Université de Montréal

ON THE DISTRIBUTION OF POLYNOMIALS HAVING A GIVEN NUMBER OF IRREDUCIBLE FACTORS OVER FINITE FIELDS

par
Arghya Datta

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maître ès sciences (M.Sc.)
en mathématiques

Août, 2022

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé:

ON THE DISTRIBUTION OF POLYNOMIALS HAVING A GIVEN NUMBER OF IRREDUCIBLE FACTORS OVER FINITE FIELDS

présenté par:

Arghya Datta

a été évalué par un jury composé des personnes suivantes:

Matilde Lalin,	président-rapporteur
Andrew Granville,	directeur de recherche
Dimitris Koukoulopoulos,	codirecteur
Alexander Fribergh,	membre du jury

Mémoire accepté le: 19/08/2022

RÉSUMÉ

Soit $q \geqslant 2$ une puissance première fixe. L'objectif principal de cette thèse est d'étudier le comportement asymptotique de la fonction arithmétique $\Pi_q(n,k)$ comptant le nombre de polynômes moniques de degré n et ayant exactement k facteurs irréductibles (avec multiplicité) sur le corps fini $\mathbb{F}_q$. Warlimont et Car ont montré que l'objet $\Pi_q(n,k)$ est approximativement distribué de Poisson lorsque $1 \leqslant k \leqslant A\log n$ pour une constante $A > 0$. Plus tard, Hwang a étudié la fonction $\Pi_q(n,k)$ pour la gamme complète $1 \leqslant k \leqslant n$. Nous allons d'abord démontrer une formule asymptotique pour $\Pi_q(n,k)$ en utilisant une technique analytique classique développée par Sathe et Selberg. Nous reproduirons ensuite une version simplifiée du résultat de Hwang en utilisant la formule de Sathe-Selberg dans le champ des fonctions. Nous comparons également nos résultats avec ceux analogues existants dans le cas des entiers, où l'on étudie tous les nombres naturels jusqu'à x avec exactement k facteurs premiers. En particulier, nous montrons que le nombre de polynômes moniques croît à un taux étonnamment plus élevé lorsque k est un peu plus grand que $\log n$ que ce que l'on pourrait supposer en examinant le cas des entiers.
Pour présenter le travail ci-dessus, nous commençons d'abord par la théorie analytique des nombres de base dans le contexte des polynômes. Nous introduisons ensuite les fonctions arithmétiques clés qui jouent un rôle majeur dans notre thèse et discutons brièvement des résultats bien connus concernant leur distribution d'un point de vue probabiliste. Enfin, pour comprendre les résultats clés, nous donnons une discussion assez détaillée sur l'analogue de champ de fonction de la formule de Sathe-Selberg, un outil récemment développé par Porrit et utilisons ensuite cet outil pour prouver les résultats revendiqués.

Mots-clés : Polynômes sur des corps finis, Nombres premiers, Polynômes irréductibles, Nombre Fixe de facteurs Irréductibles, Fonction zêta de Riemann, Méthode de Sathe-Selberg, Fonctions multiplicatives, Théorème d'Erdos-Kac, Approximation du point de selle, Théorie analytique des nombres.

ABSTRACT

Let $q \geqslant 2$ be a fixed prime power. The main objective of this thesis is to study the asymptotic behaviour of the arithmetic function $\Pi_q(n,k)$ counting the number of monic polynomials that are of degree n and have exactly k irreducible factors (with multiplicity) over the finite field $\mathbb{F}_q$. Warlimont and Car showed that the object $\Pi_q(n,k)$ is approximately Poisson distributed when $1 \leqslant k \leqslant A\log n$ for some constant $A > 0$. Later Hwang studied the function $\Pi_q(n,k)$ for the full range $1 \leqslant k \leqslant n$. We will first prove an asymptotic formula for $\Pi_q(n,k)$ using a classical analytic technique developed by Sathe and Selberg. We will then reproduce a simplified version of Hwang's result using the Sathe-Selberg formula in the function field. We also compare our results with the analogous existing ones in the integer case, where one studies all the natural numbers up to x with exactly k prime factors. In particular, we show that the number of monic polynomials grows at a surprisingly higher rate when k is a little larger than $\log n$ than what one would speculate from looking at the integer case.

To present the above work, we first start with basic analytic number theory in the context of polynomials. We then introduce the key arithmetic functions that play a major role in our thesis and briefly discuss well-known results concerning their distribution from a probabilistic point of view. Finally, to understand the key results, we give a fairly detailed discussion on the function field analogue of the Sathe-Selberg formula, a tool recently developed by Porrit and subsequently use this tool to prove the claimed results.

Keywords: Polynomials over finite fields, Prime numbers, Irreudcible polynomials, Fixed number of irreducible factors, Riemann zeta function, Sathe-Selberg method, Multiplicative functions, Erdos-Kac theorem, Saddle point approximation, Analytic number theory.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

CLT	Central Limit Theorem
CRT	Chinese Remainder Theorem
gcd	Greatest common divisor
lcm	Least common multiple
RH	Riemann Hypothesis
PNT	Prime Number Theorem
LHS	Left hand side
RHS	Right hand side
CS	Cauchy-Schwartz inequality

NOTATION

In this thesis, the sets of numbers $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, respectively, represent the positive integers, the integers, the rational numbers, the real numbers and the complex numbers. The variables p, I (and their subscripts) always represent prime numbers and irreducible polynomials unless explicitly stated otherwise. We employ some other standard notation which will be used throughout the work. For a complex number $z \in \mathbb{C}$, we denote the real and the imaginary parts by $\Re(z)$ and $\Im(z)$ respectively.

$\lfloor x \rfloor$	The greatest integer smaller than or equal to x for $x \in \mathbb{R}$.
$P, \mathscr{P}$	The set of all primes and the set of all monic irreducibles in $\mathbb{F}_q[t]$ where $q \geqslant 2$ is a prime power.
$\mathscr{M}$	The set of all monic polynomials in $\mathbb{F}_q[t]$.
$\mathscr{M}_n, \mathscr{P}_n$	The set of monics (respectively monic irreducible polynomials) of degree n.
$1_A(x)$	The indicator function of the set A which returns 1 or 0 depending on whether $x \in A$ or not.
γ	Euler-Mascheroni constant.
(a,b)	The greatest commmon divisor of two integers a and b. The same notation is also used for polynomials and for open intervals but there will be no ambiguity from the context.
$[a,b]$	The least commmon multiple of two integers a and b. The same notation is also used for polynomials and for closed intervals but there will be no ambiguity from the context.
$\#B$	The cardinality of any set B.
$f(x) = O_A(g(x))$	$f(x) \leqslant Cg(x)$ for a sufficiently large constant $C > 0$. The subscript A signifies that the constant C is allowed to depend on the quantity A.
$f(x) \ll_A g(x)$	Vinogradov's notation, same as $f(x) = O_A(g(x))$.
$f(x) \sim g(x)$	$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$
$f(x) = o(g(x))$	$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$

ACKNOWLEDGMENTS

The author would like to thank his supervisor, Prof. Andrew Granville, for suggesting that he work on this exciting project and also his co-supervisor, Prof. Dimitris Koukoulopoulos, for many helpful conversations and continuous support during this project and for their valuable suggestions and comments on the previous versions of this thesis. The dissertation would not have taken shape without their help. The author was financially supported by his supervisors and the fellowships provided by Faculté des études supérieures et postdoctorales (FESP), Bourse d'exemption of Université de Montréal, Centre interuniversitaire en calcul mathématique algébrique (CICMA) while carrying out this work. The author would especially like to thank Prof. Granville for patiently reading through the work several times and for his continuous constructive feedback to improve on the earlier versions. Moreover, everything the author tells in his dissertation is based on techniques that he learned in his analytic number theory classes with Prof. Granville and Prof. Koukoulopoulos. He would also like to thank Ofir Gorodetsky for informing him that this thesis reproduces two earlier results established by Warlimont and Hwang, which the author was initially unaware of. Finally, the author would also like to thank the jury members for their attentive reading and instructive comments.

