r_1}{d^n(e-m_1)} = \frac{\lambda_1}{d^n}, \quad \text{for all } j \in \{0, 1, 2, \ldots, d^n e - 1\}.$$

This implies that

$$v_p(B_j) \geq \frac{\lambda_1}{d^n}(d^n e - j), \quad \text{for all } j \in \{0, 1, 2, \ldots, d^n e\}. \tag{3.3}$$

From the hypothesis, the first edge of $NP_p(f)$ has slope λ. Thus, for $0 < i \leq d$, the point $(d-i, v_p(A_i))$ lies above the line joining $(0,0)$ and $(d, d\lambda)$, as shown in Figure 3.2.

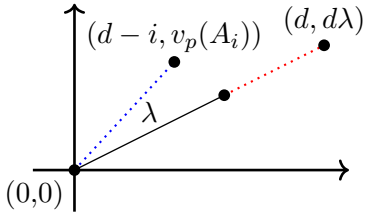


Figure 3.2: Newton polygon of f with respect to p

This implies

$$\frac{v_p(A_i) - 0}{d - i - 0} \geq \lambda, \quad \text{for all } i \in \{0, 1, 2, \ldots, d-1\};$$

which yields

$$v_p(A_i) \geq \lambda(d-i), \quad \text{for all } i \in \{0, 1, 2, \ldots, d-1, d\}. \tag{3.4}$$

The proof of the lemma is divided into three cases. We first prove the lemma for the cases $s = 0$ and $s = t$ seperately, then proceed with the case $0 < s < t$.

Case $s = 0$: We begin with $s = 0$, i.e., $k = d^{n+1}m_0 = d^{n+1}e$. In this situation, the only term of degree $k = d^{n+1}e$ in the expression of $(g \circ f^{n+1})(x)$ is $B_{d^n e}A_d^{d^n e}x^{d^{n+1}e}$, thus we have

$$v_p(C_k) = v_p(B_{d^n e}) + d^n e v_p(A_d) = 0 = r_0.$$

This proves the lemma for $s = 0$.

Case $s = t$: Now consider $s = t$, i.e., $k = d^{n+1}m_t = 0$. Then we have $C_k = C_0 = \sum_{j=0}^{d^n e} B_j A_0^j$. Recall the given fact that $r_t \leq \lambda_1(d + e - 1)$. For any $j \leq d^n e$, we use the upper bound of r_t and note that $-d^n \leq -1$ to obtain

$$r_t \leq \frac{\lambda_1}{d^n}(d^{n+1} + d^n e - d^n) \leq \frac{\lambda_1}{d^n}(d^{n+1} + d^n e - 1) = \frac{\lambda_1}{d^n}(d^n e - j) + \frac{\lambda_1}{d^n}(d^{n+1} + j - 1).$$

Note that $d^{n+1} \geq 1$, and it is easy to verify that for $j \geq 1$, $d^{n+1} + j - 1 \leq d^{n+1}j$. By applying this, along with $\lambda_1 \leq \lambda$ and using Equations (3.3) and (3.4), we obtain:

$$r_t \leq \lambda_1(d + e - 1) \leq \frac{\lambda_1}{d^n}(d^n e - j) + \frac{\lambda}{d^n}d^{n+1}j \leq v_p(B_j) + j v_p(A_0) = v_p(B_j A_0^j).$$

Remember that the above inequality holds only for $j \geq 1$. Furthermore, we note that one of the inequalities above is strict, based on the assumptions (i) and (ii) of Theorem 5; hence, we have $v_p(B_j A_0^j) > r_t$ whenever $j \geq 1$. Also, for $j = 0$, we have $v_p(B_0 A_0^0) = v_p(B_0) = r_t$. Hence, we conclude that $v_p(C_0) = r_t$, which proves the lemma for $s = t$ as well.

Case $0 < s < t$**:** Fix an integer s satisfying $0 < s < t$, and consider $k = d^{n+1}m_s$. If $j < \frac{k}{d}$, then the highest possible degree of x in the expansion of (3.2) is dj, which is strictly smaller than k. Therefore, no term of degree k exists in (3.2) whenever $j < \frac{k}{d}$.

Now, if $j > \frac{k}{d} = d^n m_s$, we observe that $j - \frac{k}{d} = j - d^n m_s \geq 1$. Suppose that k can be partitioned into j terms as $k = i_1 + i_2 + \cdots + i_j$ with each $i_\ell \leq d$ for $1 \leq \ell \leq j$. Then there exists a term in the form $B_j \prod_{\ell=1}^{j} A_{i_\ell} x^{i_\ell} = \left(B_j \prod_{\ell=1}^{j} A_{i_\ell}\right) x^k$ of degree k in the expansion of (3.2). Now, we show that for each such partition of k with $j > \frac{k}{d}$, the inequality $v_p(C_k) > r_s$ holds. Using Equations (3.3) and (3.4), we obtain

$$v_p(C_k) \geq v_p\left(B_j \prod_{\ell=1}^{j} A_{i_\ell}\right) = v_p(B_j) + \sum_{\ell=1}^{j} v_p(A_{i_\ell}) \geq \frac{\lambda_1}{d^n}(d^n e - j) + \sum_{\ell=1}^{j} \lambda(d - i_\ell).$$

Keeping in mind the given fact $\lambda \geq \lambda_1$ and the condition $d - i_\ell \geq 0$, we deduce

$$\begin{aligned} v_p(C_k) &\geq \frac{\lambda_1}{d^n}(d^n e - j) + \lambda_1 \sum_{\ell=1}^{j}(d - i_\ell) \\ &= \lambda_1 \left[e - \frac{j}{d^n} + dj - \sum_{\ell=1}^{j} i_\ell\right] \\ &= \lambda_1 \left[e - \frac{j}{d^n} + dj - k + \frac{k}{d^{n+1}} - m_{s+1}\right] - \lambda_1 \left(\frac{k}{d^{n+1}} - m_{s+1}\right) \\ &> \lambda_1 \left[e + \left(d - \frac{1}{d^n}\right)\left(j - \frac{k}{d}\right) - m_{s+1}\right] - \lambda_{s+1} \left(\frac{k}{d^{n+1}} - m_{s+1}\right) \end{aligned} \tag{3.5}$$

where the last inequality is strict because for any $s > 0$, we have $\lambda_1 < \lambda_{s+1}$ and $\frac{k}{d^{n+1}} - m_{s+1} = m_s - m_{s+1} > 0$. Additionally, using $j - \frac{k}{d} \geq 1$ and $d \geq 1$, we derive

$$v_p(C_k) > \lambda_1 \left[e + (d-1) - m_{s+1}\right] - \lambda_{s+1} \left(\frac{k}{d^{n+1}} - m_{s+1}\right).$$

Recall the given fact that $r_t \leq \lambda_1(d + e - 1)$. Applying Lemma 3.1.1 with $\alpha = e + d - 1$ for the first part of RHS and substituting the values of k, λ_{s+1}, we obtain

$$v_p(C_k) > r_{s+1} - \left(\frac{r_{s+1} - r_s}{m_s - m_{s+1}}\right)\left(\frac{d^{n+1}m_s}{d^{n+1}} - m_{s+1}\right) = r_s.$$

Thus, for $j > \frac{k}{d} = d^n m_s$, we assert that $v_p(C_k) > r_s$. Now for the case $j = \frac{k}{d}$, i.e., $j = d^n m_s$, the only term of degree k in the expansion of (3.2) is $A_d^{d^n m_s} B_{d^n m_s}$. Furthermore, by applying the hypothesis to the structure of $NP_p(g \circ f^n)$ and recalling that $p \nmid A_d$, we derive $v_p(A_d^{d^n m_s} B_{d^n m_s}) = d^n m_s v_p(A_d) + v_p(B_{d^n m_s}) = d^n m_s(0) + r_s = r_s$. Combining all of these, we obtain $v_p(C_{d^{n+1}m_s}) = r_s$. As s was chosen arbitrarily, the

lemma holds for all $0 < s < t$. This completes the proof of the lemma. □

Lemma 3.1.4. *With the notations and hypotheses of Theorem 5, denote $v_p(b_{m_i})$ by r_i for $0 \leq i \leq t$. Assume that the successive vertices of the Newton polygon of $(g \circ f^n)(x)$ with respect to p are given by the set*

$$\{(0,0), (d^n(e-m_1), r_1), \ldots, (d^n(e-m_{t-1}), r_{t-1}), (d^n e, r_t)\}.$$

If the polynomial $(g \circ f^{n+1})(x)$ is given by $(g \circ f^{n+1})(x) = \sum_{k=0}^{d^{n+1}e} C_k x^k$, then for $k \leq d^{n+1}m_s$ with $0 \leq s < t$, we have

$$v_p(C_k) \geq r_{s+1} + \lambda_{s+1}\left(m_{s+1} - \frac{k}{d^{n+1}}\right).$$

Proof. Write $f(x) = \sum_{i=0}^{d} A_i x^i$ and $(g \circ f^n)(x) = \sum_{j=0}^{d^n e} B_j x^j$. Since $(g \circ f^{n+1})(x)$ is given by $(g \circ f^{n+1})(x) = \sum_{k=0}^{d^{n+1}e} C_k x^k$, we obtain

$$(g \circ f^{n+1})(x) = \sum_{j=0}^{d^n e} B_j \left(\sum_{i=0}^{d} A_i x^i\right)^j = \sum_{k=0}^{d^{n+1}e} C_k x^k.$$

To determine $v_p(C_k)$ for a given k with $k \leq d^{n+1}m_s$, we examine the p-adic valuation of the coefficient of x^k in the expansion of the term:

$$B_j \left(\sum_{i=0}^{d} A_i x^i\right)^j \tag{3.6}$$

for each j in the range $0 \leq j \leq d^n e$.

We use arguments similar to those used for obtaining Equations (3.3) and (3.4) to conclude the following:

$$v_p(B_j) \geq \frac{\lambda_1}{d^n}(d^n e - j), \quad \forall j \in \{0, 1, 2, \ldots, d^n e\}; \tag{3.7}$$

$$v_p(A_i) \geq \lambda(d-i), \quad \forall i \in \{0, 1, 2, \ldots, d\}. \tag{3.8}$$

Now, to prove the lemma, fix an integer s within the range $0 \leq s < t$.

Case 1: We first prove the result for k in the range $d^{n+1}m_{s+1} \leq k < d^{n+1}m_s$, i.e., $d^n m_{s+1} \leq \frac{k}{d} < d^n m_s$. We split this case into two subcases according to whether $j \leq \frac{k}{d}$ or $j > \frac{k}{d}$.

Subcase (i): Suppose $j \leq \frac{k}{d} < d^n m_s$, i.e., $d^n e - j > d^n e - d^n m_s = d^n(e - m_s)$. In this situation, the point $(d^n e - j, v_p(B_j))$ lies strictly beyond the point $(d^n(e - m_s), r_s)$ as illustrated in Figure 3.1. Consequently, the slope of the segment joining $(d^n e - j, v_p(B_j))$ and $(d^n(e - m_s), r_s)$ is greater than or equal to λ_{s+1}/d^n, depicted by the blue dotted line in Figure 3.1. Using this observation for $j < d^n m_s$ and the value of λ_{s+1}, we deduce

$$\frac{v_p(B_j) - r_s}{d^n m_s - j} \geq \frac{\lambda_{s+1}}{d^n} = \frac{r_{s+1} - r_s}{d^n(m_s - m_{s+1})}.$$

Although the above inequality holds only for $j < d^n m_s$, the next inequlity deduced from above is true for all $j \leq d^n m_s$,

$$\begin{aligned} v_p(B_j) - r_s &\geq \frac{r_{s+1} - r_s}{d^n(m_s - m_{s+1})}(d^n m_s - j) \\ &= r_{s+1} - r_s + \frac{r_{s+1} - r_s}{d^n(m_s - m_{s+1})}(d^n m_{s+1} - j). \end{aligned}$$

This implies

$$v_p(B_j) \geq r_{s+1} + \frac{\lambda_{s+1}}{d^n}(d^n m_{s+1} - j) \tag{3.9}$$

Using this in (3.6) and keeping in mind that $v_p(A_i) \geq 0$ for all $i \in \{0, 1, \ldots, d\}$, we obtain

$$v_p(C_k) \geq v_p(B_j) \geq r_{s+1} + \frac{\lambda_{s+1}}{d^n}(d^n m_{s+1} - j).$$

Further, using $j \leq \frac{k}{d}$, we conclude

$$v_p(C_k) \geq r_{s+1} + \frac{\lambda_{s+1}}{d^n}\left(d^n m_{s+1} - \frac{k}{d}\right) = r_{s+1} + \lambda_{s+1}\left(m_{s+1} - \frac{k}{d^{n+1}}\right).$$

Therefore, our lemma is proved whenever $j \leq \frac{k}{d}$.

Subcase (ii): Suppose $j > \frac{k}{d}$, and let $k = i_1 + i_2 + \cdots + i_j$ be a partition of k into j terms, where $i_\ell \leq d$ for $1 \leq \ell \leq j$. Then there exists a term of degree k in the form $B_j \prod_{\ell=1}^{j} A_{i_\ell} x^{i_\ell} = \left(B_j \prod_{\ell=1}^{j} A_{i_\ell}\right) x^k$ within the expansion of (3.6). We use arguments similar to those used for (3.5) to arrive at the following conclusion:

$$\begin{aligned} v_p(C_k) &\geq \lambda_1 \left[e - \frac{j}{d^n} + dj - k + \frac{k}{d^{n+1}} - m_{s+1}\right] - \lambda_1 \left(\frac{k}{d^{n+1}} - m_{s+1}\right) \\ &\geq \lambda_1 \left[e + \left(d - \frac{1}{d^n}\right)\left(j - \frac{k}{d}\right) - m_{s+1}\right] - \lambda_{s+1} \left(\frac{k}{d^{n+1}} - m_{s+1}\right), \end{aligned}$$

where the last inequality holds because for any $s > 0$, as $\frac{k}{d^{n+1}} - m_{s+1} \geq 0$ and $\lambda_1 \leq \lambda_{s+1}$. Additionally, if $j - \frac{k}{d} \geq 1$, we use $d \geq 1$ to derive

$$v_p(C_k) \geq \lambda_1 \left[e + (d-1) - m_{s+1}\right] + \lambda_{s+1} \left(m_{s+1} - \frac{k}{d^{n+1}}\right).$$

Using the given fact that $r_t \leq \lambda_1(d + e - 1)$ in Lemma 3.1.1 with $\alpha = e + d - 1$, the above inequality becomes

$$v_p(C_k) \geq r_{s+1} + \lambda_{s+1} \left(m_{s+1} - \frac{k}{d^{n+1}}\right).$$

Therefore, our lemma holds whenever $j - \frac{k}{d} \geq 1$. The only remaining part in this subcase is when $0 < j - \frac{k}{d} < 1$, which implies $k < dj < d + k$. Thus, there exists an integer γ in the range $0 < \gamma < d$ satisfying $k + \gamma = dj$. Further, we use $k = i_1 + i_2 + \ldots + i_j$ to deduce $\left(\sum_{\ell=1}^{j} i_\ell\right) + \gamma = dj$. This implies $\gamma = \sum_{\ell=1}^{j}(d - i_\ell)$. Additionally, considering the condition $j < \frac{k}{d} + 1$ and bearing in mind that $k < d^{n+1} m_s$, we infer that $j < d^n m_s + 1$, i.e., $j \leq d^n m_s$. Now, we use reasoning similar to those used for (3.9) to deduce $v_p(B_j) \geq r_{s+1} + \frac{\lambda_{s+1}}{d^n}(d^n m_{s+1} - j)$. Using this inequality and (3.8), we obtain

$$v_p(C_k) \geq v_p(B_j) + \sum_{\ell=1}^{j} v_p(A_{i_\ell}) \geq r_{s+1} + \frac{\lambda_{s+1}}{d^n}(d^n m_{s+1} - j) + \lambda \sum_{\ell=1}^{j}(d - i_\ell).$$

Substituting $j = \frac{k}{d} + \frac{\gamma}{d}$ and using $\gamma = \sum_{\ell=1}^{j}(d - i_\ell)$, we have

$$\begin{aligned} v_p(C_k) &\geq r_{s+1} + \frac{\lambda_{s+1}}{d^n}\left(d^n m_{s+1} - \left(\frac{k}{d} + \frac{\gamma}{d}\right)\right) + \lambda\gamma \\ &\geq r_{s+1} + \lambda_{s+1}\left(m_{s+1} - \frac{k}{d^{n+1}}\right) - \frac{\lambda_{s+1}}{d^n}\frac{\gamma}{d} + \lambda_1\gamma, \end{aligned}$$

where the last inequality follows from the hypothesis $\lambda \geq \lambda_1$. Therefore, to establish our lemma in this subcase, it is enough to show that

$$\lambda_1\gamma - \frac{\lambda_{s+1}}{d^n}\frac{\gamma}{d} \geq 0.$$

Taking into account the conditions $\gamma > 0$, $n \geq 0$, and $\lambda_t \geq \lambda_{s+1}$, for all s with $0 < s \leq t$, the above inequality holds true if

$$\lambda_1 \geq \frac{\lambda_t}{d} = \frac{1}{d}\frac{r_t - r_{t-1}}{m_{t-1} - m_t}, \text{ i.e., } r_t \leq \lambda_1 d(m_{t-1} - m_t) + r_{t-1}.$$

Furthermore, noting that $\frac{r_{t-1}}{e-m_{t-1}} \geq \lambda_1$ and keeping in mind that $m_t = 0$, the inequality above holds true if

$$r_t \leq \lambda_1 d m_{t-1} + \lambda_1(e - m_{t-1}), \text{ i.e., } r_t \leq \lambda_1[e + (d-1)m_{t-1}].$$

The last inequality follows from $m_{t-1} \geq 1$ and the hypothesis that $r_t \leq \lambda_1(d + e - 1)$. This proves Subcase (ii). Thus, our lemma holds for any s, $0 \leq s < t$, whenever k lies in the range $d^{n+1}m_{s+1} \leq k < d^{n+1}m_s$. This completes the proof of Case 1.

Case 2: Now suppose that $k < d^{n+1}m_s$. Note that the sequence m_i's are decreasing; hence there exists an integer $\alpha < t$ such that $\alpha \geq s$ and $d^{n+1}m_{\alpha+1} \leq k < d^{n+1}m_\alpha$. Using exactly similar arguments to Case 1 for α, we see that

$$\begin{aligned} v_p(C_k) &\geq r_{\alpha+1} + \lambda_{\alpha+1}\left(m_{\alpha+1} - \frac{k}{d^{n+1}}\right) \qquad (3.10)\\ &= r_\alpha + r_{\alpha+1} - r_\alpha + \frac{r_{\alpha+1} - r_\alpha}{m_\alpha - m_{\alpha+1}}\left(m_{\alpha+1} - \frac{k}{d^{n+1}}\right)\\ &= r_\alpha + \frac{r_{\alpha+1} - r_\alpha}{m_\alpha - m_{\alpha+1}}\left(m_\alpha - m_{\alpha+1} + m_{\alpha+1} - \frac{k}{d^{n+1}}\right)\\ &= r_\alpha + \lambda_{\alpha+1}\left(m_\alpha - \frac{k}{d^{n+1}}\right)\\ &> r_\alpha + \lambda_\alpha\left(m_\alpha - \frac{k}{d^{n+1}}\right), \qquad (3.11) \end{aligned}$$

where the last inequality holds because $\lambda_{\alpha+1} > \lambda_\alpha$ and $k < d^{n+1}m_\alpha$. If $\alpha = s$, then the lemma is clearly true using (3.10). If $\alpha = s+1$, we use (3.11) to prove our lemma. Now, assuming $\alpha > s+1$ and keeping in mind $\frac{k}{d^{n+1}} < m_\alpha$, we apply Lemma 3.1.2 (i) to the right-hand side of (3.11) to conclude

$$v_p(C_k) > r_{s+1} + \lambda_{s+1}\left(m_{s+1} - \frac{k}{d^{n+1}}\right).$$

This completes the proof of Case 2. Thus, our lemma is proved for s. Since s was arbitrarily chosen from the range $0 \leq s < t$, our result holds for all s, $0 \leq s < t$. This concludes the demonstration of the lemma. □

3.2 Proof of Theorem 5

Proof of Theorem 5: Recall that $0 = m_t < m_{t-1} < \cdots < m_1 < m_0 = e$ are integers such that $NP_p(g)$ has vertices

$$\{(0,0), (e - m_1, v_p(b_{m_1})), \ldots, (e - m_{t-1}, v_p(b_{m_{t-1}})), (e, v_p(b_0))\}.$$

Suppose $f(x)$ is a polynomial satisfying (i) or (ii) and let n be a positive integer, our aim is show that $NP_p(g \circ f^n)$ has vertices

$$\{(0,0), (d^n(e-m_1), v_p(b_{m_1})), \ldots, (d^n(e-m_{t-1}), v_p(b_{m_{t-1}})), (d^n e, v_p(b_0))\}.$$

Let $v_p(b_{m_i})$ be denoted by r_i for $0 \leq i \leq t$. Hence, λ_i can be expressed as

$$\lambda_i = \frac{r_i - r_{i-1}}{m_{i-1} - m_i} \quad \text{for} \quad 1 \leq i \leq t.$$

We proceed by induction on $n \geq 0$. For $n = 0$, we have $g \circ f^0 = g$, and the result is trivially true.

