An Analytic Study of the Irreducibility, Monogeniety, and Squarefreeness of Certain Polynomials

By

Arunabha Mukhopadhyay

MATH10202104002

The Institute of Mathematical Sciences, Chennai

A thesis submitted to the

Board of Studies in Mathematical Sciences

In partial fulfillment of requirements

for the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

December, 2025

Homi Bhabha National Institute

Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by Arunabha Mukhopadhyay entitled "An Analytic Study of the Irreducibility, Monogeniety, and Squarefreeness of Certain Polynomials" and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

Chairman - Vijay Kodiyalam — Date: 11-12-2025

Guide/Convenor - Srinivas Kotyada — Date: 11-12-2025

Examiner - B. Sury — Date: 11-12-2025

Member 1 - Anirban Mukhopadhyay — Date: 11-12-2025

Member 2 - Anup B Dixit — Date: 11-12-2025

Member 3 - Anuj Jakhar — Date: 11-12-2025

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to HBNI.

I hereby certify that I have read this thesis prepared under my direction and recommend that it may be accepted as fulfilling the thesis requirement.

Date: 11-12-2025

Place: IMSc, Chennai

Srinivas Kotyada (Guide)

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgement the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Arunabha Mukhopadhyay

DECLARATION

I hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

Arunabha Mukhopadhyay

CERTIFICATION ON ACADEMIC INTEGRITY

1. I **Arunabha Mukhopadhyay**, HBNI Enrolment No. **MATH10202104002** hereby undertake that the Thesis, titled **"An Analytic Study of the Irreducibility, Monogeniety, and Squarefreeness of Certain Polynomials"** is prepared by me and is the original work undertaken by me.

2. I also hereby undertake that this document has been duly checked through a plagiarism detection tool and the document is found to be plagiarism free as per the guidelines of the Institute/UGC.

3. I am aware and undertake that if plagiarism is detected in my thesis at any stage in the future, suitable penalty will be imposed as per the guidelines of the Institute/UGC.

A. Mukhopadhyay

01/12/25

Signature of the Student with date

Endorsed by the Thesis Supervisor:

I certify that the thesis written by the researcher is plagiarism free as mentioned above by the student.

Name : Dr. K. Srinivas

Designation : Prof. H (retired), currently visiting Professor at IISER Tirupati

Department/ Centre : Mathematics

Name of the CI/ OCC : IMSc

K Srinivas

1-12-2025

Signature of the Thesis Supervisor with date

LIST OF PUBLICATIONS ARISING FROM THE THESIS

(1). Published / Accepted

(i) (with Anuj Jakhar and Srinivas Kotyada) Irreducibility of extended Laguerre polynomials, *Journal of Algebra and its Applications* (2025), to appear, Doi: 10.1142/S0219498826501811.

(ii) (with Anuj Jakhar and Srinivas Kotyada) Monogenic polynomials and symmetric Galois groups: a quantitative study, *Ramanujan J* **67**, 69 (2025), Doi: 10.1007/s11139-025-01110-w.

(iii) (with Anuj Jakhar and Srinivas Kotyada) On Squarefree Parts of Polynomial Discriminants and Quadratic Fields, *Results Math.*, **80**, 132 (2025), Doi: 10.1007/s00025-025-02448-9.

(iv) (with Anuj Jakhar and Srinivas Kotyada) Squarefree part of a discriminant and abc-conjecture (Accepted in Conference Proceedings on Lie Algebra and Number Theory) (2025).

(2). Preprints

(v) (with Anuj Jakhar and Srinivas Kotyada) Distinct Square-Free Parts of Discriminants of Polynomials and Quadratic Fields. (Submitted)

A. Mukhopadhyay

Arunabha Mukhopadhyay

Dedicated to My Parents and Teachers

ACKNOWLEDGEMENTS

With profound thankfulness, I bow in appreciation to all those whose guidance, encouragement, and companionship have made this journey possible.

At the very outset, I wish to express my heartfelt gratitude to my academic advisor, Prof. Srinivas Kotyada. His support, encouragement, patience, and illuminating guidance carried me through this work. He never let me lose faith in myself, which has given me more strength than I can describe. It has been an honor to work under your mentorship, sir, an experience I shall always cherish.

I am deeply grateful to Dr. Anuj Jakhar, who has been not only a collaborator but also a friend and elder figure whose support means so much to me. Your thoughtful suggestions and insightful criticism have not only shaped this work but also nurtured my growth as a scholar. Discussion with you on a mathematical problem has always been fruitful. I will miss our after-work tennis matches at IMSc tennis court.

My sincere thanks go to Dr. Anup Dixit and Prof. Sanoli Gun for maintaining a lively number-theoretic atmosphere at the institute through various courses, seminars, and conferences, which have significantly enhanced my knowledge.

I am grateful to The Institute of Mathematical Sciences for providing excellent hostel and library facilities, which made this research possible and smoother. I would like to thank all the faculty members at IMSc who taught me during my first-year coursework, from whom I learned a lot. I would also like to thank my doctoral committee members.

I remain deeply thankful to all of my mathematics teachers, from school life to college, especially Satyaranjan Karfa, Srikumar Ghosh, Partha Pratim Basu, and Gopal Adak. Their encouragement and teaching planted the seeds of a lifelong love for mathematics within me.

I greatly appreciate the support and companionship of my colleague friends Sayak, Sushant, Suraj, Tirtharaj, Ravi, Prabhakar, Dhananjay, Papiya, and many others. I've been glad to have Sayak,

Sushant, and Tirtharaj by my side since coming to the IMSc hostel. Their friendship turned hostel life into fun times, colorful and eased many challenges of academic life. I will always remember fondly the late-night food cravings, unplanned movie sessions with Suraj, Tirtharaj, and Sayak. Many other unforgettable moments and memories that I'll always treasure.

I would like to thank Ankur da, my officemate, with whom I shared not only the workspace but also countless conversations that helped us neutralize the frustrations of academic life. Our frequent sports talks, watching late night UCL matches filled with energy and laughter, brought joy and balance to this journey.

How could I forget the Monday and Friday football matches! I would like to thank all the members of the IMSc football group with whom I played from 2021 to 2025. Those games were one of the best parts of my routine, keeping my mind fresh and my spirits high throughout this journey. I am also thankful to those with whom I spent hours playing lawn tennis and table tennis, adding joy and friendship to my time here.

Whenever I went back home, I was fortunate to be accompanied by my B.Sc. and M.Sc. friends Niladri, Sayan, Raunak, Gourab, and sometimes Diptiman, as well as my school friends Kundasubhra, Subhadip, Anirban, and many others. I am truly thankful to them for their company and the time we spent together.

Lastly, but certainly not least, I owe my deepest gratitude to my Maa and Baba, the silent warriors whose constant support and boundless love have been my guiding light. Words fall short of conveying how grateful I am; this journey would not have been possible without them.

Contents

Summary i

Notations iii

0 Introduction 1

0.1 Part I . . . 2

0.2 Part II . . . 4

1 Newton Polygon and Irreducibility 11

1.1 Introduction . . . 11

1.2 Valuation on a Field . . . 14

1.3 Newton Polygon (of a Polynomial in $\mathbb{Z}[x]$) . . . 15

1.4 ϕ-Newton Polygon . . . 20

1.5 Irreducibility of Generalized ϕ-Laguerre Polynomials . . . 23

1.6 Proof of Theorems 1.1.1 and 1.1.2 . . . 25

1.7 Short Notes on Other Classical Families of Polynomials . . . 33

2 Square-free Parts of Discriminants 35

2.1 Introduction . . . 35

2.2 The Square Sieve 39

2.3 Characters of Finite Abelian Group 40

2.4 Main Theorems 47

3 *abc*-Conjecture and Counting Polynomials **59**

3.1 Introduction 59

3.2 Preliminaries 61

3.3 Monogenic Polynomials 62

3.3.1 Counting Monogenic Polynomials $t^n + c(at^k + b)^m$ 63

3.3.2 *abc*-Conjecture for Number Fields 64

3.4 Counting Polynomials $t^q + c(at^k + b)^m$ with Galois group S_q 70

3.5 Counting Distinct Squarefree Parts of $\Delta_{n,m,k}(a, b, c)$ Under *abc-Conjecture* 71

Bibliography **81**

Summary

This thesis provides a study of problems related to the irreducibility and arithmetic properties of certain families of polynomials. In particular, we emphasize generalized ϕ-Laguarre polynomials and discriminants of a special class of polynomials. We use some classical analytic methods to approach these problems. The work is divided into two parts.

In the first part we establish some results on the irreducibility of generalized ϕ-Laguerre polynomials. The principal tools we applied here are the notion of ϕ-Newton polygon introduced by Ø. Ore [68] and a generalized version of a lemma of M. Filaseta [19], together with some fundamental results from analytic number theory and the theory of Diophantine equations.

The second part of the thesis is based on a quantitative estimate in terms of degree and coefficients for the number of distinct squarefree parts of discriminants of the monic irreducible polynomials $t^n+c(at^k+b)^m \in \mathbb{Z}[t]$ of degree n. We study these problems in this part and obtain lower bounds for such quantities, using the square sieve method of D. R. Heath-Brown [28]. Furthermore, assuming the *abc*-conjecture for number fields, we derive a lower bound for the number of polynomials $t^n + c(at^k + b)^m \in \mathbb{Z}[t]$ that are monogenic with non-squarefree discriminants or have Galois group S_n.

Finally, we conclude the thesis by posing some open problems related to the topics discussed above.

Notations

Throughout this thesis, we use the following symbols:

- $\mathbb{N}$: The set of natural numbers.
- $\mathbb{Z}$: The set of rational integers.
- $\mathbb{Z}^-$: The set of negative rational integers.
- $\mathbb{Q}$: The set of rational numbers.
- $\mathbb{R}$: The set of real numbers.
- $\mathbb{C}$: The set of complex numbers.
- $\mathbb{Z}[x]$: The ring of polynomials with integer coefficients.
- $\mathbb{Q}[x]$: The ring of polynomials with rational coefficients.
- $\deg(p)$: The degree of a polynomial $p(x)$.
- (a, b) or $\gcd(a, b)$: The greatest common divisor of integers a and b.
- $f(x) \ll g(x)$ or $f(x) = O(g(x))$: There exists a constant $C > 0$ such that $|f(x)| \leq C\,|g(x)|$ for all sufficiently large x.

- $f(x) \ll_\varepsilon g(x)$ or $f(x) = O_\varepsilon(g(x))$: Same as above but the implied constant C may depend on the parameter ε.

- $f(x) \sim g(x)$: $\lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$.

- $d(r)$: The number of divisors of r.

- $\varphi(r)$: Euler's totient function.

- $[G : H]$: The index of a subgroup H in a group G.

Chapter 0

Introduction

This thesis is concerned with two important topics in number theory:

(i) Irreducibility of generalized ϕ-Laguerre polynomials.

(ii) On distinct square-free parts of the discriminants of a special class of polynomials.

The first part (i) primarily deals with results related to the irreducibility of the generalized ϕ-Laguerre polynomials $L^{\phi}_{n,\alpha}(x)$ over $\mathbb{Q}$, depending on the degree n and the number α. This topic will be discussed in Chapter 1 of this thesis. The later part (ii) involves results on lower bounds for the number of distinct squarefree parts of discriminants of the polynomial $t^n + c(at^k + b)^m \in \mathbb{Z}[t]$, and as an application, we obtain some results in monogenity and Galois group under *abc-conjecture*. This topic will be covered in Chapters 2 and 3 of this thesis. Both parts are based on joint work with Anuj Jakhar and Srinivas Kotyada (see the list of publications (i), (ii), (iii), (iv), and (v)).

In the following sections, we will briefly introduce these topics and our work in a chapter wise manner.

0.1 Part I

Generalized ϕ- Laguerre Polynomials and Their Irreducibility (over Rationals)

Laguerre polynomials, which originally arise in mathematical physics and special function theory, also exhibit rich arithmetic properties. E. Laguerre introduced these polynomials in the late 19th century. The generalized Laguerre polynomials $L_{n,\alpha}(x)$ are defined as follows,

$$L_{n,\alpha}(x) = \sum_{j=0}^{n} \frac{(n+\alpha)(n+\alpha-1)\cdots(j+1+\alpha)}{(n-j)!j!}(-x)^j,$$

where α is an arbitrary real number. $L_{n,\alpha}(x)$ are the solutions of the second order differential equation

$$x\frac{d^2y}{dx^2} + (\alpha+1-x)\frac{dy}{dx} + ny = 0, \quad y = L_{n,\alpha}(x).$$

$L_{n,0}(x)$ (i.e., when $\alpha = 0$) is known as classical Laguerre polynomial. The research problems on the topics of generalized Laguerre polynomials, in the context of number theory can be broadly classified into two themes:

A (Irreducibility). For a rational number α, what are the values of degree n of $L_{n,\alpha}(x)$ for which $L_{n,\alpha}(x)$ is irreducible over $\mathbb{Q}$.

B (Galois group). Once the irreducibility is satisfactorily ascertained, find the Galois groups over $\mathbb{Q}$ associated with the polynomials $L_{n,\alpha}(x)$.

In a series of papers [73-76], I. Schur established the irreducibility and computed the associated Galois group of $L_{n,0}(x), L_{n,1}(x)$ and $L_{n,-n-1}(x)$. In Chapter 1, we shall address theme A for the generalized ϕ- Laguerre polynomials via the method of ϕ-Newton polygon. The generalized ϕ- Laguerre polynomials and ϕ-Newton polygon are defined below.

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ be a polynomial such that $a_0 a_n \neq 0$. For a prime p, the *Newton polygon* of f with respect to p is defined as the lower convex hull of the set of points S in $\mathbb{R}^2$ given below :

$$S := \big\{(0, v_p(a_n)), (1, v_p(a_n - 1)), \cdots, ((j, v_p(a_n - j)), \cdots, (n, v_p(a_0))\big\},$$

where v_p denotes the usual *p-adic* valuation.

First, Coleman [12] and later Filaseta [19] re-established the results of Schur by invoking the main theorem of Dumas [13] on Newton polygon. The concept of the Newton polygon was further generalized to the *ϕ-Newton polygon* by replacing the variable x with an arbitrary monic polynomial $\phi(x) \in \mathbb{Z}[x]$. This generalization was due to Ore [68]. Denote by v_p^x the Gaussian valuation extending v_p defined on the polynomial ring $\mathbb{Z}[x]$ by

$$v_p^x(\sum_i b_i x^i) = \min_i\{v_p(b_i)\},\ b_i \in \mathbb{Z}.$$

ϕ-Newton polygon: Let p be a prime number and $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial. Let $f(x)$ belonging to $\mathbb{Z}[x]$ be a polynomial having ϕ-expansion $\sum_{i=0}^{n} b_i(x)\phi(x)^i$ with $b_0(x)b_n(x) \neq 0$. Let P_i stand for the point in the plane having coordinates $(i, v_p^x(b_{n-i}(x)))$ when $b_{n-i}(x) \neq 0$, $0 \leq i \leq n$. Let μ_{ij} denote the slope of the line joining the points P_i and P_j if $b_{n-i}(x)b_{n-j}(x) \neq 0$. Let i_1 be the largest index $0 < i_1 \leq n$ such that

$$\mu_{0i_1} = \min\{\mu_{0j} \mid 0 < j \leq n,\ b_{n-j}(x) \neq 0\}.$$

If $i_1 < n$, let i_2 be the largest index $i_1 < i_2 \leq n$ such that

$$\mu_{i_1 i_2} = \min\{\mu_{i_1 j} \mid i_1 < j \leq n,\ b_{n-j}(x) \neq 0\}$$

and so on. The ϕ-Newton polygon of $f(x)$ with respect to p is the polygonal path having segments $P_0P_{i_1}, P_{i_1}P_{i_2}, \ldots, P_{i_{k-1}}P_{i_k}$ with $i_k = n$.

Now let us define generalized ϕ- Laguerre polynomial.

Generalized ϕ- Laguerre polynomial: For any $\phi(x) \in \mathbb{Z}[X]$ and $\alpha \in \mathbb{R}$, we define generalized ϕ-Laguerre polynomial by

$$L_{n,\alpha}^{\phi}(x) = \frac{1}{n!}\left(a_n(x)\phi(x)^n + \sum_{j=0}^{n-1} b_j a_j(x)\phi(x)^j\right)$$

where $b_j = \binom{n}{j} \prod_{i=j+1}^{n} (i+\alpha)$ for $0 \leq j \leq n-1$, and $a_j(x) \in \mathbb{Z}[X]$ with deg $a_j <$deg ϕ.

Making use of ϕ-Newton polygon along with the prime number theorem in arithmetic progression (for our Theorem 0.1.1) and Catalan's conjecture (or Mihăilescu's theorem) (for our Theorem 0.1.2), we prove the following theorems in Chapter 1 :

Let $\alpha \in \mathbb{Q} \setminus \mathbb{Z}^-$ be fixed such that $\alpha = \frac{u}{v}$ with $\gcd(u, v) = 1$, $v > 0$. Let $\phi(x)$ belonging to $\mathbb{Z}[x]$ be a monic polynomial which is irreducible modulo all the primes less than or equal to $vn + |u|$ and $a_n = a_n(x)$ be a constant polynomial. Also assume that the content of $(a_n a_0(x))$ is not divisible by any prime less than or equal to $vn + |u|$. Then under these conditions, we have :

Theorem 0.1.1. The polynomials $L_{n,\alpha}^{\phi}(x)$ are irreducible over $\mathbb{Q}$ for all but finitely many positive integers n.

Theorem 0.1.2. The polynomials $L_{n,\alpha}^{\phi}(x)$ are irreducible over $\mathbb{Q}$ for $\alpha \in \{0, 1, 2, 3, 4\}$ unless $(n, \alpha) \in \{(1, 0), (2, 2), (4, 4), (6, 4)\}$.

We will now provide brief details of the remaining chapters.

0.2 Part II

Distinct Square-free Parts of Discriminants of $t^n + c(at^k + b)^m$

An integer n is called *squarefree*, if no square of a prime number divides n. Any integer n can be written as $n = sr^2$, where s is a square-free integer and $r \in \mathbb{Z}$. The integer s will be called the *squarefree part of* n. In analytic number theory, it is often interesting to find how many squarefree integers are there in a certain sequence of integers. Along this line we may propose the following question :

• If $f : \mathbb{Z}^r \to \mathbb{Z}$ is any integer valued function, then what is the number (asymptotically) of distinct squarefree parts (i.e., s) in a sequence of values of f.

We investigate this question for the values taken by the discriminant of the monic irreducible polynomial $t^n + c(at^k + b)^m \in \mathbb{Z}[t]$ of degree n with $\gcd(n, k) = 1$. The discriminant of this polynomial is given by (see [36]),

$$\Delta_{n,m,k}(a, b, c) := (-1)^{\binom{n}{2}} b^{m(n+k-1)-n} c^{n-1} \left[n^n b^{n-mk} + (-1)^{n+mk+k+1} a^n c^k (mk)^{mk} (n - mk)^{n-mk} \right].$$

when $n \geq 3$, the term $b^{m(n+k-1)-n} c^{n-1}$ will not be squarefree. Therefore it is natural to calculate the number of distinct square-free parts of the integer values taken by

$$T_{n,m,k}(a, b, c) := n^n b^{n-mk} + (-1)^{n+mk+k+1} a^n c^k (mk)^{mk} (n - mk)^{n-mk}.$$

In Chapter 2, this problem has been carried out for two different cases :

(i) Determine the number of tuples (a, b, c) for which $T_{n,m,k}(a, b, c)$ has distinct squarefree parts, where n and m are fixed odd integers and $k = 1$.

(ii) Determine the number of integers n for which $T_{n,m,k}(a, b, c)$ has distinct squarefree parts, where a, b, c, k, and m are fixed.

To be precise, we provide only the lower bounds of such numbers. We use *square sieve* of Heath-Brown [28] as the main tool to approach this problem. We now proceed to state the main results of Chapter 2 according to the cases (i) and (ii).

Case (i):

In this case, let us denote $\Delta_{n,m}(a, b, c) := T_{n,m,1}(a, b, c)$. For a fixed square-free integer s and positive

real numbers A, B, C, D, E, F, let

$$\mathcal{L}_{n,m}(A,B,C,D,E,F;s) := \{(a,b,c) \in [D, D+A] \times [E, E+B] \times [F, F+C] \Big|$$
$$\Delta_{n,m}(a,b,c) = sr^2, \text{ for some integer } r\}.$$

The following theorem provides an estimate for the number of (a,b,c) in $[D, D+A] \times [E, E+B] \times [F, F+C]$ such that $\Delta_{n,m}(a,b,c) = sr^2$, for a fixed square-free integer s.

Theorem 0.2.1. For sufficiently large positive real numbers $A,\ B,\ C$ and some non-negative real numbers $D,\ E,\ F$, and for a fixed squarefree number s, as well as for odd integers n and m, we have

$$\begin{aligned}|\mathcal{L}_{n,m}(A,B,C,D,E,F;s)| \ll & (ABC)^{\frac{4}{5}}(\log(ABC))^{\frac{7}{5}} + (AB+BC+CA)(\log(ABC))^3 \\ & + (ABC)^{\frac{3}{5}}(\log(ABC))^{\frac{14}{5}}\left(\frac{\log(ABCDEF)}{\log\log(ABCDEF)}\right)^2.\end{aligned}$$

The above bound is uniform in s. Therefore observe that from Theorem 0.2.1, the number of distinct squarefree s such that $\Delta_{n,m}(a,b,c) = sr^2$ for some integer r is $\gg T_{ABC}$, where

$$\begin{aligned}T_{ABC} = \min\Bigg\{ & \frac{(ABC)^{1/5}}{(\log(ABC))^{7/5}},\ \frac{A}{(\log(ABC))^3},\ \frac{B}{(\log(ABC))^3},\ \frac{C}{(\log(ABC))^3}, \\ & \frac{(ABC)^{2/5}}{(\log(ABC))^{14/5}}\left(\frac{\log\log(ABCDEF)}{\log(ABCDEF)}\right)^2\Bigg\}.\end{aligned}$$

Case (ii):

Since in this case a, b, c, k and m are fixed, so let us denote $D(n) := T_{n,m,k}(a,b,c)$.

Theorem 0.2.2. For a squarefree integer s and sufficiently large $N \geq 2$, we have

$$\Big|\{n \in [1,N] \ \Big|\ D(n) = sr^2 \text{ for some integer } r \neq 1\}\Big| \ll N^{\frac{3}{4}+\varepsilon},$$

for any arbitrary $\varepsilon > 0$.

Therefore we have the following consequence :

Corollary 0.2.3. For sufficiently large N and any arbitrary $\varepsilon > 0$, we have

$$\left|\left\{n \in [1, N] \;\middle|\; D(n) \text{ has distinct squarefree parts}\right\}\right| \gg N^{\frac{1}{4}-\varepsilon}.$$

In Chapter 3, we show some applications of *abc-conjecture* on counting square-free values of $T_{n,m,k}(a, b, c)$.

Under the *abc-conjecture* on number fields, we give lower bounds of the number of polynomials $t^n + c(at^k + b)^m \in \mathbb{Z}[t]$, where $k \geq 2$ and degree $n > mk + 1$ is fixed such that :

(I) It is monogenic for the cases $b = 1$ and $m = 1$.

(II) It has Galois group S_p when the degree is $n = p$, for any prime number p.

The above two cases are studied independently. However, these results give an infinite class of monogenic polynomials $t^n + c(at^k + b)^m \in \mathbb{Z}[t]$ having Galois group S_n under *abc-conjecture* on number fields.