CHAPTER 1

INTRODUCTION

Analytic Number theory is a branch of mathematics that studies the patterns and properties of integers using tools from real and complex analysis. One of the central aims of this subject is to understand the underlying distribution of the prime numbers that remains mysterious to this date. The prime numbers are the fundamental building blocks of the integers. It is evident that some integers can be broken down into non-trivial smaller parts, for instance, $12 = 4 \times 3 = 6 \times 2$, while the integer 7 can not be broken down any further. All these unbreakable integers share the common feature that they are only divisible by 1 and themselves and are called the **Prime numbers**. Once one learns from the Fundamental Theorem of Arithmetic that every integer can be uniquely factored into its prime divisors, one quickly realizes the importance of understanding these building blocks. Perhaps the first question that comes to our mind concerning prime numbers is whether there are finite or infinitely many primes. By elementary means, it is possible to show that there are infinitely many primes, but their occurrences do seem to get rarer as we travel further along the number line. It was a challenge for mathematicians for a long time to figure out how many primes there are up to a given large parameter x. This question was resolved in the 19th century and today is known as the **Prime number theorem**, one of the most celebrated results in analytic number theory. But then, there are still several fundamental questions that stem from the study of the distributions of primes that remain unanswered. A notable example is the **Riemann hypothesis**, a solution to which will help us quite accurately understand how the primes are distributed among integers. In this regard, there are often situations where we do not have answers to both archaic and simple questions concerning prime numbers. For instance, we already discussed that it can be shown that there are infinitely many primes. However, a natural follow-up that asks whether there are infinitely many pairs $(p, p+2)$ of primes, also known as the **Twin prime conjecture** remains wide open. Another primary goal of the subject is to understand the interaction between the two fundamental operations, addition and multiplication. It is generally believed that these two operations do not see each other in the sense that, from the prime decomposition of a given integer $a \in \mathbb{N}$, it is impossible to speculate anything about the prime decomposition of $a+1$ apart from the obvious fact that these

decompositions have no prime numbers in common.

1.1 Analytic number theory in function fields

Classical number theory is primarily concerned with studying the arithmetic properties of the set of integers $\mathbb{Z}$. While the field of number theory in function fields is definitely more recent than the old classical number theory, the resemblance of properties of the ring $\mathbb{F}_q[t]$ with $\mathbb{Z}$ has long been well known. A significant similarity between these two worlds can be observed at the nascent level. We know that every integer can be uniquely decomposed into prime factors, and likewise, every polynomial $f \in \mathbb{F}_q[t]$ can also be uniquely decomposed into irreducible elements. Also, by elementary means, it is possible to show there are infinitely many irreducible polynomials in $\mathbb{F}_q[t]$ as it is in the case for $\mathbb{Z}$. All these observations hint at the possible existence of an analogous theory in the world of polynomials. As we shall see in Chapter 1 that this is indeed the case.

The study of Algebraic number theory deals with the finite extensions K of the rationals $\mathbb{Q}$, also known as algebraic number fields. Just like the set of integers $\mathbb{Z}$ inside $\mathbb{Q}$, we can also consider the set of algebraic integers, denoted by $\mathscr{O}_K$ inside K. Formally $\mathscr{O}_K$ is defined by the integral closure of $\mathbb{Z}$ in K. All these can be summarized in the following commutative diagram,

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Q} \\ \downarrow & & \downarrow \\ \mathscr{O}_K & \longrightarrow & K \end{array}$$

where all the arrows denote the natural inclusion maps. We can now consider the field of fractions $k := \mathbb{F}_q(t)$ of the polynomial ring $\mathbb{F}_q[t]$ and carry out another similar construction. The finite extensions of the field k are called algebraic function fields.

The main focus of this thesis will be to explore the arithmetic of polynomials over finite fields. However, in what follows, we also plan to provide the resemblance (except in very rare cases) between $\mathbb{Z}$ and $\mathbb{F}_q[t]$ for every result we discuss.

1.2 Structure of the thesis

The thesis is divided into six chapters. Chapter 2 presents the function field analogues of well-known results in elementary number theory. We mention famous results due to Fermat and Euler. We also discuss the prime number theorem for both $\mathbb{Z}$ and $\mathbb{F}_q[t]$.

In chapter 3, we introduce the Riemann zeta function, an object of utmost importance in analytic number theory and discuss its key properties.

Chapter 4 gives a basic but relatively detailed introduction to arithmetic functions. In particular, we focus on the statistical behaviour of two arithmetic functions $\omega(n)$, $\Omega(n)$ which count the number of prime factors of a given integer n. We will mention a central limit theorem due to Erdos and Kac for the function $\omega(n)$ and prove an analogous CLT for $\mathbb{F}_q[t]$.

Later in chapter 5, we introduce the reader to a famous problem that was originally asked by Gauss and later was pursued by many mathematicians, including Hardy and Ramanujan and Landau. We will then briefly explore how this problem later motivated the invention of a specific analytic technique due by Sathe, Selberg and Delange, which will be one of the key stepping stones of two new theorems that we will prove in Chapter 6, where the main contribution of this thesis is made.

In Chapter 6, our goal will be to present detailed proofs of the two main results of this thesis using some techniques discussed in the earlier chapters. Our main results concern the distribution of the functions $\Omega_q(f)$ and $\omega_q(f)$ for some $f \in \mathbb{F}_q[t]$ which counts the number of irreducible factors of a given monic polynomial f.

CHAPTER 2

THE WORLD OF INTEGERS AND POLYNOMIALS

2.1 Arithmetic in $\mathbb{F}_q[t]$

In this chapter we will work with the polynomial ring $\mathbb{F}_q[t]$ and explore the basic arithmetic structure of polynomials. For the exposition of this chapter we closely follow the material presented in [22].

Let $f \in \mathbb{F}_q[t]$ be a degree n polynomial, we know f can be written as

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0,$$

where the coefficients $a_i \in \mathbb{F}_q$ for every $i \in \{0, \ldots, n\}$. If the leading coefficient a_n is 1, we call f a monic polynomial. Let us define the set

$$\mathscr{M} := \{ f \in \mathbb{F}_q[t] : \ f \text{ is monic } \}.$$

Elements of the set $\mathscr{M}$ will essentially play the role of positive integers. If the field $\mathbb{F}_q$ has q elements then the cardinality of the set $\mathscr{M}$ is q^n since there are q choices for each coefficients $a_0, \ldots, a_{n-1}$. Given two polynomials $f(t), g(t) \in \mathbb{F}_q[t]$ we say $g(t)$ divides $f(t)$ if and only if there exist a polynomial $h(t) \in \mathbb{F}_q[t]$ such that $f(t) = g(t)h(t)$. We write $g|f$ to denote that, g divides f and $g \nmid f$ to denote otherwise. With the above framework in mind we can readily prove the following proposition that reveals a key nature about the ring $\mathbb{F}_q[t]$.

Proposition 2.1.1. *Let $f(t), g(t) \in \mathbb{F}_q[t]$ be given such that $g \nmid f$ and $g \neq 0$. There exists polynomials $q(t), r(t) \in \mathbb{F}_q[t]$ such that $f(t) = g(t)q(t) + r(t)$ and $deg(r) < deg(g)$*

We refer the reader [22] for a proof of the claim using mathematical induction.

The above proposition can be used show that $\mathbb{F}_q[t]$ is a Unique Factorization Domain (UFD) which implies every polynomial $f \in \mathscr{M}$ can be uniquely written as

$$f = \prod_{1 \leqslant j \leqslant k} I_j^{\alpha_j}$$

where I_j is a monic irreducible polynomial for each $1 \leqslant j \leqslant k$. The previous proposition can actually be used to show a stronger fact that $\mathbb{F}_q[t]$ is a Euclidean Domain (ED) which implies every ideal of $\mathbb{F}_q[t]$ is generated by a single element. We have already started to see a strong connection here between $\mathbb{F}_q[t]$ and the set of integers $\mathbb{Z}$.
Our next goal is to discuss some elementary number theory over $\mathbb{F}_q[t]$ which will be helpful in later chapters, in particular, analogues of Euler's phi function and establish some related results. We record the following;

Lemma 2.1.2. *The multiplicative group of a finite field is cyclic.*

The above result from abstract algebra turns out to be useful in what we are going to prove next. The proof of the above lemma can be found in [2].

Proposition 2.1.3. *Let $I \in \mathbb{F}_q[t]$ be a monic irreducible polynomial. Then the multiplicative group $\left(\mathbb{F}_q[t]/(I)\right)^*$ is cyclic and has $q^{deg(I)} - 1$ elements.*

Proof. The polynomial ring $\mathbb{F}_q[t]$ is an Euclidean Domain and hence a Principal Ideal Domain (PID). Therefore the ideal $(I) \subset \mathbb{F}_q[t]$ generated by an irreducible element is maximal. Thus the quotient $\mathbb{F}_q[t]/(I)$ is isomorphic to a finite field. Since an element $g \in \mathbb{F}_q[t]/(I)$ in the quotient can be uniquely expressed as

$$g = \sum_{j=1}^{\deg(I)\text{-}1} b_j t^j (\bmod I) \text{ for coefficients } b_j \in \mathbb{F}_q,$$

there are $q^{\deg(I)} - 1$ choices for $g \neq 0$ as the coefficients b_j can be chosen in q different ways for each j excluding the case where they all are zero. The conclusion now follows from Lemma 2.1.2. □

The above proposition rings a bell about introducing a notion of size for a given polynomial. The norm of an integer n, is defined as

$$|n| = \begin{cases} n, & \text{if } n \geqslant 0 \\ -n, & \text{otherwise.} \end{cases}$$

As we can notice $|n|$ is also equal to the cardinality of the quotient ring $\mathbb{Z}/n\mathbb{Z}$. Inspired by this observation, we would like to define the norm for a given polynomial $f \in \mathbb{F}_q[t]$ to be the size of

the quotient ring $\mathbb{F}_q[t]/(f)$.