Now, fix an integer $n > 0$. Assume that the result holds for n, i.e., the successive vertices of $NP_p(g \circ f^n)$ are given by the set

$$\{(0,0), (d^n(e-m_1), r_1), \ldots, (d^n(e-m_{t-1}), r_{t-1}), (d^n e, r_t)\}.$$

Our goal is to show that $NP_p(g \circ f^{n+1})$, has the structure as depicted in Figure 3.3. Specifically, we need to show that the successive vertices of $NP_p(g \circ f^{n+1})$ are given by the set

$$\{(0,0), (d^{n+1}(e-m_1), r_1), \ldots, (d^{n+1}(e-m_{t-1}), r_{t-1}), (d^{n+1}e, r_t)\}.$$

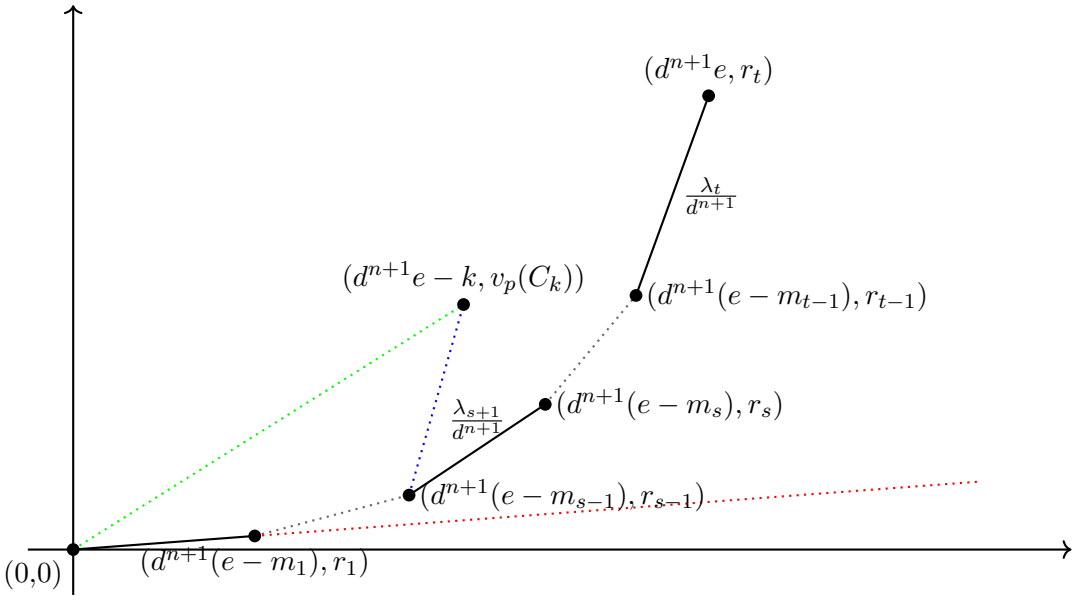


Figure 3.3: Newton polygon of $g \circ f^{n+1}$ with respect to p

Write $f(x) = \sum_{i=0}^{d} A_i x^i$ and $(g \circ f^n)(x) = \sum_{j=0}^{d^n e} B_j x^j$. Thus, we have

$$(g \circ f^{n+1})(x) = \sum_{j=0}^{d^n e} B_j \left(\sum_{i=0}^{d} A_i x^i \right)^j .$$

Let C_k denote the coefficient of x^k such that

$$(g \circ f^{n+1})(x) = \sum_{k=0}^{d^{n+1} e} C_k x^k.$$

Using Lemmas 3.1.3 and 3.1.4, we will show that the first edge of $NP_p(g \circ f^{n+1})$ has endpoints $(0,0)$ and $(d^{n+1}(e - m_1), r_1)$. For $s = 0$, we have $m_0 = e$. By applying Lemma 3.1.3 with $s = 0$, we obtain $v_p(C_{d^{n+1}e}) = r_0 = 0$, meaning that the first edge of $NP_p(g \circ f^{n+1})$ starts at the point $(0,0)$.

Next, applying Lemma 3.1.4 with $s = 0$ and $k \leq d^{n+1} m_0 = d^{n+1} e$, we deduce that

$$\begin{aligned} v_p(C_k) &\geq r_1 + \lambda_1 \left(m_1 - \frac{k}{d^{n+1}} \right) \\ &= r_0 + r_1 - r_0 + \frac{r_1 - r_0}{e - m_1} \left(m_1 - \frac{k}{d^{n+1}} \right) \\ &= r_0 + \frac{r_1 - r_0}{e - m_1} \left(e - \frac{k}{d^{n+1}} \right). \end{aligned}$$

Thus, we have

$$\frac{v_p(C_k) - r_0}{d^{n+1} e - k} \geq \frac{1}{d^{n+1}} \cdot \frac{r_1 - r_0}{e - m_1} = \frac{\lambda_1}{d^{n+1}}. \tag{3.12}$$

Hence, every point $(d^{n+1}e - k, v_p(C_k))$ lies on or above the line segment joining $(0,0)$ and $(d^{n+1}(e - m_1), r_1)$. By applying Lemma 3.1.3 for $s = 1$, we obtain $v_p(C_{d^{n+1}m_1}) = r_1$. To show that $(d^{n+1}(e - m_1), v_p(C_{d^{n+1}m_1}))$ is the endpoint of the first edge, it suffices to prove that any point $(d^{n+1}e - k, v_p(C_k))$ beyond $(d^{n+1}(e - m_1), v_p(C_{d^{n+1}m_1}))$ lies strictly above the line segment representing the first edge, as indicated by the green dotted segment in Figure 3.3.

Now, consider a point $(d^{n+1}e - k, v_p(C_k))$ lying beyond $(d^{n+1}(e - m_1), r_1)$, i.e., $d^{n+1}e - k > d^{n+1}(e - m_1)$. Then, we have $k < d^{n+1} m_1$. Lemma 3.1.4 with $s = 1$ gives

$$\begin{aligned} v_p(C_k) &\geq r_2 + \lambda_2 \left(m_2 - \frac{k}{d^{n+1}} \right) \\ &= r_1 + r_2 - r_1 + \frac{r_2 - r_1}{m_1 - m_2} \left(m_2 - \frac{k}{d^{n+1}} \right) \\ &= r_1 + \frac{r_2 - r_1}{m_1 - m_2} \left(m_1 - \frac{k}{d^{n+1}} \right) \\ &> r_1 + \lambda_1 \left(m_1 - \frac{k}{d^{n+1}} \right). \end{aligned}$$

where the last inequality follows using the fact that $k < d^{n+1}m_1$ and $\lambda_1 < \lambda_2$. Following similar reasoning as for inequality (3.12), we get

$$\frac{v_p(C_k) - r_0}{d^{n+1}e - k} > \frac{\lambda_1}{d^{n+1}}.$$

Thus, every point $(d^{n+1}e - k, v_p(C_k))$ lying beyond $(d^{n+1}(e - m_1), r_1)$ lies strictly above the line segment joining $(0, 0)$ and $(d^{n+1}(e - m_1), r_1)$. Therefore, we conclude that the first edge of $NP_p(g \circ f^{n+1})$ has endpoints $(0, 0)$ and $(d^{n+1}(e - m_1), r_1)$.

For any s in the range $0 < s \leq t$, similar arguments will show that the s-th edge of $NP_p(g \circ f^{n+1})$ has endpoints $(d^{n+1}(e - m_{s-1}), r_{s-1})$ and $(d^{n+1}(e - m_s), r_s)$. This completes the proof of the theorem. □

We now present a few examples to illustrate that the assumptions made in Theorem 5 are not only sufficient but also strictly necessary for its conclusions. For a given polynomial $g(x) \in \mathbb{Q}[x]$ of degree e, we use the notation:

$$NP_p(g) : (0, 0) \to (e - m_1, v_p(b_{m_1})) \to \cdots \to (e, v_p(b_0))$$

to represent the successive vertices of the Newton polygon of $g(x)$ with respect to the prime p. These vertices are given by the set

$$\{(0, 0), (e - m_1, v_p(b_{m_1})), \ldots, (e, v_p(b_0))\}.$$

In what follows, Example 3.2.1 illustrates the importance of the condition $\lambda \geq \lambda_1$, while Examples 3.2.2 and 3.2.3 highlights the necessity of the condition $r_t \leq \lambda_1(d+e-1)$.

Example 3.2.1. *Let* $f(x) = x^3 + 2x + 4$ *and* $g(x) = x^3 + 4x + 2^4$. *Then*

$$(g \circ f)(x) = x^9 + 6x^7 + 12x^6 + 12x^5 + 48x^4 + 60x^3 + 48x^2 + 104x + 96.$$

Furthermore, the Newton polygons of f, g, and $g \circ f$ with respect to the prime 2 are:

$$NP_2(f) : (0,0) \to (2,1) \to (3,2),$$
$$NP_2(g) : (0,0) \to (2,2) \to (3,4),$$
$$NP_2(g \circ f) : (0,0) \to (6,2) \to (8,3) \to (9,5).$$

Using the notations in Theorem 5, we observe that $t = 2$, $d = e = 3$, $\lambda = \frac{1}{2} < 1 = \lambda_1$, and $r_t = 4 < 5 = \lambda_1(d + e - 1)$. While all other conditions of Theorem 5 are satisfied, the condition $\lambda \geq \lambda_1$ is violated, leading to the failure of Newton polygon structure preservation. This underscores the necessity of the condition $\lambda \geq \lambda_1$.

Next two examples demonstrate the importance of the condition $r_t \leq \lambda_1(d + e - 1)$ for cases where $t = 2$ and $t = 3$.

Example 3.2.2. *Let $f(x) = x^3 + 2x^2 + 2x + 4$ and $g(x) = x^3 + 2x + 8$. Then*

$$(g \circ f)(x) = x^9 + 6x^8 + 18x^7 + 44x^6 + 84x^5 + 120x^4 + 154x^3 + 148x^2 + 100x + 80.$$

The Newton polygons of f, g, and $g \circ f$ with respect to the prime 2 are:

$$NP_2(f) : (0,0) \to (2,1) \to (3,2),$$
$$NP_2(g) : (0,0) \to (2,1) \to (3,3),$$
$$NP_2(g \circ f) : (0,0) \to (6,1) \to (8,2) \to (9,4).$$

Using the notations in Theorem 5, we have $t = 2$, $d = e = 3$, $\lambda = \lambda_1 = \frac{1}{2}$, and $r_t = 3 > \frac{5}{2} = \lambda_1(d + e - 1)$. This example illustrates the necessity of condition (i) of Theorem 5.

Example 3.2.3. *Consider the case $t = 3$. Let $f(x) = x^{11} + 2x^4 + 4x + 16$. The Newton polygons of f and f^2 with respect to the prime 2 are given by:*

$$NP_2(f) : (0,0) \to (7,1) \to (10,2) \to (11,4),$$
$$NP_2(f^2) : (0,0) \to (77,1) \to (110,2) \to (117,3) \to (121,4).$$

Using the notations of Theorem 5, we observe that in this example $t = 3$, $d = e = 3$, $\lambda = \lambda_1 = \frac{1}{7}$, and $r_3 = 4 > 3 = \lambda_1(d + e - 1)$. This demonstrates the necessity of the condition $r_t \leq \lambda_1(d + e - 1)$ in Theorem 5.

3.3 Proof of Theorem 7

Proof of Theorem 7: Recall that $0 = m_t < m_{t-1} < \cdots < m_1 < m_0 = e$ are integers such that $NP_p(g)$ has vertices

$$\{(0, v_p(b_e)), (e - m_1, v_p(b_{m_1})), \ldots, (e - m_{t-1}, v_p(b_{m_{t-1}})), (e, v_p(b_0))\}.$$

Suppose $f(x)$ and u satisfy assuptions of theorem, our aim is show that $NP_p(g \circ f)$ has vertices

$$\{(0, v_p(b_e)), (d(e - m_1), v_p(b_{m_1})), \ldots, (d(e - m_{t-1}), v_p(b_{m_{t-1}})), (de, v_p(b_0))\}.$$

Denote $v_p(b_{m_i})$ by r_i for $0 \leq i \leq t$. Thus, λ_i can be written as $\lambda_i = \frac{r_i - r_{i-1}}{m_{i-1} - m_i}$ for $1 \leq i \leq t$. Our goal is to show that the successive vertices of $NP_p(g \circ f)$ are given by the set

$$\{(0, r_0), (d(e - m_1), r_1), \ldots, (d(e - m_{t-1}), r_{t-1}), (de, r_t)\}.$$

Write $f(x) = \sum_{i=0}^{d} a_i x^i$. So, we have

$$(g \circ f)(x) = \sum_{j=0}^{e} b_j \left(\sum_{i=0}^{d} a_i x^i \right)^j.$$

Let c_k denote the coefficients of x^k in this expansion, so that

$$(g \circ f)(x) = \sum_{k=0}^{de} c_k x^k.$$

The proof of our theorem will proceed similarly to the proof of Theorem 5, once we establish the following two key equations:

$$\text{For } k = dm_s \text{ with } 0 \leq s \leq t, \text{ we have } v_p(c_k) = r_s, \tag{3.13}$$

$$\text{for } k \leq dm_s \text{ with } 0 \leq s \leq t, \text{ we have } v_p(c_k) \geq r_{s+1} + \lambda_{s+1} \left(m_{s+1} - \frac{k}{d} \right). \tag{3.14}$$

To prove Equations (3.13) and (3.14), we need to determine $v_p(c_k)$ for a given k within the range $0 \leq k \leq de$. That is, we need the p-adic valuation of the coefficient of x^k in the expansion of the term:

$$b_j \left(\sum_{i=0}^{d} a_i x^i \right)^j \tag{3.15}$$

for each j in the range $0 \leq j \leq e$. By hypothesis, the successive vertices of $NP_p(g)$ are given by the set

$$\{(0, r_0), (e - m_1, r_1), \ldots, (e - m_{t-1}, r_{t-1}), (e, r_t)\}.$$

Therefore, $NP_p(g)$ is as shown in Figure 3.4.

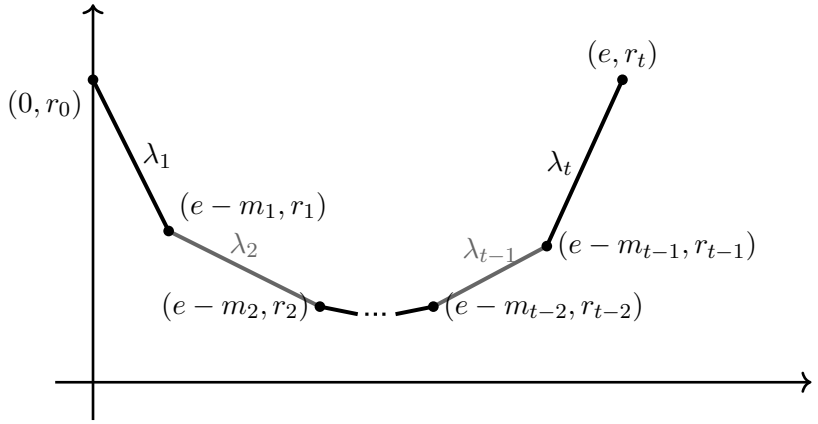


Figure 3.4: Newton polygon of $g(x)$ with respect to p

Recall the hypothesis that $v_p(a_d) = 0$ and

$$v_p(a_i) \geq \frac{u}{\beta}(d - i) \quad \text{for all } i \in \{0, 1, 2, \ldots, d\}. \tag{3.16}$$

We now prove (3.13). The proof of (3.13) is split into two cases depending on whether $s = 0$ or $0 < s \leq t$.

Case $s = 0$: For $s = 0$, we have $k = dm_0 = de$. In this situation, the only term of degree k in the expression of $(g \circ f)(x)$ is $b_e a_d^e$. Hence, we have:

$$v_p(c_k) = v_p(b_e) + e v_p(a_d) = r_0 + e(0) = r_0.$$

This proves (3.13) for $s = 0$.

Case $0 < s \leq t$: Fix an integer s with $0 < s \leq t$ and let $k = dm_s$. If $j < \frac{k}{d}$, then the highest possible degree of x in the expansion of (3.15) is dj, which is strictly less than

k. Therefore, no term of degree k exists in (3.15) whenever $j < \frac{k}{d}$.

Now assume $j > \frac{k}{d} = m_s$. Recall that the m_i's form a decreasing sequence, so there exists an integer α in the range $0 < \alpha \leq s$ such that $m_\alpha < j \leq m_{\alpha-1}$. In this case, we have $e - j \geq e - m_{\alpha-1}$, i.e., the point $(e-j, v_p(b_j))$ lies beyond $(e - m_{\alpha-1}, r_{\alpha-1})$. Thus, we obtain the inequality:

$$\begin{aligned} v_p(b_j) - r_{\alpha-1} &\geq \lambda_\alpha(m_{\alpha-1} - j), \\ \text{i.e.,} \quad v_p(b_j) &\geq r_{\alpha-1} + \lambda_\alpha(m_{\alpha-1} - j). \end{aligned} \tag{3.17}$$

Suppose that k can be partitioned into j terms as $k = i_1 + i_2 + \cdots + i_j$ with each $i_\ell \leq d$ for $1 \leq \ell \leq j$. Then, there exists a term of the form

$$b_j \prod_{\ell=1}^{j} a_{i_\ell} x^{i_\ell} = \left(b_j \prod_{\ell=1}^{j} a_{i_\ell} \right) x^k$$

of degree k in the expansion of (3.15). Our goal is to show that for each such partition of k with $j > \frac{k}{d}$, the inequality $v_p(c_k) > r_s$ holds. Using (3.16) and (3.17), we get:

$$v_p(c_k) \geq v_p\left(b_j \prod_{\ell=1}^{j} a_{i_\ell} \right) = v_p(b_j) + \sum_{\ell=1}^{j} v_p(a_{i_\ell}) \geq r_{\alpha-1} + \lambda_\alpha(m_{\alpha-1} - j) + \sum_{\ell=1}^{j} \frac{u}{\beta}(d - i_\ell).$$

Furthermore, applying Lemma 3.1.2 (ii), to prove $v_p(c_k) > r_s$, it suffices to show that:

$$\begin{aligned} r_{\alpha-1} + \lambda_\alpha(m_{\alpha-1} - j) + \frac{u}{\beta}(dj - k) &> r_s = r_{\alpha-1} + \sum_{i=\alpha}^{s} \lambda_i(m_{i-1} - m_i), \\ \text{i.e.,} \quad \lambda_\alpha(m_{\alpha-1} - j) + \frac{u}{\beta}(dj - dm_s) &> \lambda_\alpha(m_{\alpha-1} - m_\alpha) + \sum_{i=\alpha+1}^{s} \lambda_i(m_{i-1} - m_i), \\ \text{i.e.,} \quad \frac{u}{\beta} d(j - m_s) &> \lambda_\alpha(j - m_\alpha) + \sum_{i=\alpha+1}^{s} \lambda_i(m_{i-1} - m_i). \end{aligned}$$

On the contrary suppose that the above inequality does not hold. This means we have:

$$\frac{d}{\beta}(j - m_s) \leq \frac{\lambda_\alpha}{u}(j - m_\alpha) + \sum_{i=\alpha+1}^{s} \frac{\lambda_i}{u}(m_{i-1} - m_i) < j - m_\alpha + (m_\alpha - m_s),$$

where the last inequality follows from the fact that $\lambda_i \leq |\lambda_i| < u$ for all i in the range $0 < i \leq t$, along with $j > m_\alpha$ and the fact that the m_i's form a decreasing sequence. Since $j - m_s > 0$, the above inequality is equivalent to $\frac{d}{\beta} < 1$, which is a contradiction to

the fact that $\beta \leq d$. Hence, the desired inequality holds, implying $v_p(c_k) > r_s$ whenever $j > \frac{k}{d}$.

The only remaining case is $j = m_s$, for which there is only one term of degree k in (3.15), namely $b_j a_d^j$. Its p-adic valuation is:

$$v_p(b_j a_d^j) = v_p(b_{m_s}) + j v_p(a_d) = r_s.$$

Combining all of these results, we obtain $v_p(c_{dm_s}) = r_s$. Since s was chosen arbitrarily from the range $0 < s \leq t$, this completes the proof of (3.13) for all $0 < s \leq t$.

We now proceed to prove (3.14). Fix an integer s in the range $0 \leq s \leq t$.

Case 1: We first establish (3.14) for k such that $dm_{s+1} < k \leq dm_s$.

Note that if $j < \frac{k}{d}$, the highest possible degree of x in the expansion of (3.15) is dj, which is strictly smaller than k. Hence, no term of degree k exists in the expansion of (3.15) whenever $j < \frac{k}{d}$.

Now, assume $j \geq \frac{k}{d} > m_{s+1}$. Recall that the m_i's form a decreasing sequence, so there exists an integer α in the range $0 < \alpha \leq s+1$ such that $m_\alpha < j \leq m_{\alpha-1}$. Suppose that k can be partitioned into j terms as $k = i_1 + i_2 + \cdots + i_j$, where each $i_\ell \leq d$ for $1 \leq \ell \leq j$. Then, there exists a term in the form:

$$b_j \prod_{\ell=1}^{j} a_{i_\ell} x^{i_\ell} = \left(b_j \prod_{\ell=1}^{j} a_{i_\ell} \right) x^k$$

of degree k in the expansion of (3.15). Now, we will show that for each such partition of k with $j \geq \frac{k}{d}$, the inequality (3.14) holds. Using (3.16) and arguments similar to those used for (3.17), we obtain:

$$v_p(c_k) \geq v_p\left(b_j \prod_{\ell=1}^{j} a_{i_\ell} \right) = v_p(b_j) + \sum_{\ell=1}^{j} v_p(a_{i_\ell}) \geq r_{\alpha-1} + \lambda_\alpha(m_{\alpha-1} - j) + \sum_{\ell=1}^{j} \frac{u}{\beta}(d - i_\ell).$$

Recall that $\alpha - 1 < \alpha \leq s+1$. By applying Lemma 3.1.2 (ii) to r_{s+1}, we see that in order to prove (3.14), it suffices to show that

$$r_{\alpha-1} + \lambda_\alpha(m_{\alpha-1} - j) + \frac{u}{\beta}(dj - k) \geq r_{\alpha-1} + \sum_{i=\alpha}^{s+1} \lambda_i(m_{i-1} - m_i) + \lambda_{s+1}\left(m_{s+1} - \frac{k}{d}\right),$$

$$\text{i.e.,} \quad \frac{u}{\beta} d\left(j - \frac{k}{d}\right) \geq \lambda_\alpha(j - m_\alpha) + \sum_{i=\alpha+1}^{s+1} \lambda_i(m_{i-1} - m_i) + \lambda_{s+1}\left(m_{s+1} - \frac{k}{d}\right). \tag{3.18}$$

In the case where $\alpha = s+1$, inequality (3.18) becomes:

$$\frac{u}{\beta} d\left(j - \frac{k}{d}\right) \geq \lambda_{s+1}(j - m_{s+1}) + \lambda_{s+1}\left(m_{s+1} - \frac{k}{d}\right) = \lambda_{s+1}\left(j - \frac{k}{d}\right).$$

The above inequlity trivially holds for $j = \frac{k}{d}$. Now for $j > \frac{k}{d}$, if the above inequality does not hold, then we use the fact $\lambda_{s+1} \leq |\lambda_{s+1}| < u$ to conclude $\frac{d}{\beta} < 1$, which contradicts $\beta \leq d$. Therefore, inequality (3.18) holds for $\alpha = s+1$.

Now suppose $\alpha < s+1$. In this case, inequality (3.18) can be rewritten as:

$$\frac{u}{\beta} d\left(j - \frac{k}{d}\right) \geq \lambda_\alpha(j - m_\alpha) + \sum_{i=\alpha+1}^{s} \lambda_i(m_{i-1} - m_i) + \lambda_{s+1}\left(m_s - \frac{k}{d}\right).$$

Assume, for the sake of contradiction, that the last inequality is false. That is, we have:

$$\begin{aligned}\frac{d}{\beta}\left(j - \frac{k}{d}\right) &< \frac{\lambda_\alpha}{u}(j - m_\alpha) + \sum_{i=\alpha+1}^{s} \frac{\lambda_i}{u}(m_{i-1} - m_i) + \frac{\lambda_{s+1}}{u}\left(m_s - \frac{k}{d}\right) \\ &< j - m_\alpha + m_\alpha - m_s + m_s - \frac{k}{d} = j - \frac{k}{d},\end{aligned}$$

where the last inequality follows from $\lambda_i \leq |\lambda_i| < u$ for all i in the range $0 < i \leq t$, $j > m_\alpha$, $m_s \geq \frac{k}{d}$, and the fact that the m_i's are decreasing. For $j = \frac{k}{d}$, the above inequality in contradictory. So assume $j > \frac{k}{d}$. Since $j - \frac{k}{d} > 0$, the above inequality can be rewritten as $\frac{d}{\beta} < 1$, which contradicts $\beta \leq d$. Therefore, (3.14) holds for k in the range $dm_{s+1} < k \leq dm_s$.