Monogenic polynomials: Let K be a number field and $\mathcal{O}_K$ be the ring of integers. Let $K = \mathbb{Q}(\theta)$, where θ has a minimal polynomial $f(x)$ of degree n over the field $\mathbb{Q}$ of rationals. Let D_f and d_K denote the discriminant of $f(x)$ and the discriminant of the number field K, respectively. It is well known that D_f and d_K are related by the following formula:

$$D_f = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 \, d_K. \tag{0.2.1}$$

From Equation (0.2.1), if $D_f = d_K$, then $\mathcal{O}_K = \mathbb{Z}[\theta]$, which means that the set $\{1, \theta, \cdots, \theta^{n-1}\}$ forms an integral basis of K. In this case, we say that the polynomial $f(x)$ is monogenic.

In 1998, A. Granville [23] made a connection between *abc-conjecture* and squarefree values of polynomials, which is known to be true unconditionally for polynomials of degrees 2 and 3. Later, H. Pasten [70] made use of *abc-conjecture* on number fields to give an asymptotic formula for square-free values of polynomials at prime arguments. To count polynomials $t^n + c(at^k + b)^m \in \mathbb{Z}[t]$, which are

monogenic or have Galois group S_n , we will make use of *abc-conjecture* for number fields. We have used Pasten's result in the form given by L. Jones and D. White [44] to prove the following results :

Denote by S the following set,

$$S := \{(a,b,c) \mid A \leq |a| \leq 2A,\ B \leq |b| \leq 2B,\ C \leq |c| \leq 2C\}.$$

Theorem 0.2.4. For sufficiently large C, we have

$$\big|\{(a,b,c) \in S \mid \ c \text{ and } T_{n,m,k}(a,b,c) \text{ are square-free}\}\big| \gg \frac{ABC}{\log C}, \tag{0.2.2}$$

provided $k \leq 3$. Moreover, for $k \geq 4$, (0.2.2) holds under the *abc-conjecture* on number fields.

Consider the following sets

$$\mathcal{N}_{n,m,k}(A,C) := \{(|a|,|c|) \in [A,2A] \times [C,2C] \mid \gcd(n,k) = 1,\ t^n + c(at^k+1)^m \text{ is monogenic}\},$$

$$\mathcal{N}_{n,k}(A,B,C) := \{(|a|,|b|,|c|) \in [A,2A]\times[B,2B]\times[C,2C] \mid \gcd(n,k) = 1,\ t^n+act^k+bc \text{ is monogenic}\},$$

and

$\mathcal{N}_{S_q}(A,B,C) := \{(|a|,|b|,|c|) \in [A,2A] \times [B,2B] \times [C,2C] \mid \gcd(q,k) = 1, \text{ and } t^q + c(at^k + b)^m \text{ has Galois group } S_q\}$.

Theorem 0.2.5. For all sufficiently large C, we have

$$\big|\mathcal{N}_{n,m,k}(A,C)\big| \gg \frac{AC}{\log C}, \tag{0.2.3}$$

provided $k \leq 3$. Furthermore, (0.2.3) holds for $k \geq 4$ under the *abc-conjecture* on number fields.

Theorem 0.2.6. For all sufficiently large C , we have

$$\big|\mathcal{N}_{n,k}(A,B,C)\big| \gg \frac{ABC}{\log C}, \tag{0.2.4}$$

provided $k \leq 3$. Furthermore, (0.2.4) holds for $k \geq 4$ under the *abc-conjecture* on number fields.

Theorem 0.2.7. For all sufficiently large C and any prime number q, we have

$$\left|\mathcal{N}_{S_q}(A, B, C)\right| \gg \frac{ABC}{\log C}, \tag{0.2.5}$$

provided $k \leq 3$. Furthermore, (0.2.5) holds for $k \geq 4$ under the *abc-conjecture* on number fields.

In this chapter, we also show that if n (≥ 3), m, and k are fixed odd integers, then there exists a positive portion of tuples (a, b, c) for which $T_{n,m,k}(a, b, c)$ is squarefree under *abc-conjecture*.

For sufficiently large positive real numbers A, B, and C, let $D(A, B, C)$ denote the number of square-free integers d that have at least one solution to

$$d = T_{n,m,k}(a, b, c), \text{ where } (a, b, c) \in S \text{ and } \gcd(nb, acmk(n - mk)) = 1. \tag{0.2.6}$$

By estimating a mean lower bound and mean-square upper bound of a certain sum and using the Cauchy-Schwarz inequality, we derived the following theorem.

Theorem 0.2.8. Let A, B, and C be sufficiently large positive real numbers such that $B > (AC)^{1+\delta}$ for some fixed $\delta > 0$, and let n (≥ 3), m, and k be odd integers. If we assume the truth of the *abc-conjecture*, then

$$D(A, B, C) \gg ABC.$$

The implied constant may depend upon n, m, and k.

Chapter 1

Newton Polygon and Irreducibility

1.1 Introduction

The study of irreducibility of polynomials is an important area of research in algebra and number theory. A polynomial is said to be irreducible over a given field or ring if it cannot be factored into two non-constant polynomials with coefficients in that field or ring. Like prime numbers in rational integers or prime ideals in the ring of integers, irreducible polynomials play a fundamental role in polynomial rings. In the middle of the nineteenth century, Eisenstein provided a classical tool to check the irreducibility of a polynomial over $\mathbb{Q}$ by examining the prime factorization of the coefficients of the polynomial in the ring $\mathbb{Z}[X]$ (known as the Schönemann–Eisenstein criteria). In a sequence of successive papers [73-76], I. Schur established the irreducibility and computed the associated Galois group of the truncated exponential in $\mathbb{Q}[X]$ of the form

$$a_n \frac{X^n}{n!} + a_{n-1} \frac{X^{n-1}}{(n-1!)} + \cdots + a_1 X + a_0.$$

Here $a_0, a_1, \cdots, a_n$ are rational integers with $|a_n| = |a_0| = 1$.

He proved this result by considering the prime ideal factorization of the principal ideal generated by

the coefficients of the polynomial $f(x)$ in the field generated by a suitable root of $f(x)$, where

$$f(x) = n! \left(\sum_{j=0}^{n} a_j \frac{X^j}{j!} \right).$$

G. Dumas [13] introduced the concept of the Newton polygon for the product of two polynomials at the beginning of the twentieth century. It is considered one of the major tools to provide irreducibility criteria for a major class of polynomials. It is worth mentioning that Schur did not utilize the work of Dumas [13] on Newton polygon, which was already known at that time.

Almost 58 years later, R. F. Coleman [12] reproved the result of Schur by making use of the Newton polygon for $a_n = a_{n-1} = \cdots = a_0 = 1$. Later in 1995, while proving the Grosswald conjecture on the irreducibility of Bessel polynomials, M. Filaseta [19] re-established Schur's theorem regarding the irreducibility of truncated exponential polynomials using the work of Dumas, for $a_1, \cdots, a_{n-1}$ arbitrary rational integers with $a_n = \pm 1$ and $a_0 = \pm 1$. When $a_j = (-1)^j \binom{n}{j}$ for all $j = 0, \cdots, n$, the truncated exponential is known as the classical Laguerre polynomial $L_{n,0}(x)$. The generalized Laguerre polynomials are defined as follows:

$$L_{n,\alpha}(x) = \sum_{j=0}^{n} \frac{(n+\alpha)(n+\alpha-1)\cdots(j+1+\alpha)}{(n-j)!j!}(-x)^j,$$

where α is an arbitrary real number. Also $L_{n,\alpha}(x)$ satisfies the second order linear (hyper-geometric) differential equation

$$x\frac{d^2y}{dx^2} + (\alpha + 1 - x)\frac{dy}{dx} + ny = 0.$$

Schur showed that $L_{n,1}(x)$ is irreducible for all positive integers n and the associated Galois group is A_n (alternating group) if $n > 1$ is an odd integer or $n + 1$ is a square of an odd integer, and S_n (symmetric group), otherwise. Showing the irreducibility of generalized Laguerre polynomials is a very interesting problem. This problem has been widely studied by several authors, corresponding to various values of α. A brief history of the developments in this direction is in order. In 1995, F. Hajir [24] showed that $L_{n,\alpha}(x)$ are irreducible for $\alpha = -n - 2$. In 2002, Filaseta and Trifonov [20]

showed the irreducibility of $L_{n,\alpha}(x)$ for $\alpha = -2n-1$, which in turn confirms a conjecture of Grosswald on the irreducibility of Bessel polynomials. In the same year, Filaseta and Lam [21] proved that for any fixed non-negative rational numbers α, there are finitely many $L_{n,\alpha}(x)$ that are reducible, more precisely there is an effectively computable $N(\alpha)$ such that $L_{n,\alpha}(x)$ are irreducible for all $n \geq N(\alpha)$. After that in 2004, [77] E. A. Sell showed the irreducibility of generalized Laguerre polynomials for $\alpha = -n-3$. For $\alpha = -1-n-r$, Hajir and Wong [25] proved $L_{n,\alpha}(x)$ is irreducible when r is large with respect to $n \geq 5$. In this area, some recent studies have been conducted by S. Laishram, S. G. Nair, and T. N. Shorey (cf. [52], [55], [65] and [66]).

Furthermore, we can extend this generalized Laguerre polynomial by changing the polynomial variable x to $\phi(x)$, for any $\phi(x) \in \mathbb{Z}[X]$. In chapter 1 of this thesis, we will address the irreducibility over rational numbers of such extended Laguerre polynomials for some special values of α. For any $\phi(x) \in \mathbb{Z}[X]$ and $\alpha \in \mathbb{R}$, we define generalized ϕ-Laguerre polynomial by

$$L^{\phi}_{n,\alpha}(x) = \frac{1}{n!}\left(a_n(x)\phi(x)^n + \sum_{j=0}^{n-1} b_j a_j(x)\phi(x)^j\right)$$

where $b_j = \binom{n}{j} \prod_{i=j+1}^{n} (i+\alpha)$ for $0 \leq j \leq n-1$, and $a_j(x) \in \mathbb{Z}[X]$ with deg $a_j <$deg ϕ.

In this chapter, we shall prove the following theorems :

Let $\alpha \in \mathbb{Q} \setminus \mathbb{Z}^-$ be fixed such that $\alpha = \frac{u}{v}$ with $\gcd(u,v) = 1$, $v > 0$. Let $\phi(x)$ belonging to $\mathbb{Z}[x]$ be a monic polynomial which is irreducible modulo all the primes less than or equal to $vn + |u|$ and $a_n = a_n(x)$ be a constant polynomial. Also assume that the content of $(a_n a_0(x))$ is not divisible by any prime less than or equal to $vn + |u|$. Then we have :

Theorem 1.1.1. The polynomials $L^{\phi}_{n,\alpha}(x)$ are irreducible over $\mathbb{Q}$ for all but finitely many positive integers n.

Theorem 1.1.2. The polynomials $L^{\phi}_{n,\alpha}(x)$ are irreducible over $\mathbb{Q}$ for $\alpha \in \{0,1,2,3,4\}$ unless $(n,\alpha) \in \{(1,0),(2,2),(4,4),(6,4)\}$.

The above Theorem 1.1.2 gives rise to a wide class of irreducible polynomials whose irreducibility does not seem to follow from the known irreducibility criterion (cf. [6], [8], [34], [35], [39], [40], [49] and [50]).

1.2 Valuation on a Field

Definition 1.2.1. A valuation on a field K is a function

$$v : K \to \Gamma \cup \{\infty\},$$

where Γ is a totally ordered abelian group (e.g., $\mathbb{Z}$ or $\mathbb{R}$), satisfying the following properties for all $x, y \in K$:

1. $v(x) = \infty$ if and only if $x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(x + y) \geq \min\{v(x), v(y)\}$.

Examples.

1. Let $K = \mathbb{Q}$. For any non-zero $a \in \mathbb{Q}$ and a prime number p, we can always write

$$a = p^m \frac{b}{c}$$

for some integers b, c and m such that $\gcd(p, bc) = 1$. Define a map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ as $v_p(a) = m$ and put $v_p(0) = \infty$. The map v_p satisfies the properties (1)-(3). It is called *p-adic* valuation of $\mathbb{Q}$. Let $|.|$ denote the usual absolute value on $\mathbb{Q}$. Then the map $v_\infty : \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$ defined by $v_\infty(a) = -\log |a|$, is also a valuation on $\mathbb{Q}$. It is called an Archimedean valuation of $\mathbb{Q}$. The celebrated Ostrowski's theorem says that every valuation on $\mathbb{Q}$ is equivalent to a constant multiple of one of the standard valuations discussed above.

2. Let K be a number field (i.e., a finite extension of $\mathbb{Q}$) and $\mathcal{O}_K$ be the ring of integers of K. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$. For any non-zero element α in $\mathcal{O}_K$, let $v_{\mathfrak{p}}(\alpha)$ denote the highest power $\mathfrak{p}$ in the prime ideal factorization of $\alpha\mathcal{O}_K$ and $v_{\mathfrak{p}}(0) = \infty$. Then clearly, $v_{\mathfrak{p}}$ satisfies the properties (1)-(3). Since K is the field of fractions of $\mathcal{O}_K$, hence $v_{\mathfrak{p}}$ gives rise to a valuation of K.

3. Let v be a valuation on a field K. Denote the set $\mathcal{O} = \{x \in K |\ v(x) \geq 0\}$ (valuation ring) and $\mathcal{O}^*$ be its unit group. Let $\Gamma = K^*/\mathcal{O}^*$, then Γ is a totally ordered group under the order $x \bmod \mathcal{O}^* \geq y \bmod \mathcal{O}^*$ if $x/y \in \mathcal{O}$. The function $w : K \to \Gamma \cup \{\infty\}$ defined by $w(0) = \infty$, $w(x) = x \bmod \mathcal{O}^*$, is also a valuation on K. It is called a *Krull* valuation on the field K.

The following proposition provides an extension of a valuation v on K to a valuation on $K(x)$.

Proposition 1.2.2. Let $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation on a field K and c be any real number. Suppose the map $\tilde{v_c} : K[x] \to \mathbb{R} \cup \{\infty\}$ is defined by

$$\tilde{v_c}(\sum_i b_i x^i) = \min_i\{v(b_i) + ic\},$$

where $b_i \in K$. Then $\tilde{v_c}$ gives rise to a valuation on the function field $K(x)$ by the rule

$$v_c\left(\frac{f}{g}\right) = \tilde{v_c}(f) - \tilde{v_c}(g) \quad \text{when } f, g \in K[x]$$

The restriction on K of $\tilde{v_c}$ is v and also its value group is the subgroup of $\mathbb{R}$, generated by $v(K)$ and c.

Proof. See [71, Sec. 3.1] □

We now introduce the Newton polygon method as a tool to approach the irreducibility problem.

1.3 Newton Polygon (of a Polynomial in $\mathbb{Z}[x]$)

For a prime p, let v_p denote the *p-adic* valuation (as defined in the example) of $\mathbb{Q}$. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

be a polynomial satisfying $a_0 a_n \neq 0$. To each coefficient a_{n-i} of f, we associate a point $(j, v_p(a_{n-j}))$ in the extended $\mathbb{R}^2$ plane. Consider the edges of the lower convex hull of the set of points

$$S = \big\{(0, v_p(a_n)), (1, v_p(a_{n-1})), \cdots, ((j, v_p(a_{n-j})), \cdots, (n, v_p(a_0))\big\}.$$

More precisely, the edges of the convex hull satisfy the following properties:

• The left-most edge begins from the point $(0, v_p(a_n))$ and the right-most edge has $(n, v_p(a_0))$ as an endpoint.

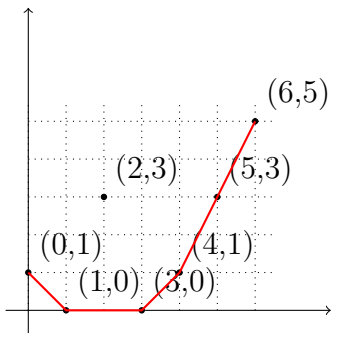
• The endpoints of each edge belong to the set S.

• If $(i, v_p(a_i))$ and $(k, v_p(a_k))$ are two endpoints of an edge, then every point $(j, v_p(a_j))$ with $i < j < k$ lies on or above the line passing through $(i, v_p(a_i))$ and $(k, v_p(a_k))$.

The polygonal path formed by these edges is called *Newton polygon* (NP) of f with respect to the prime p. By the construction of a Newton polygon, it is noticeable that slopes of the edges are increasing from left to right.

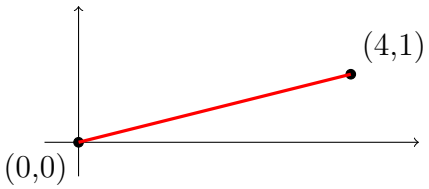
Examples.

1. Consider the polynomial $f(x) = 2x^6 + 3x^5 + 8x^4 + x^3 + 6x^2 + 8x + 32$. Then the Newton polygon of f (with respect to 2) consists of 4 edges. The Left-most edge starts from $(0, 1)$ and ends at $(1, 0)$. Other two edges are from $(1, 0)$ to $(3, 0)$ and from $(3, 0)$ to $(4, 1)$ respectively. The right-most edge starts from $(4, 1)$ and ends at $(6, 5)$ with a lattice point $(5, 3)$.



NP of $f(x) = 2x^6 + 3x^5 + 8x^4 + x^3 + 6x^2 + 8x + 32$ (with respect to 2).

2. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ be an Eisenstein polynomial, which means there exists a prime number p, such that $v_p(a_n) = 0$, $v_p(a_0) = 1$ and $v_p(a_i) \geq 1$ for all $i = 1, \cdots, n-1$. Then the Newton polygon of f (with respect to p) is single edged of slope $\frac{1}{n}$, with endpoints $(0,0)$ and $(n,1)$.

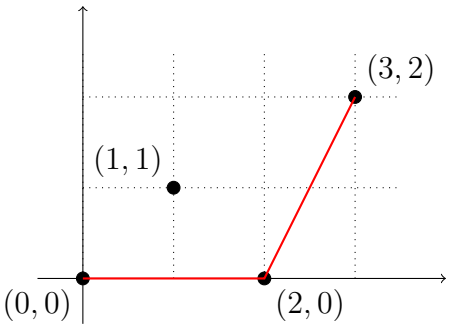


NP of an Eisenstein polynomial of degree 4.

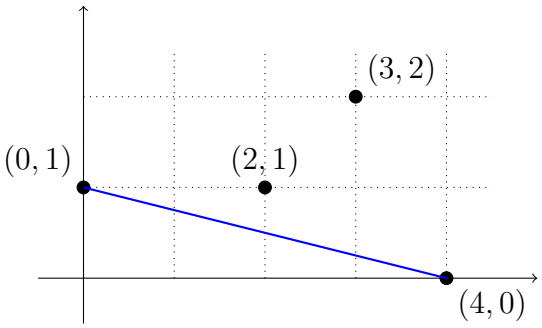
Let $f(x)$ and $g(x)$ are two polynomial in $\mathbb{Z}[x]$. The following result of G. Dumas [13] gives an idea how to construct a Newton polygon of the product $f(x)g(x)$ from the Newton polygon of $f(x)$ and $g(x)$.

Lemma 1.3.1. (Dumas, 1906) Let $f(x)$ and $g(x)$ be two polynomial in $\mathbb{Z}[x]$ with non-zero constant terms and *p-adic* valuation of the leading coefficient of $f(x)g(x)$ is ℓ. Then the Newton polygon of $f(x)g(x)$ with respect to p can be formed by constructing a polygonal path beginning from $(0, \ell)$ and using translates of the edges in the newton polygon of $f(x)$ and $g(x)$ with respect to p, using exactly one translate for each of the Newton polygons for $f(x)$ and $g(x)$. Indeed, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing.

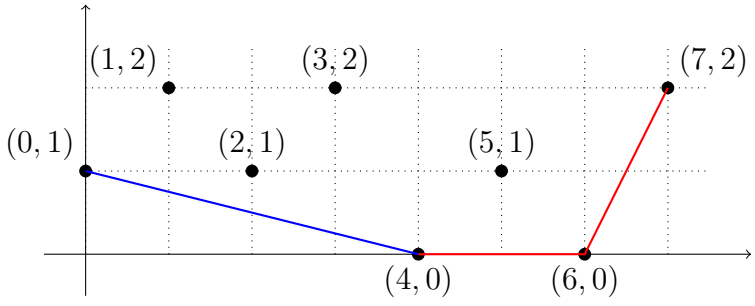
Example. Consider the polynomials $f(x) = x^3 + 6x^2 + 8x + 18$ and $g(x) = 3x^4 + 15x^2 + 9x + 10$. The Newton polygon of $f(x) = x^3 + 6x^2 + 8x + 18$ with respect to 3 has 2 edges. The left-most edge is from $(0,0)$ to $(2,0)$, with slope 0. The right-most edge has endpoints $(2,0)$ and $(3,2)$, with slope 2. The Newton polygon of $g(x) = 3x^4 + 15x^2 + 9x + 10$ has a single edge with endpoints $(0,1)$ and $(4,0)$. Its slope is $-1/4$. Then by Dumas, the Newton Polygon of the product $f(x)g(x)$ can be constructed by adjoining the edges of the Newton polygon of $f(x)$ and $g(x)$ one by one in their increasing order of slopes. The Newton Polygon of the product $f(x)g(x)$ consists of 3 edges (because of the 3 different slopes of the edges of the Newton Polygons of $f(x)$ and $g(x)$) starting from $(0,1)$.



NP of $x^3 + 6x^2 + 8x + 18$ (with respect to 3).



NP of $3x^4 + 15x^2 + 9x + 10$ (with respect to 3).



NP of $(x^3 + 6x^2 + 8x + 18)(3x^4 + 15x^2 + 9x + 10)$, (with respect to 3)

We can prove Eisenstein criteria from Lemma 1.3.1. Let $f(x) \in \mathbb{Z}[x]$ is an Eisenstein polynomial with respect to a prime p. Suppose $f(x) = g(x)h(x)$, for some two non-constant polynomials $g(x), h(x) \in \mathbb{Z}[x]$, then by Lemma 1.3.1 the Newton polygon of $f(x)$ must be translates of edges of the Newton polygon of $g(x)$ and $h(x)$. Since the Newton polygon of $f(x)$ with respect to p has single edge, therefore that edge must have at least one lattice point other than the endpoints, which is not possible. Hence $f(x)$ must be irreducible.

A beautiful application of Dumas' results was made by M. Filaseta in 1995 [19]. It concerns the degree of the factors of a polynomial by looking at the slope of the rightmost edge of its Newton polygon.

Lemma 1.3.2. (Filaseta, 1995) Let $f(x) = \sum_{j=0}^{n} b_j x^j$ be a polynomial in $\mathbb{Z}[x]$, k, and ℓ be integers with $k > \ell \geq 0$. Suppose there exists a prime p such that $v_p(b_n) = 0$, $v_p(b_j) \geq 1$ for all $j \in \{0, 1, \cdots, n - (\ell + 1)\}$, and the slope of the right-most edge of the Newton polygon of $f(x)$ with respect to p is $< 1/k$. Then for any integers $a_0, a_1, \cdots, a_n$ with $|a_0| = |a_n| = 1$, the polynomial $g(x) = \sum_{j=0}^{n} a_j b_j x^j$ cannot have a factor whose degree lies in the interval $[\ell + 1, k]$.