Definition 2.1.4 (Norm of a polynomial)**.** Let $f \in \mathbb{F}_q[t]$ be a non-zero polynomial. We define the norm of f, denoted by $|f|$, to be the quantity $q^{deg(f)}$. We also define $|f| = 0$ if f is identically 0.

Remark 2.1.5. *Given a polynomial $f \in \mathbb{F}_q[t]$, the norm defined above is multiplicative and satisfies all the properties of an usual norm.*

2.2 Euler's theorem for integers and polynomials

In elementary number theory, for a positive integer $n \in \mathbb{N}$ we define Euler's phi(ϕ) function as follows

$$\phi(n) := \#\big\{1 \leqslant m \leqslant n-1 : \ \gcd(m,n) = 1\big\} = \#(\mathbb{Z}/n\mathbb{Z})^*. \tag{2.2.1}$$

If we know the prime decomposition of n, it is not difficult to obtain an explicit formula describing $\phi(n)$ using the inclusion-exclusion principle. Let us assume the prime decomposition for n; $n = \prod_{j=1}^{k} p_j^{\alpha_j}$ where $p_1, \ldots, p_k$ are primes. We will not take the path of inclusion exclusion here and use the Chinese remainder theorem instead.

Theorem 2.2.1 (Chinese Remainder theorem for Integers)**.** *Let $m_1, m_2, \ldots m_k$ be pairwise co-prime integers. We have the following isomorphism for rings,*

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \cong \mathbb{Z}/M\mathbb{Z}$$

where M is the product $m_1 m_2 \cdots m_k$.

In the above theorem, we can only focus on the group of units of each ring and get

Corollary 2.2.2. *Let $m_1, m_2, \ldots m_k$ be pairwise co-prime integers. We have the following group isomorphism,*

$$(\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^* \cong (\mathbb{Z}/M\mathbb{Z})^*$$

where M is the product $m_1 m_2 \cdots m_k$.

In our case, the corollary readily gives us the group isomorphism

$$(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^*$$

and hence equating the cardinalities both side, we readily obtain

$$\phi(n) = \prod_{j=1}^{k} \phi(p_j^{\alpha_j}) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right),$$

since the number of elements that are co-prime to $p_j^{\alpha_j}$ in $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$ is $p_j^{\alpha_j - 1}(p_j - 1)$ for each j. An exact analogue of this result exists for polynomials as we are going to see next.

Proposition 2.2.3. *Let $I \in \mathbb{F}_q[t]$ be a monic irreducible polynomial. Then for each integer $\ell \in \mathbb{N}$ we have*

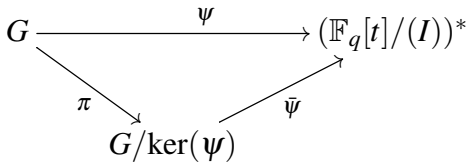
$$\#\left(\mathbb{F}_q[t]/(I^\ell)\right)^* = |I|^{\ell-1}(|I| - 1),$$

where $|I|$ denotes the norm of I.

Proof. Let us denote the group $\left(\mathbb{F}_q[t]/(I^\ell)\right)^*$ by G. We consider the group homomorphism $\psi : G \to (\mathbb{F}_q[t]/(I))^*$ defined by

$$f\left(\bmod I^\ell\right) \mapsto f(\bmod I).$$

The map ψ is surjective with the kernel $\ker(\psi) = (I)/\left(I^\ell\right)$ and we have the following commutative diagram



First isomorphism theorem says the induced map $\bar{\psi} : G/\ker(\psi) \to (\mathbb{F}_q[t]/(I))^*$ is an isomorphism which gives us $\#G = \#\ker(\psi)\#(\mathbb{F}_q[t]/(I))^* = |I|^{\ell-1}(|I| - 1)$ as the kernel has exactly $|I|^{\ell-1}$ elements. □

Let $f \in \mathbb{F}_q[t]$ be given. We define the Euler's phi(Φ) function in $\mathbb{F}_q[t]$ in the following way

$$\Phi(f) := \#(\mathbb{F}_q[t]/(f))^*$$

Using Proposition 2.2.3 we can evaluate the function Φ explicitly in terms of the irreducible factors of of f. First, we invoke the validity of CRT for general principal ideal domains and

hence in particular, for the polynomial ring $\mathbb{F}_q[t]$.

Theorem 2.2.4 (Chinese Remainder theorem for Polynomials)**.** *Let $f_1, f_2, \ldots, f_k \in \mathbb{F}_q[t]$ be pairwise co-prime polynomials. We then have the following isomorphism of rings*

$$\mathbb{F}_q[t]/(f_1) \times \cdots \times \mathbb{F}_q[t]/(f_k) \cong \mathbb{F}_q[t]/(f)$$

where f is the product $f_1 f_2 \cdots f_k$.

The above theorem implies the following analogue of Corollary 2.2.2.

Corollary 2.2.5. *Let $f_1, f_2, \ldots, f_k \in \mathbb{F}_q[t]$ be pairwise co-prime polynomials. We have the following isomorphism of groups*

$$\left(\mathbb{F}_q[t]/(f_1)\right)^* \times \cdots \times \left(\mathbb{F}_q[t]/(f_k)\right)^* \cong \left(\mathbb{F}_q[t]/(f)\right)^*,$$

where f is the product $f_1 f_2 \cdots f_k$.

Applying the corollary for $f = \prod_{j=1}^{k} I_j^{\alpha_j}$ we get

$$\left(\mathbb{F}_q[t]/(I_1^{\alpha_j})\right)^* \times \cdots \times \left(\mathbb{F}_q[t]/(I_k^{\alpha_j})\right)^* \cong \left(\mathbb{F}_q[t]/(f)\right)^*,$$

and once again equating the cardinalities we get

$$\Phi(f) = \prod_{j=1}^{k} \Phi(I_j^{\alpha_j}) = \prod_{j=1}^{k} |I_j|^{\alpha_j - 1}(|I_j| - 1) = |f| \prod_{\substack{I \mid f \\ I \text{ irreducible}}} \left(1 - \frac{1}{|I|}\right).$$

We are now in a position of establishing the analogues of Euler's theorem and as a result Fermat's little theorem for polynomials.

Theorem 2.2.6 (Euler's Theorem for polynomials)**.** *Let $f \in \mathbb{F}_q[t]$ be a non zero polynomial and g be another polynomial which is co-prime to f. We then have*

$$g^{\Phi(f)} \equiv 1 (\bmod f)$$

Proof. By definition of Φ, the group $\left(\mathbb{F}_q[t]/(f)\right)^*$ has $\Phi(f)$ elements. Therefore for every $g \in \left(\mathbb{F}_q[t]/(f)\right)^*$ such that $\gcd(g, f) = 1$, the conclusion follows from Lagrange's theorem for

finite groups. □

If $I \in \mathbb{F}_q[t]$ is a monic irreducible polynomial, then the above theorem immediately implies the analogue of Fermat's little theorem,

$$g^{|I|-1} \equiv 1 (\bmod I)$$

for any polynomial $g \in \mathbb{F}_q[t]$ such that $\gcd(g, I) = 1$.

2.3 Prime numbers and Irreducible polynomials

We have already seen that monic irreducible polynomials in $\mathbb{F}_q[t]$ play a similar role that of the prime numbers in $\mathbb{Z}$. The goal of this section will be to discuss the analogue of the famous **Prime Number Theorem (PNT)** for polynomials. We begin this section with a brief introduction to Prime Number Theorem for integers.

2.3.1 The prime counting function

When we first start studying how prime numbers are distributed among integers, perhaps the most fundamental question that comes to our mind is, how many primes are there up to a given integer, say x? More formally, let us define the prime counting function

$$\pi(x) = \#\big\{p \leqslant x : \ p \text{ is prime}\big\}.$$

Therefore, the basic question is, what can we say about the behaviour of $\pi(x)$ as x increases. This question goes back to the eminent mathematician Gauss who predicted the average nature of $\pi(x)$ by hand! According to Gauss's speculation in [9], we have

$$\pi(x) \approx \mathrm{Li}(x) \text{ where } \mathrm{Li}(x) := \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Table 2.I (below) captures the fluctuations of $\pi(x)$ from the function $x/\log x$. [28]

It took a considerable amount of time for mathematicians to prove formally that this prediction about the behavior of $\pi(x)$ was correct. In 1986, french mathematician de la Vallée Poussin [7]

x	$\pi(x)$	$\pi(x)-x/\log x$	$\frac{\pi(x)}{x/\log x}$
10	4	-0.3	0.921
10^2	25	3.3	1.151
10^3	168	23	1.161
10^4	1229	143	1.132
10^5	9592	906	1.104
10^6	78498	6116	1.084
10^7	664579	44158	1.071
10^8	5761455	332774	1.061
10^9	50847534	2592592	1.054
10^{10}	455052511	20758029	1.048
10^{15}	29844570422669	891604962452	1.031
10^{20}	2220819602560918840	49347193044659701	1.023
10^{25}	176846309399143769411680	3128516637843038351228	1.018