Case 2: Now consider the case where $k \leq dm_{s+1}$, i.e., $\frac{k}{d} \leq m_{s+1}$. Recall that the m_i's form a decreasing sequence. Therefore, there exists an integer α in the range $s+1 < \alpha \leq t$ such that $m_\alpha < \frac{k}{d} \leq m_{\alpha-1}$, i.e., $dm_\alpha < k \leq dm_{\alpha-1}$. Using arguments similar to those in Case 1, we obtain:

$$\begin{aligned}v_p(c_k) &\geq r_\alpha + \lambda_\alpha\left(m_\alpha - \frac{k}{d}\right) \\ &> r_{\alpha-1} + \lambda_{\alpha-1}\left(m_{\alpha-1} - \frac{k}{d}\right) \qquad (3.19)\end{aligned}$$

where the last inequality can be obtained using the arguments similar to those used to obtain (3.11) from (3.10). If $\alpha = s+2$, then (3.14) holds true from (3.19). So assume $\alpha > s+2$, we apply Lemma 3.1.2 (i) and use (3.19) to deduce that:

$$v_p(c_k) > r_{s+1} + \lambda_{s+1}\left(m_{s+1} - \frac{k}{d}\right)$$

for all $dm_\alpha < k \leq dm_{\alpha-1}$. This completes the proof of **Case 2**, and hence, the inequality (3.14) holds true for all $k \leq dm_s$.

Since s was chosen arbitrarily from the range $0 \leq s < t$, inequality (3.14) holds for all s, $0 \leq s < t$. This concludes the proof of inequality (3.14), and consequently, the proof of Theorem 7. □

We now provide an example to illustrate that the assumption $u > \lambda_t$ in Theorem 7 is crucial for preserving the structure of the Newton polygon of g under composition by f. Furthermore, this example demonstrates that alternative conditions, such as $u > \lambda_1$ or $u > \frac{r_t}{e}$, which generalize [22, Theorem 3.7], are insufficient to maintain the Newton polygon structure of g.

Example 3.3.1. *Consider the polynomials* $f(x) = x^5 + 4x + 4$ *and* $g(x) = x^3 + 4x + 16$. *The composition* $(g \circ f)(x)$ *is given by:*

$$(g \circ f)(x) = x^{15} + 12x^{11} + 12x^{10} + 48x^7 + 96x^6 + 52x^5 + 64x^3 + 192x^2 + 208x + 96.$$

The Newton polygons of g *and* $g \circ f$ *with respect to the prime* 2 *are:*

$$NP_2(g) : (0,0) \to (2,2) \to (3,4),$$
$$NP_2(g \circ f) : (0,0) \to (10,2) \to (14,4) \to (15,5).$$

Using the notations of Theorem 7, we find $u = 2$ *and* $\beta = 5$. *Observe that* $u = 2$ *satisfies both* $u > \lambda_1 = 1$ *and* $u > \frac{r_t}{e} = \frac{4}{3}$. *However, the Newton polygon structure of* g *is not preserved under the composition by* f, *highlighting the necessity of the condition* $u > \lambda_t$ *in Theorem 7.*

3.4 Proof of Theorem 9

To prove Theorem 9, we first establish a technical lemma that will be instrumental in the proof.

Lemma 3.4.1. *Let* $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, *where* $a_0 \neq 0$, *be a polynomial of degree* d *with rational coefficients. Let* p *be a prime, and let* $g(x) = b_e x^e + b_{e-1}x^{e-1} + \cdots + b_1 x + b_0$ *be a polynomial of degree* e *with rational coefficients. Suppose that*

$$v_p(a_0) > \max_{1 \leq j \leq e} \frac{v_p(b_0) - v_p(b_j)}{j}.$$

Then, $v_p(g(f(0))) = v_p(b_0)$.

Proof. From the given condition, for all j with $1 \leq j \leq e$, we have

$$v_p(a_0) > \frac{v_p(b_0) - v_p(b_j)}{j},$$

which implies

$$v_p(b_j) + jv_p(a_0) > v_p(b_0), \quad \forall j,\ 1 \leq j \leq e.$$

Now consider the evaluation of $g(f(0))$:

$$g(f(0)) = \sum_{j=0}^{e} b_j a_0^j.$$

For $j \geq 1$, the inequality $v_p(b_j) + jv_p(a_0) > v_p(b_0)$ ensures that all other terms $b_j a_0^j$ have strictly higher p-adic valuation than b_0. Consequently, $v_p(g(f(0))) = v_p(b_0)$. □

Proof of Theorem 9: Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0,\ a_0 \neq 0$ be such that $v_p(a_i) > 0$ for all i, $0 \leq i < d$, and $v_p(a_d) = 0$. Our aim is to show that $f(x)$ is eventually stable. We first establish the following assertion for all natural numbers n:

$$f^n(x) \equiv a_d^{\frac{d^n-1}{d-1}} x^{d^n} \pmod{p} \quad \text{and} \quad v_p(f^n(0)) = v_p(a_0). \tag{3.20}$$

The assertion clearly holds for $n = 1$ by the given conditions. Assume that the result holds for $n = k$, i.e.,

$$f^k(x) \equiv a_d^{\frac{d^k-1}{d-1}} x^{d^k} \pmod{p} \quad \text{and} \quad v_p(f^k(0)) = v_p(a_0).$$

This implies

$$\begin{aligned} f^{k+1}(x) &\equiv a_d^{\frac{d^k-1}{d-1}} \left(a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0\right)^{d^k} \pmod{p} \\ &\equiv a_d^{\frac{d^k-1}{d-1}+d^k} x^{d^{k+1}} \equiv a_d^{\frac{d^{k+1}-1}{d-1}} x^{d^{k+1}} \pmod{p}, \end{aligned}$$

where the final congruence follows since $v_p(a_i) > 0$ for all $i \in \{0, 1, \ldots, d-1\}$.

Next, let $f^k(x) = \sum_{j=0}^{d^k} b_j x^j$. By the induction hypothesis on $f^k(x)$, we have $v_p(b_j) \geq 1$ for all j, $1 \leq j \leq d^k$. Consequently, we have:

$$\max_{1 \leq j \leq d^k} \frac{v_p(b_0) - v_p(b_j)}{j} \leq \frac{v_p(b_0) - 1}{j} < v_p(b_0) = v_p(f^k(0)) = v_p(a_0),$$

where the final equality follows from the induction hypothesis. By applying Lemma 3.4.1, it follows that

$$v_p(f^{k+1}(0)) = v_p(b_0) = v_p(f^k(0)) = v_p(a_0).$$

Thus, (3.20) holds for all natural numbers n.

Since $v_p(a_d) = 0$, we have $v_p(a_d^{\frac{d^n-1}{d-1}}) = 0$, implying that the $NP_p(f^n)$ starts at $(0,0)$. Furthermore, (3.20) shows that $NP_p(f^n)$ has an endpoint at $(d^n, v_p(a_0))$, and all edges of $NP_p(f^n)$ must have positive slopes. A chain of edges with positive increasing slopes from $(0,0)$ to $(d^n, v_p(a_0))$ can have at most $v_p(a_0)$ edges. By applying Dumas' theorem to $NP_p(f^n)$, it follows that $f^n(x)$ can have at most $v_p(a_0)$ irreducible factors. Therefore, $f^n(x)$ is eventually stable. □

3.5 Some Applications

In this section, we give some applications of our main results, i.e., Theorems 5, 7 and 9. We start this section by proving Theorem 8 which is about the families of polynomials that are dynamically irreducible at Schur polynomials.

3.5.1 Proof of Theorem 8:

Choose a prime $p \mid m$ and fix $n \geq 0$. Let $G_m(x)$ be the Schur polynomial of degree m. Suppose $f(x) \in \mathbb{Q}[x]$ is such that $v_p(a_d) = 0$ and $f(x) \equiv a_d x^d \pmod{p}$. We show that $G_m \circ f^n$ is irreducible over $\mathbb{Q}$. Write $m = \sum_{i=1}^{N} b_i p^{m_i}$ with $m_1 < m_2 < \cdots < m_N$ and $0 < b_i < p$. Denote $z_j = b_1 p^{m_1} + \cdots + b_j p^{m_j}$ for $1 \leq j \leq N$. Using a method similar to that in [21, Lemma II] and keeping in mind that $\gcd(b_i, m) = 1$ for all i, $0 \leq i \leq m$, we have that $NP_p(G_m)$ has N (as shown in Figure 3.5) segments with slopes

$$\lambda_i = \frac{p^{m_i} - 1}{p^{m_i}(p-1)} < 1.$$

From the proof of Theorem 9, we have $f^n(x) \equiv a_d^{\frac{d^n-1}{d-1}} x^{d^n} \pmod{p}$. Thus, by Theorem 7, $NP_p(G_m \circ f^n)$ has N segments with slopes

$$\frac{p^{m_i} - 1}{d^n p^{m_i}(p-1)}.$$

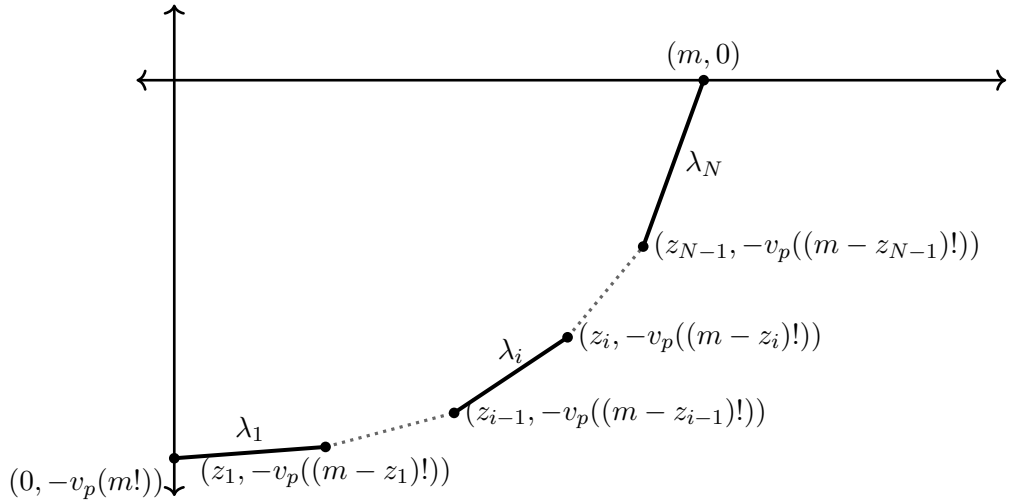


Figure 3.5: Newton polygon of G_m with respect to p

In particular, $d^n p^{v_p(m)} = d^n p^{m_1}$ divides the denominator of each slope of $NP_p(G_m \circ f^n)$. Therefore, by [21, Corollary I], $d^n p^{v_p(m)}$ divides the degree of any irreducible factor of $G_m \circ f^n$ over $\mathbb{Q}$. It follows that any irreducible factor of $G_m \circ f^n$ has degree $d^n \prod_{p|m} p^{v_p(m)} = d^n m$, which proves the result. □

Remark: To remove the restriction $\gcd(b_i, m) = 1$ for all i, $0 < i < m$, we can use a method similar to that in the proof of [33, Theorem 2].

3.5.2 Non-monogenity of number fields:

Consider an algebraic number field $K = \mathbb{Q}(\theta)$, where θ is an element within the ring of algebraic integers of K, denoted by $\mathbb{Z}_K$. Let $f(x)$ be the minimal polynomial of θ over the field of rational numbers $\mathbb{Q}$, and assume that the degree of this polynomial is n. Recall that, a number field K is termed *monogenic* if an element $\alpha \in \mathbb{Z}_K$ exists such that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. In this scenario, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ constitutes an integral basis for K, referred to as a *power integral basis*, or simply a *power basis* of K. If K lacks any such power basis, it is designated as *non-monogenic*.

Let $\operatorname{ind}\theta$ signify the index of the subgroup $\mathbb{Z}[\theta]$ within $\mathbb{Z}_K$, and let $i(K)$ denote the *index* of the field K, defined by

$$i(K) = \gcd\{\operatorname{ind}\alpha \mid K = \mathbb{Q}(\alpha) \text{ and } \alpha \in \mathbb{Z}_K\}.$$

A prime number p that divides $i(K)$ is termed a *prime common index divisor* of K. Observe that if K is monogenic, then $i(K) = 1$. As a result, any number field that has a prime common index divisor cannot be monogenic.

For a rational prime p, let $\mathbb{F}_p$ stand for the finite field containing p elements, and let $\mathbb{Z}_p$ represent the ring of p-adic integers. The subsequent result, taken from [83, Theorem 4.34], will be employed to demonstrate the non-monogeneity of the number field K.

Lemma 3.5.1. *[83, Theorem 4.34] Consider an algebraic number field K and a rational prime p. Let P_h represent the count of unique prime ideals within the ring of integers of K, $\mathbb{Z}_K$, that lie over p and possess a residual degree of h. Further, let N_h denote the quantity of irreducible polynomials of degree h in the polynomial ring over the finite field with p elements, $\mathbb{F}_p[x]$. Then, p serves as a prime common index divisor of K if and only if, for at least one value of h, the inequality $P_h > N_h$ holds.*

Recently, using the aforementioned result, many authors have constructed classes of non-monogenic number fields generated by roots of binomials, trinomials, quadrinomials, and other types of polynomials. For further details, we refer the reader to the recent survey article [39].

To understand the link between the prime ideals lying above p and the Newton polygon, we need the following definition of residual polynomial.

Definition 3.5.2. *Let $\phi(x)$ be a monic polynomial in $\mathbb{Z}_p[x]$ that remains irreducible when considered modulo a rational prime p, and let α be a root of $\phi(x)$ in an algebraic closure of the p-adic numbers, $\overline{\mathbb{Q}}_p$. Consider a monic polynomial $f(x) \in \mathbb{Z}_p[x]$ not divisible by $\phi(x)$, with its $\phi(x)$-expansion given by $\phi(x)^n + a_{n-1}(x)\phi(x)^{n-1} + \cdots + a_0(x)$, and assume that the reduction of $f(x)$ modulo p, $\overline{f}(x)$, is a power of the reduction of $\phi(x)$, $\overline{\phi}(x)$.*

Suppose the ϕ-Newton polygon of $f(x)$ with respect to p has a single edge, denoted by S, exhibiting a positive slope l/e, where l and e are coprime positive integers. This implies that

$$\min\left\{ \frac{v_{p,x}(a_{n-i}(x))}{i} \;\middle|\; 1 \le i \le n \right\} = \frac{v_{p,x}(a_0(x))}{n} = \frac{l}{e},$$

Consequently, n is divisible by e, say $n = et$, and $v_{p,x}(a_{n-ej}(x)) \ge lj$ for $1 \le j \le t$. Thus, the polynomial $b_j(x) := a_{n-ej}(x)/p^{lj}$ has coefficients in $\mathbb{Z}_p$, and $b_j(\alpha) \in \mathbb{Z}_p[\alpha]$ for $1 \le j \le t$. The polynomial $T(Y)$ in the indeterminate Y, defined as $T(Y) = Y^t + \sum_{j=1}^{t} b_j(\alpha)Y^{t-j}$ with coefficients in $\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x]/\langle \phi(x) \rangle$, is termed "the residual polynomial of $f(x)$" with respect to (ϕ, S).

Now, consider the case where the ϕ-Newton polygon of $f(x)$ possesses multiple edges, say $S_1, \ldots, S_t$, with slopes $\lambda_1 < \cdots < \lambda_t$. By applying Theorem 1.1.7, we can factor $f(x)$ as $f(x) = f_1(x) \cdots f_t(x)$, where each $f_i(x) \in \mathbb{Z}_p[x]$ has a ϕ-Newton polygon consisting of a single edge S_i', which is a translation of S_i. "The residual polynomial of $f_i(x)$ with respect to (ϕ, S_i') is then referred to as the residual polynomial of $f(x)$ with respect to

(ϕ, S_i)." *Furthermore, "the polynomial $f(x)$ is called p-regular with respect to ϕ if none of the polynomials $T_i(Y)$ exhibit a repeated root within the algebraic closure of $\mathbb{F}_p$, for all i from 1 to t."*

Definition 3.5.3. *Suppose $f(x) \in \mathbb{Z}_p[x]$ is a monic polynomial and its factorization modulo p into irreducible polynomials is given by $\overline{f}(x) = \overline{\phi_1}(x)^{e_1} \cdots \overline{\phi_r}(x)^{e_r}$, where each $\phi_i(x) \in \mathbb{Z}_p[x]$ is monic and $e_i > 0$. Then, according to Hensel's lemma [8, Ch.4, Section 3], there exist monic polynomials $f_1(x), \ldots, f_r(x)$ in $\mathbb{Z}_p[x]$ such that $f(x) = f_1(x) \cdots f_r(x)$ and $\overline{f_i}(x) = \overline{\phi_i}(x)^{e_i}$ for every i. "The polynomial $f(x)$ is defined as p-regular (with respect to $\phi_1, \ldots, \phi_r$) if each individual $f_i(x)$ exhibits p-regularity with respect to its corresponding ϕ_i."*

We now state a weaker version of [68, Theorem 1.2], which will help in the counting number of prime ideals in $\mathbb{Z}_K$ dividing a rational prime p.

Theorem 3.5.4. *[53, Theorem 3.7] Let $K = \mathbb{Q}(\theta)$ be a number field with θ satisfying an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ and p be a rational prime. Let $\phi_1(x)^{e_1} \cdots \phi_r(x)^{e_r}$ be the factorisation of $f(x)$ modulo p into powers of distinct irreducible polynomials over $\mathbb{F}_p$ with each $\phi_i(x)$ belonging to $\mathbb{Z}[x]$ monic and not dividing $f(x)$. For each i, suppose that the ϕ_i-Newton polygon of $g(x)$ have t_i edges S_{ij} with slopes $\lambda_{ij} = l_{ij}/e_{ij}$, where $\gcd(l_{ij}, e_{ij}) = 1$. If $f(x)$ is p-regular and $T_{ij}(Y) = \prod_{s=1}^{s_{ij}} U_{ijs}(Y)$ is the factorisation of the residual polynomial $T_{ij}(Y)$ into distinct irreducible factors over $\mathbb{F}_p$ with respect to (ϕ_i, S_{ij}) for $1 \leq j \leq t_i$, then*

$$p\mathbb{Z}_K = \prod_{i=1}^{r} \prod_{j=1}^{t_i} \prod_{s=1}^{s_{ij}} \mathfrak{p}_{ijs}^{e_{ij}},$$

where $\mathfrak{p}_{ijs}$ are distinct prime ideals of $\mathbb{Z}_K$ having residual degree $\deg \phi_i(x) \cdot \deg U_{ijs}(Y)$.

We highlight here that using Theorems 5 and 7 with Lemma 3.5.1, one can easily deduce a tower of non-monogenic number fields K_n generated by roots of irreducible polynomials $f^n(x)$ for $n \in \mathbb{N}$. For example:

Let $f(x) = x^d + 3^4 a x^m + 3^4 b x^l + 3^4 c \in \mathbb{Q}[x]$ with $v_3(a) = v_3(b) = v_3(c) = 0$. Suppose that the vertices of the Newton polygon $NP_2(f)$ are given by the set

$$S = \{(0,0), (d-m, v_2(a)), (d-l, v_2(b)), (d, v_2(c))\}.$$

Assuming $\gcd(d-m, v_2(a)) = \gcd(d-l, v_2(b)) = \gcd(d, v_2(c)) = 1$, define the slopes:

$$\lambda_1 = \frac{v_2(a)}{d-m}, \quad \lambda_2 = \frac{v_2(b) - v_2(a)}{m-l}, \quad \lambda_3 = \frac{v_2(c) - v_2(b)}{l}.$$

Clearly, $f(x)$ is a 3^4-Dumas polynomial. By Corollary 1.1.10, all iterates f^n of f are 3^4-Dumas and hence irreducible. Further, choose $a, b, c \in \mathbb{Q}$ such that $v_2(c) \leq \lambda_1(2d-1)$.

Under this assumption, Theorem 6 implies that for all $n \in \mathbb{N}$, the Newton polygon of f^n with respect to 2 is given by:

$$NP_2(f^n) : (0,0) \to (d^{n-1}(d-m), v_2(a)) \to (d^{n-1}(d-l), v_2(b)) \to (d^n, v_2(c)).$$

The constraints on the 2-adic valuations of $a, b, c \in \mathbb{Q}$ ensures that the residual polynomials corresponding to each edge are linear. If θ_n is a root of f^n and $K_n = \mathbb{Q}[\theta_n]$, then by Theorem 3.5.4, we see that the number of distinct prime ideals of $\mathbb{Z}_{K_n}$ lying above 2 having residual degree 1 are 3. However, we know that the number of distinct irreducible linear polynomials in $\mathbb{F}_2[x]$ are 2. Therefore, by Lemma 3.5.1, $2 \mid i(K_n)$ for all $n \in \mathbb{N}$. This establishes that for all $n \in \mathbb{N}$, f^n is non-monogenic.

There exist infinitely many such families of polynomials. One particular family is

$$f(x) = x^4 + 2 \cdot 3^4 a x^3 + 16 \cdot 3^4 b x + 128 \cdot 3^4 c,$$

where $a, b, c \in \mathbb{Q}$ satisfy $v_q(a) = v_q(b) = v_q(c) = 0$ for $q = 2, 3$. Clearly, $f(x)$ is a 3^4-Dumas polynomial.

3.5.3 Number of Irreducible Factors, Eventual Stability, and Degree of Factors:

Let $g(x) \in \mathbb{Q}[x]$ be a polynomial of degree e, and let p be a prime such that the Newton polygon of g with respect to p is given by:

$$NP_p(g) : (0,0) \to (e - m_1, r_1) \to \cdots \to (e - m_s, r_s) \to \cdots \to (e, r_t).$$

Here, we define $m_0 = e$, $m_t = r_0 = 0$, and let $0 < \lambda_1 < \lambda_2 < \cdots < \lambda_t$ be the slopes of the edges of $NP_p(g)$. If $r_t \leq \lambda_1(2e-1)$, then Theorem 5 implies that, for any $n \in \mathbb{N}$, the Newton polygon of the nth iterate of g, denoted by g^n, is given by:

$$NP_p(g^n) : (0,0) \to (e^{n-1}(e - m_1), r_1) \to \cdots \to (e^{n-1}(e - m_s), r_s) \to \cdots \to (e^n, r_t).$$

In this case, the number of irreducible factors of g^n is bounded by r_t, ensuring that g^n is *eventually stable*. Furthermore, if we assume

$$\gcd(e(m_{s+1} - m_s), r_{s+1} - r_s) = 1 \quad \text{for all } 0 \leq s < t,$$

then the vertices of the Newton polygon are the only lattice points on $NP_p(g)$. Applying Dumas' Theorem, it follows that g^n remains eventually stable, with the number of irreducible factors of g^n bounded by t.