Proof. The condition $|a_0| = |a_n| = 1$, implies that the left and right-most endpoints of the Newton polygon of $g(x)$ with respect to p is same as the left and right-most endpoints of the Newton polygon of $f(x)$, respectively. Note that $v_p(a_j b_j) \geq v_p(b_j)$ for all $j \in \{0, 1, \cdots, n\}$. Thus the Newton polygon of $g(x)$ lies exactly on or above the Newton polygon of $f(x)$ with some common edges. Also since the right-most endpoints of these Newton polygons are same, therefore the slope of the right-most edge of the Newton polygon of $g(x)$ is less than or equal to the slope of the right-most edge of Newton polygon of $f(x)$ which is $< 1/k$. Also $v_p(a_n b_n) = 0$, $v_p(a_j b_j) \geq 1$ for all $j \in \{0, 1, \cdots, n - (\ell + 1)\}$. Hence, without loss of generality, to prove the lemma, it is sufficient to show that $f(x)$ cannot have a factor with degree lies in the interval $[\ell + 1, k]$.

On the contrary, suppose there exist two polynomials $u(x)$ and $v(x)$ with integer coefficients such that $f(x) = u(x)v(x)$ and $\ell + 1 \leq \deg(u) \leq k$. Since the slopes of the edges of a Newton polygon are in increasing order from left to right and $v_p(b_n) = 0$, therefore the left-most edge of the Newton polygon of $f(x)$ may have a zero slope. Let (a, b) and (c, d) be two lattice points on an edge having a

non-zero slope. By the condition of the lemma, we have

$$\frac{1}{|c-a|} \leq \frac{|d-b|}{|c-a|} < \frac{1}{k}.$$

This implies $|c-a| > k$, which means x-coordinate of such lattices is separated by a distance greater than k. Again $\deg(u) \leq k$, this implies the translates of the edges of the Newton polygon of $u(x)$ do not lie within those edges of the Newton polygon of $f(x)$ with non-zero slope. Therefore, the left-most edge of the Newton polygon of $f(x)$ must have zero slope, and the length of this edge is $\geq \deg(u) \geq \ell + 1$. But $v_p(b_{n-j}) \geq 1$, for all $j \in \{\ell+1, \ell+2, \cdots, n\}$. So the left-most edge with slope 0 must be of length $\leq \ell$, this gives a contradiction, and the proof follows.

□

Remark 1.3.3. Observe that the slope of the right-most edge can be calculated by the following expression,

$$\max_{1 \leq j \leq n} \left\{ \frac{v_p(b_0) - v_p(b_j)}{j} \right\}.$$

The concept of Newton Polygon can be further generalized to a ϕ-Newton polygon, by changing the variable x to any monic polynomial $\phi(x) \in \mathbb{Z}[x]$. This was introduced by Ø. Ore [68] in 1928.

1.4 ϕ-Newton Polygon

We denote v_p^x, the Gaussian valuation extending v_p defined on $\mathbb{Z}[x]$ by $\tilde{v_c}$ in Proposition 1.2.2 for $c = 0$, i.e.,

$$v_p^x(\sum_i b_i x^i) = \min_i \{v_p(b_i)\}, b_i \in \mathbb{Z}.$$

Before defining ϕ-Newton polygon with respect to the valuation v_p^x , we shall recall what is ϕ-expansion of a polynomial in $\mathbb{Z}[x]$.

Definition 1.4.1. Let $\phi(x) \in \mathbb{Z}[x]$ be a fixed monic polynomial, then any $f(x) \in \mathbb{Z}[x]$ can be uniquely written as a finite sum $\sum_i b_i(x)\phi(x)^i$ with $\deg b_i(x) < \deg \phi(x)$ for each i. This expansion is called the

ϕ-expansion of $f(x)$.

For example, let $f(x) = x^5 + x + 1$ and $\phi(x) = x^2 - 1$. The ϕ-expansion of $f(x)$ is $x\phi(x)^2 + 2x\phi(x) + (2x + 1)$.

The ϕ-Newton polygon is defined as follows:

Definition 1.4.2. Let p be a prime number and $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial. Let $f(x)$ belonging to $\mathbb{Z}[x]$ be a polynomial having ϕ-expansion $\sum_{i=0}^{n} b_i(x)\phi(x)^i$ with $b_0(x)b_n(x) \neq 0$. Let P_i stand for the point in the plane having coordinates $(i, v_p^x(b_{n-i}(x)))$ when $b_{n-i}(x) \neq 0$, $0 \leq i \leq n$. Let μ_{ij} denote the slope of the line joining the points P_i and P_j if $b_{n-i}(x)b_{n-j}(x) \neq 0$. Let i_1 be the largest index $0 < i_1 \leq n$ such that

$$\mu_{0i_1} = \min\{\mu_{0j} \mid 0 < j \leq n,\ b_{n-j}(x) \neq 0\}.$$

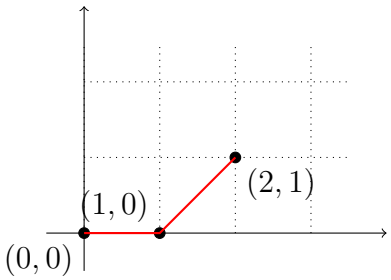
If $i_1 < n$, let i_2 be the largest index $i_1 < i_2 \leq n$ such that

$$\mu_{i_1 i_2} = \min\{\mu_{i_1 j} \mid i_1 < j \leq n,\ b_{n-j}(x) \neq 0\}$$

and so on. The ϕ-Newton polygon of $f(x)$ with respect to p is the polygonal path having segments $P_0P_{i_1}, P_{i_1}P_{i_2}, \ldots, P_{i_{k-1}}P_{i_k}$ with $i_k = n$. These segments are called the edges of the ϕ-Newton polygon of $f(x)$ and their slopes from left to right, form a strictly increasing sequence.

Example.

Let $f(x) = x^4 + x^3 + x^2 + x + 1$, $\phi(x) = x^2 - 1$ and $p = 3$, the ϕ-expansion of $f(x)$ is $x^2\phi(x)^2 + x\phi(x) + (2x + 3)$. Therefore the set of coordinates are $(0, v_3^x(x^2)) = (0, 0)$, $(1, v_3^x(x)) = (1, 0)$ and $(2, v_3^x(2x + 3)) = (2, 1)$. The ϕ-Newton polygon is given in the picture below.



ϕ-NP of $f(x) = x^4 + x^3 + x^2 + x + 1$, with respect to $\phi(x) = x^2 - 1,\ p = 3$

The following lemma is a generalization of Lemma 1.3.2.

Proposition 1.4.3. Let n, k and ℓ be integers, with $0 \leq \ell < k \leq n/2$ and p be a prime. Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial which is irreducible modulo p. Let $f(x)$ belonging to $\mathbb{Z}[x]$ be a monic polynomial not divisible by $\phi(x)$ having ϕ-expansion $\sum_{i=0}^{n} f_i(x)\phi(x)^i$ with $f_n(x) \neq 0$. Assume that $v_p^x(f_i(x)) > 0$ for $0 \leq i \leq n - \ell - 1$ and the right-most edge of the ϕ-Newton polygon of $f(x)$ with respect to p has slope less than $1/k$. Let $a_0(x), a_1(x), \ldots, a_n(x)$ be polynomials over $\mathbb{Z}$ satisfying the following conditions.

(i) $\deg a_i(x) < \deg \phi(x) - \deg f_i(x)$ for $0 \leq i \leq n$,

(ii) $v_p^x(a_0(x)) = 0$, i.e., the content[1] of $a_0(x)$ is not divisible by p,

(iii) the leading coefficient of $a_n(x)$ is not divisible by p.

Then the polynomial $\sum_{i=0}^{n} a_i(x)f_i(x)\phi(x)^i$ does not have a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[(\ell+1)\deg\phi, (k+1)\deg\phi)$.

Proof. See [41]. □

[1] means g.c.d of all the coefficients

1.5 Irreducibility of Generalized ϕ-Laguerre Polynomials

Recall that the generalized ϕ-Laguerre polynomial defined in the introduction section is given by

$$L_{n,\alpha}^{\phi}(x) = \frac{1}{n!}\left(a_n(x)\phi(x)^n + \sum_{j=0}^{n-1} b_j a_j(x)\phi(x)^j\right)$$

where $b_j = \binom{n}{j}\prod_{i=j+1}^{n}(i+\alpha)$ for $0 \leq j \leq n-1$, and $\phi(x),\ a_j(x) \in \mathbb{Z}[X]$ with deg $a_j <$deg ϕ.

Before writing the proof of Theorem 1.1.1 and 1.1.2, we first state some lemmas that are needed for the proof. We skip their proofs.

To study the irreducibility of generalized ϕ-Laguerre polynomial, it is necessary to assume the following hypothesis :

(i) The content of $(a_n a_0(x))$ is not divisible by any prime less than or equal to $vn + |u|$.

(ii) $a_n(x)$ must be a constant polynomial.

Otherwise, we can create reducible polynomials $L_{n,\alpha}^{\phi}(x)$ over $\mathbb{Q}$ as given below :

We take $\phi(x) = x^2 - x + 17$ and $n = 2$,

α	a_2	$a_1(x)$	$a_0(x)$	$L_{n,\alpha}^{\phi}(x)$
1	3	1	-4	$\frac{3}{2}(\phi(x)+4)(\phi(x)-2)$
2	1	1	-4	$\frac{1}{2}(\phi(x)-4)(\phi(x)+12)$
3	1	1	-10	$\frac{1}{2}(\phi(x)-10)(\phi(x)+20)$
4	3	1	-6	$\frac{3}{2}(\phi(x)+10)(\phi(x)-6)$

Table 1.1: The content of $a_0(x)$ is divisible by 2.

α	a_2	$a_1(x)$	$a_0(x)$	$L_{m,\alpha}^{\phi}(x)$
1	6	2	1	$3(\phi(x)+1)^2$

2	4	1	-1	$2(\phi(x)+3)(\phi(x)-1)$
3	2	1	-5	$(\phi(x)+10)(\phi(x)-5)$
4	18	1	-1	$(\phi(x)-1)(9\phi(x)+15)$

Table 1.2: a_2 is divisible by 2.

Also if $a_n(x)$ is not a constant, then consider $\phi(x) = x^2 - x + 5$, which is irreducible modulo 2 and 3. Take $a_2(x) = x - 3 = a_1(x) = a_0(x)$. Therefore the polynomial $\frac{1}{2}(a_2(x)\phi(x)^2 + 2(2+\alpha)a_1(x)\phi(x) + (2+\alpha)(1+\alpha)a_0(x))$ has 3 as a root for each $\alpha \in \{0, 1, 2, 3, 4\}$.

The following lemma is proved in [3, Theorem 3].

Lemma 1.5.1. Let a and b be fixed relatively prime integers with $b > 0$, and let $\pi(x; b, a)$ denote the number of primes $\leq x$ which are congruent to $a \pmod{b}$. If $b \leq (\log x)^A$ for some fixed $A > 0$ and $x^{\frac{11}{20}+\varepsilon} \leq h \leq \frac{x}{\log x}$, then

$$\pi(x; b, a) - \pi(x - h; b, a) \gg \frac{h}{\varphi(b) \log x} \quad \text{for every } \varepsilon > 0.$$

The following lemma is an immediate consequence of Corollary 1.2 of [80].

Lemma 1.5.2. Let a, b, c and d be integers with $bc - ad \neq 0$. Then the largest prime factor of $(an + b)(cn + d)$ tends to infinity as the integer n tends to infinity.

Lemma 1.5.3. For integers n and k with $n \geq k \geq 2$, let $P(n, k)$ denote the product $(n + 1)(n + 2) \cdots (n + k)$. For $t \geq 1$, define S_t as the set of pairs (n, k) for which $n \geq k \geq 2$ and the largest prime factor of $P(n, k)$ is $k + t$. Then

$$S_1 = \{(2, 2), (7, 2)\}, \quad S_2 = \{(3, 3), (7, 3), (5, 5)\},$$

$$S_3 = \{(3, 2), (4, 2), (8, 2), (14, 2), (23, 2), (79, 2), (4, 4), (5, 4), (6, 4)\},$$

and

$$S_4 = \{(4,3),(5,3),(6,3),(13,3),(47,3)\}.$$

It may be pointed out that, in the above lemma, for every $(n,k) \notin S_1 \cup S_2 \cup \cdots \cup S_{t-1}$ with $n \geq k \geq 2$, the largest prime factor of $P(n,k)$ is $\geq k+t$.

The proof of the above lemma relies on a method due to Lehmer [56] (for classifying all the cases where $(n+1)(n+2)$ has all its prime factors bounded below by a prescribed bound) and a result of Ecklund et. al. [14].

The next lemma concerns the solutions of certain equations. The assertion (i) is a special case of Catalan's conjecture, now Mihailescu's theorem, when $r > 1$, $s > 1$ (see [61]). The case $r = 1$ or $s = 1$ is immediate. The assertions (ii) and (iii) are due to Nagell [64]. For assertions $(iv) - (vi)$, see [51, Lemma 4].

Lemma 1.5.4. Let $r > 0, s > 0, t > 0$ be integers. The solutions of the following equations are given by

	Equations	Solutions
(i)	$a^r - b^s = \pm 1, a, b \in \{2,3,5\}$	$3-2=1, 2^2-3=1, 5-2^2=1, 3^2-2^3=1$
(ii)	$2^r + 3^s = 5^t$	$2+3=5, 2^4+3^2=5^2$
(iii)	$2^r + 5^s = 3^t$	$2+1=3, 2+25=27, 4+5=9, 8+1=9$
(iv)	$2^r 3^s - 5^t = \pm 1$	$2\cdot 3-5=1, 2^3\cdot 3-5^2=-1$
(v)	$3^r 5^s - 2^t = \pm 1$	$3\cdot 5-2^4=-1$
(vi)	$2^r 5^s - 3^t = \pm 1$	$2\cdot 5-3^2=1, 2^4\cdot 5-3^4=-1$

1.6 Proof of Theorems 1.1.1 and 1.1.2

Proof of Theorem 1.1.1. Let us fix an $\alpha \in \mathbb{Q}$ which is not a negative integer, say $\alpha = \frac{u}{v}$ with $\gcd(u,v) = 1$ and $v > 0$. It is enough to prove that $f(x) = a_n \phi(x)^n + \sum_{j=0}^{n-1} b_j a_j(x) \phi(x)^j$ is irreducible over the rationals for sufficiently large n.

We first show that $f(x)$ does not have a non-constant factor over $\mathbb{Z}$ with degree less than $\deg \phi(x)$. Let p be a prime number that divides $vn+u$. Then by hypothesis, it follows that $p \nmid a_n$. Let c denote the content of $f(x)$. As $p \nmid a_n$, we have $p \nmid c$. Now suppose, on the contrary, that there exists a primitive non-constant polynomial $h(x) \in \mathbb{Z}[x]$ dividing $f(x)$ having degree less than $\deg \phi(x)$. Then in view of Gauss Lemma, there exists $g(x) \in \mathbb{Z}[x]$ such that $\frac{f(x)}{c} = h(x)g(x)$. The leading coefficient of $f(x)$ and hence those of $h(x)$ and $g(x)$ are coprime with p. Note that p divides b_j for $0 \le j \le n-1$. Therefore on passing to $\mathbb{Z}/p\mathbb{Z}$, we see that the degree of $\bar{h}(x)$ is same as that of $h(x)$. Hence $\deg \bar{h}(x)$ is positive and less than $\deg \phi(x)$. Also note that $\bar{h}(x)$ is a divisor of $\frac{\bar{f}(x)}{\bar{c}} = \frac{\bar{a}_n}{\bar{c}}\bar{\phi}(x)^n$. Therefore $\bar{h}(x)$ must divide $\bar{\phi}(x)$. This is not possible since $\bar{\phi}(x)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$.

Now using Proposition 1.4.3, we shall show that for $k \in [1, \frac{n}{2}]$ and sufficiently large n, $f(x)$ cannot have a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[k \deg \phi(x), (k+1) \deg \phi(x))$. For using Proposition 1.4.3, we consider the polynomial $g(x) = \sum_{j=0}^{n} b_j \phi(x)^j$ with $b_n = 1$. Keeping in mind that α is not a negative integer, implies that for each $j \in \{0, 1, \cdots, n-1\}$, $n - j + \alpha$ and hence $v(n-j)+u$ cannot be zero. We assume that $g(x)$ has a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[\deg \phi(x), (\frac{n}{2} + 1) \deg \phi(x))$ and prove our theorem by obtaining a contradiction to Proposition 1.4.3.

We divide the proof into cases depending on the size of k with $1 \le k \le n/2$.

Case (i): $n^{\frac{11}{20}+\varepsilon} < k \le \frac{n}{2}$, where $\varepsilon > 0$ is an arbitrary small constant.

By considering $\pi(x; b, a) - \pi(x-h; b, a)$, it follows from Lemma 1.5.1 that for a and b fixed, the interval $[x-h, x)$ contains a prime congruent to a modulo b if $h \ge x^{\frac{11}{20}+\varepsilon}$ for all sufficiently large x. Taking $a = u$, $b = v$ and $x = vn+u$, we deduce that for some integer $j \in [0, k)$, the number $v(n-j)+u$ is prime. Call such a prime p, and observe that $p \ge 2vn/3$ (since v is a positive integer and n is large). It follows that p does not divide v. Observe that

$$b_\ell = \binom{n}{\ell} \frac{(vn+u)(v(n-1)+u)\cdots(v(\ell+1)+u)}{v^{n-\ell}} \quad \text{for } 0 \le \ell \le n-1.$$

Clearly

$$v_p(b_\ell) \ge 1 \quad \text{for } 0 \le \ell \le n-k. \tag{1.6.1}$$

The slope of the right-most edge of the ϕ- Newton polygon of $g(x)$ with respect to p is

$$\lambda := \max_{1\le j\le n}\left(\frac{v_p(b_0)-v_p(b_j)}{j}\right).$$

Keeping in mind that $v_p(b_n)=0$, to obtain a contradiction from Proposition 1.4.3 for the case under consideration, we need to show that $\lambda < \frac{1}{k}$. For this purpose, it is enough to show that $v_p(b_0)=1$, because it follows from (1.6.1), the fact $k \le n-k$ that $v_p(b_j) \ge 1 > 1-(j/k)$ for $1 \le j \le k$, and clearly $v_p(b_j) > 1-(j/k)$ for $k < j \le n$.

To show $v_p(b_0)=1$, it can be easily checked using the fact $p \ge 2vn/3$ and n sufficiently large, that

$$2p > vn+u \ge v(n-j)+u \ge v+u > -p \quad \text{for} \quad 0 \le j \le n-1.$$

As indicated earlier, none of the $v(n-j)+u$ can be zero. Hence, p itself is the only multiple of p among the number $v(n-j)+u$ with $0 \le j \le n-1$. Since $p \nmid v$ and $b_0 = ((vn+u)(v(n-1)+u)\cdots(v+u))/v^n$, we obtain $v_p(b_0)=1$. Hence, for n sufficiently large, $f(x)$ cannot have a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[k\deg\phi(x),(k+1)\deg\phi(x))$ for $n^{\frac{11}{20}+\varepsilon} < k \le \frac{n}{2}$.

Case (ii): $k_0 \le k \le n^{\frac{11}{20}+\varepsilon}$ with $k_0 = k_0(u,v)$ a sufficiently large integer.

We wish to show that $f(x)$ does not have a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[k\deg\phi(x),\ (k+1)\deg\phi(x))$ for $k \in [k_0, n^{\frac{11}{20}+\epsilon}]$.

Let $z = k\sqrt{\log k}$. We claim that there is a prime $p > z$ that divides $v(n-j)+u$ for some $j \in \{0,1,2....,k-1\}$. Then (1.6.1) follows as before, and we will obtain a contradiction to Proposition 1.4.3 by showing $v_p(b_j) > v_p(b_0)-(j/k)$ for $1 \le j \le n$ as this implies the slope of the right-most edge of the ϕ-Newton polygon of $g(x)$ with respect to p has slope $< 1/k$.

Let

$$T = \{v(n-j)+u : 0 \le j \le k-1\}.$$

Since n is large, we deduce that each elements of T is greater than or equal to $n/2$. Also, observe

that $\gcd(u,v)=1$ implies that each element of T is relatively prime to v. For each prime $p\le z$, we consider an element $a_p\in T$ with $v_p(a_p)$ as large as possible. Then we consider the set

$$S=T-\{a_p : p\nmid v,\ p\le z\}.$$

Clearly $|S|\ge k-\pi(z)$. By the well-known Chebyshev bound, we have $|S|\ge k-\frac{2k}{\sqrt{\log k}}$.

Consider the prime $p\le z$ with p not dividing v, and let $r=v_p(a_p)$. By definition of a_p, if $j>r$, then there are no multiples of p^j in T (and hence, in S). For $1\le j\le r$, there are less than or equal to $[k/p^j]+1$ multiples of p^j in T and, hence, at most $[k/p^j]$ multiples of p^j in S. Therefore,

$$v_p\Big(\prod_{s\in S} s\Big)\le \sum_{j=1}^{r}\left[\frac{k}{p^j}\right]\le v_p(k!),$$

and hence

$$\prod_{s\in S}\prod_{p\le z} p^{v_p(s)}\le k!\le k^k. \tag{1.6.2}$$

On the other hand using the fact that $k\le n^{\frac{11}{20}+\varepsilon}$, we see that

$$\prod_{s\in S} s\ge\left(\frac{n}{2}\right)^{|S|}\ge\left(\frac{k^{\frac{29}{20}-\varepsilon}}{2}\right)^{|S|}.$$

Recalling our bound on $|S|$, we obtain

$$\begin{aligned}\log\left(\prod_{s\in S} s\right)&\ge\left(k-\frac{2k}{\sqrt{\log k}}\right)\left(\left(\frac{29}{20}-\varepsilon\right)\log k-\log 2\right)\\&\ge k\log k+\left(\frac{9}{20}-\varepsilon\right)k\log k+O(k\sqrt{\log k}).\end{aligned}$$

Since $k\ge k_0$ where k_0 is sufficiently large and using (1.6.2), we have

$$\log\left(\prod_{s\in S} s\right)>k\log k\ge\log\left(\prod_{s\in S}\prod_{p\le z} p^{v_p(s)}\right).$$

It follows that there is a prime $p > z$ that divides some element of S and, hence, divides some element of T. This proves our claim.

Fix a prime $p > z$ that divides an element in T. Fix $j \in \{1, 2, ..., n\}$. It only remains to show that $v_p(b_0) - v_p(b_j) < \frac{j}{k}$. Observe that

$$\begin{aligned} v_p(b_0) - v_p(b_j) &\leq v_p((vj+u)(v(j-1)+u)\cdots(v+u)) \\ &\leq v_p((vj+|u|)!) < \frac{vj+|u|}{p-1}. \end{aligned}$$

Since $p > z = k\sqrt{\log k}$ and $k \geq k_0$, we deduce that $(vj + |u|)/(p-1) < j/k$ and the inequality $v_p(b_0) - v_p(b_j) < \frac{j}{k}$ follows. Hence, as indicated at the beginning of this case, we obtain a contradiction to Proposition 1.4.3.

Case (iii): $2 \leq k < k_0$.

By Lemma 1.5.2 (with $a = v,\ b = u,\ c = v$, and $d = u - v$), the largest prime factor of the product $(vn+u)(v(n-1)+u)$ tends to infinity. Since n is large, we deduce that there is a prime $p > (v+|u|)k_0$ that divides $(vn+u)(v(n-1)+u)$. The argument now follows as in the previous case. In particular,

$$\frac{v_p(b_0) - v_p(b_j)}{j} < \frac{vj+|u|}{j(p-1)} \leq \frac{v+|u|}{p-1} \leq \frac{1}{k_0} < \frac{1}{k} \quad \text{for } 1 \leq j \leq n.$$

Hence, in this case, we also obtain a contradiction.

Case (iv): $k = 1$.