Table 2.I – $x/\log x$ and the function $\pi(x)$.

and Jaques Hadamard [13], [12] independently proved the following asymptotic result as $x \to \infty$

$$\pi(x) \sim \int_2^x \frac{dt}{\log t}. \tag{2.3.1}$$

The **PNT** has several equivalent forms. In modern textbooks on analytic number theory, it is easy to find a proof of (2.3.1) that uses techniques from complex analysis, in particular, Cauchy's residue theorem. Most proofs do not directly show the result described in (2.3.1); instead, they take a more convenient route via the Von-Mangoldt function to show an equivalent form of (2.3.1). The Von-Mangoldt function for natural numbers is defined as follows,

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k \text{ for some prime } p \text{ and a positive integer } k \\ 0, & \text{otherwise.} \end{cases}$$

Using partial summation technique (see ref), a method often used in analytic number theory, it can be checked that (2.3.1) is equivalent to the following asymptotic result as $x \to \infty$

$$\sum_{n \leqslant x} \Lambda(n) \sim x \tag{2.3.2}$$

A significant amount of effort goes into the proof of (2.3.2). It is no surprise that an analogous prime number theorem also exists for polynomials. However, the proof in the case of $\mathbb{F}_q[t]$ is

much simpler. In what follows, we shall see the results we discuss in the later chapters; almost always, the proof techniques in the integer case are relatively "more-involved" and harder than the corresponding counterparts for polynomials. We will try to explain this phenomenon in the next section, where we introduce the Riemann zeta function and discuss its properties for both integers and function fields.

2.3.2 Prime number theorem for polynomials

We turn our attention to the prime number theorem in $\mathbb{F}_q[t]$ for now. We wish to count how many irreducible polynomials there are of a given degree. We define

$$\pi_q(n) = \#\big\{I \in \mathscr{M}_n : \ I \text{ is irreducible}\big\},$$

where the subscript q denotes the number of elements in the ground field $\mathbb{F}$.
We follow an elegant proof outlined in [11]. It is possible to define an analogue of the Von-Mangoldt function that only detects the contribution of irreducible polynomials, similar to the one we saw in the integer setting.
Let $f \in \mathscr{M}$ be given. We define

$$\Lambda_q(f) = \begin{cases} \deg(f), & \text{if } f = I^k \text{ for some irreducible } I \text{ and a positive integer } k \\ 0, & \text{otherwise.} \end{cases}$$

We observe the following identity

$$\deg(f) = \sum_{\substack{g|f \\ g \in \mathscr{M}}} \Lambda_q(g)$$

holds, since the only degree contribution to the sum on the right hand side comes from the monic polynomials that divide f and are powers some irreducible. Our idea is to sum the above identity over all possible monics of degree n, so that we get

$$\sum_{f \in \mathscr{M}_n} \deg(f) = \sum_{f \in \mathscr{M}_n} \sum_{\substack{g|f \\ g \in \mathscr{M}}} \Lambda_q(g).$$

We have already seen in the beginning of the section 2.1 that there are q^n monic polynomials of degree n which means the left hand side is equal to nq^n. We also interchange the order of double summation and obtain

$$nq^n = \sum_{\substack{1\leqslant k\leqslant n\\ g\in\mathscr{M}_k}} \sum_{\substack{f=gh\\ h\in\mathscr{M}_{n-k}}} \Lambda_q(g) = \sum_{\substack{1\leqslant k\leqslant n\\ g\in\mathscr{M}_k}} \sum_{h\in\mathscr{M}_{n-k}} \Lambda_q(g) = \sum_{\substack{1\leqslant k\leqslant n\\ g\in\mathscr{M}_k}} \Lambda_q(g)q^{n-k}. \tag{2.3.3}$$

The final equality follows as the term $\Lambda_q(g)$ is independent of h and there are exactly q^{n-k} possible candidates for h, since given a degree k monic polynomial g, every choice for h with $\deg(h) = n-k$ would be valid and will contribute to the sum. Rewriting the identity with $n-1$ instead of n gives us

$$(n-1)q^{n-1} = \sum_{\substack{1\leqslant k\leqslant n-1\\ g\in\mathscr{M}_k}} \Lambda_q(g)q^{n-k-1}. \tag{2.3.4}$$

Multiplying both sides by q of (2.3.4) and subtracting from (2.3.3) we get

$$q^n = nq^n - (n-1)q^n = \sum_{\substack{1\leqslant k\leqslant n-1\\ g\in\mathscr{M}_k}} \left[\Lambda_q(g)q^{n-k} - \Lambda_q(g)q^{n-k}\right] + \sum_{\substack{g \text{ monic}\\ \deg(g)=n}} \Lambda_q(g).$$

Thus we arrive at the following conclusion

$$\sum_{\substack{g \text{ monic}\\ \deg(g)=n}} \Lambda_q(g) = q^n. \tag{2.3.5}$$

This is already good news as we established the analogue of (2.3.2). Also, passing to π_q from Λ_q will be less painful here as the partial summation will not be required, and in particular, using a simple Mobius inversion will be enough.

In (2.3.5) the summands on the left hand side is only non zero if $g = I^k$ for some monic irreducible polynomial I and some positive integer k. Therefore a contribution of $\deg(I)$ is made $\pi_q(\deg(I))$ times where I varies over the set of all monic irreducibles whose degree is at most n. Also, we have an additional constraint $n = \deg(g) = k\deg(I)$ which implies $\deg(I)|n$. Letting $d = \deg(I)$ we get (2.3.5) is equivalent to

$$\sum_{d|n} d\pi_q(d) = q^n. \tag{2.3.6}$$

Mobious inversion of the above gives

$$\pi_q(n) = \frac{1}{n} \sum_{ab=n} \mu(a) q^b = \frac{q^n}{n} + O\left(\frac{q^{\frac{n}{2}}}{n}\right), \tag{2.3.7}$$

where we absorbed the lower order terms inside big O. (2.3.7) is the polynomial analogue of (2.3.1), since letting x the number of irreducible polynomials of degree n we see the expression for $\pi_q(n)$ is $\sim x/\log_q x$ as $x \to \infty$.

As mentioned earlier, in the next chapter we will try to explore why proofs in the polynomial case often turn out to be considerably "less-harder" than their counterpart in the integer case.

CHAPTER 3

THE RIEMANN ZETA FUNCTION

The Riemann zeta function is one of the most fundamental objects in number theory. It has a rich connection with the distribution of prime numbers, as we shall see in this section. We begin this section with the following definition.

3.1 Definition and a brief introduction of $\zeta(s)$

Definition 3.1.1 (The Riemann Zeta function)**.** For every complex number $s \in \mathbb{C}$ with $\Re(s) > 1$, we define Riemann zeta (ζ) function as

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Furthermore, in what follows, we shall always assume $s = \sigma + it$ where σ and t are real numbers. We know the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges absolutely in $\{s \in \mathbb{C} : \Re(s) > 1\}$ since it is dominated by the series $\sum_{n=1}^{\infty} \frac{1}{n^\sigma}$ which converges absolutely if $\sigma > 1$. Thus $\zeta(s)$ defines an analytic function in the region $\{s \in \mathbb{C} : \Re(s) > 1\}$. Moreover, we also have an Euler product representation of $\zeta(s)$ in this region given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{3.1.1}$$

The convergence of the above product can be checked easily. Since $|p^{-s}| < 1$ we have the following identity

$$\prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right).$$

Upon expanding the infinite product above we obtain an infinite sum where each term in the summation looks like

$$\frac{1}{p_1^{e_1 s} \cdots p_k^{e_k s}} = \frac{1}{\left(p_1^{e_1} \cdots p_k^{e_k}\right)^s}.$$

The conclusion in (3.1.1) is an immediate consequence of the Fundamental theorem of Arithmetic which says that every integer $n \geqslant 2$ can be uniquely decomposed into product of prime

numbers. However it is possible to extend $\zeta(s)$ beyond the region $\{s : \Re(s) > 1\}$ of absolute convergence. The following result partially accomplishes this.

Lemma 3.1.2. *There is a function $H_0(s)$, analytic for $\sigma > 0$ such that the following formula*

$$\zeta(s) = \frac{s}{s-1} - sH_0(s)$$

holds for every $s \neq 1$ and hence provides a meromorphic continuation of $\zeta(s)$ for $\Re(s) > 0$.