Additionally, Dumas' Theorem implies that the degree of any irreducible factor of g^n belongs to the set:

$$\left\{ \sum_{j=1}^{k} (m_{i_j+1} - m_{i_j}) : 1 \leq k \leq n \text{ and } 1 \leq i_1, i_2, \ldots, i_k \leq n \right\}.$$

3.5.4 Conjecture of Sookdeo:

Consider a number field K and a non-constant rational function $f(x) \in K(x)$. The *backward orbit* of $\alpha \in \mathbb{P}^1(K)$ under f, denoted by $O_f^-(\alpha)$, is defined as

$$O_f^-(\alpha) := \bigcup_{n \geq 0} f^{-n}(\alpha) = \bigcup_{n \geq 0} \{\beta \in \mathbb{P}^1(\overline{K}) : f^n(\beta) = \alpha\}.$$

Recall that, a point α is *preperiodic* for f if its forward orbit $O_f^+(\alpha) = \{\alpha, f(\alpha), f^2(\alpha), \ldots\}$ is finite. Similarly, α is said to be *exceptional* for f if its backward orbit $O_f^-(\alpha)$ is finite.

Consider a point $\alpha \in \mathbb{P}^1(K)$. For each $n \geq 1$, choose coprime $a_n, b_n \in K[x]$ with $f^n(z) = a_n(x)/b_n(x)$. If $\alpha \neq \infty$, we say that the pair (f, α) is *eventually stable*, if the number of irreducible factors of $a_n(x) - \alpha b_n(x)$ in $K[x]$ is bounded by a constant independent of n. We say that (f, ∞) is *eventually stable*, if the number of irreducible factors of $b_n(z)$ is similarly bounded.

Let S be a finite set of places of K containing all Archimedean places. A point $\beta \in \mathbb{P}^1(\overline{K})$ is called *S-integral with respect to* $\gamma \in \mathbb{P}^1(K)$ if there is no prime $\mathfrak{p}$ of $K(\beta)$ lying over a prime outside of S such that the images of β and γ modulo $\mathfrak{p}$ coincide. Define the set

$$\mathcal{O}_{S,\gamma} := \{\beta \in \mathbb{P}^1(\overline{K}) : \beta \text{ is } S\text{-integral with respect to } \gamma\}.$$

If S consists only of the Archimedean places of K, then $\mathcal{O}_{S,\infty}$ is the ring of algebraic integers in $\overline{K}$.

With the above definitions, Silverman [94] in 1993 proved that: For a rational function $f(x) \in \mathbb{Q}(x)$ of degree at least 2 and $\alpha \in \mathbb{P}^1(K)$, if α is not exceptional for f, then the forward orbit $O_f^+(\alpha)$ contains only finitely many points in $\mathbb{P}^1(K)$ that are S-integral relative to α. Motivated by this result, Sookdeo [97] in 2011, gave the following conjecture for S-integral points in backward orbit.

Conjecture 3.5.5. *If $\alpha \in \mathbb{P}^1(K)$ is not preperiodic for f, then the backward orbit $O_f^-(\alpha)$ contains at most finitely many points in $\mathbb{P}^1(\overline{K})$ which are S-integral relative to α.*

In the same paper, Sookdeo [97, Theorem 2.5 and 2.6] proved the following result relating eventual stability with S-integral points in $\mathcal{O}_f^-(\alpha)$.

Theorem 3.5.6. *Let K be a number field, S a finite set of places of K containing all Archimedean places, $\alpha \in \mathbb{P}^1(K)$, and $f(x) \in K(x)$ be a rational function of degree $d \geq 2$. If (f, α) is eventually stable, then*

$$\mathcal{O}_{S,\gamma} \cap O_f^-(\alpha) \text{ is finite for all } \gamma \in \mathbb{P}^1(K) \text{ not preperiodic under } f.$$

From Theorem 3.5.6, we observe that *eventual stability* plays a crucial role in proving the Conjecture of Sookdeo. Using Theorems 5 and 7, one can easily generate infinitely many families of polynomials in $\mathbb{Q}[x]$ satisfying the conjecture. One such family is described below.

For an integer $n \geq 3$, consider the polynomial

$$g(x) = x^{3n} + 2ax^{2n-2} + 4bx^{n-2} + 8c,$$

where a and b are positive rationals with $v_2(a) = v_2(b) = 0$, and c is an odd positive integer. A simple application of Theorem 5 shows that $g^n(x)$ is eventually stable. Moreover, it can be easily verified that

$$8 \leq g(0) < g^2(0) < \cdots < g^n(0) < \cdots,$$

which implies that 0 is not preperiodic under g. Applying Theorem 3.5.6, it follows that Sookdeo's conjecture [97, Conjecture 1.2] holds for the polynomial $g(x)$.

Chapter 4

Primitive prime divisors

For the polynomial $f(x) \in \mathbb{Q}[x]$, we consider the Zsigmondy set $\mathcal{Z}(f,0)$ associated to the numerators of the sequence $\{f^n(0)\}_{n\geq 0}$. In this chapter, we provide an upper bound on the largest element of $\mathcal{Z}(f,0)$. As an application, we show that the largest element of the set $\mathcal{Z}(f,0)$ is bounded above by 6 when $f(x) = x^d + x^e + c \in \mathbb{Q}[x]$, with $d > e \geq 2$ and $|c| > 2$. Furthermore, when $f(x) = x^d + c \in \mathbb{Q}[x]$ with $|f(0)| > 2^{\frac{d}{d-1}}$ and $d > 2$, we also deduce a result of Krieger [Int. Math. Res. Not. IMRN, 23 (2013), pp. 5498-5525] as a consequence of our main result. All the proofs and results in this chapter are taken from [74].

4.1 Preliminaries

Throughout the chapter, p will denote a prime number, and $v_p(\alpha)$ will denote the p-adic valuation of an integer α. Let $f(x)$ be a polynomial such that

$$f(x) = a_d x^d + \cdots + a_1 x + a_0, \text{with } a_i \in \mathbb{Q}, a_d \neq 0, \text{and } a_1 = 0 \tag{4.1}$$

Write the n^{th}-iteration $f^n(0)$ in lowest form as

$$f^n(0) = \frac{A_n}{B_n}, \tag{4.2}$$

where $B_n > 0$ and co-prime to A_n. Recall the definition

$$\mathcal{Z}(f,0) := \{n \in \mathbb{N} : A_n \text{ has no primitive prime divisor}\}.$$

At first we will establish the rigid divisibility of the sequence $(A_n)_{n\geq 0}$ and state lemmas related to this property. Next, we define the concepts of local and global canonical heights and state results related to properties of canonical heights.

4.1.1 Rigid divisibility property

A sequence $(u_n)_{n\geq 0}$ of integers is said to be a *rigid divisibility sequence* if for every prime p the following properties hold:

1. If $v_p(u_n) > 0$, then $v_p(u_{kn}) = v_p(u_n)$ for all $k \geq 1$.
2. If $v_p(u_n) > 0$ and $v_p(u_m) > 0$, then $v_p(u_{\gcd(n,m)}) > 0$.

Let p be a prime such that $p \mid A_{n_0}$ for some $n_0 \in \mathbb{N} \cup \{0\}$. Set $k(p) = \min\{n : p \mid A_n\}$.

Lemma 4.1.1. *Let $f(x)$ be as above in (4.1) and A_n as in (4.2). Suppose that p is a prime that divides some element of the sequence $(A_n)_{n\geq 0}$. Then for every $n \in \mathbb{N}$, the p-adic valuation of A_n and $A_{k(p)}$ are related in the following way:*

$$v_p(A_n) = \begin{cases} v_p(A_{k(p)}) & \text{if } k(p) \mid n, \\ 0 & \text{else.} \end{cases}$$

Proof. The proof follows from [72, Lemma 2.3]. □

One can see that the following result is a consequence of Lemma 4.1.1.

Lemma 4.1.2. *Let $f(x)$ be as above in (4.1) and A_n as in (4.2). For a natural number n, suppose that $n \in \mathcal{Z}(f, 0)$, i.e., A_n does not have a primitive prime divisor. Then A_n satisfies the following relation*

$$A_n \mid \prod_{\substack{q \mid n \\ q \text{ prime}}} A_{\frac{n}{q}}. \tag{4.3}$$

Taking logarithms of the absolute values in the above corollary, we obtain our next result which will be helpful in computations.

Corollary 4.1.3. *Let $f(x)$ be as above in (4.1) and A_n as in (4.2). Suppose A_n has no primitive prime divisor. Then*

$$\log |A_n| \leq \sum_{\substack{q \mid n \\ q:\text{prime}}} \log |A_{\frac{n}{q}}|.$$

4.1.2 Canonical heights

Let $V_{\mathbb{Q}}$ be the set of places of $\mathbb{Q}$. For $p \in V_{\mathbb{Q}}$, we choose a normalized absolute value $|\cdot|_p$ in the following way. When $p = \infty$, the notation $|\cdot|_p$ refers to the standard absolute value defined on the set of rational numbers $\mathbb{Q}$. Alternatively, if p represents a prime number, then $|\cdot|_p$ denotes the p-adic absolute value on $\mathbb{Q}$, where for any non-zero rational number $x \in \mathbb{Q}^\times$, its absolute value is given by $|x|_p = p^{-v_p(x)}$, with $v_p(x)$ being the p-adic valuation of x. These absolute values satisfy the product formula

$$\prod_{v \in V_{\mathbb{Q}}} |x|_v = 1,$$

for any $x \in \mathbb{Q}^\times$. The standard (global) height function on $\mathbb{Q}$ is the function $h : \mathbb{Q} \to \mathbb{R}$ given by $h(x) = \log \max\{|m|_\infty, |n|_\infty\}$, where $x = m/n$ in lowest terms. Equivalently,

$$h(x) = \sum_{v \in V_{\mathbb{Q}}} \log \max\{1, |x|_v\}, \quad \text{for any } x \in \mathbb{Q}^\times. \tag{4.4}$$

This height function h extends to the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ (see [95, Section 3.1]). For any fixed polynomial $f(x) \in \mathbb{Q}[x]$ (or more generally, rational function) of degree $d \geq 2$, the canonical height function $\hat{h}_f : \bar{\mathbb{Q}} \to \mathbb{R}$ for f is given by

$$\hat{h}_f(x) := \lim_{n \to \infty} \frac{h\left(f^n(x)\right)}{d^n}. \tag{4.5}$$

Lemma 4.1.4 ([14, 95])**.** *The canonical height function satisfy the following properties:*

(a) There is a constant C depending only on f such that $|\hat{h}_f(x) - h(x)| \leq C$ for every $x \in \bar{\mathbb{Q}}$.

(b) $\hat{h}_f\left(f(x)\right) = d \cdot \hat{h}_f(x)$ for all $x \in \bar{\mathbb{Q}}$.

Definition 4.1.5. *For $v \in V_{\mathbb{Q}}$, let $\mathbb{C}_v$ denote the completion of an algebraic closure of $\mathbb{Q}$ with respect to v. The function $h_v : \mathbb{C}_v \to [0, \infty)$ given by*

$$h_v(x) := \log \max\{1, |x|_v\}$$

is called the standard local height at v. Using this, (4.4) can be rewritten as

$$h(x) = \sum_{v \in V_{\mathbb{Q}}} h_v(x), \quad \text{for any } x \in \mathbb{Q}^\times.$$

If $f(x) \in \mathbb{Q}[x]$ is a polynomial of degree $d \geq 2$, the associated local canonical height is the function $\hat{h}_{v,f}(x) : \mathbb{C}_v \to [0, \infty)$ given by

$$\hat{h}_{v,f}(x) = \lim_{n\to\infty} \frac{h_v\left(f^n(x)\right)}{d^n}. \tag{4.6}$$

The local canonical heights provide a similar decomposition for $\hat{h}_f$, as follows.

Lemma 4.1.6 ([14], Theorem 2.3)**.** *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree $d \geq 2$. Then for all $x \in \mathbb{Q}$*

$$\hat{h}_f(x) = \sum_{v\in V_{\mathbb{Q}}} \hat{h}_{v,f}(x).$$

The following result of Benedetto *et al.* [4, Proposition 2.1] is needed to estimate the constant C in Lemma 4.1.4(a).

Lemma 4.1.7. *Let K be a field with absolute value v, let $f(x) \in K[x]$ be a polynomial of degree $d \geq 2$, and let $\hat{h}_{v,f}$ be the associated local canonical height. Write $f(x) = a_d x^d + \cdots + a_1 x + a_0 = a_d(x - \alpha_1)\cdots(x - \alpha_d)$, with $a_i \in K$, $a_d \neq 0$, and $\alpha_i \in \mathbb{C}_v$. Let $A = \max\{|\alpha_i|_v : i = 1, 2, \ldots, d\}$ and $B = |a_d|_v^{-1/d}$, and define real constant $C_v \geq 1$ by*

$$C_v = \begin{cases} \max\{1, A, B, |a_0|_v, |a_1|_v, \ldots, |a_d|_v\} & \text{if } v \text{ is nonarchimedean,} \\ \max\{1, A + B, |a_0|_v + |a_1|_v + \ldots + |a_d|_v\} & \text{if } v \text{ is archimedean.} \end{cases}$$

Then for all $x \in \mathbb{C}_v$,

$$\frac{-d \log C_v}{d-1} \leq \hat{h}_{v,f}(x) - h_v(x) \leq \frac{\log C_v}{d-1}.$$

Remark 4.1.8. *Note that from [4, Remark 2.3], if v is nonarchimedean then $A = \max\{|\alpha_i|_v\}$ can be directly computed from the coefficients of f. Specifically,*

$$A = \max\left\{ \left|\frac{a_j}{a_d}\right|_v^{1/(d-j)} : 0 \leq j \leq d-1 \right\}.$$

On the other hand, if v is archimedean then $A \leq \sum_{j=0}^{d-1} |a_j/a_d|_v^{1/(d-j)}$. Hence, the constant C_v can be easily computed from the coefficients of f.

Remark 4.1.9. *For $f(x) \in \mathbb{Q}[x]$, taking sum over all places v of $\mathbb{Q}$, we obtain*

$$\frac{-dC}{d-1} \leq \hat{h}_f(x) - h(x) \leq \frac{dC}{d-1} \tag{4.7}$$

where C is a constant satisfying $C \geq \sum_{v\in V_K} \log C_v$.

4.2 Proof of Theorem 10

For $d \geq 2$, let $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ be such that $a_d \neq 0$ and $a_1 = 0$. In this section, we prove Theorem 10 which establishes an upper bound of the Zsigmondy set for the sequence $(f^n(0))_{n\geq 1}$. At first we will establish the lower bound for $|f^k(x)|$. Precisely, we will prove that $|f^k(x)| \geq 1$ for all $k \geq 1$. This observation will help us to use $h(f^k(0))$ and $\log |A_n|$ interchangeably.

Proposition 4.2.1. *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree $d \geq 2$. Write $f(x) = a_d x^d + \cdots + a_1 x + a_0$, with $a_i \in \mathbb{Q}, a_d \neq 0$. Let x be such that $|x| \geq 1$ and satisfies (1.3). Then for all $k \in \mathbb{N}$, we have $|f^k(x)| \geq |x|$.*

Proof. Let $x \in \mathbb{R}$ be such that $|x| \geq 1$ and satisfies (1.3). If $x \geq 1$, then from (1.2) and (1.3), we get

$$\begin{aligned} |f(x)| &= \left| \sum_{i\in P^+} a_i x^i + \sum_{i\in N^+} a_i x^i \right| \geq \left| \sum_{i\in P^+} a_i x^i \right| - \left| \sum_{i\in N^+} a_i x^i \right| \\ &\geq \sum_{i\in P^+} |a_i||x|^i - |x|^{n^+} \sum_{i\in N^+} |a_i| \\ &\geq |x|^{n^+} \left(\sum_{n^+<i\leq d} |a_i||x|^{i-n^+} - \sum_{i\in N^+} |a_i| \right) \geq |x|^{n^+} \geq |x|. \end{aligned} \tag{4.8}$$

If $x \leq -1$, then proceeding as in (4.8) with the sets P^- and N^- and then using the assumption in (1.3), we obtain

$$|f(x)| \geq |x|^{n^-} \geq |x|.$$

Note that $|f(x)| \geq |x| \geq 1$. If $f(x) \geq 1$, then by the last inequality of (4.8),

$$\begin{aligned} |f^2(x)| &\geq |f(x)|^{n^+} \left(\sum_{n^+<i\leq d} |a_i||f(x)|^{i-n^+} - \sum_{i\in N^+} |a_i| \right) \\ &\geq |x|^{n^+} \left(\sum_{n^+<i\leq d} |a_i||x|^{i-n^+} - \sum_{i\in N^+} |a_i| \right) \geq |x|^{n^+} \geq |x|. \end{aligned}$$

Similarly, if $f(x) \leq -1$, then $|f^2(x)| \geq |x|^{n^-} \geq |x| \geq 1$. Now Proposition 4.2.1 follows by induction on k. □

Proof of Theorem 10: For $d \geq 2$, let $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ be such that $a_d \neq 0$ and $a_1 = 0$. Then from (4.2), we get

$$f^{k-1}(a_0) = f^k(0) = \frac{A_k}{B_k}.$$

We proceed to find an upper bound of $n \in \mathcal{Z}(f, 0)$. Since $|a_0| \geq 1$ and a_0 satisfies the inequality (1.3), by Proposition 4.2.1, we have for all $k \geq 1$, $|f^{k-1}(a_0)| \geq |a_0| \geq 1$ and hence $|A_k| \geq B_k$. Thus,

$$h(f^{k-1}(a_0)) = h(f^k(0)) = \log(|A_k|), \quad \text{for all } k \geq 1. \tag{4.9}$$

Suppose that $n \in \mathcal{Z}(f, 0)$. By Corollary 4.1.3, we have

$$\log |A_n| \leq \sum_{p|n} \log |A_{\frac{n}{p}}| \tag{4.10}$$

where the sum is taken over all distinct prime divisors p of n. Then from (4.9) and (4.10), we get

$$h(f^{n-1}(a_0)) \leq \sum_{p|n} h(f^{\frac{n}{p}-1}(a_0)). \tag{4.11}$$

Let C be the constant given in Remark 4.1.9. From (4.7), we have

$$\hat{h}_f(f^{n-1}(a_0)) - \frac{dC}{d-1} \leq \sum_{p|n} \left(\hat{h}_f(f^{\frac{n}{p}-1}(a_0)) + \frac{dC}{d-1} \right).$$

Further, using functional relation in Lemma 4.1.4(b), we get

$$d^{n-1}\hat{h}_f(a_0) - \frac{dC}{d-1} \leq \hat{h}_f(a_0) \sum_{p|n} d^{\frac{n}{p}-1} + \omega(n)\frac{dC}{d-1}.$$

where $\omega(n)$ represents the count of the distinct prime factors of the integer n. A simple calculation gives

$$\frac{d^{n-1} - \omega(n) d^{\frac{n}{2}-1}}{\omega(n)+1} \leq \frac{d^{n-1} - \frac{1}{d}\sum_{p|n} d^{\frac{n}{p}}}{\omega(n)+1} \leq \frac{dC}{(d-1)\hat{h}_f(a_0)}. \tag{4.12}$$

Further, for $n \geq 4$, one can easily obtain that $2\omega(n) + 1 \leq n - 1 \leq 2^{\frac{n}{2}} - 1 < d^{\frac{n}{2}}$. This yields

$$2\omega(n) + 1 < d^{\frac{n}{2}}, \text{ for all } d \geq 3 \text{ and } n \geq 2. \tag{4.13}$$

Hence, from (4.12), we get

$$d^{\frac{n}{2}-1} \leq d^{\frac{n}{2}-1}\frac{d^{\frac{n}{2}}-\omega(n)}{\omega(n)+1} \leq \frac{dC}{(d-1)\hat{h}_f(a_0)}$$

implying

$$n \leq \frac{2}{\log d}\log\left(\frac{dC}{(d-1)\hat{h}_f(a_0)}\right)+2.$$

This completes the proof of Theorem 10. □

Remark 4.2.2. *We use (1.3) and $|a_0| \geq 1$ to prove that $|f^n(a_0)| \geq 1$, so that we can replace $\log|A_n|$ by $h(f^n(a_0))$. If we can ensure $|f^n(a_0)| \geq 1$, then without the assumptions (1.3) and $|a_0| \geq 1$ in Theorem 10, we can directly use the bound on n given there.*

4.2.1 Proof of Corollary 1.1.17:

From Remark 4.1.9, we can easily see that $C = \log 2 + h(c)$ will work for the polynomial $f(x)$. Further, the remark following [51, Lemma 6] gives the lower bound $\hat{h}_f(c) \geq \frac{1}{d}h(c)$ for $|c| > 2^{\frac{d}{d-1}}$. Using the above values in Theorem 10, we deduce that $n \leq 5$. Further, with the simple observation $|f(x)| \geq |x|^{d-1}$ whenever $|x| > 2$ and the rigid divisibility of numerator of the sequence $f^n(0)$, we deduce that $\mathcal{Z}(f,0) = \emptyset$. □

4.3 Proof of Theorem 11

The following result of Benedetto *et al.* [3, Lemma 2.1] will be used to establish the lower bound of $\hat{h}_f(x)$ for $x \in \mathbb{Q}^\times$.

Lemma 4.3.1. *Let $f(x) = f_1(x)/f_2(x) \in \mathbb{Q}(x)$ where f_1, f_2 are relatively prime polynomials in $\mathbb{Z}[x]$ with degree $d := \max\{\deg f_1, \deg f_2\} \geq 2$. Let $R = Res(f_1, f_2) \in \mathbb{Z}$ be the resultant of f_1 and f_2, and let*

$$D := \min_{t\in\mathbb{R}\cup\{\infty\}} \frac{\max\left\{|f_1(t)|, |f_2(t)|\right\}}{\max\{|t|^d, 1\}}. \tag{4.14}$$

Then $D > 0$, and for all $x \in \mathbb{P}^1(\mathbb{Q})$ and all integers $i \geq 0$,

$$\hat{h}_f(x) \geq d^{-i}\left[h(f^i(x)) - \frac{1}{d-1}\log\left(\frac{|R|}{D}\right)\right]. \tag{4.15}$$

Proof of Theorem 11: Suppose that $f(x) = x^d + x^e + \frac{a}{b}$ where $c = \frac{a}{b} \in \mathbb{Q}$ for a, b relatively prime integers and $|c| \geq 1$. We proceed to show that 6 is an upper bound of $\mathcal{Z}(f,0)$.