It only remains to prove that $f(x)$ does not have a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[\deg \phi(x), 2\deg \phi(x))$. This will be achieved once we show that there exists a prime $p > v + |u|$ such that $p|b_j$ for $0 \leq j \leq n-1$. If $u = 0$, then it is always true for $n \geq 2$. Hence we can assume that $u \neq 0$. In this situation, from Lemma 1.5.2, the largest prime factor of $n(vn+u)$ tends to infinity with n. We consider a large prime factor p of this product. Note that this implies $p \nmid v$. As in the previous case, we are through if p divides $vn + u$. So suppose $p|n$. The binomial coefficient $\binom{n}{j}$ appears in the

definition of b_j, and this is sufficient to guarantee that $v_p(b_j) \geq 1$ and $v_p(b_{n-j}) \geq 1$ for $1 \leq j \leq p-1$. On the other hand,

$$b_j = \binom{n}{j} \frac{(vn+u)(v(n-1)+u)\cdots(v(j+1)+u)}{v^{n-j}}.$$

For $j \leq n-p$, the numerator of the fraction on the right is a product of $\geq p$ consecutive terms in the arithmetic progression $vt+u$ with $\gcd(p,v)=1$; thus, $v_p(b_{n-j}) \geq 1$ for $j \geq p$. This implies that (1.6.1) holds with $k=1$. It follows, along the lines of the previous two cases, that $v_p(b_0) - v_p(b_j) < \frac{j}{k}$ for $1 \leq j \leq n$. A contradiction to Proposition 1.4.3 is again obtained.

Therefore combining Cases (i)-(iv), we have shown that for $k \in [1, \frac{n}{2}]$ and sufficiently large n, $f(x)$ cannot have a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[k \deg \phi(x), (k+1)\deg \phi(x))$. This completes the proof of the theorem. □

Proof of Theorem 1.1.2: Since $\alpha \in \{0,1,2,3,4\}$, we have $u \in \{0,1,2,3,4\}$ and $v=1$. We define $f(x)$ and $g(x)$ as we did in the proof of Theorem 1.1.1. As there always exists a prime p dividing $n+u$ except $(n,u)=(1,0)$, it follows from the second paragraph of the proof of Theorem 1.1.2 that $f(x)$ cannot have a non-constant factor over $\mathbb{Z}$ with degree less than $\deg \phi(x)$.

Therefore, it is enough to prove that $f(x)$ does not have a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[k \deg \phi(x), (k+1)\deg \phi(x))$ with $k \in [1, \frac{n}{2}]$ and $n \geq 2$. We divide our remaining proof into two cases depending on whether $k \geq 2$ or $k=1$.

Suppose first that $k \geq 2$ and $n \geq 2$. In the notation of Lemma 1.5.3, observe that $P(n-k+u,k)$ divides b_j for $0 \leq j \leq n-k$. Since $n-k+u \geq n-k \geq k$, Lemma 1.5.3 implies that $P(n-k+u,k)$ has a prime divisor $p \geq k+u+1$ unless

$$(n-k+u,k) \in S = S_1 \cup S_2 \cup \cdots \cup S_u, \tag{1.6.3}$$

where S_i is as given in Lemma 1.5.3 for $1 \leq i \leq 4$. We first assume that $(n-k+u,\ k) \notin S$ and fix a prime p with $p \geq k+u+1$ as above. Since p divides $P(n-k+u,k)$, we have p divides b_j for $0 \leq j \leq n-k$. We wish to point here that if there exists a prime $p \geq u+2$ with $p|b_j$ with $0 \leq j \leq n-1$, then all the following arguments will work even for $k=1$. By hypothesis $p \nmid b_n$. For using Proposition

1.4.3, we are left with verifying that the slope of the right-most edge of the ϕ-Newton polygon of $g(x)$ with respect to p has slope $< \frac{1}{k}$ for $k \geq 2$. The slope of the right-most edge is given by

$$\max_{1 \leq j \leq n} \left\{ \frac{v_p(b_0) - v_p(b_j)}{j} \right\}.$$

Observe that

$$\frac{b_0}{b_j} = \frac{(j+u)(j-1+u)\cdots(1+u)}{\binom{n}{j}}. \tag{1.6.4}$$

It follows that

$$v_p(b_0) - v_p(b_j) \leq v_p((j+u)(j-1+u)\cdots(1+u)) \leq v_p((j+u)!).$$

If $j \leq k$, then $p \geq k+u+1$ implies that $v_p(b_0) - v_p(b_j) \leq 0$. If $j > k$, then using the simple inequality $(j+\alpha)/(k+\alpha) < j/k$, we obtain

$$v_p(b_0) - v_p(b_j) \leq v_p((j+\alpha)!) < \frac{j+\alpha}{p-1} \leq \frac{j+\alpha}{k+\alpha} < \frac{j}{k}.$$

We combine the above to deduce, as desired, that the right-most edge has slope $< \frac{1}{k}$. Hence, using Proposition 1.4.3, $f(x)$ cannot a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[k \deg \phi(x), (k+1)\deg \phi(x))$ with $k \in [2, \frac{n}{2}]$, unless $(n-k+u, k) \in S$. Now suppose $(n-k+u, k) \in S$. The following table provides us all the exceptional cases corresponding to each u with $2k \leq n$.

u	(n,k)
1	$(8,2)$
2	$(7,2), (8,3)$
3	$(6,2), (7,3), (7,2), (13,2), (22,2), (78,2)$
4	$(5,2), (6,2), (12,2), (21,2), (77,2), (6,3), (12,3), (46,3)$

For all these pairs (n,k) except for $(n,k,u) \in \{(6,2,4), (6,3,4)\}$, we now provide a prime number

p (see the following tables) such that p divides b_j for $0 \leq j \leq n-k$ and the right-most edge has slope $< \frac{1}{k}$, and hence we are done for all these cases in view of Proposition 1.4.3.

u	k	n	p
1	2	8	7
2	2	7	7
2	3	8	7
3	2	6	5
3	3	7	7
3	2	7	7

u	k	n	p
3	2	13	13
3	2	22	7
3	2	78	7
4	2	5	11
4	2	6	$--$
4	2	12	11

u	k	n	p
4	2	21	7
4	2	77	7
4	3	6	$--$
4	3	12	11
4	3	46	23

Now we deal with the case when $k = 1$, $n \geq 2$. We divide this case into five sub-cases according to the values of u. We first recall, as pointed out in the previous case, that if there exists a prime $p \geq u+2$ such that $p|b_j$ for $0 \leq j \leq n-1$, then we are done in this case in view of Proposition 1.4.3.

Subcase (i) $u = 0$. In this situation, note that $k+u+1 = 2$ and there is clearly a prime $p \geq 2$ dividing n for $n \geq 2$ and hence, in view of Proposition 1.4.3, $f(x)$ cannot have a factor in $\mathbb{Z}[x]$ with degree lying in the interval $[\deg \phi(x), 2\deg \phi(x))$. So, we are done.

Subcase (ii) $u = 1$. This subcase follows by observing that there always exists a prime $p \geq 3 (= u+2)$ dividing $n(n+1)$ for $n \geq 2$.

Subcase (iii) $u = 2$. Observe that $n(n+2)$ always divides b_j for $0 \leq j \leq n-1$ for $n \geq 3$. Note that $n = 2$ is an exceptional case. Keeping in mind Lemma 1.5.4, one can easily verify that there always exists a prime $p \geq 5$ dividing $n(n+2)$ unless $n \in \{4, 6, 16\}$.

Let $n \in \{4, 6, 16\}$. We set $p = 2$ or 3 according as $n \in \{4, 16\}$ or $n = 6$. One can easily check that p divides b_j for $0 \leq j \leq n-1$. Keeping in mind Equation (1.6.3), one can check that the right-most edge of the ϕ-Newton polygon of $g(x)$ with respect to p has slope < 1. Thus we are done in view of Proposition 1.4.3.

Subcase (iv) $u = 3$. Note that $n(n+3)$ always divides b_j for $0 \leq j \leq n-1$ for $n \geq 2$. Keeping in mind Lemma 1.5.4, it can be easily seen that there always exists a prime $p \geq 5$ dividing $n(n+3)$ unless

$n \in \{3, 6, 9, 24\}$.

If $n \in \{3, 6, 9, 24\}$, then one can check that 3 divides b_j for $0 \leq j \leq n-1$ and the right-most edge of the ϕ-Newton polygon of $g(x)$ with respect to 3 has slope < 1. So, using again Proposition 1.4.3, we are done.

Subcase (v) $u = 4$. Using Lemma 1.5.4, it can be verified that there always exists a prime $p \geq 7$ dividing $n(n+4)$, and hence b_j, for $0 \leq j \leq n-1$ unless $n \in \{2, 4, 5, 8, 12, 16, 20, 32, 36, 60, 96, 320\}$.

Consider $p = 3$ if $n \in \{2, 8, 12, 32, 36, 96\}$, $p = 2$ if $n = 16$, and $p = 5$ if $n \in \{5, 20, 60, 320\}$. One can check that p divides b_j for $0 \leq j \leq n-1$ and the right-most edge of the ϕ-Newton polygon of $g(x)$ with respect to p has slope < 1. Therefore, using Proposition 1.4.3, we are done.

This completes the proof of the theorem. □

1.7 Short Notes on Other Classical Families of Polynomials

There are also many other families of classical polynomials like Laguerre polynomials, among them Bernoulli, Bessel, and Hermite polynomials play a central role due to their deep connections with number theory, approximation theory, and orthogonal polynomial systems.

Bernoulli polynomials. The Bernoulli polynomials $B_n(x)$ are defined by the generating function

$$\frac{te^{tx}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!} \in \mathbb{Q}[x][[t]].$$

They satisfy $B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}x^k$, where $B_m = B_m(0)$, $m \geq 0$ are the Bernoulli numbers. Some integral formulas of Bernoulli polynomials are related to special values of the Riemann zeta function. It is conjectured that $B_n(x)$ is irreducible over $\mathbb{Q}$ for every even $n \geq 2$. For odd $n \geq 5$, the polynomial $B_n(x)$ has factors, namely x, $x - 1/2$ and $x - 1$, therefore one studies the irreducibility of $B_n(x)/(x(x-1)(x-1/2))$. Several authors (Carlitz [10]- [11], McCarthy [58]- [60], Adelberg [1]- [2], etc.) establish irreducibility for infinitely many cases of n and for various higher-order Bernoulli polynomials, although full irreducibility is still open in general.

Bessel polynomials. For any integer $n \geq 0$, the Bessel polynomials $y_n(x)$ are defined by

$$y_n(x) = \sum_{k=0}^{n} \frac{(n+k)!}{(n-k)!k!} \left(\frac{x}{2}\right)^k.$$

They arise in solutions of Bessel-type differential equations $x^2y'' + 2(x+1)y' - n(n+1)y = 0$. These polynomials are orthogonal (in L^2 -sense) with respect to the weight $w(x) = e^{-2/x}$ on the unit circle. Emil Grosswald initiated the systematic study of the irreducibility of the Bessel polynomials and conjectured that $y_n(x)$ is irreducible over $\mathbb{Q}$ for all n. A celebrated result of Filaseta [19] shows that all but finitely many Bessel polynomials are irreducible over $\mathbb{Q}$. In fact, subsequent work of Filaseta and Trifonov [20] proves that $y_n(x)$ is irreducible for every $n \geq 1$, supported by Newton polygon arguments, confirming the earlier conjecture of E. Grosswald.

Hermite polynomials. The Hermite polynomials $H_n(x)$ are defined by

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}, \quad n \geq 0.$$

$\{H_n(x)\}_{n\geq 0}$ forms an orthogonal system in $L^2(\mathbb{R})$ with respect to the weight function $w(x) = e^{-x^2}$. Hermite polynomials are related to generalized Laguerre polynomials (for $\alpha = \pm\frac{1}{2}$) by the relation $H_{2n}(x) = (-1)^n 2^{2n} n!\, L_{n,-\frac{1}{2}}(x^2)$, and $H_{2n+1}(x) = (-1)^n 2^{2n+1} n!\, x\, L_{n,\frac{1}{2}}(x^2)$. These polynomials are known to be irreducible over $\mathbb{Q}$ for all $n \geq 0$, except that $H_{2n+1}(x)$ has the trivial factor x. The classical work of I. Schur ([74], [76]) showed that $H_{2n}(x)$ is irreducible over $\mathbb{Q}$ for all $n \geq 1$, and also $H_{2n+1}(x)/x$ is irreducible except for $n = 12$. Modern results extend this irreducibility to generalized Hermite-Laguerre families (cf. [52]- [54]) .

While the irreducibility of Bessel and Hermite polynomials is now well understood, the complete resolution of irreducibility for Bernoulli polynomials remains an open problem, supported by strong heuristic and computational evidence. One may investigate the irreducibility of a more general ϕ-version of these types of polynomials by the Newton polygon method.

Chapter 2

Square-free Parts of Discriminants

2.1 Introduction

The study of when a polynomial takes squarefree values is a rich and deep area of study in number theory. Especially in analytic number theory, it is often of interest to find an asymptotic formula for

$$\sum_{\tilde{n}\leq x} \mu^2(f(\tilde{n})),$$

where $f : \mathbb{N}^r \to \mathbb{N}$ is a certain arithmetic function, and μ is Möbius function. This sum essentially counts the number of r-tuples of positive integers $\tilde{n} = (n_1, \ldots, n_r)$ (with $n_i \leq x$) such that $f(\tilde{n})$ is squarefree. We will now review the existing literature related to this problem.

We begin with a classical example of the density of squarefree numbers. In 1885, Gegenbauer [22] proved the following asymptotic formula,

$$\sum_{n\leq x} \mu^2(n) = \frac{6}{\pi^2}x + O(x^{1/2}).$$

Another example is due to Estermann [17], where he considered the polynomial $f(t) = t^2 + 1$ and proved that for $x \geq 2$,

$$\sum_{n\leq x}\mu^2(n^2+1)=\prod_{p\equiv 1(\text{mod } 4)}\left(1-\frac{2}{p^2}\right)x+O(x^{2/3}\log x).$$

After 80 years, Heath-Brown [29] improved the error term using a variant of the determinant method, obtaining $O(x^{7/12+\varepsilon})$.

Let $f(t)\in\mathbb{Z}[t]$ be a non-constant, separable polynomial. It is natural to ask whether $f(n)$ takes infinitely many squarefree values for $n\in\mathbb{Z}$. For the linear case, i.e., $an+b$ takes infinitely many squarefree values provided $\gcd(a,b)$ is squarefree, is well known. If the degree of the polynomial is 2, then it can be proven using the sieve of Eratosthenes. Further, when the degree is 3, C. Hooley (see [31] and [32, Chapter 4]) showed that $f(n)$ takes infinitely many squarefree values. In fact, we can provide asymptotic results for these.

For higher degree polynomials (especially those that are irreducible) the situation becomes far more subtle and intriguing.

A stronger conjecture by V. Bunyakovsky states that if $f(t)\in\mathbb{Z}[t]$ is an irreducible polynomial over $\mathbb{Q}$ with a positive leading coefficient and $\gcd\{f(n)|n\in\mathbb{Z}\}=1$, then $f(n)$ takes infinitely many prime values for $n\in\mathbb{Z}$. For linear polynomials, it follows from Dirichlet theorem on primes in arithmetic progression. For polynomials of degree greater than 1, the conjecture remains unproven and open.

In 1932, Carlitz [9] proved the following asymptotic formula about consecutive squarefree integers (i.e., for the polynomial $f(t)=t(t+1)$),

$$\sum_{n\leq x}\mu^2(n)\mu^2(n+1)=\prod_{p}\left(1-\frac{2}{p^2}\right)x+O(x^{2/3+\varepsilon}).$$

In 1984, Heath-Brown [28] used his *square sieve* method and improved the above error term by obtaining $O(x^{7/11+\varepsilon})$. In 2012, for the case $r=2$ (i.e., f with two variables), Tolev [83] shows the following asymptotic formula (although the formula was previously known, he improved the error bound):

$$\sum_{n_1,n_2\leq x}\mu^2(n_1^2+n_2^2+1)=\prod_{p}\left(1-\frac{\rho(p^2)}{p^4}\right)x^2+O(x^{4/3+\epsilon}),$$

where $\rho(\ell)$ is the number of solutions $1 \leq x, y \leq \ell$, such that $x^2 + y^2 + 1 \equiv 0 \pmod{\ell}$.

The discriminant of a polynomial $f(X) = X^r + a_1 X^{r-1} + \cdots + a_r$ with integer coefficients is also a polynomial in the variables $(a_1, \ldots, a_r)$. Therefore, it is interesting to determine the number of r-tuples of positive integers $(a_1, \ldots, a_r)$ for which the discriminant is square-free or has distinct square-free parts.

In 2012, Kedlaya [48] developed a method to exhibit infinitely many (monic irreducible) polynomials with squarefree discriminants of prescribed degree ≥ 2. Recently, Bhargava et al. [5] showed that when monic integer polynomials $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ of degree n are ordered by $H(f) = \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}$, the density of polynomials with squarefree discriminants exists and equals $\lambda_n > 0$, where λ_n is defined as the limit as $R \to \infty$ (which exists) of the number of such polynomials with $H(f) \leq R$ and squarefree discriminants, divided by the number of polynomials with $H(f) \leq R$. Furthermore, they showed that $\lim_{n\to\infty} \lambda_n$ exists and $\lim_{n\to\infty} \lambda_n = \lambda \approx 0.307056$.

Let $\Delta_{n,m,k}(a, b, c)$ be the discriminant of the monic irreducible polynomial $f(t) = t^n + c(at^k + b)^m$ of degree n, with coefficients from the ring $\mathbb{Z}$ of integers and $\gcd(n, k) = 1$. It is known from Theorem 1.1 of [36] that:

$$\Delta_{n,m,k}(a, b, c) = (-1)^{\binom{n}{2}} b^{m(n+k-1)-n} c^{n-1} \left[n^n b^{n-mk} + (-1)^{n+mk+k+1} a^n c^k (mk)^{mk} (n - mk)^{n-mk} \right].$$

Let us denote

$$T_{n,m,k}(a, b, c) = n^n b^{n-mk} + (-1)^{n+mk+k+1} a^n c^k (mk)^{mk} (n - mk)^{n-mk}. \tag{2.1.1}$$

In this chapter, we investigate the problem of distinct squarefree parts of the values taken by $T_{n,m,k}(a, b, c)$. This analysis is carried out for two distinct cases :

(i) We determine the number of tuples (a, b, c) for which $T_{n,m,k}(a, b, c)$ have distinct squarefree parts, where n and m are fixed odd integers and $k = 1$.

(ii) We determine the number of integers n for which $T_{n,m,k}(a,b,c)$ has distinct squarefree parts, where a, b, c, k, and m are fixed.

To be precise, we will provide only the lower bounds of such numbers. Theorem 2.4.1 is concerned with case (i) and Theorem 2.4.6 addresses the case (ii).

In this direction, in 2010, Shparlinski [78] provided a quantitative lower bound on the number of distinct quadratic fields generated by discriminants of irreducible trinomials $t^n + at + b$ with integer coefficients $(a,b) \in [C, C+A] \times [D, D+B]$, for arbitrary positive real numbers A, B, C, D. He showed that the number of such distinct quadratic fields is at least a positive multiple of

$$\min\left\{\frac{(AB)^{1/3}}{(\log(AB))^{4/3}}, \frac{A}{(\log(AB))^2}, \frac{B}{(\log(AB))^2}, (AB)^{2/3}\left(\frac{\log\log(ABCD)}{\log(ABCD)\log(AB)}\right)^2\right\}.$$

He [79] also obtained a lower bound on the number of distinct squarefree parts of discriminants of the trinomials $t^n - t - 1$ in 2014. In the next year, Boyd, Martin, and Thom [7] showed that the set of positive integers n such that $n^n + (-1)^n(n-1)^{n-1}$ (which is the discriminant of the trinomial $t^n - t - 1$) is squarefree has an asymptotic upper density of 0.99344679 and conjectured that the exact density should be approximately 0.9934466, correct to that many decimal places.

Remark. If $m = k = 1$, $a = b = -1$, and $c = 1$, then our polynomial $t^n + c(at^k + b)^m$ reduces to the trinomial $t^n - t - 1$, and Theorem 2.4.6 extends the main result of [78].

Notation:

Let p be an odd prime. The *Legendre symbol* $\left(\frac{\cdot}{p}\right)$ on integers is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a square modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$

$\left(\frac{\cdot}{p}\right)$ is a character on $\mathbb{F}_p^*$ (see example 2 in the section characters of finite abelian group).

Definition 2.1.1. (Jacobi Symbol): Let a be an integer and n be a positive odd integer with prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where each p_i is an odd prime. The *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined as:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

where $\left(\frac{a}{p_i}\right)$ denotes the Legendre symbol.

To prove Theorem 2.4.1 and 2.4.6, we make use of the *square sieve* technique. This elementary method was introduced in a paper of Heath-Brown [28]. Its aim is to estimate how many squares are contained in a particular set of integers. We shall provide a brief overview of this technique.

2.2 The Square Sieve

Let $\mathcal{X}$ a finite set of non zero integers and $\mathcal{P}$ be a set of primes ≥ 3. Denote

$$S(\mathcal{X}) := \#\{x \in \mathcal{X} : x \text{ is a square}\} \text{ and } w_{\mathcal{P}}(x) = \sum_{\substack{p \in \mathcal{P} \\ p|x}} 1.$$

Then we have

$$S(\mathcal{X}) \leq \frac{\#\mathcal{X}}{\#\mathcal{P}} + \max_{\substack{p,q \in \mathcal{P} \\ p \neq q}} \left| \sum_{x \in \mathcal{X}} \left(\frac{x}{pq}\right) \right| + O\left(\frac{1}{\#\mathcal{P}} \sum_{x \in \mathcal{X}} w_{\mathcal{P}}(x) + \frac{1}{(\#\mathcal{P})^2} \sum_{x \in \mathcal{X}} w_{\mathcal{P}}(x)^2 \right). \tag{2.2.1}$$

It follows from the simple fact that, if x is square then

$$\sum_{p \in \mathcal{P}} \left(\frac{x}{p}\right) = \#\mathcal{P} - w_{\mathcal{P}}(x).$$

This implies

$$S(\mathcal{X})(\#\mathcal{P})^2 \leq \sum_{x\in\mathcal{X}} \left(\sum_{p\in\mathcal{P}} \left(\frac{x}{p}\right) + w_{\mathcal{P}}(x) \right)^2 .$$

After squaring and interchanging the sums, one can find the required inequality 2.2.1.

2.3 Characters of Finite Abelian Group

Let G be an abelian group of finite order. A *character* χ of G is a group homomorphism from G into $\mathbb{C}^*$. Since G is finite, the image $\chi(G)$ is contained in $\mathbb{S}^1$ (unit circle). Also note that, the values of χ are exactly $|G|$-th roots of unity. The trivial character χ_0 on G is defined by $\chi_0(g) = 1$ for all $g \in G$.

Examples.

1. Let G be a cyclic group of order n and g be a generator of G. Then its characters are χ_j for all $j = 0, \cdots, n-1$, where

$$\chi_j(g^k) = e^{2\pi ijk/n}, \quad k = 0, 1, \ldots, n-1.$$

2. For an odd prime p, consider the group $G = \mathbb{F}_p^*$ (*i.e.*, $\mathbb{F}_p \setminus \{0\}$). Let $\chi_p : \mathbb{F}_p^* \to \{\pm 1\} \subset \mathbb{C}^\times$ be defined by $\chi_p(a) = 1$ if a is a square modulo p and $\chi_p(a) = -1$, otherwise. It is easy to check that χ_p is a character of $\mathbb{F}_p^*$.