Proof. Let $x > 0$ and $s = \sigma + it$ with $\sigma > 1$ be given. Using partial summation we obtain

$$\sum_{n \leqslant x} \frac{1}{n^s} = \frac{\lfloor x \rfloor}{x^s} + s \int_1^x \frac{\lfloor t \rfloor}{t^{s+1}} dt.$$

Letting $x \to \infty$ we get that

$$\begin{aligned}
\zeta(s) &= 0 + s \int_1^\infty \frac{\lfloor t \rfloor}{t^{s+1}} dt \\
&= s \int_1^\infty \frac{t - (t - \lfloor t \rfloor)}{t^{s+1}} dt \\
&= s \int_1^\infty \frac{dt}{t^s} - s \int_1^\infty \frac{t - \lfloor t \rfloor}{t^{s+1}} dt \\
&= s \frac{t^{1-s}}{1-s} \Bigg|_{t=0}^\infty - s \int_1^\infty \frac{t - \lfloor t \rfloor}{t^{s+1}} dt \\
&= \frac{s}{s-1} - s \int_1^\infty \frac{t - \lfloor t \rfloor}{t^{s+1}} dt.
\end{aligned}$$

Now we observe the function H_0 defined by

$$H_0(s) := \int_1^\infty \frac{t - \lfloor t \rfloor}{t^{s+1}} dt$$

is analytic for every s with $\sigma = \Re(s) > 0$ since the integral in the definition of $|H_0(s)| \leqslant \int_1^\infty dt/t^{\sigma+1}$ and hence converges absolutely in the concerned region. □

3.2 Meromorphic continuation $\zeta(s)$ on $\mathbb{C}$

Having continued $\zeta(s)$ partially beyond the region of absolute convergence, let us begin this section by introducing Γ function which is intimately linked to $\zeta(s)$ and will be essential for

obtaining the analytic continuation of ζ to the whole complex plane.

Definition 3.2.1. For $s \in \mathbb{C}$, we define **Gamma function** via the following infinite product

$$\frac{1}{\Gamma(s)} := se^{\gamma s} \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-s/n},$$

where γ is known as Euler's constant and is defined by

$$\gamma = \lim_{N\to\infty} \sum_{i=1}^{N} \frac{1}{i} - \log N.$$

A detailed introduction aboubt Gamma function can be found in [25]. Here we only note the two following important properties of $\Gamma(s)$ which we shall use repeatedly.

— $\Gamma(s)$ is an analytic function on $\mathbb{C}$ except the simple poles at non positive integers $s = 0, -1, \ldots$ with residue $(-1)^n/n!$ at $s = -n$.

— Gamma function satisfies the following recurrence relation for each $s \in \mathbb{C}$

$$\Gamma(s+1) = s\Gamma(s).$$

3.2.1 Functional equation of $\zeta(s)$

In Lemma 3.1.2, we have already seen a way to analytically extend $\zeta(s)$ for $\sigma > 0$ except a simple pole at $s = 1$. In this section we talk about the functional equation that ζ satisfies and as a result we will be able to further extend ζ analytically to the entire complex plane.

Definition 3.2.2 (The completed zeta function)**.** We define the **completed zeta function** by

$$\xi(s) := \pi^{-s}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

The above definition is purely for convenience; as we shall see later functional equation looks much nicer in terms of the completed zeta function than the zeta function. Using techniques from complex analysis, one can prove the following result [25].

Proposition 3.2.3. *The function $\xi(s)$ is analytic for $\sigma > 1$ and has an analytic continuation to all of $\mathbb{C}$ with simple poles at $s = 0$ and $s = 1$. Additionally ξ also satisfies the following*

functional equation

$$\xi(s) = \xi(1-s) \qquad \textit{for all } s \in \mathbb{C}.$$

As a consequence, we can quickly prove the following result.

Corollary 3.2.4. *The Riemann zeta function $\zeta(s)$ analytically extends to all of $\mathbb{C}$ as a meromorphic function only with a simple pole at $s = 1$.*

Proof. We re-write the definition of completed zeta function and get

$$\zeta(s) = \pi^{s/2} \frac{\xi(s)}{\Gamma\left(\frac{s}{2}\right)}.$$

From the definition of gamma function we note that $1/\Gamma(s/2)$ is an entire function with zeros at $s = 0$ and the negative even integers $s = -2, -4, \ldots$, resulting a cancellation of the simple pole of $\xi(s)$ at $s = 0$. Thus $\zeta(s)$ only has a simple pole at $s = 1$ and admits an analytic continuation to all of $\mathbb{C}$. □

It is possible to play with the functional equation of the completed zeta function and obtain an analogous equation for $\zeta(s)$. Rewriting the functional equation in Proposition 3.2.3 and expanding we get

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

and consequently,

$$\zeta(s) = \frac{\pi^{s-1/2}\Gamma((1-s)/2)}{\Gamma(s/2)}\zeta(1-s).$$

We now observe a few things about the zeros of the Riemann zeta function. For $\sigma > 1$, we can infer that $\zeta(s) \neq 0$ since $\zeta(s)$ has a Euler product representation in the concerned domain given by (3.1.1). This observation combined with the functional equation discussed above immediately implies $\zeta(s) \neq 0$ for $\sigma < 0$ unless $s = -2, -4, \ldots$ since $\Re(1-s) > 1$, $\Gamma((1-s)/2)$ is zero free and $1/\Gamma(s/2)$ has zeros only at $s = -2, -4, \ldots$. We are only left to analyze $\zeta(s)$ in the region $0 \leqslant \sigma \leqslant 1$, called the **critical strip**.

We can now state one of the most celebrated open problems in mathematics concerning the zeros of the **Riemann zeta function** inside the critical strip. Before doing so, it is a good time

to summarize the important facts and results about $\zeta(s)$ that we briefly glanced upon so far.

— For $s \in \mathbb{C}$ with $\sigma > 1$ we have

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

— $\zeta(s)$ meromorphically continues to the entire complex plane with a simple pole at $s = 1$.

— The Riemann zeta function $\zeta(s)$ satisfies the following functional equation

$$\zeta(s) = \frac{\pi^{s-1/2}\Gamma((1-s)/2)}{\Gamma(s/2)}\zeta(1-s).$$

— $\zeta(s) \neq 0$ for $\sigma > 1$ and $\sigma < 0$ except at $s = -2, -4 \ldots$.

— $\zeta(s) = 0$ for negative even integers $s = -2, -4, \ldots$, and these are called the **trivial zeros.**

3.3 The Riemann Hypothesis

The zeros of Riemann zeta function in the region $0 \leqslant \sigma \leqslant 1$, i.e. the critical strip lie on the line $\sigma = 1/2$. Riemann himself said: "It would certainly be desirable to have a rigorous demonstration of this proposition; nevertheless, I have for the moment set this aside, after several quick but unsuccessful attempts, because it seemed unneeded for the immediate goal of my study." [25] It is noteworthy that despite the significant effort by several brilliant mathematicians for over a century and a half now, we are yet to discover a rigorous proof and numerical experiments continue to speak for the validity of the Riemann Hypothesis. Today the Riemann hypothesis is widely considered one of the most famous unsolved problems in mathematics.

3.4 Riemann zeta function for polynomials

This section is devoted to developing the analogue of the Riemann zeta function for the ring $\mathbb{F}_q[t]$. As we shall see, analyzing the zeta function for polynomials will be much simpler than its integer counterpart, which partly explains why one should expect a more straightforward argument for many results, including the prime number theorem in the polynomial setting. The corresponding zeta function will be more subtle to handle in more general function fields.

However, we will confine our discussion mostly to the simpler version of the zeta function concerning only polynomials.

Definition 3.4.1 (Riemann zeta function for polynomials)**.** The Riemann zeta function for the polynomial ring $\mathbb{F}_q[t]$ is defined by

$$\zeta_q(s) = \sum_{f \in \mathscr{M}} \frac{1}{|f|^s} \qquad \text{for } \Re(s) > 1.$$

Since there are exactly q^j monic polynomials of degree j, it is possible to quickly obtain a closed form of the infinite sum above.

$$\zeta_q(s) = \lim_{d\to\infty} \sum_{\deg(f)\leq d} \frac{1}{|f|^s} = \lim_{d\to\infty} \sum_{j=0}^{d} \frac{q^j}{q^{js}} = \frac{1}{1-\dfrac{q}{q^s}} = \frac{1}{1-q^{1-s}} \qquad \text{for } \Re(s) > 1.$$

In the classical integer setting, it took us a considerable amount of work to analytically continue $\zeta(s)$ beyond the region of absolute convergence $\Re(s) > 1$. Also, proving the functional equation for the completed zeta function $\xi(s) = \xi(1-s)$ was not at all a trivial job. As we shall see in this section, it is possible to establish analogous results for $\zeta_q(s)$ with much less work.
It is immediate from the closed form of $\zeta_q(s) = 1/(1-q^{1-s})$ that, ζ_q can be meromorphically continued to all of $\mathbb{C}$ with a simple pole at $s = 1$. We now move onto the following definition.