Rewrite $f(x)$ as

$$f(x) = \frac{f_1(x)}{f_2(x)}, \text{ where } f_1(x) = bx^d + bx^e + a \in \mathbb{Z}[x] \text{ and } f_2(x) = b \in \mathbb{Z}[x].$$

The resultant of f_1 and f_2 is given by $R = \text{Res}(f_1, f_2) = b^d$. Now we will compute the lower bound for D defined in (4.14). Let $s := \max\{2, |c|\}$. Then for $|t| \leq s$, we have $\max\{1, |t|^d\} \leq s^d$. Since $b \geq 1$, for $t \in \mathbb{R} \cup \{\infty\}$,

$$\frac{\max\{|f_1(t)|, |f_2(t)|\}}{\max\{|t|^d, 1\}} \geq \frac{|f_2(t)|}{s^d} = \frac{b}{s^d} \geq \frac{1}{s^d}. \tag{4.16}$$

Again for $|t| > s \geq 2$, we obtain

$$\begin{aligned} \frac{\max\{|f_1(t)|, |f_2(t)|\}}{\max\{|t|^d, 1\}} &\geq \frac{|f_1(t)|}{|t|^d} \geq b\left(1 - \frac{1}{|t|^{d-e}} - \frac{|c|}{|t|^d}\right) \\ &> \left(1 - \frac{1}{2} - \frac{1}{2^{d-1}}\right) \geq \frac{1}{4} \geq \frac{1}{s^d} \end{aligned} \tag{4.17}$$

since $|a| > b > 1, |t| > s \geq 2$ and $d \geq 3$. From (4.16) and (4.17), we get $D \geq \frac{1}{s^d}$. Substituting the lower bound for D and the value of resultant R in (4.15), for any integer $i \geq 0$, $x \in \mathbb{P}^1(\mathbb{Q})$ and $|c| \geq 2$, we obtain

$$\begin{aligned} \hat{h}_f(x) &\geq d^{-i}\left[h(f^i(x)) - \frac{1}{d-1}\log b^d + \frac{1}{d-1}\log\left(\frac{1}{s^d}\right)\right] \\ &= d^{-i}\left[h(f^i(x)) - \frac{d}{d-1}\log|a|\right]. \end{aligned}$$

Therefore,

$$\hat{h}_f(x) \geq d^{-i}\left[h(f^i(x)) - \frac{d}{d-1}h(c)\right]. \tag{4.18}$$

For any $x \in \mathbb{R}$ with $|x| \geq |c| > 2$,

$$|f(x)| = |x^d + x^e + c| \geq |x|^d - |x|^e - |c| \geq |x|^{d-1} - |x|^e + |x|^{d-2} - |c| + |x|^{d-2} \geq |x|^{d-2}$$

where the last inequality holds since $|x| \geq |c| > 2$ and the fact that $d > e \geq 2$. This implies that $h(f(c)) \geq (d-2)h(c)$ and hence for $d \geq 5$, we have

$$(d-1)h(f(c)) - dh(c) \geq ((d-1)(d-2) - d)h(c) \geq dh(c). \tag{4.19}$$

For $d = 4$, the above inequality implies that

$$(d-1)h(f(c)) - dh(c) \geq 2h(c). \tag{4.20}$$

For $d = 3$, one can notice that $\operatorname{sgn}(c^d) = \operatorname{sgn}(c)$, and hence

$$|f(c)| \geq |c|^3 - |c|^2 \geq |c|^2.$$

Using similar argument as in (4.19), for $d = 3$ we obtain that

$$(d-1)h(f(c)) - dh(c) \geq h(c). \tag{4.21}$$

Setting $i = 1$ and $|c| > 2$ in (4.18), then from (4.19), (4.20) and (4.21), we get the lower bound for $\hat{h}_f(c)$

$$(d-1)\hat{h}_f(c) \geq \begin{cases} h(c) & \text{if } d \geq 5, \\ \frac{1}{3}h(c) & \text{if } d = 4, 3. \end{cases}$$

Using the computations from Remark 4.1.8 and Lemma 4.1.7, we obtain that

$$C_v = \begin{cases} |b^{-1}|_v & \text{if } v \text{ is nonarchimedean}, \\ 2 + |c| & \text{if } v \text{ is archimedean}. \end{cases} \tag{4.22}$$

Hence, the constant C in Theorem 10 for $f(x) = x^d + x^e + c$ can be taken as

$$C = \log 2 + h(c). \tag{4.23}$$

We would like to point out that (1.3) is satisfied for $d > e+1 \geq 3$. For the case $d = e+1$, recall that (1.3) was only needed to show that $|f^n(c)| \geq 1$ for all $n \in \mathbb{N}$, which can easily established using the relation $|f(x)| \geq |x|^{d-2}$, for all $|x| \geq |c| > 2$. So, for $d \geq 3$ and $|c| > 2$, if $n \in \mathcal{Z}(f, 0)$, then from (1.4), we infer that

$$\begin{aligned} n &\leq \frac{2}{\log d} \log \left(\frac{dC}{(d-1)\hat{h}_f(c)} \right) + 2 \leq \frac{2}{\log d} \log \left(\frac{3d(\log 2 + h(c))}{h(c)} \right) + 2 \\ &\leq \frac{2}{\log d} \log \left(3d \left(\frac{\log 2}{\log 5} + 1 \right) \right) + 2 < 7, \end{aligned}$$

where the last inequality follows from the fact that $h(c) \geq \log 5$ which is clearly true as $|c| > 2$ and $c \in \mathbb{Q} \backslash \mathbb{Z}$. This completes the proof of Theorem 11. □

4.4 Few cases when $|c| < 2$

In this section, we establish the upper bound on Zsigmondy set of the sequence $(f^n(0))_{n \geq 1}$ where $f(x) = x^d + x^e + c \in \mathbb{Q}[x]$ with $|c| < 2$. In this, we are only able to establish the upper bound on $\mathcal{Z}(f, 0)$ under certain cases, that is,

(a) $c \in (0, 2)$,

(b) $c \in (-1, 0)$ and d is odd,

(c) $c \in (-2, -1)$ and either d is odd or e is even.

The case (a) is proved in Propositions 4.4.1 and 4.4.2, the case (b) and (c) are proved in Propositions 4.4.3 and 4.4.4, respectively. For the remaining cases, one can use the ideas of Ren [87] to bound the cardinality of $\mathcal{Z}(f, 0)$.

Proposition 4.4.1. *Let $f(x) = x^d + x^e + c \in \mathbb{Q}[x]$ be a polynomial of degree $d \geq 3$ with $c \in \mathbb{Q}$ and $1 < c < 2$. Then $n \leq 7$, whenever $n \in \mathcal{Z}(f, 0)$.*

Proof. We will proceed as in the proof of Theorem 11. In this case, we have $s \leq 2c$. Hence, for any integer $i \geq 0$, $x \in \mathbb{Q}$ and $1 < c < 2$, we have

$$\begin{aligned}\hat{h}_f(x) &\geq d^{-i}\left[h(f^i(x)) - \frac{1}{d-1}\log|b^d| + \frac{1}{d-1}\log\left(\frac{1}{s^d}\right)\right] \\ &\geq d^{-i}\left[h(f^i(x)) - \frac{d}{d-1}\log(2a)\right].\end{aligned}$$

Thus,

$$\hat{h}_f(x) \geq d^{-i}\left[h(f^i(x)) - \frac{d}{d-1}h(2c)\right]. \tag{4.24}$$

For $1 < c < 2$, we get

$$f(c) = c^d + c^e + c = c(c^{d-1} + c^{e-1} + 1) > 2c > 2$$

and this implies

$$h(f^2(c)) \geq dh(f(c)) \geq dh(2c). \tag{4.25}$$

Multiplying $(d-1)$ on both sides of (4.25) and then simplifying, we get

$$(d-1)h(f^2(c)) - dh(2c) \geq (d(d-1) - d)h(2c) \geq d(d-2)h(2c). \tag{4.26}$$

Then from (4.24) and (4.26), we deduce that

$$(d-1)\hat{h}_f(c) \geq d^{-1}(d-2)h(2c).$$

Note that $f^n(c) > 1$ as $c > 1$. Also, the constant C in Theorem 10 for $f(x) = x^d + x^e + c$ can be taken as $C = \log 2 + h(c)$. If $n \in \mathcal{Z}(f, 0)$, then from (1.4), we have

$$\begin{aligned} n &\leq \frac{2}{\log d} \log \left(\frac{dC}{(d-1)\hat{h}_f(c)} \right) + 2 \\ &\leq \frac{2}{\log d} \log \left(\frac{d^2(\log 2 + h(c))}{(d-2)h(2c)} \right) + 2 \\ &\leq \frac{2}{\log d} \log \left(\frac{2d^2}{d-2} \right) + 2 \leq 2\frac{\log 6d}{\log d} + 2 < 8. \end{aligned}$$

This completes the proof. □

Proposition 4.4.2. *Let $f(x) = x^d + x^e + c \in \mathbb{Q}[x]$ be a polynomial of degree $d > e \geq 2$ with $c \in \mathbb{Q}$ and $0 < c < 1$. Then $\mathcal{Z}(f, 0) = \emptyset$.*

Proof. Observe that for any $x > 0$, $f(x) \geq x$. Using this observation and induction on n, we can conclude that $|f^n(c)| \geq c$ for all $n \geq 1$ since $c > 0$. Also,

$$|f(c)| = c^d + c^e + c \leq c(c^2 + c + 1) = \alpha c$$

where $\alpha = c^2 + c + 1$. Clearly $1 < \alpha < 3$. A simple induction will imply that

$$|f^n(c)| \leq \alpha^{\frac{d^n - 1}{d-1}} c.$$

Hence, for $0 < c < 1$, we obtain that

$$c \leq |f^n(0)| \leq \alpha^{\frac{d^{n-1} - 1}{d-1}} c. \tag{4.27}$$

From (4.2), we have $f^n(0) = \frac{A_n}{B_n}$ with $B_n = b^{d^{n-1}}$. If $n \in \mathcal{Z}(f, 0)$, then from Corollary 4.1.3, we obtain

$$\log |f^n(0)| + d^{n-1} \log b \leq \sum_{q|n} \left(\log |f^{\frac{n}{q}}(0)| + d^{\frac{n}{q} - 1} \log b \right)$$

where the summation on the right-hand side extends over all unique prime numbers q that are divisors of n. Multiplying d and using (4.27), we have

$$d \log c + d^n \log b \leq \sum_{q|n} \left[\frac{d^{\frac{n}{q}} - d}{d-1} \log \alpha + d \log c + d^{\frac{n}{q}} \log b \right],$$

rearranging above inequality, we get

$$d(1 - \omega(n)) \log c + [d^n - s_d(n)] \log b \leq \frac{\log \alpha}{d-1} [s_d(n) - d\omega(n)],$$

where $s_d(n) := \sum_{q|n} d^{\frac{n}{q}}$. Since $d(1-\omega(n))\log c$ is always non-negative, we have

$$[d^n - s_d(n)]\log b \leq \frac{\log \alpha}{d-1}[s_d(n) - d\omega(n)] \leq \frac{\log \alpha}{d-1} s_d(n).$$

As $\alpha < 3 < b^2$, we get

$$d^n - s_d(n) \leq \frac{2}{d-1} s_d(n)$$

and hence using $s_d(n) \leq d^{n/2}\omega(n)$ and (4.13), we get

$$d^n \leq \frac{d+1}{d-1} s_d(n) \leq 2d^{n/2}\omega(n) < d^n,$$

for any $d \geq 3$ and $n \geq 2$. This is a contradiction. □

Proposition 4.4.3. *Let $f(x) = x^d + x^e + c \in \mathbb{Q}[x]$ be a polynomial of odd degree $d > e \geq 2$ with $c \in \mathbb{Q}$. Suppose $-1 < c < 0$, then $\mathcal{Z}(f, 0) = \emptyset$.*

Proof. Case I: (e is odd). In this case, we have the following inequality

$$|c| \leq |f^n(0)| \leq |\alpha|^{\frac{d^{n-1}-1}{d-1}}|c|,$$

where $\alpha = c^2 + |c| + 1$. If $n \in \mathcal{Z}(f, 0)$. Proceeding as in the proof of Proposition 4.4.2, we get a contradiction.

Case II: (e is even). Since $-1 < c < 0$, d is odd and e is even, we have $c^d + c^e$ is positive and has absolute value less than $|c|$. So, we conclude that $|f(c)| = |c^d + c^e + c| \leq |c|$ and $f(c) < 0$. Suppose that $|f^n(c)| \leq |c| < 1$ and $f^n(c) < 0$. Then

$$|f^{n+1}(c)| = |f(f^n(c))| = |(f^n(c))^d + (f^n(c))^e + c| \leq |c|.$$

As $-1 < c < f^n(0) < 0$, clearly we have $f^{n+1}(c) < 0$. Thus induction hypothesis yields

$$-1 < c \leq f^n(c) < 0, \quad \text{for all } n \in \mathbb{N}.$$

Note that $d - e$ is odd. Thus, from above equation, we get

$$|1 + (f^n(c))^{d-e}| < 1 \ \text{ and } \ |f^n(c)| \leq |c| \ \text{ for all } n \geq 0.$$

Now for $n \geq 1$, we have

$$\begin{aligned} |f^n(c)| &\geq |c| - |f^{n-1}(c)|^e |1 + (f^{n-1}(c))^{d-e}| \\ &> |c| - |c|^e \geq |c|(1 - |c|^{e-1}). \end{aligned}$$

Thus,

$$|c|(1-|c|^{e-1}) \le |f^n(c)| \le |c|.$$

For $-1 < c = \frac{a}{b} < 0$, note that $|c|^{e-1} \le |c| = \frac{|a|}{b}$. So,

$$(1-|c|^{e-1}) \ge \frac{b-|a|}{b} \ge b^{-1}.$$

If $n \in \mathcal{Z}(f,0)$, then from Corollary 4.1.3, we obtain

$$\log(|c|(1-|c|^{e-1})) + d^{n-1}\log b \le \omega(n)\log|c| + \log b \sum_{q|n} d^{\frac{n}{q}-1}.$$

Upon multiplying both sides by d and subsequently rearranging the terms, we obtain

$$\begin{aligned}[d^n - s_d(n)]\log b &\le d(\omega(n)-1)\log|c| - d\log((1-|c|^{e-1})) \\ &\le -d\log((1-|c|^{e-1})) \le d\log b.\end{aligned}$$

By using $s_d(n) \le d^{n/2}\omega(n)$ and (4.13), we obtain

$$d^n \le s_d(n) + d \le d^{n/2}\omega(n) + d \le d^{n/2}(\omega(n)+1) < d^n$$

for $d \ge 3$ and $n \ge 2$. This is a contradiction. □

Proposition 4.4.4. *Let $f(x) = x^d + x^e + c \in \mathbb{Q}[x]$ be a polynomial of degree $d > e \ge 2$ with $c \in \mathbb{Q}$. Suppose $-2 < c < -1$ and d is odd or e is even. Then $\mathcal{Z}(f,0) = \emptyset$.*

Proof. Using simple inductive arguments, we obtain the upper bound

$$|f^n(c)| \le 3^{\frac{d^n-1}{d-1}}|c|^{d^n} \text{ for all } n \in \mathbb{N}.$$

Now we consider different cases to get a lower bound for $|f^(c)|$.
Case I: (d is odd). As $c < -1$ and d is odd, from

$$f(c) = c^d + c^e + c = -|c|(|c|^{d-1} \pm |c|^{e-1} + 1),$$

we observe that $f(c)$ is negative and $|f(c)| \ge |c| > 1$. Inductively using $f^{n-1}(c) < 0$ and $|f^{n-1}(c)| \ge |c| > 1$, we obtain from

$$f^n(c) = (f^{n-1}(c))^d + (f^{n-1}(c))^e + c < c < 0,$$

that $f^n(c)$ is negative and $|f^n(c)| \ge |c| > 1$ for all $n \in \mathbb{N}$.

Thus, we may assume that d is even, then e is also even.

Case II: (d and e are even). Since $c < -1$ and both d, e are even, from $f(c) = c^d + c^e + c \geq c^d = |c|^d > 1$ we observe that $f(c)$ is positive and $|f(c)| \geq |c|^d$. Inductively using $f^{n-1}(c) > 0$ and $|f^{n-1}(c)| \geq |c|^{d^{n-1}} > 1$, we obtain from

$$f^n(c) = (f^{n-1}(c))^d + (f^{n-1}(c))^e + c > f^{n-1}(c)^d > |c|^{d^n},$$

i.e., $f^n(c)$ is positive and $|f^n(c)| \geq |c|^{d^n}$ for all $n \in \mathbb{N}$.

If $n \in \mathcal{Z}(f, 0)$, then proceeding as in Proposition 4.4.2, we get a contradiction for $d \geq 3$ and $n \geq 5$. For $n \leq 4$, simple manual check also contradicts the inequality arising from the Corollary 4.1.3. □

4.5 Concluding Remark

Let $f(x) = x^d + x^e + c \in \mathbb{Q}[x]$ be the polynomial of even degree d. If $c \in (-1, 0)$ or $c \in (-2, -1)$ and e is odd, then obtaining a non-trivial lower bound of $|f^n(c)|$ seems to be difficult. Hence, as a consequence, it is not easy to provide an explicit upper bound of $\mathcal{Z}(f, 0)$ in such cases.

Chapter 5

Monogenity

Consider an algebraic number field $K = \mathbb{Q}(\theta)$, where θ is a root of the irreducible polynomial $f(x) = x^{n-km}(x^k+a)^m+b$, which belongs to the ring of polynomials with integer coefficients $\mathbb{Z}[x]$. We are given that $1 \leq km < n$, and $\mathbb{Z}_K$ denotes the ring of algebraic integers of the field K. In this chapter, we explicitly compute the discriminant of $f(x)$. Furthermore, we establish a set of necessary and sufficient conditions, expressed solely in terms of the parameters a, b, m, k, and n, for $f(x)$ to be monogenic. Additionally, we provide a characterization of all prime numbers that divide the index of the subgroup $\mathbb{Z}[\theta]$ within the ring of integers $\mathbb{Z}_K$. As a specific application of our result, we also present a class of monogenic polynomials that possess a discriminant which is not square-free and whose Galois group is isomorphic to S_n, the symmetric group acting on n elements. Furthermore, using analytic techniques, we produce asymptotics for number of such monogenic polynomials with $b \leq X$. All the proofs and results in this chapter are taken from [57] and [59].

5.1 Preliminaries

For a prime p and a polynomial $h(x) \in \mathbb{Z}[x]$, the notation $\bar{h}(x)$ will be used to represent the polynomial resulting from the reduction of each coefficient of $h(x)$ modulo p.

The subsequent straightforward lemmas will be referenced in the following sections. Their proofs are omitted.

Lemma 5.1.1. *[55, Lemma 2.1] Let p be a prime number and b, b' be integers. Suppose that m, n, m_1, n_1 are positive integers with $\gcd(m, n) = t$, $n_1 = \frac{n}{t}$ and $m_1 = \frac{m}{t}$. Then the polynomials $x^m - \bar{b}'$ and $x^n - \bar{b}$ have a common root in the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$ iff $b^{m_1} \equiv (b')^{n_1} \pmod{p}$.*

Lemma 5.1.2. *[54, Corollary 2.3] Consider a prime number p and let $v_p(n) = j \geq 1$, so we can write $n = p^j s'$, where p does not divide s'. Let c be an integer not divisible by p. Suppose that the factorization of $x^{s'} - \bar{c}$ into a product of distinct monic irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ is given by $\bar{g}_1(x) \cdots \bar{g}_r(x)$, where each $g_i(x) \in \mathbb{Z}[x]$ is a monic polynomial. Then, we can express $x^n - c$ as:*

$$x^n - c = (g_1(x) \cdots g_r(x) + pH_1(x))^{p^j} + pg_1(x) \cdots g_r(x)H_2(x) + p^2 H_3(x) + c^{p^j} - c$$

where $H_1(x), H_2(x), H_3(x)$ are polynomials with integer coefficients.

Following results on Discriminant and Norm will be used in the proof of Theorem 12.

Lemma 5.1.3. *[69, Lemma 2.6] Consider a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n. Let $f(\theta) = 0$ and $K = \mathbb{Q}(\theta)$. Then*

$$D_f = (-1)^{n(n-1)/2} \mathcal{N}_{K/\mathbb{Q}}(f'(\theta)).$$

Lemma 5.1.4. *[69, Theorem 1.20] Let K/F be an extension of degree n and α be an element of K with $[F(\alpha) : F] = d$. Then*

$$\mathcal{N}_{K/F}(\alpha) = \left(\mathcal{N}_{F(\alpha)/F}(\alpha)\right)^{n/d}.$$

Now we state the result known as Dedekind criterion. The equivalence of assertions (i) and (ii) of this lemma was proved by Dedekind (cf. [18, Theorem 6.1.4], [24]). A straightforward demonstration of the equivalence between conditions (ii) and (iii) can be found in [54, Lemma 2.1].

Lemma 5.1.5. *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial. Consider its factorization modulo a prime p as $\bar{g}_1(x)^{e_1} \cdots \bar{g}_r(x)^{e_r}$, where this is a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, and $g_i(x) \in \mathbb{Z}[x]$ are monic polynomials. Let $K = \mathbb{Q}(\theta)$, where θ is a root of $f(x)$. Then the following conditions are equivalent:*

- *(i) The prime p does not divide the index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$.*
- *(ii) For every i in the range $1 \leq i \leq r$, either $e_i = 1$ or the polynomial $\bar{g}_i(x)$ does not divide $\overline{M}(x)$, where $M(x)$ is defined as $M(x) = \frac{1}{p}(f(x) - g_1(x)^{e_1} \cdots g_r(x)^{e_r})$.*
- *(iii) The polynomial $f(x)$ is not an element of the ideal $\langle p, g_i(x)\rangle^2$ in $\mathbb{Z}[x]$ for any i such that $1 \leq i \leq r$.*

Let β be an integer, and let $\rho, \gamma, \alpha, \alpha_0, \beta_0$ be positive integers that satisfy the conditions below:

$$\boxed{\begin{array}{l}\text{(i) } \gcd(\alpha_0\beta_0\rho, \gamma) = 1 \text{ and } \gcd(\alpha, \beta) = 1, \\ \text{(ii) for all prime divisors } p \text{ of } \beta, \text{ we have } p^2 \mid \beta, \\ \text{(iii) } \alpha_0, \beta_0 \text{ be squarefree divisors of } \alpha, \beta \text{ respectively,} \\ \text{(iv) } \alpha\beta_0\rho + \beta \not\equiv 0 \pmod{p^2} \text{ for every } p \mid \gamma.\end{array}} \tag{5.1}$$

Using the above notations, Jones and White [63, Theorem 3.8] proved an asymptotic result for the set defined by

$$U(X) = U(X; \rho, \gamma, \alpha, \alpha_0, \beta, \beta_0) := |\{y \leq X : y \equiv \rho \pmod{\gamma^2}, \gcd(y, \alpha_0\beta_0) = 1, \\ \mu(y) \neq 0, \mu(\alpha\beta_0 y + \beta) \neq 0\}|.$$

Lemma 5.1.6. *[63, Theorem 3.8] Given the restrictions on the variables $\rho, \gamma, \alpha, \alpha_0, \beta$ and β_0 as in (5.1), we have*

$$U(X) = X\left(\frac{\phi(\alpha_0\beta_0)}{\alpha_0\beta_0\gamma^2\zeta(2)}\right)\prod_{p\mid\alpha_0\beta_0\gamma}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p\nmid\alpha\beta\gamma}\left(1-\frac{1}{p^2-1}\right) + O(X^{3/4})$$

where the implied constant is dependent on $\gamma, \alpha, \alpha_0, \beta$ and β_0.