Lemma 2.3.1. Let χ be a nontrivial character of a finite abelian group G, then

$$\sum_{g\in G} \chi(g) = 0.$$

Proof. Since χ is nontrivial, let g' be an element of G such that $\chi(g') \neq 1$. Also if g runs through G, then so is gg'. Therefore we have

$$\left(\sum_{g\in G} \chi(g) \right) \chi(g') = \sum_{g\in G} \chi(gg') = \sum_{g\in G} \chi(g).$$

Since $\chi(g') \neq 1$, thus we get $\sum_{g \in G} \chi(g) = 0$. □

Let p be an odd prime and $\mathbb{F}_q$ be a finite field of characteristic p. Let χ be a nontrivial character on the additive group $\mathbb{F}_q$. Consider the sum of the form

$$\sum_{a \in \mathbb{F}_q} \chi(f(a)),$$

where $f \in \mathbb{F}_q[x]$ is any non-constant polynomial. The sum is zero by Lemma 2.3.1 when f is linear. In general, it is difficult to find its value explicitly. But we can give an upper bound of this sum, which is trivially q. Since χ is nontrivial character, it is quite natural to expect that the sum is much smaller than q. The following lemma (which is a theorem due to André Weil) provides a nontrivial upper bound of the sum.

Lemma 2.3.2 (André Weil)**.** Let $f \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree n such that $\gcd(n, q) = 1$ and if χ be a nontrivial character of $\mathbb{F}_q$, then

$$\left| \sum_{a \in \mathbb{F}_q} \chi(f(a)) \right| \leq (n-1) q^{\frac{1}{2}}.$$

Proof. See [57, Theorem 5.38]. □

The next lemma is a well-known result on quadratic Gauss sums [33, Chapter 3, Sec 3.5].

Lemma 2.3.3. For any integer $k \geq 1$, we have

$$\sum_{\ell=1}^{k} \mathbf{e}_k(\ell^2) = \theta_k k^{\frac{1}{2}},$$

where $\mathbf{e}_k(z) := e^{\frac{2\pi i z}{k}}$ and the constant θ_k is given by

$$\theta_k = \begin{cases} (1+i) & \text{if } k \equiv 0 \pmod 4, \\ 1 & \text{if } k \equiv 1 \pmod 4, \\ 0 & \text{if } k \equiv 2 \pmod 4, \\ i & \text{if } k \equiv 3 \pmod 4. \end{cases}$$

Note that if k is any odd prime, then $|\theta_k| = 1$.

Lemma 2.3.4. For any integer α not divisible by a prime $p > 2$, we have

$$\sum_{\ell=1}^{p} \left(\frac{\ell}{p}\right) \mathbf{e}_p(\alpha\ell) = \theta_p p^{\frac{1}{2}} \left(\frac{\alpha}{p}\right).$$

Proof. Since $\gcd(\alpha, p) = 1$, by substituting $\ell \mapsto \alpha\ell$ we get

$$\begin{aligned} \sum_{\ell=1}^{p} \left(\frac{\ell}{p}\right) \mathbf{e}_p(\alpha\ell) &= \sum_{\ell=1}^{p} \left(\frac{\alpha\ell}{p}\right) \mathbf{e}_p(\alpha^2\ell) \\ &= \left(\frac{\alpha}{p}\right) \sum_{\ell=1}^{p} \left(\frac{\ell}{p}\right) \mathbf{e}_p(\alpha^2\ell). \end{aligned}$$

Note that $\sum_{\ell=1}^{p} \mathbf{e}_p(\alpha^2\ell) = 0$, therefore we have

$$\sum_{\ell=1}^{p} \left(\frac{\ell}{p}\right) \mathbf{e}_p(\alpha\ell) = \left(\frac{\alpha}{p}\right) \sum_{\ell=1}^{p} \left(1 + \left(\frac{\ell}{p}\right)\right) \mathbf{e}_p(\alpha^2\ell). \tag{2.3.1}$$

Also observe that, $1 + \left(\frac{\ell}{p}\right)$ is the number of solutions of $j^2 \equiv \ell \pmod p$. Hence from equality 2.3.1, we obtain

$$\sum_{\ell=1}^{p} \left(\frac{\ell}{p}\right) \mathbf{e}_p(\alpha\ell) = \left(\frac{\alpha}{p}\right) \sum_{j=1}^{p} \mathbf{e}_p(\alpha^2 j^2),$$

and the result follows from Lemma 2.3.3. □

Next we consider a Gauss sum associated to the $\Delta_{n,m}(a,b,c) := T_{n,m,1}(a,b,c)$ (which has already

been defined in the introduction).

For any integer $\ell \geq 2$, consider the Gauss sum

$$S_{n,m}(\ell;\lambda,\mu,\gamma) := \sum_{u,v,w=1}^{\ell} \left(\frac{\Delta_{n,m}(u,v,w)}{\ell}\right) \mathbf{e}_\ell(\lambda u + \mu v + \gamma w),$$

where λ, μ, and γ are arbitrary integers and $\mathbf{e}_\ell(z) := e^{\frac{2\pi i z}{\ell}}$.

It is easy to see that $S_{n,m}(\ell;\lambda,\mu,\gamma)$ is a multiplicative function of ℓ. Therefore, it is natural to investigate its values at odd prime factors of ℓ.

We shall take n and m as odd integers in Lemmas 2.3.5 to 2.3.8.

Lemma 2.3.5. Let p be an odd prime such that $\gcd(p, m(n-m)) = 1$. Then we have

$$S_{n,m}(p;0,0,0) = \left(\frac{n^n}{p}\right) p(p-1).$$

Proof. Let $Y = m^m(m-n)^{m-n}$. By hypothesis, we have $\gcd(p, Y) = 1$. Recall that $\Delta_{n,m}(u,v,w) = n^n v^{n-m} + w u^n Y$. Therefore, we have

$$\begin{aligned} S_{n,m}(p;0,0,0) &= \sum_{u,v,w=1}^{p} \left(\frac{\Delta_{n,m}(u,v,w)}{p}\right) \\ &= \sum_{u,v,w=1}^{p} \left(\frac{n^n v^{n-m} + w u^n Y}{p}\right) \\ &= \sum_{u,w=1}^{p} \sum_{v=1}^{p-1} \left(\frac{n^n v^{n-m} + w u^n Y}{p}\right) + \sum_{u=1}^{p} \left(\frac{u^n Y}{p}\right) \sum_{w=1}^{p} \left(\frac{w}{p}\right). \end{aligned}$$

Keeping in mind that $\sum_{\ell=1}^{p} \left(\frac{\ell}{p}\right) = 0$ (follows from Lemma 2.3.1), we have

$$S_{n,m}(p;0,0,0) = \sum_{u,w=1}^{p} \sum_{v=1}^{p-1} \left(\frac{n^n v^{n-m} + w u^n Y}{p}\right).$$

Since $\gcd(p, v) = 1$, we have used the substitutions $u \mapsto uv$ and $w \mapsto wv^{-m}$. Therefore, we obtain

$$S_{n,m}(p; 0, 0, 0) = \sum_{u,w=1}^{p} \left(\frac{n^n + wu^n Y}{p}\right) \sum_{v=1}^{p-1} \left(\frac{v^{n-m}}{p}\right).$$

Since $n - m$ is even, we have $\left(\frac{v^{n-m}}{p}\right) = 1$. So, we obtain

$$\begin{aligned} S_{n,m}(p; 0, 0, 0) &= \sum_{u,w=1}^{p} \left(\frac{n^n + wu^n Y}{p}\right)(p-1) \\ &= \sum_{w=1}^{p} \sum_{u=1}^{p-1} \left(\frac{n^n + wu^n Y}{p}\right)(p-1) + \left(\frac{n^n}{p}\right)(p-1). \end{aligned}$$

Set $h = n^n + wu^n Y$. Since $\gcd(p, uY) = 1$, then h will range from 1 to p as w runs from 1 to p. Hence,

$$\begin{aligned} S_{n,m}(p; 0, 0, 0) &= \sum_{h=1}^{p} \left(\frac{h}{p}\right)(p-1)^2 + \left(\frac{n^n}{p}\right)(p-1) \\ &= \left(\frac{n^n}{p}\right)(p-1). \end{aligned}$$

This completes the proof. □

We now prove the following result.

Lemma 2.3.6. Let p be an odd prime such that $\gcd(p, \lambda, \mu, \gamma) = 1$ and $\gcd(p, m(n-m)) = 1$. Then

$$S_{n,m}(p; \lambda, \mu, \gamma) = O(p^2).$$

Proof. Set $Y = m^m(m-n)^{m-n}$. Clearly, $\gcd(p, Y) = 1$. Recall that

$$\begin{aligned} S_{n,m}(p; \lambda, \mu, \gamma) &= \sum_{u,v,w=1}^{p} \left(\frac{\Delta_{n,m}(u, v, w)}{p}\right) \mathbf{e}_p(\lambda u + \mu v + \gamma w) \\ &= \sum_{u,v,w=1}^{p} \left(\frac{n^n v^{n-m} + wu^n Y}{p}\right) \mathbf{e}_p(\lambda u + \mu v + \gamma w). \end{aligned}$$

If we separate out the terms for $u = p$ and $v = p$, each of these contributes $O(p^2)$ to the sum

$S_{n,m}(p;\lambda,\mu,\gamma)$. Therefore, we obtain

$$S_{n,m}(p;\lambda,\mu,\gamma)=\sum_{w=1}^{p}\sum_{u,v=1}^{p-1}\left(\frac{n^n v^{n-m}+wu^nY}{p}\right)\mathbf{e}_p(\lambda u+\mu v+\gamma w)+O(p^2).$$

Now, substituting $w\mapsto wv^{n-m}$, we obtain

$$\begin{aligned}S_{n,m}(p;\lambda,\mu,\gamma)&=\sum_{w=1}^{p}\sum_{u,v=1}^{p-1}\left(\frac{n^n+wu^nY}{p}\right)\left(\frac{v^{n-m}}{p}\right)\mathbf{e}_p(\lambda u+\mu v+\gamma wv^{n-m})+O(p^2)\\&=\sum_{w=1}^{p}\sum_{u,v=1}^{p-1}\left(\frac{n^n+wu^nY}{p}\right)\mathbf{e}_p(\lambda u+\mu v+\gamma wv^{n-m})+O(p^2).\end{aligned}$$

The last equality follows from the fact that $n-m$ is even.

Since $\gcd(p,uY)=1$, we set $h=n^n+wu^nY$, and h runs through the complete residue system modulo p. Thus,

$$\begin{aligned}S_{n,m}(p;\lambda,\mu,\gamma)&=\sum_{h=1}^{p}\sum_{u,v=1}^{p-1}\left(\frac{h}{p}\right)\mathbf{e}_p\left(\lambda u+\mu v+\gamma(h-n^n)u^{-n}v^{n-m}Y^{-1}\right)+O(p^2)\\&=\sum_{u,v=1}^{p-1}\left(\sum_{h=1}^{p}\left(\frac{h}{p}\right)\mathbf{e}_p(\gamma u^{-n}v^{n-m}Y^{-1}h)\right)\mathbf{e}_p(\lambda u+\mu v-\gamma n^n u^{-n}v^{n-m}Y^{-1})+O(p^2).\end{aligned}$$

Using Lemma 2.3.4, we obtain

$$\begin{aligned}S_{n,m}(p;\lambda,\mu,\gamma)&=\theta_p p^{\frac{1}{2}}\sum_{u,v=1}^{p-1}\left(\frac{\gamma u^{-n}v^{n-m}Y^{-1}}{p}\right)\mathbf{e}_p(\lambda u+\mu v-\gamma n^n u^{-n}v^{n-m}Y^{-1})+O(p^2)\\&=\theta_p p^{\frac{1}{2}}\sum_{u=1}^{p-1}\left(\frac{\gamma u^{-n}Y^{-1}}{p}\right)\mathbf{e}_p(\lambda u)\sum_{v=1}^{p-1}\mathbf{e}_p(\mu v-\gamma n^n u^{-n}v^{n-m}Y^{-1})+O(p^2).\end{aligned}$$

Since $\gcd(p,n-m)=1$, applying Lemma 2.3.2 to the sum over v, we get

$$\sum_{v=1}^{p-1}\mathbf{e}_p(\mu v-\gamma n^n u^{-n}v^{n-m}Y^{-1})=O(p^{\frac{1}{2}}).$$

Taking the trivial bound on the sum over u, we conclude that

$$S_{n,m}(p;\lambda,\mu,\gamma) = O(p^2).$$

This completes the proof. □

Lemma 2.3.7. Let $\ell = pq$ be the product of two distinct odd prime numbers p and q, with $\gcd(\ell, m(n-m)) = 1$. Then, for any integers λ, μ, and γ, we have

$$S_{n,m}(\ell;\lambda,\mu,\gamma) = O(\ell^2).$$

Proof. Using the multiplicative property of character sums, the proof of this lemma follows from Lemmas 2.3.5 and 2.3.6. □

The next lemma provides an estimate of the character sum over a cuboid.

Lemma 2.3.8. Suppose $\ell = pq$ is the product of two distinct odd primes p and q with $\gcd(\ell, m(n-m)) = 1$. Then, for any positive real numbers A, B, C, and D, we have

$$\sum_{D\le u\le D+A}\sum_{E\le v\le E+B}\sum_{F\le w\le F+C}\left(\frac{\Delta_{n,m}(u,v,w)}{\ell}\right) \ll (\ell^2+AB+BC+CA)(\log\ell)^3 + \frac{ABC}{\ell}.$$

Proof. Observe that if we divide the cuboid $[D, D+A]\times[E, E+B]\times[F, F+C]$ into smaller cubes with side length ℓ, there will be at most $O\left(\frac{ABC}{\ell^3}\right)$ small cubes. From Lemma 2.3.7, the total sum over these small cubes will be $O\left(\frac{ABC}{\ell}\right)$.

After removing the small cubes of side length ℓ, there will be at most $O\left(\frac{AB+BC+CA}{\ell^2}+1\right)$ cuboids remaining inside the original cuboid $[D, D+A]\times[E, E+B]\times[F, F+C]$. The sum over each of these remaining cuboids represents an incomplete sum, which can be approximated by $S_{n,m}(\ell;0,0,0)$ (see [33, Chapter 12]) and therefore the sum will be at most $O(\ell^2(\log\ell)^3)$. Therefore, the total sum over the remaining cuboids is $O\left((\ell^2+AB+BC+CA)(\log\ell)^3\right)$. This completes the proof. □

2.4 Main Theorems

Now we are ready to embark on case (i), which was alluded to in the introduction.

For a fixed square-free integer s and positive real numbers A, B, C, D, E, F, let $\mathcal{L}_{n,m}(A, B, C, D, E, F; s)$ denote the set of all tuples (a, b, c) in $[D, D+A] \times [E, E+B] \times [F, F+C]$ such that $\Delta_{n,m}(a, b, c) = sr^2$ for some integer r.

The following theorem provides an estimate for the number of (a, b, c) in $[D, D+A] \times [E, E+B] \times [F, F+C]$ such that $\Delta_{n,m}(a, b, c) = sr^2$ for a fixed square-free integer s.

Theorem 2.4.1. For sufficiently large positive real numbers $A,\ B,\ C$ and some non-negative real numbers $D,\ E,\ F$, and for a fixed square-free number s, as well as for odd integers n and m, we have

$$\begin{aligned}|\mathcal{L}_{n,m}(A, B, C, D, E, F; s)| \ll & (ABC)^{\frac{4}{5}}(\log(ABC))^{\frac{7}{5}} + (AB + BC + CA)(\log(ABC))^3 \\ & + (ABC)^{\frac{3}{5}}(\log(ABC))^{\frac{14}{5}} \left(\frac{\log(ABCDEF)}{\log\log(ABCDEF)}\right)^2.\end{aligned}$$

Proof. For $z > 3$, let $\mathcal{P}_z$ denote the set of primes $p \in [z, 2z]$, and let $w(d)$ represent the number of prime divisors of d. By the prime number theorem, we have $\#\mathcal{P}_z \gg \frac{z}{\log z}$.

Observe that if d is a perfect square, then

$$\sum_{p \in \mathcal{P}_z} \left(\frac{d}{p}\right) \geq \#\mathcal{P}_z - w(d).$$

Note that if $(a, b, c) \in \mathcal{L}_{n,m}(A, B, C, D, E, F; s)$, then $s\Delta_{n,m}(a, b, c)$ is a perfect square. Therefore, we have

$$\sum_{p \in \mathcal{P}_z} \left(\frac{s\Delta_{n,m}(a, b, c)}{p}\right) \geq \#\mathcal{P}_z - w(s\Delta_{n,m}(a, b, c)) = \#\mathcal{P}_z - w(\Delta_{n,m}(a, b, c)).$$

Applying the Arithmetic Mean-Geometric Mean (AM-GM) inequality, we obtain

$$(\#\mathcal{P}_z)^2 \leq 2\left(\left(\sum_{p \in \mathcal{P}_z} \left(\frac{s\Delta_{n,m}(a, b, c)}{p}\right)\right)^2 + w(\Delta_{n,m}(a, b, c))^2\right).$$

Summing over all tuples $(a,b,c) \in \mathcal{L}_{n,m}(A,B,C,D,E,F;s)$, we get

$$(\#\mathcal{P}_z)^2 \left|\mathcal{L}_{n,m}(A,B,C,D,E,F;s)\right| \ll Z_1 + Z_2, \tag{2.4.1}$$

where

$$Z_1 = \sum_{D\le a\le D+A} \sum_{E\le b\le E+B} \sum_{F\le c\le F+C} \left(\sum_{p\in\mathcal{P}_z} \left(\frac{s\Delta_{n,m}(a,b,c)}{p} \right) \right)^2$$

and

$$Z_2 = \sum_{D\le a\le D+A} \sum_{E\le b\le E+B} \sum_{F\le c\le F+C} w(\Delta_{n,m}(a,b,c))^2.$$

First, we calculate an upper bound for Z_1. Expanding the square term in Z_1 as a product of two sums, and then interchanging the summations, we get

$$\begin{aligned} Z_1 &= \sum_{D\le a\le D+A} \sum_{E\le b\le E+B} \sum_{F\le c\le F+C} \left(\sum_{p\in\mathcal{P}_z} \left(\frac{s\Delta_{n,m}(a,b,c)}{p} \right) \sum_{q\in\mathcal{P}_z} \left(\frac{s\Delta_{n,m}(a,b,c)}{q} \right) \right) \\ &= \sum_{p,q\in\mathcal{P}_z} \left(\frac{s}{pq} \right) \sum_{D\le a\le D+A} \sum_{E\le b\le E+B} \sum_{F\le c\le F+C} \left(\frac{\Delta_{n,m}(a,b,c)}{pq} \right). \end{aligned}$$

We break the double sum over p and q into two parts, Z_1' and Z_2'. Here, Z_1' is the sum when $p=q$, and Z_2' is the sum when $p\neq q$. Taking a trivial bound on Z_1', we have $|Z_1'| \le (\#\mathcal{P}_z)ABC$. Applying Lemma 2.3.8 to the sum Z_2', we obtain

$$|Z_2'| \ll (\#\mathcal{P}_z)^2(z^4+AB+BC+CA)(\log z)^3 + (\#\mathcal{P}_z)^2\frac{ABC}{z^2}.$$

Thus, we conclude

$$Z_1 \ll (\#\mathcal{P}_z)ABC + (\#\mathcal{P}_z)^2(z^4+AB+BC+CA)(\log z)^3 + (\#\mathcal{P}_z)^2\frac{ABC}{z^2}. \tag{2.4.2}$$

Now, we estimate Z_2. It is well-known that $w(d) \ll \frac{\log d}{\log\log d}$ for any large integer d (see [72]). For

$(a,b,c) \in [D, D+A] \times [E, E+B] \times [F, F+C]$, we have

$$\Delta_{n,m}(a,b,c) \ll (A+B+C+D+E+F)^n.$$

Using this bound and the fact that $\frac{\log x}{\log\log x}$ is monotonically increasing, we get

$$w(\Delta_{n,m}(a,b,c)) \ll \frac{\log(A+B+C+D+E+F)}{\log\log(A+B+C+D+E+F)} \ll \frac{\log(ABCDEF)}{\log\log(ABCDEF)}.$$

Therefore,

$$Z_2 \ll ABC\left(\frac{\log(ABCDEF)}{\log\log(ABCDEF)}\right)^2. \tag{2.4.3}$$

Substituting the upper bounds for Z_1 and Z_2 in (2.4.1), and noting that $\#\mathcal{P}_z \gg \frac{z}{\log z}$, we obtain

$$\begin{aligned}|\mathcal{L}_{n,m}(A,B,C,D,E,F;s)| \ll ABC\frac{\log z}{z} + (z^4 + AB + BC + CA)(\log z)^3 \\ + \frac{ABC}{z^2} + ABC\left(\frac{\log(ABCDEF)\log z}{\log\log(ABCDEF)z}\right)^2.\end{aligned} \tag{2.4.4}$$

In (2.4.4), for large A, B, and C, the term $ABC\left(\frac{\log z}{z}\right)$ dominates the term $\frac{ABC}{z^2}$. On taking $z = (ABC)^{\frac{1}{5}}(\log(ABC))^{-\frac{2}{5}}$, we find that both of the terms $ABC\left(\frac{\log z}{z}\right)$ and $z^4(\log z)^3$ are $\ll (ABC)^{\frac{4}{5}}(\log(ABC))^{\frac{7}{5}}$. This proves the theorem. □

Note that the above bound is uniform in s. Therefore we observe that from Theorem 2.4.1, the number of distinct square-free s such that $\Delta_{n,m}(a,b,c) = sr^2$ for some integer r is $\gg T_{ABC}$, where

$$T_{ABC} = \min\left\{\frac{(ABC)^{1/5}}{(\log(ABC))^{7/5}}, \frac{A}{(\log(ABC))^3}, \frac{B}{(\log(ABC))^3}, \frac{C}{(\log(ABC))^3}, \frac{(ABC)^{2/5}}{(\log(ABC))^{14/5}}\left(\frac{\log\log(ABCDEF)}{\log(ABCDEF)}\right)^2\right\}.$$

Define $J_{n,m}(A,B,C,D,E,F)$ to be the number of tuples (a,b,c) in $[D,D+A]\times[E,E+B]\times[F,F+C]$ such that $\Delta_{n,m}(a,b,c)$ has a distinct square-free part s. Thus, the following corollary is an immediate consequence of the above theorem.

Corollary 2.4.2. For sufficiently large positive real numbers $A,\ B,\ C$ and some non-negative real numbers $D,\ E,\ F$, as well as odd integers n and m, we have

$$J_{n,m}(A,B,C,D,E,F) \gg T_{ABC}.$$

Also note that, since n and m are odd integers, we have

$$\mathbb{Q}\left(\sqrt{\Delta_{n,m,1}(a,b,c)}\right) = \mathbb{Q}\left(\sqrt{(-1)^{\binom{n}{2}}\Delta_{n,m}(a,b,c)}\right).$$

Therefore, there are at least $\gg T_{ABC}$ distinct quadratic fields of the form $\mathbb{Q}\left(\sqrt{D_{n,m}(a,b,c)}\right)$.

We will now study the case (ii). Before presenting the main result, we first establish several preliminary lemmas.

For any integer $r \geq 2$, let $t_r(u)$ denote the order of u in the multiplicative group $\left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*$.