Definition 3.4.2 (The completed zeta function for polynomials)**.** The completed zeta function for $\mathbb{F}_q[t]$ is defined as follows

$$\xi_q(s) = q^{-s}(1-q^{-s})^{-1}\zeta_q(s)$$

It can be easily verified that ξ_q satisfies an analogous functional equation as that of $\xi(s)$ in the

classical case of the completed Riemann zeta function.

$$\begin{aligned}
\xi_q(1-s) &= q^{-1+s}\left(1-q^{-1+s}\right)^{-1}\zeta_q(1-s) \\
&= \frac{1}{qu}\left(1-\frac{1}{qu}\right)^{-1}\frac{1}{1-\frac{1}{u}} \qquad (u=q^{-s}) \\
&= \frac{1}{qu}.\frac{qu}{qu-1}\frac{u}{u-1} \\
&= u(1-u)^{-1}.\frac{1}{1-qu} \\
&= \xi_q(s)
\end{aligned}$$

A polynomial analogue of (3.1.1) also exists. We have the following Euler product expansion of $\zeta_q(s)$ for $s \in \mathbb{C}$ with $\Re(s) > 1$

$$\zeta_q(s) = \prod_{I \in \mathscr{P}}\left(1-\frac{1}{|I|^s}\right)^{-1}. \tag{3.4.1}$$

The above equality holds precisely because the ring $\mathbb{F}_q[t]$ is an unique factorization domain (UFD) which is the main crux of the argument we used to establish (3.1.1).

3.5 A second proof of Prime number theorem using the zeta function

It is possible to give yet another proof of prime number theorem for polynomials using the Euler product expansion. For this proof we closely follow the notation and the ideas discussed in [22]. Using the definition of norm of a polynomial, we can rewrite the product in (3.4.1) in the following way

$$\zeta_q(s) = \prod_{d=1}^{\infty}(1-q^{-ds})^{-\pi_q(d)} \text{ for } \Re(s) > 1$$

At this point it is often convenient to substitute $u = q^{-s}$. Since $\zeta_q(s) = 1/(1-q^{1-s})$ we arrive at the following identity

$$\frac{1}{1-qu} = \prod_{d=1}^{\infty}(1-q^{-ds})^{-\pi_q(d)}$$

Taking logarithmic derivatives we obtain

$$\frac{qu}{1-qu} = \sum_{d=1}^{\infty}\frac{d\pi_q(d)u^d}{1-u^d}.$$

Since $\Re(s) > 1$, we have that $|qu| < 1$. This allows us to expand both sides of the above equality and get

$$qu\left(1+qu+q^2u^2+\ldots\right) = \sum_{d=1}^{\infty} d\pi_q(d)(u^d+u^{2d}+u^{3d}+\ldots).$$

Equating the coefficient of u^n both sides, we get $q^n = \sum_{d|n} d\pi_q(d)$ which is same as (2.3.6) in the previous chapter and the conclusion follows.

CHAPTER 4

A BRIEF INTRODUCTION TO ARITHMETIC FUNCTIONS

This chapter aims to understand the fundamental properties and distribution of two interesting classes of arithmetic functions called additive and multiplicative functions. We will mainly focus on a few examples of each class and study their distribution using standard tools from probability theory. Materials presented in this chapter also motivate the natural problems that arise in this context and call for their subsequent solutions, which we will sketch in later chapters.

4.1 Additive and Multiplicative functions

We begin with the definition of additive and multiplicative functions.

Definition 4.1.1. An arithmetic function $f : \mathbb{N} \to \mathbb{C}$ is called additive if it satisfies the following relation

$$f(mn) = f(m) + f(n) \qquad \text{for all co-prime positive integers } m \text{ and } n.$$

Definition 4.1.2. An arithmetic function $f : \mathbb{N} \to \mathbb{C}$ is called multiplicative if it satisfies the following relation

$$f(mn) = f(m)f(n) \qquad \text{for all co-prime positive integers } m \text{ and } n.$$

We see that if f is additive and $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $f(n) = f(p_1^{\alpha_1}) + \cdots + f(p_k^{\alpha_k})$ and thus the value of $f(n)$ is determined by the values of f on the prime powers.
Similarly if f is multiplicative then $f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$ and hence the value of $f(n)$ is also determined by the values of f on the prime powers. We now look at few common examples of such arithmetic functions.

Example 4.1.3 (The divisor function)**.** *The divisor function* $\tau(n) := \#\{d : d|n\}$ *is a multiplicative function. For instance, we have* $\tau(6) = 4 = \tau(2)\tau(3)$.

It is possible to argue quickly that the function τ is multiplicative. Indeed if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then

every divisor d of n must be of the form $d = p_1^{e_1} \cdots p_k^{e_k}$ where $0 \leqslant e_j \leqslant \alpha_j$ for each $1 \leqslant j \leqslant k$. This observation allows us to count the number of such divisors which is given by the product $\prod_{j=1}^{k}(1+\alpha_j)$ and hence $\tau(n) = \prod_{j=1}^{k}(1+\alpha_j)$.
If two co-prime integers $m = q_1^{\beta_1} \cdots q_\ell^{\beta_\ell}$ and $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ are given (we note that $q_i \neq p_j$ for every i and j due to co-primality condition) then

$$\tau(mn) = \tau\left(q_1^{\beta_1} \cdots q_\ell^{\beta_\ell} p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right) = \prod_{i=1}^{\ell}(1+\beta_i)\prod_{j=1}^{k}(1+\alpha_j) = \tau(m)\tau(n).$$

Example 4.1.4 (Euler's phi function)**.** *The Euler's phi function $\phi(n)$ defined in (2.2.1) is multiplicative as can be directly verified either by Chinese remainder theorem, corollary 2.2.2 or the explicit formula derived as a consequence of CRT.*

Example 4.1.5 (The functions ω and Ω)**.** *The functions $\Omega(n)$ and $\omega(n)$ count the number of prime factors of an integer n with and without the multiplicity respectively. For instance, $\omega(12) = 2$ since $12 = 2^2 \times 3$ has only two **distinct** prime factors while $\Omega(12) = 3$.*

It is very easy to check both ω and Ω are additive functions and the function Ω even satisfies the following stronger condition

$$\Omega(mn) = \Omega(n) + \Omega(m) \qquad \text{for all positive integers } m \text{ and } n.$$

Justification of the above claim is immediate once we observe for $m = q_1^{\beta_1} \cdots q_\ell^{\beta_\ell}$ and $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ given, we have

$$\Omega(mn) = \Omega\left(q_1^{\beta_1} \cdots q_\ell^{\beta_\ell} p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right) = \sum_{i=1}^{\ell}\beta_i + \sum_{j=1}^{k}\alpha_j = \Omega(m) + \Omega(n).$$

Functions like above are called **completely additive functions**. Likewise, one can also define **completely multiplicative functions**. It is worth noting that the exponentiation of an additive function naturally leads to a multiplicative function. For example the function $f(n) := z^{\Omega(n)}$ is multiplicative (in fact completely multiplicative) where $z \in \mathbb{C}$ is a fixed complex number.

4.2 Mean behaviour of interesting arithmetic functions?: introducing ω and Ω

Let $f : \mathbb{N} \to \mathbb{C}$ be an arithmetic function, possibly additive or multiplicative. As we have already seen in the previous section, the values of common arithmetic functions fluctuate considerably. (for instance, the value of $\Omega(n)$ is 1 whenever n is prime, but it can also attain arbitrarily large values for large prime powers) It is, therefore, reasonable to seek to understand the mean behaviour of f up to some integer x defined by

$$\mathrm{Ave}_{\leqslant x}(f) := \frac{1}{x}\sum_{n\leqslant x} f(n).$$

Once we have a good understanding of the average $\mathrm{Ave}_{\leqslant x}(f)$, we can also ask how much f deviates from this average and how often it does so. In particular, we may want to consider the mean squared deviation and also ask what proportion of the integers in $\{1,2,\ldots,x\}$ fluctuates from $\mathrm{Ave}_{\leqslant x}(f)$ by a significant margin,

$$\frac{1}{x}\sum_{n\leqslant x} |f - \mathrm{Ave}_{\leqslant x}(f)|^2 \qquad \frac{1}{x}\#\{n \leqslant x : |f(n) - \mathrm{Ave}_{\leqslant x}(f)| \geqslant \text{ a large quantity}\}.$$

Above expressions remind us about the variance and large deviations from probability theory. We shall see in the later sections techniques from probability theory will enable us to study the behaviour of erratic arithmetic functions (such as ω and Ω). Once we set up a suitable probability space we will be able to study large deviations, higher moments and finally establish a central limit theorem for $\omega(n)$, one of the most celebrated results in probabilistic number theory. We can also ask similar questions for $\Omega(n)$. It is evident that the difference $|\Omega - \omega|$ can become arbitrarily large on the prime powers. However, on average one expects them to behave in a very alike fashion in view of the following observation

$$\mathrm{Ave}_{\leqslant x}(\Omega-\omega) = \frac{1}{x}\sum_{n\leqslant x}(\Omega(n)-\omega(n)) = \frac{1}{x}\sum_{n\leqslant x}\sum_{\substack{p^a\|n\\ a\geqslant 2}} 1 = \frac{1}{x}\sum_{p,a\geqslant 2}\sum_{\substack{n\leqslant x\\ p^a\|n}} 1 = \frac{1}{x}\sum_{p,a\geqslant 2}\left\lfloor \frac{x}{p^a}\right\rfloor.$$