For the proof of Theorem 16, we require a result which ensures that for any given polynomial $F(x)$, there are infinitely many primes p such that $F(p)$ is squarefree. For the statement of this theorem, we need the following definition of local obstruction.

Definition 5.1.7. *Let p be a prime and $F(x)$ be a polynomial with integer coefficients. The polynomial $F(x)$ is said to have a local obstruction at p if for all $z \in (\mathbb{Z}/p^2\mathbb{Z})^*$, $F(z) \equiv 0 \pmod{p^2}$.*

The statement in Theorem 5.1.8 is a special case of a a general result proved in [86, Theorem 1.1]. It is a well known concept among the analytic number theorists. For a thorough explanation and discussion on this theorem, refer [63, Remark 2.6] and the subsequent discussion therein.

Lemma 5.1.8. *[63, Corollary 2.7] Let $F(x) \in \mathbb{Z}[x]$, and assume that $F(x)$ decomposes into a product of distinct irreducible polynomials, where the highest degree of any irreducible factor is d. Further, assume that $F(x)$ does not have a local obstruction at any prime q. If $d \geq 4$, assume that the abc-conjecture for number fields holds for $F(x)$, then there are infinitely many primes p such that $F(p)$ is squarefree.*

5.2 Proof of Theorems 12 and 13

Let n, m and k be positive integers with $n > km$. Let $t = \gcd(n, k)$ and define the integers $k_1 = k/t$ and $n_1 = n/t$. Let $f(x) = x^{n-km}(x^k + a)^m + b$ be the polynomial with integer coeffecients. Suppose $f(x)$ is irreducible and has a root θ. Let $K = \mathbb{Q}(\theta)$ be a number field having ring of integers $\mathbb{Z}_K$. In Theorem 12, we give the formula for the discriminant of the polynomial $f(x)$ explicitly in terms of integers n, m, k, t, a, b, n_1 and k_1.

Proof of Theorem 12: Suppose that $f(x)$ is irreducible with $f(\theta) = 0$. Then, we have

$$\theta^{n-km}(\theta^k + a)^m = -b. \tag{5.2}$$

Since $f'(x) = (n - km)x^{n-km-1}(x^k + a)^m + mkx^{k-1}x^{n-km}(x^k + a)^{m-1}$, it follows that

$$\begin{aligned} f'(\theta) &= (n - km)\theta^{n-km-1}(\theta^k + a)^m + mk\theta^{k-1}\theta^{n-km}(\theta^k + a)^{m-1} \\ &= \theta^{n-km-1}(\theta^k + a)^{m-1}\left(n\theta^k + a(n - km)\right). \end{aligned}$$

Observe that θ and $\theta^k + a$ are non-zero, otherwise in view of (5.2) we have $b = 0$; which is impossible as $f(x)$ is irreducible. So we have

$$\theta(\theta^k + a)f'(\theta) = \theta^{n-km}(\theta^k + a)^m\left(n\theta^k + a(n - km)\right). \tag{5.3}$$

From (5.2) and (5.3), we have

$$\theta(\theta^k + a)f'(\theta) = -b\left(n\theta^k + a(n - km)\right). \tag{5.4}$$

We simply write $\mathcal{N}$ for the norm $\mathcal{N}_{K/\mathbb{Q}}$, where $K = \mathbb{Q}(\theta)$. Since $\mathcal{N}(\theta) = (-1)^n b$, taking norm on both sides of (5.4) we have

$$\mathcal{N}(\theta)\mathcal{N}(\theta^k + a)\mathcal{N}(f'(\theta)) = (-b)^n\mathcal{N}\left(n\theta^k + a(n - km)\right). \tag{5.5}$$

Now we first calculate $\mathcal{N}(n\theta^k + a(n - km))$. Let $n\theta^k + a(n - km) = z$. We can write $\theta^k = \frac{z-a(n-km)}{n}$. Taking power k_1 on both sides in (5.2) and using $n = kd + r$, we obtain

$$(\theta^{kd+r})^{k_1}(\theta^k)^{-k_1 m}(\theta^k + a)^{k_1 m} = (-b)^{k_1}.$$

Since $k = k_1 t$ and $r = r_1 t$, we have $rk_1 = r_1 k$. So the above equation can be rewritten as

$$\begin{aligned}(\theta^k)^{k_1 d}(\theta^k)^{r_1}(\theta^k)^{-k_1 m}(\theta^k + a)^{k_1 m} &= (-b)^{k_1},\\ \text{i.e., } (\theta^k)^{(k_1 d + r_1 - k_1 m)}(\theta^k + a)^{k_1 m} &= (-b)^{k_1}. \end{aligned} \tag{5.6}$$

Substituting $\theta^k = \frac{z - a(n-km)}{n}$ and $k_1 d + r_1 = n_1$ in above equation, we obtain

$$\left(\frac{z - a(n-km)}{n}\right)^{n_1 - k_1 m}\left(\frac{z - a(n-km)}{n} + a\right)^{k_1 m} = (-b)^{k_1}.$$

Hence, we conclude that z satisfies the polynomial

$$h_1(x) = (x - a(n-km))^{n_1 - k_1 m}(x + akm)^{k_1 m} - (-b)^{k_1} n^{n_1}.$$

Now, we will prove that $h_1(x)$ is the minimal polynomial for z. It is easy to verify that $\mathbb{Q}(z) = \mathbb{Q}(\theta^k)$. Therefore, in order to establish that the minimal polynomial of z over $\mathbb{Q}$ has degree n_1, it is enough to show that $[\mathbb{Q}(\theta^k) : \mathbb{Q}] = n_1$. To prove this, it is enough to show that (i) $\mathbb{Q}(\theta^k) = \mathbb{Q}(\theta^t)$ and (ii) $[\mathbb{Q}(\theta^t) : \mathbb{Q}] = n_1$ holds.
We first show that $\mathbb{Q}(\theta^k) = \mathbb{Q}(\theta^t)$. Since $k = k_1 t$, we have $\theta^k = (\theta^t)^{k_1} \in \mathbb{Q}(\theta^t)$; this implies that $\mathbb{Q}(\theta^k) \subset \mathbb{Q}(\theta^t)$. Now we show that $\mathbb{Q}(\theta^t) \subset \mathbb{Q}(\theta^k)$. Using (5.2) we can easily deduce that $\theta^n \in \mathbb{Q}(\theta^k)$. Since $\gcd(n, k) = t$, there exists $u_1, u_2 \in \mathbb{Z}$ such that $nu_1 + ku_2 = t$. Now we have $\theta^t = (\theta^n)^{u_1}(\theta^k)^{u_2} \in \mathbb{Q}(\theta^k)$ which implies that $\mathbb{Q}(\theta^t) \subset \mathbb{Q}(\theta^k)$. This proves (i). Now define a polynomial $g(x) = x^{n_1 - k_1 m}(x^{k_1} + a)^m + b \in \mathbb{Z}[x]$. We will prove that $g(x)$ is minimal polynomial for θ^t, i.e., $g(x)$ is irreducible and $g(\theta^t) = 0$.

$$g(\theta^t) = (\theta^t)^{n_1 - k_1 m}((\theta^t)^{k_1} + a)^m + b = f(\theta) = 0.$$

Now suppose $g(x)$ is reducible say $g(x) = g_1(x)g_2(x) \in \mathbb{Z}[x]$ with $\deg(g_1), \deg(g_2) \geq 1$. Clearly $g(x^t) = f(x)$. Using this, we obtain $f(x) = g(x^t) = g_1(x^t)g_2(x^t)$. This contradicts the irreducibility of $f(x)$. Hence, $g(x)$ is irreducible. This proves (ii). Combining (i) and (ii), we conclude that the minimal polynomial of z over $\mathbb{Q}$ has degree n_1. As $h_1(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree n_1 satisfying $h_1(z) = 0$, we conclude that $h_1(x)$ is the minimal polynomial of z over $\mathbb{Q}$. Thus,

$$\mathcal{N}_{\mathbb{Q}(z)/\mathbb{Q}}(z) = (-1)^{n_1} h_1(0).$$

Using Lemma 5.1.4, we have

$$\mathcal{N}(n\theta^k + a(n-km)) = \mathcal{N}_{K/\mathbb{Q}}(n\theta^k + a(n-km)) = ((-1)^{n_1}\ h_1(0))^t.$$

Substituting value of $h_1(0)$ in above equation, we obtain

$$\mathcal{N}(n\theta^k+a(n-km)) = (-1)^n \left[(-1)^{n_1-k_1m}(n-km)^{n_1-k_1m}a^{n_1}(km)^{k_1m} + (-1)^{k_1+1}b^{k_1}n^{n_1}\right]^t. \tag{5.7}$$

Similarly, if we let $z = \theta^k + a$. Then using Equation (5.6), we obtain

$$(\theta^k)^{n_1-k_1m}(\theta^k+a)^{k_1m} = (-b)^{k_1},$$
$$\text{i.e., } (z-a)^{n_1-k_1m}(z)^{k_1m} = (-b)^{k_1}.$$

Hence, using similar argument as above the minimal polynomial for z in this case is

$$h_2(x) = (x-a)^{n_1-k_1m}x^{k_1m} - (-b)^{k_1}.$$

Using Lemma 5.1.4, we have

$$\mathcal{N}(\theta^k+a) = \mathcal{N}_{K/\mathbb{Q}}(\theta^k+a) = ((-1)^{n_1}\ h_2(0))^t.$$

Substituting value of $h_2(0)$ in above equation, we obtain

$$\mathcal{N}(\theta^k+a) = (-1)^{n+k+t}\ b^k. \tag{5.8}$$

Therefore, keeping in mind that $b \neq 0$, the theorem follows from Lemma 5.1.3 and Equations (5.5), (5.7) and (5.8). □

In Theorem 13, we use th discriminant formula of $f(x)$ obtained in Theorem 12 to characterize the primes dividing the index of the ring $\mathbb{Z}[\theta]$ in $\mathbb{Z}_K$. We give the necessary and sufficient condition for primes dividing a, b, m, n, k to divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$.

Proof of Theorem 13: Consider a prime divisor p of the discriminant D_f. Based on Lemma 5.1.5, p will not be a divisor of the index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ iff, for every monic polynomial $g(x) \in \mathbb{Z}[x]$ that remains irreducible modulo p and satisfies the condition that its reduction modulo p, denoted as $\bar{g}(x)$, divides the reduction of $f(x)$ modulo p, it holds that $f(x) \notin \langle p, g(x)\rangle^2$. It is worth noting that the condition $f(x) \notin \langle p, g(x)\rangle^2$ holds iff the polynomial $\bar{g}(x)$ is not a repeated factor in the factorization of $\bar{f}(x)$.

Case (i). In the scenario where p divides b and also p divides a, we have the congruence $f(x) \equiv x^n \pmod p$. It is evident that $f(x) \in \langle p, x\rangle^2$ holds precisely when p^2 divides b. As a result, p does not divide the index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ iff p^2 does not divide b. Now assume that $p|b$, $p \nmid a$ and $m \geq 2$, then $f(x) \equiv x^{n-km}(x^k+a)^m \pmod p$. Consider the factorization of $x^k + a$ modulo p over $\mathbb{Z}/p\mathbb{Z}$, expressed as $x^k + a \equiv \prod_{i=1}^{r} g_i(x)^{e_i} \pmod p$. In this representation, e_i's are positive integers, each $g_i(x) \in \mathbb{Z}[x]$ denotes a monic polynomial

that is irreducible modulo p, and these polynomials are distinct. Given $m \geq 2$, the condition $f(x) \in \langle p, g_i(x)\rangle^2$ holds for every i in the range $1 \leq i \leq r$ iff p^2 is a divisor of b. Moreover, in the scenario where $n - km \geq 2$, the condition $f(x) \in \langle p, x\rangle^2$ is equivalent to p^2 dividing b. As a consequence, p does not divide the index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ iff p^2 is not a divisor of b. This establishes the proof of the theorem for Case (i).

Case (ii). When $p \mid b$, $m = 1$ and $p \nmid a$. Let $k = p^j s$ with $p \nmid s$. In the case where $j = 0$, the polynomial $x^k + a$ exhibits separability over the field $\mathbb{Z}/p\mathbb{Z}$. Considering the condition that p divides b, and referring to equation (1.6), it can be deduced that $n - k \geq 2$. In this situation $f(x)$ lies in the ideal $\in \langle p, x\rangle^2$ iff p^2 is a divisor of b; consequently $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ iff $p^2 \nmid b$.

Now assume that $j \geq 1$. Applying Binomial theorem, we deduec that

$$f(x) \equiv x^{n-k}(x^s + a)^{p^j} \pmod{p}.$$

If $n - k \geq 2$, then clearly $f(x) \in \langle p, x\rangle^2$ iff $p^2 \mid b$. If $n - k = 1$, then x is simple factor of $\bar{f}(x)$. As $p \nmid s$, the polynomial $x^s + a$ is separable. Suppose $\bar{g}_1(x) \cdots \bar{g}_r(x)$ is the decomposition of $x^s + \bar{a}$ in $\mathbb{Z}/p\mathbb{Z}$, where $g_i(x)$ are monic polynomials with integer coefficients that are not reducible modulo p, obviously g_i's must be distinct modulo p. We can express $x^s + a$ in the form $g_1(x) \cdots g_r(x) + pH(x)$, where $H(x)$ is some polynomial in $\mathbb{Z}[x]$. By applying Lemma 5.1.2 to the polynomial $h(x) = x^s + a$ and observing that $f(x) = x^{n-k}(h(x^{p^j})) + b$ with the condition that p divides b, we deduce that

$$\begin{aligned} f(x) &= x^{n-k}\left(\left(\prod_{i=1}^{r} g_i(x) + pH(x)\right)^{p^j} + p\prod_{i=1}^{r} g_i(x)T(x) + p^2U(x) + a + (-a)^{p^j}\right) + b \\ &= x^{n-k}\left(\prod_{i=1}^{r} g_i(x)\right)^{p^j} + px\prod_{i=1}^{r} g_i(x)M_1(x) + p^2M_2(x) + x^{n-k}(a + (-a)^{p^j}) + b, \end{aligned}$$

where $T(x), U(x), M_1(x), M_2(x)$ are some polynomials with integer coefficients. Using $j \geq 1$, we see that the first three terms on the RHS of the above equation are elements of $\langle p, g_i(x)\rangle^2$ for each i, where $1 \leq i \leq r$. Therefore, $f(x)$ belongs to the square of the ideal $\langle p, g_i(x)\rangle$ for some i in the above range, iff $x^{n-k}(a + (-a)^{p^j}) + b = p(a_1x^{n-k} + b_1)$ does so. Evidently, the term $p(a_1x^{n-k} + b_1)$ is an element of the ideal $\langle p, g_i(x)\rangle^2$ for some index i iff one of the following conditions is met: either p is a divisor of both a_1 and b_1, or p does not divide a_1 and the polynomials $\bar{a}_1x^{n-k} + \bar{b}_1$ and $x^k + \bar{a}$ share a common root. By Lemma 5.1.1, the polynomials $\bar{a}_1x^{n-k} + \bar{b}_1$ and $x^k + \bar{a}$ have no common root iff $p \nmid a_1[(-a)^{n_1-k_1}a_1^{k_1} - (-b_1)^{k_1}]$. By Lemma 5.1.5, $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ iff either $p \mid a_1$ and $p \nmid b_1$ or $p \nmid b_1^{n-k-1}a_1[(-a)^{n_1-k_1}a_1^{k_1} - (-b_1)^{k_1}]$.

Case (iii). In the case where p does not divide b but p does divide a, and given that p divides the discriminant D_f, it follows directly from equation (1.6) that p must divide n. We can express n as $n = p^j s'$, where p does not divide s'. Applying the Binomial Theorem, we obtain

$$f(x) \equiv x^n + b \equiv (x^{s'} + b)^{p^j} \pmod{p}.$$

As $p \nmid s'$, the polynomial $x^{s'} + b$ is separable over $\mathbb{Z}/p\mathbb{Z}$. Consider the factorization of $x^{s'} + \bar{b}$ modulo p over $\mathbb{Z}/p\mathbb{Z}$ as $\bar{g}_1(x) \cdots \bar{g}_r(x)$, where each $g_i(x) \in \mathbb{Z}[x]$ is a monic polynomial that is distinct and irreducible modulo p. We can express $x^{s'} + b$ in the form $g_1(x) \cdots g_r(x) + pH(x)$ for some polynomial $H(x) \in \mathbb{Z}[x]$. Applying Lemma 5.1.2 to the polynomial $h(x) = x^{s'} + b$, and observing that $f(x) = h(x^{p^j}) + amx^{n-k} + \cdots + ma^{m-1}x^{n+k-km} + a^m x^{n-km}$ with the condition that p divides a, we can deduce that

$$f(x) = \left(\prod_{i=1}^{r} g_i(x) + pH(x)\right)^{p^j} + pT(x)\prod_{i=1}^{r} g_i(x) + p^2U(x) + b + (-b)^{p^j} + max^{n-k}, \quad (5.9)$$

where $T(x), U(x)$ are some polynomials with integer coefficients. Since $j \geq 1$, the initial three terms on the right-hand side of equation (5.9) are elements of $\langle p, g_i(x)\rangle^2$ for every i in the range $1 \leq i \leq r$. Consequently, $f(x) \in \langle p, g_i(x)\rangle^2$ for some i, where $1 \leq i \leq r$, iff $amx^{n-k} + b + (-b)^{p^j} = p(a_2x^{n-k} + b_2)$ does so. Hence, $p(a_2x^{n-k} + b_2)$ lies in the square of the ideal $\langle p, g_i(x)\rangle$ for some i iff either p divides both a_2, b_2 or $p \nmid a_2$ and the polynomials $\bar{a}_2x^{n-k} + \bar{b}_2$, $x^n + \bar{b}$ have a common root. Using Lemma 5.1.1, the polynomials $\bar{a}_2x^{n-k} + \bar{b}_2$ and $x^n + \bar{b}$ have no common root modulo p iff $p \nmid a_2\left[(a_2b)^{n_1} - (-b)^{k_1}b_2^{n_1}\right]$. By Lemma 5.1.5, $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ iff either $p \mid a_2$ and $p \nmid b_2$ or $p \nmid a_2\left[a_2^{n_1}b^{n_1-k_1} - (-1)^{k_1}b_2^{n_1}\right]$. This completes the proof of the theorem for Case (iii).

Case (iv). When $p \nmid ab$ and $p \mid k$. Using $p \mid D_f$, we obtain $p \mid n$. Let $n = p^j s'$ and $k = p^j s$ with $p \nmid \gcd(s, s')$. Using Binomial theorem, we obtain

$$f(x) \equiv (x^{s'-sm}(x^s + a)^m + b)^{p^j} \pmod{p}.$$

Denote $h(x) = x^{s'-sm}(x^s + a)^m + b = x^{s'} + \sum_{i=1}^{m}\binom{m}{i}x^{s'-si}a^i + b$, then keeping in mind that $f(x) = h(x^{p^j})$ we see that

$$\left(h(x) - \sum_{i=1}^{m}\binom{m}{i}x^{s'-si}a^i - b\right)^{p^j} = x^n = h(x^{p^j}) - \left(\sum_{i=1}^{m}\binom{m}{i}x^{n-ki}a^i + b\right).$$

Using Binomial theorem to the left hand side of the above equation, we obtain

$$\begin{aligned}
&h(x)^{p^j} + ph(x)H'(x) + (-1)^{p^j}\left(\sum_{i=1}^{m}\binom{m}{i}x^{s'-si}a^i + b\right)^{p^j} \\
&= h(x^{p^j}) - \left(\sum_{i=1}^{m}\binom{m}{i}x^{p^j(s'-si)}a^i + b\right) \\
&= f(x) - \left(\sum_{i=1}^{m}\binom{m}{i}x^{p^j(s'-si)}a^i + b\right)
\end{aligned}$$

for some polynomials $H'(x) \in \mathbb{Z}[x]$. Let $\prod_{i=1}^{r}\bar{g}_i(x)^{e_i}$ be the factorization of $h(x)$ over $\mathbb{Z}/p\mathbb{Z}$, where $g_i(x)$ are monic polynomials with integer coefficients that are not reducible modulo p. Further, e_i's are positive and g_i's are distinct.Let $h(x) = \prod_{i=1}^{r} g_i(x)^{e_i} + pH(x)$ for some polynomial $H(x) \in \mathbb{Z}[x]$, then we obtain

$$\begin{aligned}
f(x) = &\left(\prod_{i=1}^{r} g_i(x)^{e_i}\right)^{p^j} + p\prod_{i=1}^{r} g_i(x)^{e_i}H_2(x) + p^2H_3(x) \\
&+ (-1)^{p^j}\left(\sum_{i=1}^{m}\binom{m}{i}x^{s'-si}a^i + b\right)^{p^j} + \sum_{i=1}^{m}\binom{m}{i}x^{p^j(s'-si)}a^i + b \qquad (5.10)
\end{aligned}$$

Write $f(x) = \left(\prod_{i=1}^{r} g_i(x)^{e_i}\right)^{p^j} + pM(x)$ for some $M(x) \in \mathbb{Z}[x]$. In view of Lemma 5.1.5, $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ iff $\overline{M}(x)$ is co-prime to $\bar{h}(x)$, which by virtue of (5.10) holds iff $\frac{1}{p}\left[(-1)^{p^j}\left(\sum_{i=1}^{m}\binom{m}{i}x^{s'-si}a^i + b\right)^{p^j} + \sum_{i=1}^{m}\binom{m}{i}x^{p^j(s'-si)}a^i + b\right]$ is co-prime to $h(x)$ modulo p.