Lemma 2.4.3. For any prime number p, we have

$$\#\left\{u \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \mid t_p(u) \leq X\right\} \leq X\, d(p-1).$$

Proof. For any prime number p, $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ is cyclic. Therefore, for each divisor d of $p-1$, there are exactly $\varphi(d)$ elements in $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ whose order is d. Thus

$$\#\left\{u \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \mid t_p(u) \leq X\right\} \leq \sum_{\substack{d|(p-1)\\ d\leq X}} \varphi(d) \leq X d(p-1).$$

□

Lemma 2.4.4. Let $r = pq$ be the product of two distinct primes. Then

$$\sum_{u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*} \frac{1}{t_r(u)} \leq \gcd(p-1, q-1)\,(d(p-1)\,d(q-1))^2.$$

Proof. Since $r = pq$, by the Chinese remainder Theorem we have

$$\left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^* \cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)^*.$$

Therefore, $t_p(u) \mid t_r(u)$ and $t_q(u) \mid t_r(u)$. Consequently,

$$\frac{t_p(u)t_q(u)}{\gcd(t_p(u), t_q(u))} \text{ divides } t_r(u).$$

Since $t_p(u) \mid (p-1)$ and $t_q(u) \mid (q-1)$, we also have

$$\frac{t_p(u)t_q(u)}{\gcd(p-1, q-1)} \leq t_r(u).$$

For each divisor d_1 of $p-1$ and d_2 of $q-1$, we can obtain a value of $u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*$ with $t_p(u) = d_1$ and $t_q(u) = d_2$. Hence, by Lemma 2.4.3, there are at most $d_1 d_2 d(p-1)d(q-1)$ such values of u. Thus,

$$\begin{aligned}\sum_{u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*} \frac{1}{t_r(u)} &\leq \sum_{u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*} \frac{\gcd(p-1, q-1)}{t_p(u)t_q(u)} \\ &\leq \gcd(p-1, q-1) \sum_{\substack{d_1 \mid (p-1) \\ d_2 \mid (q-1)}} \frac{1}{d_1 d_2} d_1 d_2 d(p-1)d(q-1),\end{aligned}$$

and the result follows. □

By decomposing the range of the sum from 0 to $M-1$, into intervals of length $t_r(u)$ and applying the bound of the character sum given in Theorem 1 of [84] for each of the decomposed sum, we get (alternatively, one can see Lemma 7 of [78]) :

Lemma 2.4.5. For any integers $r \geq 2$ and $a, b, u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*$, we have

$$\sum_{w=0}^{M-1} \left(\frac{au^w + b}{r}\right) \ll \left(\frac{M}{t_r(u)} + 1\right) r^{\frac{1}{2}} \log r.$$

Since the next theorem deals with case (ii) given in the introduction, where a, b, c, k and m are fixed, so let us denote $D(n) := T_{n,m,k}(a, b, c)$.

Theorem 2.4.6. For a squarefree integer s and sufficiently large $N \geq 2$, we have

$$\left|\left\{n \in [1, N] \;\middle|\; D(n) = sr^2 \text{ for some integer } r \neq 1\right\}\right| \ll N^{\frac{3}{4}+\varepsilon},$$

for any arbitrary $\varepsilon > 0$.

Proof. Let us denote

$$\mathcal{T}(N, s) = \left\{n \in [1, N] \;\middle|\; D(n) = sr^2 \text{ for some integer } r \neq 1\right\}$$

and

$$T(N, s) = \left|\mathcal{T}(N, s)\right|.$$

Recall that we want to estimate an upper bound for $T(N, s)$.

Let $\mathcal{P}_z$ be the set of primes $p \in [z, 2z]$, and let $w_z(d)$ denote the number of distinct prime divisors of d in $[z, 2z]$, for $z > 2$. By the Prime Number Theorem, we know that

$$\#\mathcal{P}_z \gg \frac{z}{\log z}.$$

Since $sD(n)$ is a perfect square, we have

$$\sum_{p \in \mathcal{P}_z} \left(\frac{sD(n)}{p}\right) = \#\mathcal{P}_z - w_z(sD(n)) = \#\mathcal{P}_z - w_z(D(n)).$$

Using the arithmetic mean-geometric mean (AM-GM) inequality, we obtain

$$(\#\mathcal{P}_z)^2 \leq 2\left(\left(\sum_{p\in\mathcal{P}_z}\left(\frac{sD(n)}{p}\right)\right)^2 + w_z(D(n))^2\right),$$

which implies

$$T(N,s)\,(\#\mathcal{P}_z)^2 \ll W_1 + W_2, \tag{2.4.5}$$

where

$$W_1 = \sum_{n\in\mathcal{T}(N,s)}\left(\sum_{p\in\mathcal{P}_z}\left(\frac{sD(n)}{p}\right)\right)^2$$

and

$$W_2 = \sum_{n\in\mathcal{T}(N,s)} w_z(D(n))^2.$$

Now, we will derive an upper bound for W_1:

$$W_1 \leq \sum_{n=1}^{N}\left(\sum_{p\in\mathcal{P}_z}\left(\frac{sD(n)}{p}\right)\right)^2 = \sum_{n=1}^{N}\left(\sum_{p\in\mathcal{P}_z}\left(\frac{sD(n)}{p}\right)\sum_{q\in\mathcal{P}_z}\left(\frac{sD(n)}{q}\right)\right).$$

Interchanging the order of summation, we obtain

$$W_1 \leq \sum_{p,q\in\mathcal{P}_z}\left(\frac{s}{pq}\right)\sum_{n=1}^{N}\left(\frac{D(n)}{pq}\right),$$

and therefore,

$$|W_1| \leq \sum_{p,q\in\mathcal{P}_z}\left|\sum_{n=1}^{N}\left(\frac{D(n)}{pq}\right)\right|. \tag{2.4.6}$$

To estimate $|W_1|$, we first need to provide an upper bound for the sum

$$S(N,r) = \sum_{n=1}^{N}\left(\frac{D(n)}{r}\right).$$

Suppose $r = pq$ is the product of two primes p and q such that $p < q < 2p$. We can write $n = h + wr$, where $1 \le h \le r$ and let $M = \lfloor \frac{N}{r} \rfloor$. Then,

$$S(N, r) = \sum_{h=1}^{r} \sum_{w=0}^{M} \left(\frac{D(h + wr)}{r} \right) + O(r).$$

Note that

$$D(h + wr) \equiv h^{h+wr} b^{n-mk} \pm a^n c^k (mk)^{mk} (h - mk)^{h-mk+wr} \pmod{r}.$$

Therefore, we have

$$S(N, r) = \sum_{h=1}^{r} \sum_{w=0}^{M} \left(\frac{h^{h+wr} b^{n-mk} \pm a^n c^k (mk)^{mk} (h - mk)^{h-mk+wr}}{r} \right) + O(r).$$

If $\gcd(r, abchmk(h - mk)) > 1$, then there are only $O(\sqrt{r})$ such values of h contributing to the sum $S(N, r)$, so in this case the sum is at most $O(M\sqrt{r})$, which is $O\left(\frac{N}{\sqrt{r}}\right)$. Now, in the total sum, we are left with the case when $\gcd(r, abchmk(h - mk)) = 1$.

Denote

$$\mathcal{K} = \left\{ h \in [1, r] \;\middle|\; \gcd(r, abchmk(h - mk)) = 1 \right\},$$

then consider the sum

$$\begin{aligned} V &= \sum_{h \in \mathcal{K}} \sum_{w=0}^{M} \left(\frac{h^{h+wr} b^{n-mk} \pm a^n c^k (mk)^{mk} (h - mk)^{h-mk+wr}}{r} \right) \\ &= \sum_{h \in \mathcal{K}} \sum_{w=0}^{M} \left(\left(\frac{h^r}{r} \right) \right)^w \left(\frac{h^h b^{n-mk} \pm a^n c^k (mk)^{mk} (h - mk)^{h-mk} (1 - mkh^{-1})^{wr}}{r} \right). \end{aligned}$$

Thus, we obtain $\left| V \right| \ll V_0 + V_1$, where

$$V_i = \sum_{h \in \mathcal{K}} \left| \sum_{\substack{w=0 \\ w \equiv i \pmod 2}}^{M} \left(\frac{h^h b^{n-mk} \pm a^n c^k (mk)^{mk} (h - mk)^{h-mk} (1 - mkh^{-1})^{wr}}{r} \right) \right|$$

for $i = 0, 1$.

Since $p < q < 2p$, we note that $\gcd(r, \varphi(r)) = 1$. This implies that u and u^r have the same order in $\left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*$. Further, for each $u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*$, there is at most one $h \in [2, r]$ with $u \equiv 1 - mkh^{-1} \pmod{r}$.

Applying Lemma 2.4.5, we obtain

$$|V_i| \ll \sum_{u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*} \left(\frac{M}{t_r(u^r)} + 1\right) r^{\frac{1}{2}} \log r = Mr^{\frac{1}{2}} \log r \sum_{u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*} \frac{1}{t_r(u)} + \varphi(r) r^{\frac{1}{2}} \log r.$$

Also, using Lemma 2.4.4, we get that

$$\begin{aligned} |V_i| &\ll M \gcd(p-1, q-1)(d(p-1)d(q-1))^2 r^{\frac{1}{2}} \log r + \varphi(r) r^{\frac{1}{2}} \log r \\ &\ll M \gcd(p-1, q-1) r^{\frac{1}{2}+\varepsilon} + r^{\frac{3}{2}+\varepsilon} \\ &\ll N \gcd(p-1, q-1) r^{-\frac{1}{2}+\varepsilon} + r^{\frac{3}{2}+\varepsilon}. \end{aligned}$$

Combining the cases where $\gcd(r, abchmk(h-mk)) = 1$ or not, we derive the following bound:

$$S(N, r) \ll N \gcd(p-1, q-1) r^{-\frac{1}{2}+\varepsilon} + r^{\frac{3}{2}+\varepsilon}. \tag{2.4.7}$$

Now, returning to the estimation of W_1, as obtained before in (2.4.6) and (2.4.7),

$$\begin{aligned} |W_1| &\leq \sum_{p,q \in \mathcal{P}_z} \left| \sum_{n=1}^{N} \left(\frac{D(n)}{pq}\right) \right| \\ &\ll \sum_{p,q \in \mathcal{P}_z} \left(N \gcd(p-1, q-1)(pq)^{-\frac{1}{2}+\varepsilon} + (pq)^{\frac{3}{2}+\varepsilon} \right) \\ &\ll \sum_{p,q \in \mathcal{P}_z} \left(N \gcd(p-1, q-1) z^{-1+\varepsilon} + z^{3+\varepsilon} \right) \\ &\ll \sum_{p,q \in \mathcal{P}_z} \left(N \gcd(p-1, q-1) z^{-1+\varepsilon} \right) + z^{5+\varepsilon}. \end{aligned}$$

For every $d \leq 2z$, there are $O\left(\frac{z^2}{d^2}\right)$ pairs (p, q) with $\gcd(p-1, q-1) = d$. Thus,

$$\sum_{p,q \in \mathcal{P}_z} \gcd(p-1, q-1) \ll \sum_{d \leq 2z} d \cdot \frac{z^2}{d^2} \ll z^{2+\varepsilon}. \tag{2.4.8}$$

Hence, we obtain the following bound for W_1:

$$W_1 \ll Nz^{1+\varepsilon} + z^{5+\varepsilon}. \tag{2.4.9}$$

Now, we proceed to derive an upper bound for the sum W_2. We have:

$$|W_2| \leq \sum_{n=1}^{N} w_z \left(D(n)\right)^2 = \sum_{n=1}^{N} \left(\sum_{\substack{p|D(n) \\ p\in\mathcal{P}_z}} 1 \right) \left(\sum_{\substack{q|D(n) \\ q\in\mathcal{P}_z}} 1 \right) = \sum_{p,q\in\mathcal{P}_z} \sum_{\substack{n=1 \\ p,q|D(n)}}^{N} 1. \tag{2.4.10}$$

Let us denote by $\rho(N,r)$ the number of integers $n \in [1,N]$ such that $D(n) \equiv 0 \pmod{r}$. If $r = pq$ with $p < q < 2p$, then $\rho(N,r)$ provides an estimation for

$$\sum_{\substack{n=1 \\ p,q|D(n)}}^{N} 1.$$

Write $n = h + wr$, where $1 \leq h \leq r$, and let $M = \left\lfloor \frac{N}{r} \right\rfloor$. Then, $D(n) \equiv 0 \pmod{r}$ is equivalent to finding solutions in (h,w) of the congruence:

$$h^{h+wr} b^{n-mk} \pm a^n c^k (mk)^{mk} (h-mk)^{h-mk+wr} \equiv 0 \pmod{r}. \tag{2.4.11}$$

If $\gcd(r, abchmk(h-mk)) > 1$, then (2.4.11) has no solution in h, because $n \equiv h \pmod{r}$ and $\gcd(bn, acmk(n-mk)) = 1$.

Now, if $\gcd(r, abchmk(h-mk)) = 1$, then we have the following congruence:

$$\pm h^h a^{-n} b^{n-mk} c^{-k} (mk)^{-mk} (h-mk)^{-h+mk} \equiv (1 - mkh^{-1})^{wr} \pmod{r}.$$

Since $\gcd(r, mk) = 1$, for each $u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*$, there is at most one $h \in [2,r]$ such that $u \equiv (1 - mkh^{-1}) \pmod{r}$. Also, observe that $\gcd(r, \varphi(r)) = 1$, so $t_r(u^r) = t_r(u)$.

Therefore, for each $\ell \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*$, the congruence $u^{wr} \equiv \ell \pmod{r}$, $0 \leq w \leq M$, has at most $\frac{M}{t_r(u^r)} + 1 = \frac{M}{t_r(u)} + 1$ solutions in w. Hence, by Lemma 2.4.4, we obtain the following bound:

$$\rho(N, r) \leq \sum_{u \in \left(\frac{\mathbb{Z}}{r\mathbb{Z}}\right)^*} \left(\frac{M}{t_r(u)} + 1\right) \ll N \gcd(p-1, q-1) r^{-1+\varepsilon} + r. \tag{2.4.12}$$

Using Equations (2.4.8) and (2.4.12) in Equation (2.4.10), we obtain:

$$\begin{aligned} W_2 &\ll \sum_{p \in \mathcal{P}_z} \left(Np^{-1+\varepsilon} + p\right) + \sum_{p,q \in \mathcal{P}_z} \left(N \gcd(p-1, q-1)(pq)^{-1+\varepsilon} + pq\right) \\ &\ll (Nz^{\varepsilon} + z^2) + (Nz^{\varepsilon} + z^4) \\ &\ll Nz^{\varepsilon} + z^4. \end{aligned}$$

Observe that $|W_2|$ is dominated by the upper bound of $|W_1|$. Hence, from Equation (2.4.5), we conclude:

$$T(N, s)(\#\mathcal{P}_z)^2 \ll Nz^{1+\varepsilon} + z^{5+\varepsilon}. \tag{2.4.13}$$

Thus, putting $\#\mathcal{P}_z \gg \frac{z}{\log z}$ and $z = N^{\frac{1}{4}}$, we establish the required estimation. □

Since the bound given in Theorem 2.4.6 is uniform in s, we can see from Theorem 2.4.6 that for $n \in [1, N]$, the number of distinct squarefree integers s such that $D(n) = sr^2$ for some integer r is $\gg N^{\frac{1}{4}-\varepsilon}$. Also observe that, for each of such s, we can get a n in $[1, N]$.

Therefore, as a consequence, we obtain the following :

Corollary 2.4.7. For sufficiently large N and any arbitrary $\varepsilon > 0$, we have

$$\left|\left\{n \in [1, N] \;\middle|\; D(n) \text{ has distinct squarefree parts}\right\}\right| \gg N^{\frac{1}{4}-\varepsilon}.$$

Remark. A similar analysis can be done with the polynomials of the form $t^{n-mk}(t^k + ac)^m + bc \in$

$\mathbb{Z}[t]$, under the condition that $\gcd(bn, acmk(n - mk)) = 1$. The discriminant of such polynomials is discussed in detail in [38].

Chapter 3

abc-Conjecture and Counting Polynomials

3.1 Introduction

The *abc-conjecture*, proposed independently by Joseph Oesterlé (1985) and David Masser (1988), is one of the most powerful and far-reaching unsolved problems in number theory. The *abc-conjecture* has remarkable implications across various branches of number theory, especially in the topics of integral points on elliptic curves, solving diophantine equations, and many more. The conjecture received significant attention in august 2012, when Shinichi Mochizuki claimed a proof of the *abc-conjecture* using his newly developed Inter-universal Teichmüller Theory. Nevertheless, the proof has been met with skepticism, largely due to its complexity and the difficulty of independently verifying its claims. As of now, the conjecture remains unproven.

One of the applications of this conjecture is studying the frequency of squarefree values in a polynomial sequence, i.e., for a given separable polynomial $F(x) \in \mathbb{Z}[x]$, what proportion of integers n for which $F(n)$'s are squarefree. Naturally, one has to impose the condition that $\gcd\{F(\ell) \mid \ell \in \mathbb{Z}\}$ is squarefree. A heuristic argument suggests that the probability of the existence of such integers is

$$\delta_F = \prod_{p \text{ prime}} \left(1 - \frac{\rho_F(p^2)}{p^2}\right),$$

where $\rho_F(\ell) = \big|\{N \pmod{\ell} \mid F(N) \equiv 0 \pmod{\ell}\}\big|$ for any positive integer ℓ. Therefore one can expect the following asymptotic formula,

$$\big|\{1 \leq \ell \leq X \mid F(\ell) \text{ is squarefree}\}\big| \sim \delta_F X.$$

In 1998, A. Granville [23] established this asymptotic result, assuming *abc-conjecture*. This result holds unconditionally for $\deg(F) = 3$, as shown by C. Hooley (see [31] and [32, Chapter 4]). Moreover, for $n \leq 2$, this result can be proven using the sieve of Eratosthenes, without assuming the *abc-conjecture*. Later, B. Poonen [69] proved a similar result for several variable polynomials $F \in \mathbb{Z}[x_1, \cdots, x_n]$, and computed the density of $x \in \mathbb{Z}^n$ for which $F(x)$ is squarefree. A. Mukhopadhyay, M. R. Murty, and K. Srinivas [62] made use of the *abc-conjecture*, to show that for a positive proportion of integer pairs (a, b), the discriminants of trinomials of the form $t^n + at + b$ are squarefree.

Erdös [15] asked a similar question of whether $F(p)$ is squarefree for infinitely many primes p. Using *abc-conjecture* for number fields, H. Pasten [70] proved an expected asymptote of such prime numbers for which $F(p)$ is squarefree. He proved

$$\big|\{1 \leq p \leq X \mid p \text{ is prime and } F(p) \text{ is squarefree}\}\big| \sim c_F \frac{X}{\log X},$$

holds under *abc-conjecture* for number fields $\mathbb{Q}(\alpha)$, where α varies over irrational roots of F. The constant c_F is given by

$$c_F = \prod_{p \text{ prime}} \left(1 - \frac{\omega_F(p^2)}{p(p-1)}\right),$$

where $\omega_F(p^2)$ is the number of solutions to $F(x) \equiv 0 \pmod{p^2}$ in $(\mathbb{Z}/p^2\mathbb{Z})^*$.

The above result is known to hold unconditionally for $\deg(F) \leq 3$; the cubic case was addressed by H. A. Helfgott (see [30] for further references).

In this chapter, our concern is how *abc-conjecture* helps us to count the polynomials $t^n + c(at^k + b)^m \in \mathbb{Z}[t]$, that are monogenic or have a symmetric group as their Galois group.

3.2 Preliminaries

Let K be an algebraic number field of degree n, which means K is a n dimensional vector space over $\mathbb{Q}$. Let $\sigma_1, \sigma_2, \cdots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. For any $\alpha \in K$, we shall denote $\sigma_i(\alpha) := \alpha^{(i)}$.

An element $\alpha \in K$ is said to be an algebraic integer if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. The set of all algebraic integers of K forms a ring. Let $\mathcal{O}_K$ denote the ring of algebraic integers of K.

Definition 3.2.1. A set of algebraic integers $\{w_1, w_2, \cdots, w_n\}$ in K is said to be an *integral basis* of K, if $\mathcal{O}_K = \mathbb{Z}w_1 + \mathbb{Z}w_2 + \cdots + \mathbb{Z}w_n$.

Proposition 3.2.2. Let K be an algebraic number field of degree n. Then K always admits an integral basis, and any integral basis of K has n elements.

Proposition 3.2.3. Let M be a finitely generated $\mathbb{Z}$-module with generators $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$. Then for any sub-module N of M, there exists $\{\beta_1, \beta_2, \cdots, \beta_k\}$ in N with $k \leq m$ such that $N = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \cdots + \mathbb{Z}\beta_k$ and $\beta_i = \sum_{j \geq i} c_{ij}\alpha_i$, with $c_{ij} \in \mathbb{Z}$ and $c_{ii} > 0$ for all $1 \leq i \leq k \leq m$. Also, if $m = k$ then $[M : N] = \prod_{1 \leq i \leq n} c_{ii}$.

Definition 3.2.4. For any $a_1, a_2, \cdots, a_n \in K$, the *discriminant* of $\{a_1, a_2, \cdots, a_n\}$ is defined as the square of the determinant of the $n \times n$ matrix $\left(a_i^{(j)}\right)_{i,j}$. It will be denoted by $D_{K/\mathbb{Q}}(a_1, a_2, \cdots, a_n)$.

Note that the change of basis matrix of any two integral bases of K is unimodular. Therefore the discriminant of any two integral bases of K remains the same, and it will be denoted by d_K.

Proposition 3.2.5. Let $\{a_1, a_2, \cdots, a_n\}$ be a $\mathbb{Q}$-basis of K and N be a finitely generated $\mathbb{Z}$-module with generators $\{a_1, a_2, \cdots, a_n\}$. Then we have

$$D_{K/\mathbb{Q}}(a_1, a_2, \cdots, a_n) = [\mathcal{O}_K : N]^2 \, d_k.$$

The proof of Proposition 3.2.2 - 3.2.5 can be found in any standard book on algebraic number theory (cf. [16], [67]).

3.3 Monogenic Polynomials

Definition 3.3.1. An algebraic number field K of degree n is said to be monogenic if $\mathcal{O}_K$ admits a power integral basis of the form $\{1, \eta, \ldots, \eta^{n-1}\}$ for some $\eta \in \mathcal{O}_K$.

Examples.

1. Every quadratic field $\mathbb{Q}(\sqrt{d})$ (for a squarefree integer d) is monogenic. If $d \equiv 1 \pmod 4$, an integral basis of $\mathbb{Q}(\sqrt{d})$ is $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$. Otherwise, the integral basis is $\{1, \sqrt{d}\}$, if $d \equiv 2, 3 \pmod 4$.

2. If $d \not\equiv \pm 1 \pmod 9$, then the cubic field $\mathbb{Q}(d^{1/3})$ is monogenic. An integral basis of this field is $\{1,\ d^{1/3},\ d^{2/3}\}$.

In 1960, Hasse [27] sought to establish a criterion for an arithmetic characterization of monogenic number fields.

Let $K = \mathbb{Q}(\theta)$ where θ has a minimal polynomial $f(x)$ of degree n over the field $\mathbb{Q}$ of rationals. Denote D_f be the discriminant of the polynomial f, which is $\prod_{1 \le i < j \le n} \left(\theta^{(i)} - \theta^{(j)}\right)^2$. Using determinant of Vandermonde matrix, it is easy to see that $D_{K/\mathbb{Q}}(1, \theta, \cdots, \theta^{n-1}) = \prod_{1 \le i < j \le n} \left(\theta^{(i)} - \theta^{(j)}\right)^2$. Therefore from above Proposition 3.2.5, it implies that

$$D_f = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 \, d_K. \tag{3.3.1}$$

From Equation (3.3.1), if $D_f = d_K$, then $\mathcal{O}_K = \mathbb{Z}[\theta]$, which means that the set $\{1, \theta, \cdots, \theta^{n-1}\}$ forms an integral basis of K. In this case, we say that the polynomial $f(x)$ is *monogenic*. Therefore, if $f(x)$ is monogenic, then the number field K is also monogenic; however, the converse is not true. For example, let $d \equiv 1 \pmod 4$ then the quadratic field $K = \mathbb{Q}(\sqrt{d})$ is monogenic, since $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. But the polynomial $f(x) = x^2 - d$ is not a monogenic polynomial, as $\left[\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]\right] = 2$. Through the efforts of various mathematicians, considerable progress has been achieved in recent years on monogenic number fields and polynomials, encompassing both qualitative and quantitative results (cf. [4], [5], [37], [42], [45], [46], [47]).