We infer the average difference $\mathrm{Ave}_{\leqslant x}(\Omega-\omega)$ is at most 1 since the rightmost sum is;

$$\frac{1}{x}\sum_{p,a\geqslant 2}\left\lfloor \frac{x}{p^a}\right\rfloor \leqslant \sum_{p,a\geqslant 2}\frac{1}{p^a} \leqslant \sum_{p,a\geqslant 2}\frac{1}{p(p-1)} \leqslant \sum_{n}\frac{1}{n(n-1)} = 1.$$

4.2.1 Distribution of the function ω for integers: a probabilistic set up

To have a better understanding of the arithmetic functions it is essential to study their distributions. To do that we first consider the set of all integers up to x and define

$$\mathscr{S} := \{1,2,\dots x\}.$$

Given a set $\mathscr{B} \subset \mathscr{S}$, then we define the probability that a randomly chosen integer from $\mathscr{S}$ will land inside $\mathscr{B}$ by the proportion that $\mathscr{B}$ occupies inside $\mathscr{S}$. Hence we write

$$\mathbb{P}(\mathscr{B}) = \frac{\#\mathscr{B}}{\#\mathscr{S}} = \frac{1}{x}\#\mathscr{B}$$

In this setting it is convenient to replace the usual average by the expectation operator; Thus for an arithmetic function f we write

$$\mathbb{E}(f) := \frac{1}{x}\sum_{n\leqslant x} f(n).$$

Similarly one can also define the variance which measures on average how much the function f fluctuates from its mean.

$$\mathrm{Var}(f) := \mathbb{E}(f-\mathbb{E}(f))^2 = \frac{1}{x}\sum_{n\leqslant x} f^2(n) - \left(\frac{1}{x}\sum_{n\leqslant x} f(n)\right)^2.$$

We also define the covariance between two arithmetic function f and g which encapsulates the interaction between these two functions.

$$\mathrm{Cov}(f,g) := \mathbb{E}(fg) - \mathbb{E}(f)\mathbb{E}(g) = \frac{1}{x}\sum_{n\leqslant x} f(n)g(n) - \left(\frac{1}{x}\sum_{n\leqslant x} f(n)\right)\left(\frac{1}{x}\sum_{n\leqslant x} g(n)\right)$$

Let us try to calculate the average value of $\omega(n)$ with the above definition in mind. We first note that the identity $\omega(n) = \sum_{p\leq x} 1_{p|n}$ holds for every $n \in \mathscr{S}$, where $1_{p|n}$ denotes the indicator function that detects the divisibility by a fixed prime $p \leqslant x$. Therefore, from the definition of expectation

$$\mathbb{E}(\omega) = \frac{1}{x}\sum_{n\leqslant x}\omega(n) = \frac{1}{x}\sum_{n\leqslant x}\sum_{\substack{p|n\\ p\leqslant x}} 1 = \frac{1}{x}\sum_{p\leqslant x}\sum_{\substack{p|n\\ n\leqslant x}} 1 = \frac{1}{x}\sum_{p\leqslant x}\left\lfloor\frac{x}{p}\right\rfloor = \sum_{p\leqslant x}\frac{1}{p} + O\left(\frac{\pi(x)}{x}\right).$$

The sum appearing above is well known in analytic number theory. Also by using $\pi(x) \ll x/\log x$, we get

$$\mu := \mathbb{E}(\omega) = \log\log x + c + O\left(\frac{1}{\log x}\right) \qquad \text{for some } c > 0.$$

The variance calculation is a bit trickier since the indicator functions $1_{p|n}$ and $1_{q|n}$ are not in general independent when n is randomly sampled from the interval $[1,x]$, which means we have to take care of the covariance terms very carefully.

Lemma 4.2.1. *We have the following estimate*

$$Var(\omega) = \log\log x + O\left((\log\log x)^{1/2+\delta}\right) \text{ for every } \delta \in (0,1/2).$$

Proof. We shall begin by introducing a truncated version of $\omega(n)$ to avoid some technical difficulties in the proof. We define another arithmetic function $\omega_0(n) := \sum_{p\leqslant y} 1_{p|n}$. It would then be possible to estimate $\mathrm{Var}(\omega)$ by estimating $\mathrm{Var}(\omega_0)$ if the difference $(\mathrm{Var}(\omega) - \mathrm{Var}(\omega_0))$ is not too large for an appropriate choice of the parameter $y \leqslant x$ such that $y = x^{o(1)}$. We will decide the value of exponent of y later in the proof in terms of x.
Therefore the average value of ω_0 is given by

$$\mathbb{E}(\omega_0) = \frac{1}{x}\sum_{n\leqslant x}\omega_0(n) = \frac{1}{x}\sum_{n\leqslant x}\sum_{\substack{p|n\\ p\leqslant y}} 1 = \frac{1}{x}\sum_{p\leqslant y}\sum_{\substack{p|n\\ n\leqslant x}} 1 = \frac{1}{x}\sum_{p\leqslant y}\left\lfloor\frac{x}{p}\right\rfloor = \sum_{p\leqslant y}\frac{1}{p} + O\left(\frac{\pi(y)}{x}\right).$$

Using PNT and keeping in mind that $y \leqslant x$, we obtain

$$\mu_0 := \mathbb{E}(\omega_0) = \log\log y + c + O\left(\frac{1}{\log y}\right) + O\left(\frac{y}{x\log y}\right) = \log\log y + c + O\left(\frac{1}{\log y}\right). \quad (4.2.1)$$

The variance of ω_0 is given by

$$\begin{aligned}
\mathrm{Var}\omega_0 &= \mathbb{E}(\omega_0^2) - (\mathbb{E}\omega_0)^2 \\
&= \mathbb{E}\left(\sum_{p,q\leqslant y} 1_{p|n}1_{q|n}\right) - \left(\sum_{p\leqslant y}\mathbb{P}(p|n)\right)^2 \\
&= \sum_{p\leqslant y}\left[\mathbb{P}(p|n) - \mathbb{P}(p|n)^2\right] + \sum_{\substack{p\neq q\\ p,q\leqslant y}} \mathrm{Cov}(1_{p|n}, 1_{q|n}) \\
&= \sum_{p\leqslant y}\left[\frac{1}{p} - \frac{1}{p^2} + O\left(\frac{1}{x}\right)\right] + \sum_{\substack{p\neq q\\ p,q\leqslant y}} \mathrm{Cov}(1_{p|n}, 1_{q|n}), \qquad (4.2.2)
\end{aligned}$$

where we used $\mathbb{P}(p|n) = \{n \leqslant x : n \equiv 0(\bmod p)\}/x = \frac{1}{x}\left\lfloor \frac{x}{p}\right\rfloor = \frac{1}{p} + O\left(\frac{1}{x}\right)$ and now we observe the covariance term equals

$$\begin{aligned}
\mathrm{Cov}(1_{p|n}, 1_{q|n}) &= \mathbb{E}(1_{p|n}1_{q|n}) - \mathbb{E}(1_{p|n})\mathbb{E}(1_{q|n}) \\
&= \mathbb{E}(1_{pq|n}) - \mathbb{E}(1_{p|n})\mathbb{E}(1_{q|n}) \\
&= \mathbb{P}(pq|n) - \mathbb{P}(p|n)\mathbb{P}(q|n) \\
&= \frac{1}{pq} + O\left(\frac{1}{x}\right) - \left(\frac{1}{p} + O\left(\frac{1}{x}\right)\right)\left(\frac{1}{q} + O\left(\frac{1}{x}\right)\right) \\
&= O\left(\frac{1}{x}\right).
\end{aligned}$$

Hence the right sum in (4.2.2) is at most $O(1/x)\left(\sum_{p\leqslant y} 1\right)^2$ and using prime number theorem it is seen to be bounded by $O(y^2/x\log^2 y)$ and hence we obtain from (4.2.2)

$$\begin{aligned}
\mathrm{Var}\omega_0 &= \log\log y + O(1) + O\left(\frac{1}{\log y}\right) + O\left(\frac{\pi(y)}{x}\right) + O\left(\frac{y^2}{x\log^2 y}\right) \\
&= \log\log y + O(1) + O\left(\frac{1}{\log y}\right) + O\left(\frac{y}{x\log y}\right) + O\left(\frac{y^2}{x\log^2 y}\right) \qquad (4.2.3)
\end{aligned}$$

At this point we set $y = x^{1/(\log\log x)^\delta}$ and $\delta \in (0,1)$ is a free variable at the moment. We observe $O(1/\log y)$ dominates the last two big-O terms, which we justify below. Our choice of y

essentially has the form $y = x^{o(1)}$, which means for x sufficiently large we have

$$\frac{y}{x} \leqslant \frac{1}{\sqrt{x}} \text{ and } \frac{y^2}{x} \leqslant \frac{1}{\sqrt{x}}.$$