Case (v). When $p \nmid abk$ and $p \mid m$. It is clear from (1.6) that $p \mid (n - km)$. Write $n - km = p^j s,\ m = p^j s'$ with $p \nmid \gcd(s, s')$. A direct use of Binomial theorem will yield

$$f(x) \equiv (x^s(x^k + a)^{s'} + b)^{p^j} \pmod{p}.$$

As $p \nmid k\gcd(s, s')$, the polynomial $x^s(x^k + a)^{s'} + b$ is separable. Suppose $\bar{g}_1(x)\cdots\bar{g}_r(x)$ is the decomposition of $x^s(x^k + \bar{a})^{s'} + \bar{b}$ in $\mathbb{Z}/p\mathbb{Z}$, where $g_i(x)$ are monic polynomials with integer coefficients that are not reducible modulo p, obviously g_i's must be distinct modulo p. Let $x^s(x^k + a)^{s'} + b = g_1(x)\cdots g_r(x) + pH(x)$, where $H(x) \in \mathbb{Z}[x]$. Denote $x^s(x^k + a)^{s'} + b$ by $h(x)$, then we have

$$(x^s(x^k + a)^{s'})^{p^j} = (h(x) - b)^{p^j}.$$

Applying Binomial theorem to the right-hand side, we obtain

$$x^{n-km}(x^k+a)^m = (h(x))^{p^j} + ph(x)M_1(x) + (-b)^{p^j},$$

for some integer coefficient polynomial $M_1(x)$. Substituting the expression $h(x) = \prod_{i=1}^{r} g_i(x) + pH(x)$, we can deduce that

$$\begin{aligned} f(x) &= (h(x))^{p^j} + ph(x)M_1(x) + (-b)^{p^j} + b \\ &= \left(\prod_{i=1}^{r} g_i(x) + pH(x)\right)^{p^j} + p\left(\prod_{i=1}^{r} g_i(x) + pH(x)\right) M_1(x) + (-b)^{p^j} + b \\ &= \left(\prod_{i=1}^{r} g_i(x)\right)^{p^j} + p\left(\prod_{i=1}^{r} g_i(x)\right) M_2(x) + p^2 M_3(x) + (-b)^{p^j} + b, \end{aligned}$$

for some $M_2(x), M_3(x) \in \mathbb{Z}[x]$. As $j \geq 1$, the initial three terms of the aforementioned expression are contained in $\langle p, g_i(x)\rangle^2$ for each i, where $1 \leq i \leq r$. Thus, $f(x)$ lies in the square of the ideal $\langle p, g_i(x)\rangle$ for some i, with $1 \leq i \leq r$, iff $(-b)^{p^j} + b$ does so. Clearly $(-b)^{p^j} + b$ lies in the square of the ideal $\langle p, g_i(x)\rangle$ for some i in above range iff $p^2 \mid [(-b)^{p^j} + b]$. Lemma 5.1.5$(iii)$ yields that $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ iff $p^2 \nmid [(-b)^{p^j} + b]$. Note that if $p \nmid b$, then it can be easily checked that $v_p(b^{p^j-1} - 1) = v_p(b^{p-1} - 1)$. Hence, for $p \nmid b$ we obtain $p^2 \nmid [(-b)^{p^j} + b]$ iff $p^2 \nmid [(-b)^p + b]$. Similar conclusion holds when $p \mid b$. This completes the proof of the theorem for the current case.

Case (vi). We now turn our attention to the final scenario where the prime p does not divide the product $abkm$. Since $p \mid D_f$, it follows from (1.6) that $p \nmid n(n-km)$. We claim that there exists an integer α such that the polynomial $x^t - \bar{\alpha}$ is the product of all the monic irreducible divisors of $\bar{f}(x)$ over $\mathbb{Z}/p\mathbb{Z}$ that appear with a multiplicity greater than one.

Let's consider any root β of the polynomial $f(x) = x^{n-km}(x^k+a)^m+b$ in the algebraic closure of the field $\mathbb{Z}/p\mathbb{Z}$ that has a multiplicity greater than one (i.e., a repeated root). Note that $\beta \neq \bar{0}$ as $p \nmid b$. Also, we have

$$f(\beta) \equiv \beta^{n-km}(\beta^k + a)^m + b \equiv 0 \pmod{p}, \tag{5.11}$$

$$f'(\beta) \equiv (n-km)\beta^{n-km-1}\ (\beta^k + a)^m + km\beta^{n-km+k-1}(\beta^k + a)^{m-1} \equiv 0 \pmod{p}. \tag{5.12}$$

In view of the above equations, we obtain

$$\beta^{n-km-1}(\beta^k + a)^{m-1}\left(n\beta^k + a(n-km)\right) \equiv 0 \pmod{p}.$$

Observe that $(\beta^k + a) \not\equiv 0 \pmod{p}$, otherwise in view of (5.11) we obtain $p \mid b$, which is not possible. Therefore, keeping in mind that $p \nmid n$, we have

$$\beta^k \equiv \frac{-a(n-km)}{n} \pmod{p}.$$

Clearly $\beta^k \in \mathbb{Z}/p\mathbb{Z}$ and $f(\beta) \equiv 0 \pmod{p}$ implies that $\beta^n \equiv -b(1+a\beta^{-k})^{-m} \in \mathbb{Z}/p\mathbb{Z}$. As $\gcd(n,k) = t$ so there exist $u_1, u_2 \in \mathbb{Z}$ such that $nu_1 + ku_2 = t$. Using this we obtain $\beta^t = (\beta^k)^{u_2}(\beta^n)^{u_1} \in \mathbb{Z}/p\mathbb{Z}$, i.e., $\beta^t \equiv \left(-b(\frac{-km}{n-km})^{-m}\right)^{u_1} \left(\frac{-a(n-km)}{n}\right)^{u_2} \pmod{p}$. Therefore, there exists an integer $\alpha \in \mathbb{Z}/p\mathbb{Z}$, defined as $\alpha \equiv \left(-b(\frac{-km}{n-km})^{-m}\right)^{u_1} \left(\frac{-a(n-km)}{n}\right)^{u_2} \pmod{p^2}$. This establishes that any repeated root of $\bar{f}(x)$ is also a root of $x^t - \bar{\alpha}$. We now proceed to prove that if β_1 is a root of $x^t - \bar{\alpha}$ with $\alpha \equiv \left(-b(\frac{-km}{n-km})^{-m}\right)^{u_1} \left(\frac{-a(n-km)}{n}\right)^{u_2} \pmod{p^2}$, then β_1 is a repeated root of $\bar{f}(x)$. Note that

$$f(\beta_1) \equiv (\beta_1^t)^{n_1 - k_1 m}((\beta_1^t)^{k_1} + a)^m + b \equiv \alpha^{n_1 - k_1 m}(\alpha^{k_1} + a)^m + b \pmod{p}. \tag{5.13}$$

As $p \mid D_f$ and $p \nmid b$, we get $p \mid (U + V)$. This implies

$$(-1)^{n_1 - k_1 m}(n - km)^{n_1 - k_1 m} a^{n_1} (km)^{k_1 m} \equiv -(-1)^{k_1+1} b^{k_1} n^{n_1} \pmod{p}.$$

Since $p \nmid n(n - km)$, the above equation can be rewritten as

$$\left(\frac{-a(n-km)}{n}\right)^{n_1} \equiv \left(-b\left(\frac{-km}{n-km}\right)^{-m}\right)^{k_1} \pmod{p}. \tag{5.14}$$

Let α_1, α_2 be integers such that $\alpha_1 \equiv -b\left(\frac{-km}{n-km}\right)^{-m} \pmod{p^2}$ and $\alpha_2 \equiv \frac{-a(n-km)}{n} \pmod{p^2}$, then by the definition of α we have $\alpha \equiv \alpha_1^{u_1} \cdot \alpha_2^{u_2} \pmod{p^2}$ where $u_1, u_2 \in \mathbb{Z}$ are such that $nu_1 + ku_2 = t$. Also, by (5.14) we see that $\alpha_2^{n_1} \equiv \alpha_1^{k_1} \pmod{p}$. First we show that $f(\beta_1) \equiv 0 \pmod{p}$. In view of (5.13), we have

$$\begin{aligned} f(\beta_1) &\equiv \alpha^{n_1 - k_1 m}(\alpha^{k_1} + a)^m + b \pmod{p} \\ &\equiv (\alpha_1^{u_1} \cdot \alpha_2^{u_2})^{n_1 - k_1 m}\left[(\alpha_1^{u_1} \cdot \alpha_2^{u_2})^{k_1} + a\right]^m + b \pmod{p}. \end{aligned} \tag{5.15}$$

Using $k_1 u_2 + n_1 u_1 = 1$ and $\alpha_2^{n_1} \equiv \alpha_1^{k_1} \pmod{p}$ in (5.15), we obtain

$$f(\beta_1) \equiv \alpha_1 \cdot \alpha_2^{-m}\ (\alpha_2 + a)^m + b \pmod{p}.$$

Substituting values of α_1 and α_2 in the above equation, we obtain

$$\begin{aligned} f(\beta_1) &\equiv -b\left(\frac{-km}{n-km}\right)^{-m}\left(\frac{-a(n-km)}{n}\right)^{-m}\left(\frac{-a(n-km)}{n} + a\right)^m + b \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned} \tag{5.16}$$

Now we show that $f'(\beta_1) \equiv 0 \pmod{p}$. Keeping in mind (5.12) and $\beta_1 \not\equiv 0 \pmod{p}$, we have

$$\begin{aligned} f'(\beta_1) &\equiv (n-km)\beta_1^{n-km-1}(\beta_1^k+a)^m + km\beta_1^{n-km+k-1}(\beta_1^k+a)^{m-1} \pmod{p} \\ &\equiv \beta_1^{n-km-1}(\beta_1^k+a)^{m-1}\left[n\beta_1^k + a(n-km)\right] \pmod{p} \\ &\equiv \beta_1^{-1}\left[\beta_1^{n-km}(\beta_1^k+a)^{m-1}\left(n\beta_1^k + a(n-km)\right)\right] \pmod{p} \\ &\equiv \beta_1^{-1}\left[(\alpha_1^{u_1}\cdot\alpha_2^{u_2})^{n_1-k_1m}((\alpha_1^{u_1}\cdot\alpha_2^{u_2})^{k_1}+a)^{m-1}\left(n(\alpha_1^{u_1}\cdot\alpha_2^{u_2})^{k_1} + a(n-km)\right)\right] \pmod{p}. \end{aligned}$$

Using $k_1u_2 + n_1u_1 = 1$ and $\alpha_2^{n_1} \equiv \alpha_1^{k_1} \pmod{p}$ in the above equation, we obtain

$$f'(\beta_1) \equiv \beta_1^{-1}\left[\alpha_1\alpha_2^{-m}(\alpha_2+a)^{m-1}(n\alpha_2 + a(n-km))\right] \pmod{p}.$$

Substituting values of α_1 and α_2 in the above equation, we obtain

$$\begin{aligned} f'(\beta_1) &\equiv \beta_1^{-1}\left[-b\left(\frac{kma}{n}\right)^{-1}(-a(n-km)+a(n-km))\right] \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned} \tag{5.17}$$

Combining equations (5.16) and (5.17), we deduce that every root of the polynomial $x^t - \bar{\alpha}$ appears as a repeated root of $f(x)$ modulo p. Hence, we have shown that $x^t - \bar{\alpha}$ represents the product of all distinct monic irreducible divisors of $\bar{f}(x)$ in $\mathbb{Z}/p\mathbb{Z}$ that occur with multiplicity greater than one. Since $t = \gcd(n,k)$, it is easy to see that

$$f(x) = (x^t)^{n_1-k_1m}((x^t)^{k_1}+a)^m + b = (x^t-\alpha)q(x) + \alpha^{n_1-k_1m}(\alpha^{k_1}+a)^m + b, \tag{5.18}$$

for some $q(x) \in \mathbb{Z}[x^t]$. As $x^t - \bar{\alpha}$ divides $\bar{f}(x)$, we have $\bar{f}(x) = (x^t-\bar{\alpha})\bar{q}(x)$. Consider the factorization of the polynomial $\bar{f}(x)$ modulo p into a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ as $\bar{f}(x) = \bar{g}_1(x)^{e_1}\cdots\bar{g}_r(x)^{e_r}$, where each $g_i(x) \in \mathbb{Z}[x]$ is a monic polynomial. Without loss of generality, we can assume, possibly after reordering the factors, that the exponents satisfy $e_i > 1$ for $1 \le i \le r_1$ and $e_i = 1$ for $r_1 < i \le r$. Then $x^t - \bar{\alpha} = \prod_{i=1}^{r_1}\bar{g}_i(x)$. Write

$$x^t - \alpha = \prod_{i=1}^{r_1} g_i(x) + ph_1(x), \quad q(x) = \prod_{i=1}^{r_1} g_i(x)^{e_i-1} \prod_{i=r_1+1}^{r} g_i(x) + ph_2(x)$$

where $h_1(x)$ and $h_2(x)$ are some polynomials with integer coefficients. Substituting the

expression from the preceding equation into equation (5.18), we obtain

$$f(x) = \prod_{i=1}^{r} g_i(x)^{e_i} + ph_1(x) \prod_{i=1}^{r_1} g_i(x)^{e_i-1} \prod_{i=r_1+1}^{r} g_i(x) + ph_2(x) \prod_{i=1}^{r_1} g_i(x) + p^2 h_1(x)h_2(x) + \alpha^{n_1-k_1m}(\alpha^{k_1}+a)^m + b.$$

It is evident that every term in the summation on the right-hand side of the equation above, with the possible exception of $\alpha^{n_1-k_1m}(\alpha^{k_1}+a)^m + b$, is an element of the ideal $\langle p, g_i(x)\rangle^2$ for each i in the range $1 \leq i \leq r_1$. So $f(x)$ lies in the ideal $\langle p, g_i(x)\rangle^2$ for some i, with $1 \leq i \leq r_1$ iff p^2 divides $\alpha^{n_1-k_1m}(\alpha^{k_1}+a)^m+b$. Since $\bar{f}(x)$ is not divisible by $\bar{g}_i(x)^2$ for any i in range $r_1 < i \leq r$, it follows directly that $f(x)$ is not an element of $\langle p, g_i(x)\rangle^2$ for these values of i. Combining this with the previous observation, we conclude that $f(x) \notin \langle p, g_i(x)\rangle^2$ for any i in the range $1 \leq i \leq r$. iff $p^2 \nmid (\alpha^{n_1-k_1m}(\alpha^{k_1}+a)^m + b)$. To prove this case, it only remains to prove that $\alpha^{n_1-k_1m}(\alpha^{k_1}+a)^m + b \equiv 0 \pmod{p^2}$ iff $U + V \equiv 0 \pmod{p^2}$.

Using $\alpha \equiv \alpha_1^{u_1}\alpha_2^{u_2} \pmod{p^2}$, we see that

$$\alpha^{n_1-k_1m}(\alpha^{k_1}+a)^m + b \equiv (\alpha_1^{u_1} \cdot \alpha_2^{u_2})^{n_1-k_1m}((\alpha_1^{u_1} \cdot \alpha_2^{u_2})^{k_1}+a)^m + b \pmod{p^2}.$$

Recall that $U = b^{k_1}n^{n_1}$ and $V = (-1)^{n_1-k_1m+k_1+1}\, a^{n_1}\, m^{k_1m}\, k^{k_1m}\, (n-km)^{n_1-k_1m}$. Keeping in mind that $p \nmid abn(n-km)$, $\alpha_1 \equiv -b\left(\frac{-km}{n-km}\right)^{-m} \pmod{p^2}$, $\alpha_2 \equiv \frac{-a(n-km)}{n} \pmod{p^2}$ and $n_1u_1 + k_1u_2 = 1$, where $u_1, u_2 \in \mathbb{Z}$, one can verify that

$$(\alpha_1^{u_1} \cdot \alpha_2^{u_2})^{n_1-k_1m}((\alpha_1^{u_1} \cdot \alpha_2^{u_2})^{k_1}+a)^m + b \equiv 0 \pmod{p^2} \text{ iff } U + V \equiv 0 \pmod{p^2},$$

which completes the proof of the theorem. □

5.3 Proof of Theorem 14

In this section, we show that the Galois group of the polynomial $f(x) = x^{q-km}(x^k + a)^m + b \in \mathbb{Z}[x]$ is the symmetric group S_q. The results presented below concerning the Galois group of a polynomial will play a crucial role in the proof of Theorem 14.

Theorem 5.3.1. *[7, Theorem 2.1] Let $f(x)$ be a monic irreducible polynomial of degree n with coefficients from the ring $\mathbb{Z}$ of integers, having a root θ. Let p be a rational prime which is ramified in $\mathbb{Q}(\theta)$. Suppose that $f(x) \equiv (x-\beta)^2\phi_1(x)\cdots\phi_r(x) \pmod{p}$, where $(x-\beta), \phi_1(x), \cdots, \phi_r(x)$ are monic polynomials over $\mathbb{Z}$ which are distinct and irreducible modulo p. Then the Galois group of $f(x)$ over $\mathbb{Q}$ contains a non-trivial automorphism which keeps $n-2$ roots of $f(x)$ fixed.*

Lemma 5.3.2. *[36, Lemma 2] Let $f(x)$ be an irreducible polynomial of degree $n \geq 2$. If the Galois group of $f(x)$ over $\mathbb{Q}$ contains a transposition and a p-cycle for some prime $p > n/2$, then the Galois group of $f(x)$ is S_n.*

Proof of Theorem 14: Let γ be a root of $f(x)$. Since $f(x)$ is of degree q, it follows that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = q$. By the Fundamental Theorem of Galois Theory, the Galois group G_f of $f(x)$ must contain a subgroup of index q. According to Lagrange's theorem, this implies that G_f is divisible by q. Consequently, by Cauchy's theorem, G_f must contain an order q element, i.e., a q-cycle.

We now proceed to establish that the Galois group G_f also includes a transposition. Since $k < q$, it follows that $t = 1$. According to the given assumptions, there exists a prime p such that $p \mid D_f$, $p \nmid abkm$, and $p^2 \nmid D_f$. By employing reasoning analogous to that in the proof of Theorem 13(vi), we deduce that α is the sole repeated root of $\bar{f}(x)$, and that its multiplicity is precisely 2. Consequently, we can write $f(x) \equiv (x-\alpha)^2 q_1(x) \pmod{p}$, where $q_1(x)$ is a separable polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$. Furthermore, let $K = \mathbb{Q}(\theta)$, where θ is a root of $f(x)$. Given that $p^2 \nmid D_f$ and using the identity $D_f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 d_K$, we infer that $p \mid d_K$, which implies that p ramifies in K. Therefore, applying Theorem 5.3.1, we conclude that G_f contains a transposition. It then follows from Lemma 5.3.2 that $G_f \cong S_q$. □

5.4 Proof of Theorem 15

The following lemma will be used to show that the polynomials obtained in Theorems 15 and 16 are monogenic.

Lemma 5.4.1. *Let n, k, m, t and κ be as in Theorem 15. For positive integers a and b with $\gcd(a, b) > 1$, define*

$$T := bt^t + (-1)^{t+m} a^t m^m (t-m)^{t-m}. \tag{5.19}$$

Given that b and T are square-free integers and that κ is a divisor of the greatest common divisor of a and b (i.e., $\kappa \mid \gcd(a, b)$), then the polynomial $f(x) = x^{n-km}(x^k + a)^m + b$ is monogenic.

Proof. Given that $\gcd(a, b) > 1$, there exists a prime p dividing $\gcd(a, b)$. Furthermore, as b is squarefree, it follows that $f(x)$ is p-Eisenstein. Therefore, $f(x)$ is irreducible over $\mathbb{Q}$. Applying Theorem 12 with the above notations, we obtain

$$D_f = (-1)^{\binom{n}{2}} b^{n-k-1} k^n T^k. \tag{5.20}$$

Now to prove that $f(x)$ is monogenic, it is enough to show that all the cases from Theorem 13 holds. Throughtout the proof, p will be a prime dividing D_f. Given that b is square-free, it is straightforward to observe that statement (i) holds true.

Suppose that $p \mid b,\ m = 1,\ p \nmid a$. Then $p \nmid \gcd(a, b)$. Keeping in mind the definition of κ and $\kappa \mid \gcd(a, b)$ we conclude that $p \nmid k$. Hence in Theorem 13 (ii), we have $j = v_p(k) = 0$. This implies that $a_1 = 0$, i.e., $p \mid a_1$. Using b is squarefree, we have p does not divide $b_1 = \frac{b}{p}$, i.e., (ii) holds.

Assume now that p divides a but not b. Then again as above, we obtain $p \nmid \gcd(a, b)$ and $p \nmid k$. In this case $p \mid n$, then using $p \nmid k$, we conclude that $p \mid t$. This implies $t \geq 2$, i.e., $p^2 \mid a^t$ and $p^2 \mid t^t$ which gives $T \equiv 0 \pmod{p^2}$. This contradicts the assumption that T is squarefree. Thus (iii) holds.

From the assumption that κ divides $\gcd(a, b)$ and the definition of κ, it follows that there do not exist any prime p such that $p \mid km$ but $p \nmid ab$. Hence, Cases (iv) and (v) are trivially true.

For Case (vi), suppose that $p \nmid abkm$. Using $p \nmid kb$ and (5.20), we conclude that $p \mid D_f$ iff $p \mid T$. In view of (1.7), we have $U + V = Tk^t$. Now the conclusion $p^2 \nmid (U + V)$ follows using $p \nmid k$ and T squarefree. Thus by Theorem 13, our contention is established. □

Under certain assumptions on integers n, m, k and a, Theorem 15 estimates the total number of integers $b \leq X$ such that $f(x) = x^{n-km}(x^k + a)^m + b$ is monogenic.

Proof of Theorem 15. Since b is squarefree and divisible by κ, we can write $b = \kappa b$ for some $b \in \mathbb{Z}$. Note that $\gcd(b, \kappa) = 1$. Let $\rho, \gamma, \alpha, y, \alpha_0, \beta_0$ and β be integers such that

$$\rho = \gamma = 1,\ \alpha = t^t,\ y = b,\ \alpha_0 = 1,\ \beta_0 = \kappa,$$
$$\beta = (-1)^{t+m} a^t m^m (t - m)^{t-m}.$$

One can easily verify that these variables satisfy the conditions given in (5.1). By equation (5.19), one can see that

$$T = \alpha\beta_0 y + \beta.$$

We wish to count $b \leq X$ such that $b \equiv 0 \pmod{\kappa}$ and both b, T are squarefree, i.e., we want to estimate the following

$$U(X) := |\{b \leq X/\kappa : \gcd(b, \kappa) = 1, \mu(b) \neq 0, \mu(T) \neq 0\}|.$$

Applying Theorem 5.1.6, we obtain

$$U(X) = \frac{X}{\kappa}\frac{\phi(\kappa)}{\kappa\zeta(2)}\prod_{p\mid\kappa}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p\nmid atm(t-m)}\left(1-\frac{1}{p^2-1}\right)+O(X^{3/4})$$
$$= \frac{X}{\kappa\zeta(2)}\prod_{p\mid\kappa}\left(1+\frac{1}{p}\right)^{-1}\prod_{p\nmid atm(t-m)}\left(1-\frac{1}{p^2-1}\right)+O(X^{3/4}),$$

where the last equality follows by noting that $\phi(\kappa) = \kappa\prod_{p\mid\kappa}\left(1-\frac{1}{p}\right)$. Using $\kappa > 1$ and $\gcd(a,b) \equiv 0 \pmod{\kappa}$, we conclude $\gcd(a,b) > 1$. Applying Lemma 5.4.1 completes the proof of this theorem. □

5.5 Proof of Theorem 16

Under certain assuptions on integers n, m, k and sqaurefree b, Theorem 16 shows that there are infinitely many sqaurefree integers a such that $f(x) = x^{n-km}(x^k+a)^m + b$ is monogenic.