From Equation (3.3.1), it follows that if D_f is squarefree, then $f(x)$ is always monogenic. In general, the discriminant of a polynomial is not necessarily squarefree. Along these lines, a construction similar to that used by Kedlaya in [48] was employed by Jones [43] to provide a new infinite family of monogenic polynomials with prime degrees and non-squarefree discriminants. More recently, Jones and White [44] gave an asymptotic formula for the number of trinomials $t^{mn} + at^n + a \in \mathbb{Z}[t]$ (for $a \geq 2$) with non-squarefree discriminants under certain conditions.

In the next section, we will discuss about the number of monogenic polynomials, $f(t) = t^n + c(at^k + b)^m$ of degree $n > mk + 1$ with integer coefficients and $\gcd(n, k) = 1$, $k \geq 2$.

The following lemmas classify when the polynomials $t^n + c(at^k + 1)^m$ and $t^n + act^k + bc$ will be monogenic.

Lemma 3.3.2. Let $K = \mathbb{Q}(\theta)$ and $g_1(t) = t^n + c(at^k + 1)^m \in \mathbb{Z}[t]$ be a monic irreducible polynomial of degree n with root θ, where $\gcd(n, amk) = 1$. Then $\mathcal{O}_K = \mathbb{Z}[\theta]$ if and only if for each prime p dividing the discriminant D_{g_1} of $g_1(t)$, either (i) $p \mid c$ and $p^2 \nmid c$, or (ii) $p \nmid c$ and $p^2 \nmid D_{g_1}$.

Lemma 3.3.3. Let $g_2(t) = t^n + act^k + bc \in \mathbb{Z}[t]$ be a monic irreducible polynomial of degree n, where bc is squarefree, $\gcd(nb, ak(n-k)) = 1$. Let D_{g_2} denote the discriminant of $g_2(t)$. Suppose that $p^2 \nmid D_{g_2}$ whenever $p \mid D_{g_2}$ and $p \nmid abck$. Then $g_2(t)$ is monogenic.

For proof of the above two lemmas, readers are referred to [36]

3.3.1 Counting Monogenic Polynomials $t^n + c(at^k + b)^m$

Recall that the discriminant of the monic irreducible polynomial $f(t) = t^n + c(at^k + b)^m$, with $\gcd(n, k) = 1$, is

$$\Delta_{n,m,k}(a, b, c) = (-1)^{\binom{n}{2}} b^{m(n+k-1)-n} c^{n-1} \left[n^n b^{n-mk} + (-1)^{n+mk+k+1} a^n c^k (mk)^{mk} (n - mk)^{n-mk} \right].$$

Let us define

$$T_{n,m,k}(a,b,c) := n^n b^{n-mk} + (-1)^{n+mk+k+1} a^n c^k (mk)^{mk} (n-mk)^{n-mk}. \tag{3.3.2}$$

Note that we have assumed $n > mk+1$ and $k \geq 2$, observe if $T_{n,m,k}(a,b,c)$ is squarefree, then we must have $\gcd(nb, acmk(n-mk)) = 1$. Therefore we have

$$\Delta_{n,m,k}(a,b,c) = (-1)^{\binom{n}{2}} b^{m(n+k-1)-n} c^{n-1} T_{n,m,k}(a,b,c) \tag{3.3.3}$$

From Lemma 3.3.2 we note that if we assume c (resp. bc) is squarefree, then for monogenicity of $t^n + c(at^k+1)^m$ (resp. $t^n + act^k + bc$), it is enough to count (a,c) (resp. (a,b,c)) for which $T_{n,m,k}(a,1,c)$ (resp. $T_{n,1,k}(a,b,c)$) is squarefree. To count this we will make use of *abc-conjecture* for number fields as follows.

3.3.2 *abc*-Conjecture for Number Fields

Let us denote by

M_K : the set of all places of K.

M_K^0 : set of finite places, and

M_K^∞: the set of infinite places.

For any $v \in M_K$, we write $\|.\|_v$ for the normalized norm at v, which for $\alpha \in K^\star$ is defined by

$$\|\alpha\|_v = \begin{cases} \left(\frac{1}{[\mathcal{O}_K : \mathfrak{p}]}\right)^{-ord_{\mathfrak{p}}(\alpha)} & \text{if } v \in M_K^0 \text{ corresponds to the prime ideal } \mathfrak{p} \subseteq \mathcal{O}_K, \\ |\sigma(\alpha)| & \text{if } v \in M_K^\infty \text{ corresponds to the real embedding } \sigma : K \to \mathbb{R}, \\ |\sigma(\alpha)|^2 & \text{if } v \in M_K^\infty \text{ corresponds to the complex embedding } \sigma : K \to \mathbb{C}, \end{cases}$$

and $\|0\|_v = 0$ for all $v \in M_K$.

The height of α (with respect to K) is defined by

$$h_K(\alpha) = \sum_{v \in M_K} \log \max\{1, \|\alpha\|_v\}.$$

If $S \subset M_K$ is a finite set, the *truncated counting function* for $\alpha \neq 0$ is defined by

$$N^{(1)}_{K,S}(\alpha) = \sum_{v \in M^0_K \setminus S} \min\{1, \max\{0, \mathrm{ord}_{\mathfrak{p}_v}(\alpha)\}\} \log[\mathcal{O}_K : \mathfrak{p}_v].$$

where $\mathfrak{p}_v$ is the prime ideal corresponding to $v \in M^0_K$.

The abc-conjecture (for number fields): Let K be a number field. Let $\epsilon > 0$ and fix mutually distinct elements $b_1, \cdots, b_m \in K$. Let S be a finite set of places of K. Then for all but finitely many $\alpha \in K$, one has

$$(m - 2 - \epsilon) h_K(\alpha) < \sum_{i=1}^{m} N^{(1)}_{K,S}(\alpha - b_i).$$

We write down the case when $K = \mathbb{Q}$, the classical Oesterlè and Masser's *abc-conjecture* which states that :

If $a,\ b$, and c are coprime integers satisfying $a + b = c$, then for every $\varepsilon > 0$,

$$\max(|a|, |b|, |c|) \ll_\varepsilon \mathrm{rad}(abc)^{1+\varepsilon},$$

where $\mathrm{rad}(\ell)$ denotes the product of distinct prime factors of ℓ. This will be required in the last section of this chapter.

Now we turn to a theorem of Jones and White [44, Theorem 2.5], which gives an asymptotic for the number of primes p, for which $F(p)$ is squarefree simultaneously, for any separable polynomial $F(x) \in \mathbb{Z}[x]$. This result comes from the main theorem of H. Pasten's Paper [70].

The number field taken in next Proposition (followed by Theorem 3.3.8, 3.3.9, and 3.4.2) is $\mathbb{Q}(\alpha)$,

where α varies over the irrational roots of $F(x) \in \mathbb{Z}[x]$.

Proposition 3.3.4 (Theorem 2.5, [44])**.** Let $F(t) \in \mathbb{Z}[t]$ be a separable polynomial, and let d be the highest degree of any irreducible factor of $F(t)$. Then, we have

$$\big|\{1 \le p \le X \mid p \text{ is prime and } F(p) \text{ is squarefree}\}\big| \sim h_F \frac{X}{\log X}, \tag{3.3.4}$$

where

$$h_F = \prod_{p \text{ prime}} \left(1 - \frac{\omega_F(p^2)}{p(p-1)}\right),$$

and

$$\omega_F(\ell) = \big|\{N \pmod{\ell} \mid \gcd(N, \ell) = 1, F(N) \equiv 0 \pmod{\ell}\}\big|.$$

The asymptotic formula (3.3.4) holds unconditionally for $d \le 3$ and is conditional on the *abc*-conjecture for number fields when $d \ge 4$.

The constant h_F is positive if and only if $F(t)$ has no *local obstruction* for all prime p, which has been defined below.

Definition 3.3.5. A polynomial $F(t)$ has a *local obstruction* at a prime q if there does not exist $\ell \in (\mathbb{Z}/q^2\mathbb{Z})^*$ such that $F(\ell)$ is not divisible by q^2.

Define the polynomial $T^{a,b}_{n,m,k}(x)$ as

$$T^{a,b}_{n,m,k}(x) = n^n b^{n-mk} + (-1)^{n+mk+k+1} a^n (mk)^{mk} (n-mk)^{n-mk} x^k$$

in $\mathbb{Z}[x]$ of degree k, with $\gcd(nb, amk(n-mk)) = 1$. Note that the polynomial $T^{a,b}_{n,m,k}(x)$ is irreducible (cf. [34, Theorem 1.2]).

Lemma 3.3.6. The polynomial $T^{a,b}_{n,m,k}(x)$ has no *local obstruction* at any prime. More precisely, for each prime p, there exists $\ell \in (\mathbb{Z}/p^2\mathbb{Z})^*$ such that $T^{a,b}_{n,m,k}(\ell)$ is not divisible by p^2.

Proof. Suppose that for all primes p, we have

$$T^{a,b}_{n,m,k}(1) = n^n b^{n-mk} + (-1)^{n+mk+k+1} a^n (mk)^{mk} (n-mk)^{n-mk} \not\equiv 0 \pmod{p^2}.$$

Then we are done. Assume instead that there exists a prime q such that $T^{a,b}_{n,m,k}(1) \equiv 0 \pmod{q^2}$. Since $\gcd(nb, amk(n-mk)) = 1$, we must have $q \nmid nbamk(n-mk)$. Observe that

$$T^{a,b}_{n,m,k}(\ell + q) - T^{a,b}_{n,m,k}(\ell) \equiv k(mk)^{mk}(n-mk)^{n-mk} q \ell^{k-1} \pmod{q^2},$$

for any $\ell \in (\mathbb{Z}/q^2\mathbb{Z})^*$. Since $q \nmid nbamk(n-mk)\ell$, it follows that

$$T^{a,b}_{n,m,k}(\ell + q) \not\equiv T^{a,b}_{n,m,k}(\ell) \pmod{q^2}.$$

Thus, at least one of $\ell + q$ or ℓ is not a solution to $T^{a,b}_{n,m,k}(x) \equiv 0 \pmod{q^2}$ for all $\ell \in (\mathbb{Z}/q^2\mathbb{Z})^*$. This proves the lemma. □

To prove the Theorem 3.3.8, 3.3.9 and 3.4.2, it is necessary to count the number of (a, b, c) for which $T_{n,m,k}(a, b, c)$ is squarefree, as defined in (3.3.2).

For convenience, we denote by S the following set:

$$S := \{(a, b, c) \mid A \le |a| \le 2A,\ B \le |b| \le 2B,\ C \le |c| \le 2C\}.$$

We now present the following result, which is also of independent interest.

Theorem 3.3.7. For sufficiently large C, we have

$$\left|\{(a, b, c) \in S \mid \ c \text{ and } T_{n,m,k}(a, b, c) \text{ are square-free}\}\right| \gg \frac{ABC}{\log C}, \tag{3.3.5}$$

provided $k \le 3$. Moreover, for $k \ge 4$, (3.3.5) holds under the *abc-conjecture* for number fields.

Proof. We aim to count the number of $(a, b, c) \in S$ such that c and $T_{n,m,k}(a, b, c)$ are squarefree.

We note that, $T_{n,m,k}(a,b,c) = T^{a,b}_{n,m,k}(c)$. Now, by Proposition 3.3.4, unconditionally for $k \leq 3$ and under the assumption of the *abc-conjecture* on number fields for $k \geq 4$, we obtain for sufficiently large C

$$\left|\{C \leq c \leq 2C \mid c \text{ is prime and } T^{a,b}_{n,m,k}(c) \text{ is squarefree}\}\right| \sim h_{T^{a,b}_{n,m,k}} \frac{C}{\log C},$$

where

$$h_F = \prod_{p \text{ prime}} \left(1 - \frac{\omega_F(p^2)}{p(p-1)}\right),$$

and

$$\omega_F(\ell) = \left|\{N \pmod{\ell} \mid \gcd(N,\ell) = 1, F(N) \equiv 0 \pmod{\ell}\}\right|.$$

Thus from Lemma 3.3.6 and for squarefree c, we get

$$\left|\{C \leq |c| \leq 2C \mid c \text{ and } T^{a,b}_{n,m,k}(c) \text{ are squarefree}\}\right| \gg \frac{C}{\log C}. \tag{3.3.6}$$

Therefore for sufficiently large C,

$$\left|\{(a,b,c) \in S \mid \ c \text{ and } T^{a,b}_{n,m,k}(c) \text{ are squarefree}\}\right| \gg \frac{ABC}{\log C}.$$

This completes the proof of the theorem. □

Let us denote the following sets by

$$\mathcal{N}_{n,m,k}(A,C) := \{(|a|,|c|) \in [A,2A] \times [C,2C] \mid \gcd(n,k) = 1,\ t^n + c(at^k+1)^m \text{ is monogenic}\},$$

and

$$\mathcal{N}_{n,k}(A,B,C) := \{(|a|,|b|,|c|) \in [A,2A]\times[B,2B]\times[C,2C] \mid \gcd(n,k) = 1,\ t^n + act^k + bc \text{ is monogenic}\}.$$

Theorem 3.3.8. For all sufficiently C, we have

$$\left|\mathcal{N}_{n,m,k}(A,C)\right| \gg \frac{AC}{\log C}, \tag{3.3.7}$$

provided $k \leq 3$. Furthermore, (3.3.7) holds for $k \geq 4$ under the *abc-conjecture* for number fields.

Proof. Our goal is to obtain a lower bound for $|\mathcal{N}_{n,m,k}(A,C)|$. Instead, we will count a lower bound for the cardinality of a subset of $\mathcal{N}_{n,m,k}(A,C)$.

Let $N(A,C)$ denote the set of all pairs (a,c) such that $A \leq |a| \leq 2A$, $C \leq |c| \leq 2C$, $\gcd(n, amk) = 1$, $c \neq \pm 1$ is a squarefree integer, and $t^n + c(at^k+1)^m$ is monogenic.

Note that the discriminant of $t^n + c(at^k+1)^m$ is

$$\Delta(a,1,c) = (-1)^{\binom{n}{2}} c^{n-1} T_{n,m,k}(a,1,c).$$

If $c \neq \pm 1$ is squarefree, then by Eisenstein's criterion, the polynomial $t^n + c(at^k+1)^m$ is irreducible. Therefore, from Lemma 3.3.2, it follows that for squarefree $c \neq \pm 1$, $t^n + c(at^k+1)^m$ is monogenic if and only if for all primes p dividing $\Delta(a,1,c)$, we have $p^2 \nmid T_{n,m,k}(a,1,c)$.

From Theorem 3.3.7, by fixing $b = 1$, we obtain

$$|\{(|a|,|c|) \in [A,2A] \times [C,2C] \mid \ c \text{ and } T_{n,m,k}(a,1,c) \text{ are squarefree}\}| \gg \frac{AC}{\log C}.$$

Thus we get $\big|N(A,C)\big| \gg \frac{AC}{\log C}$. Since $N(A,C) \subset \mathcal{N}_{n,m,k}(A,C)$, we conclude that $\big|\mathcal{N}_{n,m,k}(A,C)\big| \gg \frac{AC}{\log C}$. This completes the proof. □

Theorem 3.3.9. For all sufficiently large C , we have

$$\big|\mathcal{N}_{n,k}(A,B,C)\big| \gg \frac{ABC}{\log C}, \tag{3.3.8}$$

provided $k \leq 3$. Furthermore, (3.3.8) holds for $k \geq 4$ under the *abc-conjecture* on number fields.

Proof. Let $N_1(A,B,C)$ denote the set of all $(a,b,c) \in S$ such that $\gcd(nb, ack(n-k)) = 1$, $bc \neq \pm 1$, bc is squarefree, and $t^n + act^k + bc$ is monogenic.

Note that $N_1(A,B,C) \subset \mathcal{N}_{n,k}(A,B,C)$. If $bc \neq \pm 1$ and bc is squarefree, then by Eisenstein's criterion, the polynomial $t^n + act^k + bc$ is irreducible. Therefore, from Lemma 3.3.3, it follows that for

squarefree bc, with $bc \neq \pm 1$, the polynomial $t^n + act^k + bc$ is monogenic if and only if $T_{n,1,k}(a,b,c)$ is squarefree.

By Theorem 3.3.7 (for $m = 1$), we have

$$|\{(a,b,c) \in S \mid c \text{ and } T_{n,1,k}(a,b,c) \text{ are squarefree}\}| \gg \frac{ABC}{\log C}.$$

Above relation holds uniformly over b and since there are approximately $\frac{12}{\pi^2}B$ squarefree integers b satisfying $B \leq |b| \leq 2B$, hence $\left|N_1(A,B,C)\right| \gg \frac{ABC}{\log C}$. Therefore we conclude that $\left|\mathcal{N}_{n,k}(A,B,C)\right| \gg \frac{ABC}{\log C}$.

□

3.4 Counting Polynomials $t^q + c(at^k + b)^m$ with Galois group S_q

Lemma 3.4.1. Let $h(t) = t^q + c(at^k + b)^m \in \mathbb{Z}[t]$ be a monic irreducible polynomial of prime degree q. If there exists a prime p such that p divides the discriminant D_h of $h(t)$, but $p^2 \nmid D_h$ and $p \nmid abcmk$, then the Galois group of $h(t)$ is S_q.

Proof. See [36]. □

For any prime number q, consider the following set defined by

$\mathcal{N}_{S_q}(A,B,C) := \{(|a|,|b|,|c|) \in [A,2A] \times [B,2B] \times [C,2C] \mid \gcd(q,k) = 1, \text{ and } t^q + c(at^k + b)^m \text{ has Galois group } S_q\}$.

Theorem 3.4.2. For all sufficiently large C and any prime number q, we have

$$\left|\mathcal{N}_{S_q}(A,B,C)\right| \gg \frac{ABC}{\log C}, \tag{3.4.1}$$

provided $k \leq 3$. Furthermore, (3.4.1) holds for $k \geq 4$ under the *abc-conjecture* on number fields.

Proof. we shall focus on finding a lower bound for the cardinality of a subset of $\mathcal{N}_{S_q}(A, B, C)$ for any prime number q.

Let $N_{S_q}(A, B, C)$ denote the set of all $(a, b, c) \in S$ such that $\gcd(qb, acmk(q - mk)) = 1$, $c \neq \pm 1$, c is squarefree, and the polynomial $t^q + c(at^k + b)^m$ has Galois group S_q.

Note that $N_{S_q}(A, B, C) \subset \mathcal{N}_{S_q}(A, B, C)$. If $c \neq \pm 1$ and c is squarefree, then by Eisenstein's criterion, the polynomial $t^q + c(at^k + b)^m$ is irreducible. Therefore, from Lemma 3.4.1, it follows that for squarefree c, with $c \neq \pm 1$, the polynomial $t^q + c(at^k + b)^m$ has Galois group S_q if and only if $T_{q,m,k}(a, b, c)$ is squarefree.

By Theorem 3.3.7, we have

$$|\{(a, b, c) \in S \mid c \text{ and } T_{q,m,k}(a, b, c) \text{ are squarefree}\}| \gg \frac{ABC}{\log C}.$$

Hence, $\left|N_{S_q}(A, B, C)\right| \gg \frac{ABC}{\log C}$, and we conclude that $\left|\mathcal{N}_{S_q}(A, B, C)\right| \gg \frac{ABC}{\log C}$. This completes the proof of the theorem. □

3.5 Counting Distinct Squarefree Parts of $\Delta_{n,m,k}(a, b, c)$ Under *abc-Conjecture*

In this section, we will show that for n (≥ 3), m, and k being odd integers, there exists a positive portion of tuples (a, b, c) of integers for which $T_{n,m,k}(a, b, c)$ is squarefree under *abc-conjecture*.

For sufficiently large positive real numbers A, B, and C, let $D(A, B, C)$ denote the number of square-free integers d that have at least one solution to

$$d = T_{n,m,k}(a, b, c), \text{ where } (a, b, c) \in S \text{ and } \gcd(nb, acmk(n - mk)) = 1. \tag{3.5.1}$$

The following theorem provides a lower bound for $D(A, B, C)$ assuming the *abc-conjecture*.

Theorem 3.5.1. Let A, B, and C be sufficiently large positive real numbers such that $B > (AC)^{1+\delta}$ for some fixed $\delta > 0$, and let n (≥ 3), m, and k be odd integers. If we assume the truth of the *abc-conjecture*, then

$$D(A, B, C) \gg ABC.$$

The implied constant may depend upon n, m, and k.

For a squarefree integer d, let us define

$$S(d) := |\{(a, b, c) \in S \mid d = T_{n,m,k}(a, b, c)\}|.$$

We begin by computing a lower bound for $\sum_{d \leq X} S(d)$ and an upper bound for $\sum_{d \leq X} S(d)^2$. Then, by applying the Cauchy-Schwarz inequality, we will derive the desired lower bound for $D(A, B, C)$. This kind of argument and technique can also be found in papers [62], [63], and [81].

Lemma 3.5.2. Let n (≥ 3), m, k be odd integers such that $\gcd(nb, acmk(n - mk)) = 1$. Let A, B, C be sufficiently large positive real numbers such that $B > (AC)^{1+\delta}$ or $C > (AB)^{1+\delta}$, for some fixed $\delta > 0$. Then, under the *abc*-conjecture, we have

$$\sum_{d} S(d) \gg ABC.$$

The implied constant may depend upon n, m, and k.

Proof. Without loss of generality, assume $B > (AC)^{1+\delta}$.

Let us define

$$H(a, b, c) := T_{n,m,k}(-a, b, c)T_{n,m,k}(a, b, c) = n^{2n}b^{2(n-mk)} - a^{2n}c^{2k}(mk)^{2mk}(n - mk)^{2(n-mk)}. \tag{3.5.2}$$

Let $\mathcal{M}_1$ denote the set of tuples (a, b, c) of integers such that $A \leq a \leq 2A$, $B \leq |b| \leq 2B$, $C \leq |c| \leq 2C$, and $H(a, b, c)$ is not divisible by the square of any prime $p \leq \log B$. Let $M_1 = |\mathcal{M}_1|$ and $P = \prod_{p \leq \log B} p$.

We know that for any integer α,

$$\sum_{\ell^2|(\alpha,P^2)} \mu(\ell) = \begin{cases} 1 & \text{if } p^2 \nmid \alpha \text{ for all } p \leq \log B, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, we get

$$M_1 = \sum_{\substack{A\leq a\leq 2A \\ B\leq |b|\leq 2B \\ C\leq |c|\leq 2C}} \sum_{\ell^2|(H(a,b,c),P^2)} \mu(\ell) = \sum_{\substack{A\leq a\leq 2A \\ C\leq |c|\leq 2C}} \sum_{\ell|P} \mu(\ell) \sum_{\substack{B\leq |b|\leq 2B \\ H(a,b,c)\equiv 0 \pmod{\ell^2}}} 1. \tag{3.5.3}$$

We now calculate the sum over b. For any integer $\ell \geq 1$, define

$$\rho_{a,c}(\ell) := |\{b \pmod{\ell} \mid H(a,b,c) \equiv 0 \pmod{\ell}\}|.$$

Note that since $T_{n,m,k}(\pm a, b, c)$ is a polynomial in b of degree $n - mk$, so it will have at most $(n - mk)$ solutions modulo p. Therefore for a prime $p \nmid abnmk(n - mk)$ and an integer $\alpha \geq 1$, it follows that $\rho_{a,c}(p^\alpha) = \rho_{a,c}(p) \leq (n - mk)$.

Observe that, by the Chinese remainder theorem, $\rho_{a,c}(\ell)$ is a multiplicative function of ℓ. Dividing the sum over b in (3.5.3) into intervals of length ℓ^2, we get

$$\sum_{\substack{B\leq |b|\leq 2B \\ H(a,b,c)\equiv 0 \pmod{\ell^2}}} 1 = \frac{2B\rho_{a,c}(\ell^2)}{\ell^2} + O(1).$$

Thus, we have

$$\begin{aligned} \sum_{\ell|P} \mu(\ell) \sum_{\substack{B\leq |b|\leq 2B \\ H(a,b,c)\equiv 0 \pmod{\ell^2}}} 1 &= 2B \sum_{\ell|P} \mu(\ell) \frac{\rho_{a,c}(\ell^2)}{\ell^2} + O\left(\sum_{\ell|P} 1\right) \\ &= 2B \prod_{p|P} \left(1 - \frac{\rho_{a,c}(p)}{p^2}\right) + O(P^\varepsilon) \\ &= 2\beta B + O(B^\varepsilon), \end{aligned}$$

where $\beta = \prod_{p|P} \left(1 - \frac{\rho_{a,c}(p)}{p^2}\right)$ is a constant, since the product converges as B becomes large.

From (3.5.3), we obtain

$$M_1 = \gamma ABC + O(AB^{\varepsilon}C) = \gamma ABC + o(ABC),$$

for some constant $\gamma > 0$.

Let $\mathcal{M}_2$ be the set of all tuples (a, b, c) with $A \le a \le 2A$, $B \le |b| \le 2B$, and $C \le |c| \le 2C$, such that $H(a, b, c)$ is divisible by the square of a prime $p \in (\log B, B]$. Define $M_2 = |\mathcal{M}_2|$. Then

$$M_2 = \sum_{\substack{A \le a \le 2A \\ C \le |c| \le 2C}} \sum_{\log B < p \le B} \sum_{\substack{B \le |b| \le 2B \\ H(a,b,c) \equiv 0 \,(\mathrm{mod}\, p^2)}} 1$$

$$= 2B \sum_{\substack{A \le a \le 2A \\ C \le |c| \le 2C}} \sum_{\log B < p \le B} \frac{\rho_{a,c}(p^2)}{p^2} + O\left(\sum_{\substack{A \le a \le 2A \\ C \le |c| \le 2C}} \sum_{\log B < p \le B} 1 \right).$$

Note that

$$2B \sum_{\substack{A \le a \le 2A \\ C \le |c| \le 2C}} \sum_{\log B \le p \le B} \frac{\rho_{a,c}(p^2)}{p^2} \ll ABC \sum_{p > \log B} \frac{1}{p^2} \ll \frac{ABC}{\log B} = o(ABC).$$

By the prime number theorem, we have

$$\sum_{\substack{A \le a \le 2A \\ C \le |c| \le 2C}} \sum_{\log B < p \le B} 1 \ll \frac{ABC}{\log B} = o(ABC).$$

Thus, $M_2 = o(ABC)$.

Now, consider $\mathcal{M}_1 \setminus \mathcal{M}_2$, which is the set of all tuples (a, b, c) with $A \le a \le 2A$, $B \le |b| \le 2B$, and $C \le |c| \le 2C$, such that neither $T_{n,m,k}(-a, b, c)$ nor $T_{n,m,k}(a, b, c)$ is divisible by the square of any $p \le B$. Clearly, $|\mathcal{M}_1 \setminus \mathcal{M}_2| \ge M_1 - M_2$.

We define a tuple (a, b, c) as "good" if $T_{n,m,k}(a, b, c)$ is not divisible by p^2 for any prime $p > B$. Otherwise, we call (a, b, c) as "bad".

We claim that $(-a, b, c)$ and (a, b, c) cannot both be bad.

Suppose both $(-a, b, c)$ and (a, b, c) are bad. Then there exist primes $p > B$ and $q > B$ such that

$$T_{n,m,k}(-a, b, c) = p^2 r_1 \quad \text{and} \quad T_{n,m,k}(a, b, c) = q^2 r_2,$$

for some integers r_1 and r_2.

Clearly, p and q must be distinct, since if $p = q$, then p^2 would divide $T_{n,m,k}(-a, b, c) + T_{n,m,k}(a, b, c)$, implying $p \leq B$, which is a contradiction.

Now, using the *abc*-conjecture, for any $\varepsilon > 0$, we get

$$pq \ll_\varepsilon (ABC)^{1+\varepsilon}.$$

Since $p, q > B$ and $B > (AC)^{1+\delta}$ for some $\delta > 0$, we have

$$(AC)^{1+\delta} B < pq \ll_\varepsilon (ABC)^{1+\varepsilon},$$

which leads to a contradiction. This proves our claim.

Therefore, at least half of the tuples (a, b, c) in $\mathcal{M}_1 \setminus \mathcal{M}_2$ are good. Hence

$$\sum_d S(d) \geq \frac{1}{2}(M_1 - M_2) \gg ABC.$$

This completes the proof of the lemma. □

Lemma 3.5.3. Let n (≥ 3), m, and k be odd integers, and let A, B, and C be sufficiently large

positive real numbers with $B > (AC)^{1+\delta}$ for some fixed $\delta > 0$. Then

$$\sum_{d \leq X} S(d)^2 \ll ABC.$$

Proof. The sum $\sum_{d \leq X} S(d)^2 - \sum_{d \leq X} S(d)$ is bounded by the number of tuples $(a_1, a_2, b_1, b_2, c_1, c_2)$ such that $(a_1, b_1, c_1) \neq (a_2, b_2, c_2)$ with $T_{n,m,k}(a_1, b_1, c_1) = T_{n,m,k}(a_2, b_2, c_2)$.

Now, the condition $T(a_1, b_1, c_1) = T(a_2, b_2, c_2)$ implies that

$$n^n \left(b_1^{n-mk} - b_2^{n-mk}\right) = (-1)^{n+mk+k} \left(a_1^n c_1^k - a_2^n c_2^k\right) (mk)^{mk} (n - mk)^{n-mk}.$$

However, for fixed (a_1, a_2, c_1, c_2), there are $O(X^\varepsilon)$ many choices for b_1 and b_2.

Hence

$$\sum_{d \leq X} S(d)^2 - \sum_{d \leq X} S(d) \ll X^\varepsilon A^2 C^2.$$

Since $B > (AC)^{1+\delta}$, we therefore have

$$\sum_{d \leq X} S(d)^2 \ll X^\varepsilon A^2 C^2 + ABC \ll ABC,$$

which concludes the proof. □

Now we can conclude the proof of our main theorem.

Proof of Theorem 3.5.1. By the Cauchy-Schwarz inequality, we get

$$\left(\sum_{d \leq X} S(d)\right)^2 \leq D(A, B, C) \left(\sum_{d \leq X} S(d)^2\right).$$

Therefore, from Lemmas 3.5.2 and 3.5.3, the result follows. □

For each square-free integer d, let $\mathcal{D}(A, B, C)$ denote the set of (a, b, c), taken exactly once from the solution set of the equation (3.5.1). Then we have the following corollary:

Corollary 3.5.4. Under the hypothesis of Theorem 3.5.1, we have

$$|\mathcal{D}(A, B, C)| \gg ABC.$$

Remark. Again note that, since n (≥ 3), m, and k are odd integers, from equation 3.3.3 we get

$$\mathbb{Q}\left(\sqrt{\Delta_{n,m,k}(a,b,c)}\right) = \mathbb{Q}\left(\sqrt{(-1)^{\binom{n}{2}} T_{n,m,k}(a,b,c)}\right).$$

Therefore Corollary 3.5.4 implies that under the hypothesis of Theorem 3.5.1, the number of distinct quadratic fields $\mathbb{Q}\left(\sqrt{\Delta_{n,m,k}(a,b,c)}\right)$ is $\gg ABC$.

Further Work Plan

The results established in this thesis point toward several consequential problems and possible extensions that lead to further study. We outline below a few questions for future investigation, organized according to the chapters of the thesis.

Chapter 1

Theorem 1.1.1 asserts that if $\alpha \in \mathbb{Q}$ is not a negative integer, then there exists a positive integer $N(\alpha)$ such that the generalized ϕ-Laguerre polynomials $L_{n,\alpha}^{\phi}(x)$ are irreducible over $\mathbb{Q}$ for all $n \geq N(\alpha)$.

Question 1. Find an effective lower bound for $N(\alpha)$, or obtain an explicit expression of $N(\alpha)$ in terms of α.

Suppose $\alpha \in \{5, 6, 7, 8, 9, 10\}$. In this case, it can be shown that $L_{n,\alpha}^{\phi}(x)$ is irreducible over $\mathbb{Q}$ for all $n \geq 151$. Hence, one may verify the irreducibility of $L_{n,\alpha}^{\phi}(x)$ for degrees $n \leq 150$ by implementing an appropriate computer algorithm.

Question 2. Develop a computer programme (for example, using SageMath, Maple, or Python, etc.) to determine for which values of $n \in [1, N(\alpha)]$, the polynomials $L_{n,\alpha}^{\phi}(x)$ remain irreducible over $\mathbb{Q}$.

Such a computation would provide a comprehensive study of the irreducibility of $L_{n,\alpha}^{\phi}(x)$ for all $\alpha \in \mathbb{Q} \setminus \mathbb{Z}^{-}$. However, it should be noted that for large values of α, the implementation may require strong computational resources.

Another type of problem on generalized ϕ-Laguerre polynomials may be posed as follows:

Question 3. Determine the Galois groups associated with the polynomials $L_{m,\alpha}^{\phi}(x)$ at least for certain special choices of $\phi(x) \in \mathbb{Z}[x]$.

Chapter 2

Here using *square sieve*, we have computed a lower bound of the number of tuples (a, b, c) of integers,

for which $T_{n,m,k}(a,b,c)$ possesses distinct squarefree parts, where n and m are fixed odd integers and $k=1$.

Question 4. Establish a lower bound for the number of distinct squarefree parts of the discriminants of the irreducible polynomials $t^n + c(at^k + b)^m \in \mathbb{Z}[t]$ for fixed n, m, and $k \geq 2$.

Chapter 3

In the section 3.5, we proved under *abc-conjecture* that there exists a positive portion of tuples (a,b,c) of integers for which $T_{n,m,k}(a,b,c)$ is squarefree, where n (≥ 3), m, and k be odd integers. This result in turn motivates the following question :

Question 5. Determine whether there exists a positive proportion of tuples $(a,b,c) \in \mathbb{Z}^3$ such that the irreducible polynomials $t^n + c(at^k + b)^m$ are monogenic or have a Galois group S_n over $\mathbb{Q}$.

Bibliography

[1] A. Adelberg, Higher Order Bernoulli Polynomials and Newton Polygons, In G.E. Bergum, A.N. Philippou, A.F. Horadam (eds), *Applications of Fibonacci Numbers*, **7** (1998), 1-8, Springer, Dordrecht.

[2] A. Adelberg, M. Filaseta, On mth order Bernoulli polynomials of degree m that are Eisenstein, *Colloq. Math.*, **93** (2002), 21-26.

[3] R.C. Baker, G. Harman, J. Pintz, The exceptional set for Goldbach's problem in short intervals, In G. Greaves, G. Harman, & M. Huxley, *Sieve Methods, Exponential Sums, and their Applications in Number Theory,* London Math. Soc. Lecture Note Series, 1-54.

[4] M. Bhargava, On the number of monogenizations of a quartic order, *Pub. Math. Debrecen*, **100** (2022), 513-531.

[5] M. Bhargava, A. Shankar, and X. Wang, Squarefree values of polynomial discriminants *I*, *Invent. Math.*, **228** (2022), 1037-1073.

[6] A. Bishnoi, S.K. Khanduja, On Eisenstein-Dumas and generalized Schönemann polynomials, *Comm. Algebra,* **38** (2010), 3163-3173.

[7] D. W. Boyd, G. Martin, and M. Thom, Squarefree values of trinomial discriminants, *LMS J. Comput. Math.*, **18(1)** (2015), 148-169.

[8] R. Brown, Roots of generalized Schönemann polynomials in henselian extension fields, *Indian J. Pure Appl. Math.*, **39** (2008), 403-410.

[9] L. Carlitz, On a problem in additive arithmetic II, *Quart. J. Math.*, **3** (1932), 273-290.

[10] L. Carlitz, Note on irreducibility of the Bernoulli and Euler polynomials, *Duke Math. J.*, **19** (1952), 475-481.

[11] L. Carlitz, A note on Bernoulli numbers and polynomials of higher order, *Proc. Amer. Math. Soc.*, **3** (1952), 608-613.

[12] R.F. Coleman, On the Galois groups of the exponential Taylor polynomials, *L'Enseignement Math.*, **33** (1987), 183-189.

[13] G. Dumas, Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels, *Journal de Math. Pure et Appl.,* **2** (1906), 191–258.

[14] E.F. Ecklund, R.B. Eggleton, P. Erdös, J.L. Selfridge, On the prime factorization of binomial coefficients, *J. Austral. Math. Soc., Ser. A*, **26** (1978), 257-269.

[15] P. Erdös, Arithmetical properties of polynomials, *J. London Math. Soc.*, 28 (1953), 416–425.

[16] J. Esmonde and M. R. Murty, *Problems in Algebraic Number Theory*, 2nd ed. GTM **190** (2005), Springer New York.

[17] T. Estermann, Einige Sätze über quadratfeie Zahlen, *Math. Ann.*, **105** (1931), 653–662.

[18] M. Filaseta, A generalization of an irreducibility theorem of I. Schur, in: Analytic Number Theory, Proc. Conf. in Honor of Heini Halberstam, Vol. 1, B. C. Berndt, H. G. Diamond, and A. J. Hildebrand (eds.), BirkhÂ¨auser, Boston, 1996, 371-395.

[19] M. Filaseta, The irreducibility of all but finitely many Bessel polynomials, *Acta Math.* **174** (1995), 383-397.

[20] M. Filaseta and O. Trifonov, The Irreducibility of the Bessel polynomials, *J. Reine Angew. Math.*, **550** (2002), 125-140.

[21] M. Filaseta, T.Y. Lam, On the irreducibility of the generalised Laguerre polynomials, *Acta Arith.*, **105** (2002), 177-182.

[22] L. Gegenbauer, Asymptotische Gesetze der Zahlentheorie *Denkschriften Akad. Wiss. Wien,* **49**, (1885), 37–80.

[23] A. Granville, ABC allows us to count squarefrees, *Int. Math. Res. Not.*, **19** (1998), 991-1009. MR1654759

[24] F. Hajir, Some A_n-extensions obtained from generalized Laguerre polynomials, *J. Number Theory* **50** (1995), 206-212.

[25] F. Hajir and S. Wong, Specializations of one-parameter families of polynomials. *Ann. Inst. Fourier (Grenoble)* **56** (2006), no. 4, 1127–163.

[26] F. Hajir, Algebraic properties of a family of generalized Laguerre polynomials, *Canad. J. Math.*, **61** (2009), 583-603.

[27] H. Hasse, *Zahlentheorie*, Akademie-Verlag, Berlin, 1963.

[28] D. R. Heath-Brown, The square sieve and consecutive square-free numbers, *Math. Ann.*, **266** (1984), 251-259.

[29] D. R. Heath-Brown, Square-free values of $n^2 + 1$, *Acta Arith.*, **155** (2012), 1-13.

[30] H. A. Helfgott, Square-free values of $f(p)$, f cubic, *Acta Math.*, **213** (2014), 107-135.

[31] C. Hooley, On the power free values of polynomials, *Mathematika*, **14** (1967), 21-26.

[32] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Mathematics, No. 70, Cambridge University Press, Cambridge, New York, Melbourne, 1976.

[33] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.

[34] A. Jakhar, On the factors of a polynomial, *Bull. London Math. Soc.* **52** (2020), 158-160.

[35] A. Jakhar, A simple generalization of the Schönemann-Eisenstein irreducibility criterion, *Arch. Math.*, **117** (2021), 375-378.

[36] A. Jakhar, R. Kalwaniya and S. Kotyada, On Monogenity of Number Fields and Galois Group, *Int. J. Number Theory*, **21** (8) (2025), 1995-2013.

[37] A. Jakhar, S. K. Khanduja, and N. Sangwan, Characterisation of primes dividing the index of a trinomial, *Int. J. Number Theory*, **13** (10) (2017), 2505-2514.

[38] A. Jakhar, S. Laishram and P. Yadav, Explicit discriminant of a class of polynomial, monogenity and Galois group. Communications in Algebra, **53** (7) (2025), 2937–2948.

[39] A. Jakhar, N. Sangwan, On a mild generalization of the Schönemann irreducibility criterion, *Comm. Algebra*, **45** (2017), 1757-1759.

[40] B. Jhorar, S. K. Khanduja, A Generalization of the Eisenstein-Dumas-Schönemann Irreducibility Criterion, *Proc. Edinb. Math. Soc.*, **60** (2017), 937-945.

[41] A. Jindal, S. K. Khanduja, An extension of Schur's irreducibility result, *J. Algebra*, **664** (2025), 398-409.

[42] L. Jones, A brief note on some infinite families of monogenic polynomials, *Bull. Aust. Math. Soc.*, **100** (2019), 239-244.

[43] L. Jones, Monogenic polynomials with non-squarefree discriminant, *Proc. Amer. Math. Soc.*, **148** (2020), 1527-1533.

[44] L. Jones and D. White, Monogenic trinomials with non-squarefree discriminant, *Int. J. Math.*, **32** (2021), 2150089, 21 pages.

[45] L. Jones, On necessary and sufficient conditions for the monogenity of a certain class of polynomials, *Math. Slovaca*, **72**(3) (2022), 591-600.

[46] L. Jones and T. Phillips, Infinite families of monogenic trinomials and their Galois groups, *Int. J. Math.*, **29** (2018), 1850039, 11 pages.

[47] S. Kaur and S. Kumar, On a conjecture of Lenny Jones about certain monogenic polynomials, *Bull. Aust. Math. Soc.*, **110** (2023), 72-76.

[48] K. S. Kedlaya, A construction of polynomials with squarefree discriminants, *Proc. Amer. Math. Soc.*, **140** (9) (2012), 3025-3033.

[49] S.K. Khanduja, R. Khassa, A generalization of Eisenstein-Schönemann irreducibility criterion, *Manuscripta Math.*, **134** (2011), 215-224.

[50] S.K. Khanduja, J. Saha, On a generalization of Eisenstein's irreducibility criterion, *Mathematika* **44** (1997), 37-41.

[51] S. Laishram, T.N. Shorey, The greatest prime divisor of a product of terms in an arithmetic progression, *Indag. Math.*, **20** (2009), 427-434.

[52] S. Laishram and T. N. Shorey, Irreducibility of generalized Hermite-Laguerre Polynomials, *Funct. Approx.*, **47** (2012), 51-64.

[53] S. Laishram and T. N. Shorey, Irreducibility of generalized Hermite–Laguerre polynomials II, *Indag. Math.*, **20** (2009), 427-434.

[54] S. Laishram and T. N. Shorey, Irreducibility of generalized Hermite–Laguerre polynomials III, *J. Number Theory*, **164** (2016), 303-322.

[55] S. Laishram, S.G. Nair and T. N. Shorey, Irreducibility of generalized Laguerre polynomials $L_n^{(\frac{1}{2}+u)}(x)$ with integer u, *J. Number Theory*, **160** (2016), 76-107.

[56] D.H. Lehmer, On a problem of Störmer, *Illinios J. Math.*, **8** (1964), 57-79.

[57] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997. MR1429394

[58] P. J. McCarthy, Some irreducibility theorems for Bernoulli polynomials of higher order, *Duke Math. J.*, **27** (1960), 313-318.

[59] P. J. McCarthy, Irreducibility of certain Bernoulli polynomisAs, *Amer. Math. Monthly*, **68** (1961), 352-353.

[60] P. J. McCarthy, Irreducibility of Bernoulli polynomials of higher order, *Can. J. Math.*, **14** (1962), 565-567.

[61] P. Mihailescu, Primary cyclotomic units and a proof of Catalan's conjecture, *J. Reine Angew. Math.*, **572** (2004), 167-195.

[62] A. Mukhopadhyay, M. R. Murty, and K. Srinivas, Counting squarefree discriminants of trinomials under abc, *Proc. Amer. Math. Soc.*, **137** (2009), 3219-3226. MR2515392

[63] M. R. Murty, Exponents of class groups of quadratic fields, *Topics in Number Theory* (University Park, PA, 1997), Math. Appl., **467**, Kluwer Acad. Publ., Dordrecht, 1999, 229-239. MR1691322

[64] T. Nagell, Sur une classe d'équations exponentielles, *Ark. Mat.*, **3** (1958), 569-582.

[65] S. G. Nair and T. N Shorey, Irreducibility of Laguerre Polynomial $L_n^{(-1-n-r)}(x)$, *Indag. Math.* **26** (2015), 615-625.

[66] S. G. Nair and T.N. Shorey, Generalised Laguerre Polynomials with applications, *Math. Student* **86**, (2017), 87-101.

[67] J. Neukirch, *Algebraic Number Theory*, Translated by Norbert Schappacher, Springer-Verlag, 1999.

[68] Ø. Ore, Newtonsche Polygone in der Theorie der algebraischen Körper, *Mathematische Annalen*, **99** (1928), 84-117.

[69] B. Poonen, Squarefree values of multivariable polynomials, *Duke Math. J.* **118** (2) (2003), 353-373.

[70] H. Pasten, The ABC conjecture, arithmetic progressions of primes and squarefree values of polynomials at prime arguments, *Int. J. Number Theory*, **11** (3) (2015), 721-737.

[71] P. Ribenboim, *The Theory of Classical Valuations*, Springer Monographs in Math. Springer, NY, 1999.

[72] G. Robin, Estimation de la fonction de Tchebychev θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$, nombre de diviseurs premiers de n, *Acta Arith.*, **42** (4) (1983), 367-389.

[73] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzi- bilitätsfragen, I, *Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl.*, **14** (1929), 125-136.

[74] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzi- bilitätsfragen, II, *Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl.*, **14** (1929), 370-391.

[75] I. Schur, Gleichungen ohne Affekt, *Sitzungsberichte der Preussischen Akademie der Wissenschaften, physikalisch-Mathematische Klasse* (1930), 443-449.

[76] I. Schur, Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen polynome, *J. für die reine und angew. math.*, **165** (1931), 52-58.

[77] E.A. Sell, On a certain family of generalized Laguerre polynomials, *J. Number Theory* **107** (2004), 266-281.

[78] I. E. Shparlinski, On quadratic fields generated by discriminants of irreducible trinomials, *Proc. Amer. Math. Soc.*, **138** (2010), no. 1, 125-132.

[79] I.E. Shparlinski, Squarefree parts of discriminants of trinomials, *Arch. Math.*, **102** (2014), 545-554.

[80] T.N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts. in Math. Cambridge, Cambridge University Press, **87**, 1986.

[81] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc.*, **61**(2) (2000), 681-690.

[82] L. B. Soroker, O. B. Porath, On the Galois theory of generalized Laguerre polynomials and trimmed exponential, *Acta Arith.*, **200** (2021), 183-196.

[83] D. I. Tolev, On the number of pairs of positive integers $x,\ y \leq H$ such that x^2+y^2+1 is squarefree, *Monatsh Math.,* **165** (2012), 557–567.

[84] H. B. Yu, Estimates of character sums with exponential function, *Acta Arith.*, **97** (2001), 211–218.