Proof of Theorem 16: Fix a squarefree integer b and consider the polynomial

$$F(x) = m^m(t-m)^{t-m}\kappa^t x^t + (-1)^{t+m}t^t b \in \mathbb{Z}[x].$$

We wish to apply Theorem 5.1.8 to the polynomial $F(x)$. For this we first have to ensure that $F(x)$ has no repeated roots. Furthermore, the polynomial $F(x)$ must not exhibit any local obstructions. This means that for every prime number q, we need to prove the existence of some element z in the multiplicative group of integers modulo q^2, denoted by $(\mathbb{Z}/q^2\mathbb{Z})^*$, such that $F(z)$ is not congruent to 0 modulo q^2 (i.e., $F(z) \not\equiv 0 \pmod{q^2}$).

One can easily verify that the only possible repeated root of $F(x)$ is 0 which is clearly not a root of $F(x)$. Therefore, the polynomial $F(x)$ does not have any repeated factors. We now proceed with the proof that $F(x)$ has no local obstruction.Let q be a prime and suppose that $m(t-m)\kappa \equiv 0 \pmod{q}$. This implies either $q \mid m$ or $q \mid (t-m)$ or $q \mid \kappa$. If $q \mid m$ (or $q \mid (t-m)$), then we have $q^2 \mid m^m$ ($q^2 \mid (t-m)^{t-m}$ respectively). If $q \mid \kappa$, then keeping in mind $t \geq 2$, we conclude that $q^2 \mid \kappa^t$. Combining all the above, we have

$$F(1) \equiv (-1)^{t+m}t^t b \pmod{q^2}. \tag{5.21}$$

Recall that $\gcd(m(t-m)\kappa, t) = 1$, hence $q \nmid t$. Therefore we conclude that q^2 divides right side of equation (5.21) iff q^2 divides b, which is not possible as b is sqaurefree.

Therefore, we have $F(1) \not\equiv 0 \pmod{q^2}$, i.e., $F(x)$ does not have a local obstruction at primes q dividing $m(t-m)\kappa$.

Now assume that $q \nmid m(t-m)\kappa$. If q is a prime dividing t, then we have q^2 divides t^t. Using this, we obtain $F(1) \equiv m^m(t-m)^{t-m}\kappa^t \pmod{q^2}$. Keeping in mind that $\gcd(m(t-m)\kappa, t) = 1$ and using $q \mid t$, we have q does not divide the right side of this congruence, hence $F(1) \not\equiv 0 \pmod{q^2}$.

Now assume that q is a prime such that $q \nmid m(t-m)\kappa t$. Consider,

$$\begin{aligned} F(1+q) - F(1) &= m^m(t-m)^{t-m}\kappa^t[(1+q)^t - 1^t] \\ &\equiv m^m(t-m)^{t-m}\kappa^t(qt) \pmod{q^2}. \end{aligned}$$

We use $q \nmid m(t-m)\kappa t$, to deduce that the right side of the above congruence is not divisible by q^2 in this case. This implies $F(1+q) \not\equiv F(1) \pmod{q^2}$. Hence, we obtain that either $F(1+q)$ or $F(1)$ is not congruent to 0 modulo q^2. This concludes the proof that $F(x)$ has no local obstruction at any prime q.

Thus, by Theorem 5.1.8, there exist infinitely many prime numbers p for which $F(p)$ is square-free. The existence of such primes is unconditional when $t = 2$ or $t = 3$, and it relies on the *abc*-conjecture for number fields when $t \geq 4$. For any of these primes p such that $p > t$, let $a = \kappa p$. Then,

$$\begin{aligned} (-1)^{t+m}T &= m^m(t-m)^{t-m}a^t + (-1)^{t+m}bt^t \\ &= m^m(t-m)^{t-m}\kappa^t p^t + (-1)^{t+m}bt^t = F(p) \end{aligned}$$

is squarefree. Hence, by Lemma 5.4.1 and keeping in mind that $\gcd(a,b) \geq \kappa > 1$, $f(x) = x^{n-km}(x^k + \kappa p)^m + b$ is monogenic. This completes the proof of Theorem 16. $\square$

List of Publications

Included in Thesis

1. Anuj Jakhar, Shanta Laishram, Kotyada Srinivas, and Prabhakar Yadav, *Behaviour of newton polygon over polynomial composition*, arXiv:2501.06883, 2025.

2. Anuj Jakhar, Shanta Laishram, and Prabhakar Yadav, *Explicit discriminant of a class of polynomial, monogenity and galois group*, Comm. Algebra, 53(7):2937–2948, 2025.

3. Anuj Jakhar, Kotyada Srinivas, and Prabhakar Yadav, *Monogenic polynomials having squarefull discriminant*, Acta Arith., Accepted for publication, 2025.

4. Shanta Laishram, Sudhansu S. Rout, and Prabhakar Yadav, *Primitive prime divisors in the forward orbit of a polynomial*, arXiv:2502.02600, 2025.

5. Shanta Laishram and Prabhakar Yadav, *Irreducibility and galois groups of truncated binomial polynomials*, Int. J. Number Theory, 20(6):1663–1680, 2024.

Not included in Thesis

6. Anuj Jakhar, Ravi Kalwaniya, and Prabhakar Yadav, *A study of monogenity of binomial composition*, Acta Arith., Accepted for publication, 2025.

7. Anuj Jakhar, Ravi Kalwaniya, and Prabhakar Yadav, *On the monogenity and Galois group of certain classes of polynomials*, Mathematica Slovaca, 74(5):1147-1154, 2024.

8. Anuj Jakhar, Ravi Kalwaniya, and Prabhakar Yadav, *A study of monogenity of polynomial compositions: qualitative and quantitative aspects*, Submitted, 2024.

Bibliography

[1] Alan Baker. Experiments on the *abc*-conjecture. *Publ. Math. Debrecen*, 65(3-4):253–260, 2004.

[2] A. S. Bang. Taltheoretiske undersøgelser. *Tidsskrift for Mathematik*, 4:70–80, 1886.

[3] Robert L. Benedetto, Ruqian Chen, Trevor Hyde, Yordanka Kovacheva, and Colin White. Small dynamical heights for quadratic polynomials and rational functions. *Exp. Math.*, 23(4):433–447, 2014.

[4] Robert L. Benedetto, Benjamin Dickman, Sasha Joseph, Benjamin Krause, Daniel Rubin, and Xinwen Zhou. Computing points of small height for cubic polynomials. *Involve*, 2(1):37–64, 2009.

[5] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. Squarefree values of polynomial discriminants I. *Invent. Math.*, 228(3):1037–1073, 2022.

[6] Yuri F. Bilu, Guillaume Hanrot, and Paul M. Voutier. Existence of primitive divisors of lucas and lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[7] Anuj Bishnoi and Sudesh K. Khanduja. A class of trinomials with Galois group S_n. *Algebra Colloq.*, 19:905–911, 2012.

[8] Zenon I. Borevich and Igor R. Shafarevich. *Number theory*, volume Vol. 20 of *Pure and Applied Mathematics*. Academic Press, New York-London, 1966. Translated from the Russian by Newcomb Greenleaf.

[9] Alexander A. Borisov, Michael Filaseta, Tsit Y. Lam, and Ognian Trifonov. Classes of polynomials having only one non-cyclotomic irreducible factor. *Acta Arith.*, 90(2):121–153, 1999.

[10] David W. Boyd, Greg Martin, and Mark Thom. Squarefree values of trinomial discriminants. *LMS J. Comput. Math.*, 18(1):148–169, 2015.

[11] Andrew Bridy, John R. Doyle, Dragos Ghioca, Liang-Chung Hsia, and Thomas J. Tucker. Finite index theorems for iterated Galois groups of unicritical polynomials. *Trans. Amer. Math. Soc.*, 374(1):733–752, 2021.

[12] Andrew Bridy and Thomas J. Tucker. Finite index theorems for iterated Galois groups of cubic polynomials. *Math. Ann.*, 373(1-2):37–72, 2019.

[13] Egbert Brieskorn and Horst Knörrer. *Plane Algebraic Curves: Translated by John Stillwell*. Springer Science & Business Media, 2012.

[14] Gregory S. Call and Joseph H. Silverman. Canonical heights on varieties with morphisms. *Compositio Math.*, 89(2):163–205, 1993.

[15] Robert D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15(1-4):49–70, 1913/14.

[16] Mohamed E. Charkani and Abdulaziz Deajim. Generating a power basis over a Dedekind ring. *J. Number Theory*, 132(10):2267–2276, 2012.

[17] Teng Cheng. Primitive prime divisors for weighted homogeneous polynomial. *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 62(110)(2):173–182, 2019.

[18] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[19] Stephen D. Cohen, Abbas Movahhedi, and Alain Salinier. Double transitivity of Galois groups of trinomials. *Acta Arith.*, 82(1):1–15, 1997.

[20] Stephen D. Cohen, Abbas Movahhedi, and Alain Salinier. Factorization over local fields and the irreducibility of generalized difference polynomials. *Mathematika*, 47(1-2):173–196, 2000.

[21] Robert F. Coleman. On the Galois groups of the exponential Taylor polynomials. *Enseign. Math. (2)*, 33(3-4):183–189, 1987.

[22] Mohamed O Darwish and Mohammad Sadek. Eventual stability of pure polynomials over the rational field. *arXiv preprint arXiv:2211.11095*, 2022.

[23] Richard Dedekind. Über den zusammenhang zwischen der theorie der ideale und der theorie der höheren congruenzen. 1878.

[24] Richard Dedekind. Über den zusammenhang zwischen der theorie der ideale und der theorie der höheren kongruenzen. *Abh. der Konig. Gesell. der Wiss. zu Göttingen*, 23:1–23, 1878.

[25] Kevin Doerksen and Anna Haensch. Primitive prime divisors in zero orbits of polynomials. *Integers*, 12(3):465–472, 2012.

[26] Artūras Dubickas and Jonas Šiurys. Some irreducibility and indecomposability results for truncated binomial polynomials of small degree. *Proc. Indian Acad. Sci. Math. Sci.*, 127(1):45–57, 2017.

[27] Gustave Dumas. Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels. *Journal de Mathématiques Pures et Appliquées*, 2:191–258, 1906.

[28] Pierre Dusart. Autour de la fonction qui compte le nombre de nombres premiers, 1998.

[29] Lhoussain El Fadil. Prime ideal factorization in a number field via newton polygons. *Czechoslovak Math. J.*, 71(146)(2):529–543, 2021.

[30] Lhoussain El Fadil, Jesús Montes, and Enric Nart. Newton polygons and p-integral bases of quartic number fields. *J. Algebra Appl.*, 11(4):1250073, 33, 2012.

[31] Graham Everest, Gerard Mclaren, and Thomas Ward. Primitive divisors of elliptic divisibility sequences. *J. Number Theory*, 118(1):71–89, 2006.

[32] Xander Faber and José Felipe Voloch. On the number of places of convergence for Newton's method over number fields. *J. Théor. Nombres Bordeaux*, 23(2):387–401, 2011.

[33] Michael Filaseta. The irreducibility of all but finitely many Bessel polynomials. *Acta Math.*, 174(2):383–397, 1995.

[34] Michael Filaseta, Travis Kidd, and Ognian Trifonov. Laguerre polynomials with Galois group A_m for each m. *J. Number Theory*, 132(4):776–805, 2012.

[35] Michael Filaseta, Angel Kumchev, and Dmitrii V. Pasechnik. On the irreducibility of a truncated binomial expansion. *Rocky Mountain J. Math.*, 37(2):455–464, 2007.

[36] Michael Filaseta and Richard Moy. On the Galois group over $\mathbb{Q}$ of a truncated binomial expansion. *Colloq. Math.*, 154(2):295–308, 2018.

[37] Michael Filaseta and Ognian Trifonov. The irreducibility of the Bessel polynomials. *J. Reine Angew. Math.*, 550:125–140, 2002.

[38] István Gaál. *Diophantine equations and power integral bases*. Birkhäuser/Springer, Cham, second edition, 2019. Theory and algorithms.

[39] István Gaál. Monogenity and power integral bases: recent developments. *Axioms*, 13(7):429, 2024.

[40] István Gaál and László Remete. Integral bases and monogenity of composite fields. *Exp. Math.*, 28(2):209–222, 2019.

[41] Rylan Gajek-Leonard and Uri Tomer. Stretching newton polygons using pure polynomials. *arXiv preprint arXiv:2405.10926*, 2024.

[42] Chad Gratton, Khoa D. Nguyen, and Thomas J. Tucker. *ABC* implies primitive prime divisors in arithmetic dynamics. *Bull. Lond. Math. Soc.*, 45(6):1194–1208, 2013.

[43] Jordi Guàrdia, Jesús Montes, and Enric Nart. Newton polygons of higher order in algebraic number theory. *Trans. Amer. Math. Soc.*, 364(1):361–416, 2012.

[44] Jordi Guàrdia, Jesús Montes, and Enric Nart. Higher Newton polygons and integral bases. *J. Number Theory*, 147:549–589, 2015.

[45] Farshid Hajir. On the Galois group of generalized Laguerre polynomials. *J. Théor. Nombres Bordeaux*, 17(2):517–525, 2005.

[46] Joshua Harrington and Lenny Jones. The irreducibility of power compositional sextic polynomials and their Galois groups. *Math. Scand.*, 120(2):181–194, 2017.

[47] Joshua Harrington and Lenny Jones. Some new polynomial discriminant formulas. *Lith. Math. J.*, 61(4):483–490, 2021.

[48] Helmut Hasse. *Zahlentheorie*. Akademie-Verlag, Berlin, 1963. Zweite erweiterte Auflage.

[49] Joshua Ide and Lenny Jones. Infinite families of A_4-sextic polynomials. *Canad. Math. Bull.*, 57(3):538–545, 2014.

[50] Patrick Ingram. Elliptic divisibility sequences over certain curves. *J. Number Theory*, 123(2):473–486, 2007.

[51] Patrick Ingram. Lower bounds on the canonical height associated to the morphism $\phi(z) = z^d + c$. *Monatsh. Math.*, 157(1):69–89, 2009.

[52] Patrick Ingram and Joseph H. Silverman. Primitive divisors in arithmetic dynamics. *Math. Proc. Cambridge Philos. Soc.*, 146(2):289–302, 2009.

[53] Anuj Jakhar. Nonmonogenity of number fields defined by truncated exponential polynomials. *Bull. Aust. Math. Soc.*, pages 1–8, 2024.

[54] Anuj Jakhar, Sudesh K. Khanduja, and Neeraj Sangwan. On prime divisors of the index of an algebraic integer. *J. Number Theory*, 166:47–61, 2016.

[55] Anuj Jakhar, Sudesh K. Khanduja, and Neeraj Sangwan. Characterization of primes dividing the index of a trinomial. *Int. J. Number Theory*, 13(10):2505–2514, 2017.

[56] Anuj Jakhar, Shanta Laishram, Kotyada Srinivas, and Prabhakar Yadav. Behaviour of newton polygon over polynomial composition. *arXiv preprint arXiv:2501.06883*, 2025.

[57] Anuj Jakhar, Shanta Laishram, and Prabhakar Yadav. Explicit discriminant of a class of polynomial, monogenity and galois group. *Comm. Algebra*, 53(7):2937–2948, 2025.

[58] Anuj Jakhar and Neeraj Sangwan. Some results for the irreducibility of truncated binomial expansions. *J. Number Theory*, 192:143–149, 2018.

[59] Anuj Jakhar, Kotyada Srinivas, and Prabhakar Yadav. Monogenic polynomials having squarefull discriminant. *Acta Arith., Accepted for publication*, 2025.

[60] Lenny Jones. Monogenic polynomials with non-squarefree discriminant. *Proc. Amer. Math. Soc.*, 148(4):1527–1533, 2020.

[61] Lenny Jones. Some new infinite families of monogenic polynomials with non-squarefree discriminant. *Acta Arith.*, 197(2):213–219, 2021.

[62] Lenny Jones and Tristan Phillips. Infinite families of monogenic trinomials and their Galois groups. *Internat. J. Math.*, 29(5):1850039, 11, 2018.

[63] Lenny Jones and Daniel White. Monogenic trinomials with non-squarefree discriminant. *Internat. J. Math.*, 32(13):Paper No. 2150089, 21, 2021.

[64] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc. (2)*, 78(2):523–544, 2008.

[65] Rafe Jones and Alon Levy. Eventually stable rational functions. *Int. J. Number Theory*, 13(9):2299–2318, 2017.

[66] Kiran S. Kedlaya. A construction of polynomials with squarefree discriminants. *Proc. Amer. Math. Soc.*, 140(9):3025–3033, 2012.

[67] Sudesh K. Khanduja, Ramneek Khassa, and Shanta Laishram. Some irreducibility results for truncated binomial expansions. *J. Number Theory*, 131(2):300–308, 2011.

[68] Sudesh K. Khanduja and Sanjeev Kumar. On prolongations of valuations via Newton polygons and liftings of polynomials. *J. Pure Appl. Algebra*, 216(12):2648–2656, 2012.

[69] Sudesh Kaur Khanduja. *A textbook of algebraic number theory*, volume 135 of *La Matematica per il 3+2*. Springer, Singapore, [2022] ©2022. Unitext.

[70] Kwang-Seob Kim and John C. Miller. Class numbers of large degree nonabelian number fields. *Math. Comp.*, 88(316):973–981, 2019.

[71] Benjamin Klahn and Marc Technau. Galois groups of $\binom{n}{0} + \binom{n}{1}X + \cdots + \binom{n}{6}X^6$. *Int. J. Number Theory*, 19(10):2443–2450, 2023.

[72] Holly Krieger. Primitive prime divisors in the critical orbit of $z^d + c$. *Int. Math. Res. Not. IMRN*, (23):5498–5525, 2013.

[73] Munish Kumar and Sudesh K. Khanduja. A generalization of Dedekind criterion. *Comm. Algebra*, 35(5):1479–1486, 2007.

[74] Shanta Laishram, Sudhansu S. Rout, and Prabhakar Yadav. Primitive prime divisors in the forward orbit of a polynomial. *arXiv preprint arXiv:2502.02600*, 2025.

[75] Shanta Laishram and Tarlok N. Shorey. Baker's explicit *abc*-conjecture and applications. *Acta Arith.*, 155(4):419–429, 2012.

[76] Shanta Laishram and Prabhakar Yadav. Irreducibility and galois groups of truncated binomial polynomials. *Int. J. Number Theory*, 20(6):1663–1680, 2024.

[77] Derrick H. Lehmer. On a problem of Störmer. *Illinois J. Math.*, 8:57–79, 1964.

[78] Pascual Llorente, Enric Nart, and Núria Vila. Discriminants of number fields defined by trinomials. *Acta Arith.*, 43(4):367–373, 1984.

[79] Florian Luca and Filip Najman. On the largest prime factor of $x^2 - 1$. *Math. Comp.*, 80(273):429–435, 2011.

[80] Khosro Monsef Shokri. The Zsigmondy set for zero orbit of a rigid polynomial. *Khayyam J. Math.*, 8(1):115–119, 2022.

[81] Jesús Montes and Enric Nart. On a theorem of Ore. *J. Algebra*, 146(2):318–334, 1992.

[82] Anirban Mukhopadhyay and Tarlok N. Shorey. Square free part of products of consecutive integers. *Publ. Math. Debrecen*, 64(1-2):79–99, 2004.

[83] Władysł aw Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer-Verlag, Berlin; PWN—Polish Scientific Publishers, Warsaw, second edition, 1990.

[84] Öystein Ore. Zur Theorie der Algebraischen Körper. *Acta Math.*, 44(1):219–314, 1923.

[85] Öystein Ore. Newtonsche Polygone in der Theorie der algebraischen Körper. *Math. Ann.*, 99(1):84–117, 1928.

[86] Hector Pasten. The ABC conjecture, arithmetic progressions of primes and square-free values of polynomials at prime arguments. *Int. J. Number Theory*, 11(3):721–737, 2015.

[87] Rufei Ren. Primitive prime divisors in the critical orbits of one-parameter families of rational polynomials. *Math. Proc. Cambridge Philos. Soc.*, 171(3):569–584, 2021.

[88] Brian Rice. Primitive prime divisors in polynomial arithmetic dynamics. *Integers*, 7:A26, 16, 2007.

[89] N. Saradha and Tarlok N. Shorey. Almost squares and factorisations in consecutive integers. *Compositio Math.*, 138(1):113–124, 2003.

[90] Inna Scherbak. Intersections of schubert varieties and highest weight vectors in tensor products of sl_ {N+ 1}-representations. *arXiv preprint math/0409329*, 2004.

[91] Andrzej Schinzel. Primitive divisors of the expression $A^n - B^n$ in algebraic number fields. *J. Reine Angew. Math.*, 268/269:27–33, 1974.

[92] Issai Schur. *Einige Sätze über Primzahlen: mit Anwendungen auf Irreduzibilitätsfragen*. Akademie der Wissenschaften in Kommission bei Walter de Gruyter, 1929.

[93] Joseph H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory*, 30(2):226–237, 1988.

[94] Joseph H. Silverman. Integer points, Diophantine approximation, and iteration of rational maps. *Duke Math. J.*, 71(3):793–829, 1993.

[95] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[96] Joseph H. Silverman and José Felipe Voloch. A local-global criterion for dynamics on $\mathbb{P}^1$. *Acta Arith.*, 137(3):285–294, 2009.

[97] Vijay A. Sookdeo. Integer points in backward orbits. *J. Number Theory*, 131(7):1229–1239, 2011.

[98] Cameron L. Stewart. Primitive divisors of lucas and lehmer numbers. In *Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976)*, pages 79–92. Academic Press, London-New York, 1977.

[99] Paul M. Voutier. Primitive divisors of Lucas and Lehmer sequences. III. *Math. Proc. Cambridge Philos. Soc.*, 123(3):407–419, 1998.

[100] Karl Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.