Thus after substituting the value of y, we have that from (4.2.1) and (4.2.3)

$$\mu_0 = \log\log x + c + O\left(\frac{(\log\log x)^\delta}{\log x}\right) \text{ and } \mathrm{Var}\omega_0 = \log\log x + O(1) + O\left(\frac{(\log\log x)^\delta}{\log x}\right).$$

Next we compare $\mathrm{Var}\omega$ with $\mathrm{Var}\omega_0$. We call the difference $D := \mathrm{Var}\omega - \mathrm{Var}\omega_0$. We have

$$\begin{aligned} D &= \frac{1}{x}\sum_{n\leqslant x}(\omega(n)-\mu)^2 - \frac{1}{x}\sum_{n\leqslant x}(\omega_0(n)-\mu_0)^2 \\ &= \frac{1}{x}\sum_{n\leqslant x}[A(n)+B(n)]^2 - \frac{1}{x}\sum_{n\leqslant x}A^2(n). \end{aligned} \tag{4.2.4}$$

where the functions $A(n)$ and $B(n)$ are such that

$$A(n)+B(n) := \omega(n)-\mu \text{ and } A(n) = \omega_0(n)-\mu_0.$$

Before proceeding with (4.2.4), we would like to have an upper bound on the average of $\sum_{n\leqslant x} B^2(n)$. Since there can be at most $(\log\log x)^\delta$ distinct prime factors $> y$ of any integer $n \in [1,x]$, the inequality $(\omega(n)-\omega_0(n)) \leqslant (\log\log x)^\delta$ holds. Hence we have that, $\frac{1}{x}\sum_{n\leqslant x}(\omega(n)-\omega_0(n))^2 = O((\log\log x)^{2\delta})$. Also from the values of μ and μ_0 from the previous calculations, the upper bound $\frac{1}{x}\sum_{n\leqslant x}(\mu-\mu_0)^2 = O((\log\log x)^{2\delta}/\log^2 x)$ holds. Therefore we get

$$\begin{aligned} \frac{1}{x}\sum_{n\leqslant x}B^2(n) &= \frac{1}{x}\sum_{n\leqslant x}[(\omega(n)-\omega_0(n))+(\mu_0-\mu)]^2 \\ &\leqslant \frac{2}{x}\left(\sum_{n\leqslant x}(\omega(n)-\omega_0(n))^2 + \sum_{n\leqslant x}(\mu-\mu_0)^2\right) \\ &= 2\left(O((\log\log x)^{2\delta}) + O\left(\frac{(\log\log x)^{2\delta}}{\log^2 x}\right)\right) \\ &= O((\log\log x)^{2\delta}). \end{aligned}$$

Thus from (4.2.4) after expanding and using Cauchy-Schwartz inequality, we get an upper

bound on D.

$$\begin{aligned}
D &\leqslant \frac{1}{x}\left(\sum_{n\leqslant x}A^2(n)+\sum_{n\leqslant x}B^2(n)\right)+\frac{2}{x}\sum_{n\leqslant x}|A(n)||B(n)|-\frac{1}{x}\sum_{n\leqslant x}A^2(n)\\
&\leqslant \frac{1}{x}\left(\sum_{n\leqslant x}A^2(n)+\sum_{n\leqslant x}B^2(n)\right)+\frac{2}{x}\sqrt{\left(\sum_{n\leqslant x}A^2(n)\right)\left(\sum_{n\leqslant x}B^2(n)\right)}-\frac{1}{x}\sum_{n\leqslant x}A^2(n) \quad \text{(CS inequality)}\\
&= \frac{1}{x}\sum_{n\leqslant x}B^2(n)+2\sqrt{\left(\frac{1}{x}\sum_{n\leqslant x}A^2(n)\right)\left(\frac{1}{x}\sum_{n\leqslant x}B^2(n)\right)}\\
&= O\left((\log\log x)^{2\delta}\right)+2\sqrt{O(\log\log x)O((\log\log x)^{2\delta})} \qquad \left(\frac{1}{x}\sum_{n\leqslant x}A^2(n)=\mathrm{Var}\omega_0=O(\log\log x)\right)\\
&= O\left(\max\left\{(\log\log x)^{2\delta},(\log\log x)^{1/2+\delta}\right\}\right).
\end{aligned}$$

We have $\mathrm{Var}\omega=\mathrm{Var}\omega_0+D$ and $\mathrm{Var}\omega_0=\log\log x+O(1)+O((\log\log x)^{\delta}/\log x)$. Therefore, we pick a fixed δ such that $0<\delta<1/2$ so that the error term becomes $D=O((\log\log x)^{1/2+\delta})$ leading to the conclusion. We also note the smaller $\delta\in(0,1/2)$ we choose, the better our estimate becomes. □

Lemma 4.2.1 immediately calls for an application in the form of a large deviation inequality which says if an integer is picked at random from the interval $[1,\dots,x]$ then with high probability, it has about $\log\log x$ distinct prime factors. More formally, we have the following result;

Corollary 4.2.2 (Hardy and Ramanujan)**.** *Let $\xi(x)$ be any function that tends to infinity as $x\to\infty$. If an integer $n\in[1,x]$ is picked uniformly at random, then we have*

$$\mathbb{P}\left(|\omega(n)-\log\log x|\geqslant\sqrt{\xi(x)\log\log x}\right)\ll\frac{1}{\xi(x)}.$$

Proof. Let us consider the following set

$$S=\{n:1\leqslant n\leqslant x \text{ and } |\omega(n)-\log\log x|\geqslant\sqrt{\xi(x)\log\log x}\},$$

where $\xi(x)$ is any function that tends to infinity as $x\to\infty$. We have

$$\frac{\#S}{x}=\mathbb{P}\left(|\omega(n)-\log\log x|\geqslant\sqrt{\xi(x)\log\log x}\right) \tag{4.2.5}$$

We note the inclusion of events $\left\{|\omega(n)-\log\log x| \geqslant \sqrt{\xi(x)\log\log x}\right\} \subset \left\{ \left| \omega - \log\log x - c - O\left(\frac{1}{\log x}\right)\right| \geqslant \sqrt{\xi(x)\log\log x} - c - O\left(\frac{1}{\log x}\right) \right\}$ and hence applying Chebyechev's inequality from classical probability theory in (4.2.4) we get

$$\begin{aligned}
\frac{\#S}{x} &\leqslant \mathbb{P}\left(\left|\omega - \log\log x - c - O\left(\frac{1}{\log x}\right)\right| \geqslant \sqrt{\xi(x)\log\log x} - c - O\left(\frac{1}{\log x}\right)\right) \\
&\leqslant \frac{\mathrm{Var}(\omega)}{\left[\sqrt{\xi(x)\log\log x} - c - O\left(\frac{1}{\log x}\right)\right]^2} \qquad \left(\mathrm{Var}(\omega) = \mathbb{E}\left|\omega - \log\log x - c - O\left(\frac{1}{\log x}\right)\right|^2\right) \\
&= O\left(\frac{1}{\xi(x)}\right) \quad (\text{ from Lemma 4.2.1}),
\end{aligned}$$

□

The above result shows as $x \to \infty$, 100% of the integers in the interval $[1,x]$ have very close to $\log\log x$ distinct prime factors in the sense that the following inequality holds

$$\log\log x - \sqrt{\xi(x)\log\log x} \leqslant \omega(n) \leqslant \log\log x + \sqrt{\xi(x)\log\log x}$$

for almost all $n \in [1,x]$ and for every function $\xi(x)$ that increases to infinity, no matter how slowly.

4.2.2 Erdos Kac theorem: rates of convergence and a generalization

Having explored the average behaviour and the variability of ω, we now might want to ask if there is a limiting distribution for the normalized arithmetic functions $(\omega - \mathbb{E}\omega)/\sqrt{\mathrm{Var}(\omega)}$. We have already noticed the identity, $\omega = \sum_{p \leqslant x} 1_{p|n}$ and since the summands, $1_{p|n}$ and $1_{q|n}$ are approximately independent when n is sampled uniformly at random from the interval $[1,x]$, as we checked in the covariance calculation in the proof of Lemma 4.2.1, it is therefore, reasonable to expect a central limit theorem for this normalized function. This is indeed the case and was first proved jointly by Erdos and Kac [16]. However, we do not give their proof here and instead outline a simplified sketch due to Billingsley [5]. The essential idea is to consider a sequence of independent random variables indexed by prime numbers whose sum closely approximates ω. More specifically, by closely approximate, we mean the difference of k-th moment of ω and

this newly constructed sum of independent random variables will be very small for every $k \in \mathbb{N}$. The construction involves truncation of the original function $\omega(n)$ by getting rid of the large primes p appearing in the sum $\sum_{p \leqslant x} 1_{p|n}$ which will help us maintain enough independence in the structure while retaining most information about ω.

In the next section, we shall also establish an analogous result for polynomials. As one would expect, the proof there will be quite similar to the one in the integer case. We now state the celebrated Erdos-Kac theorem for integers.

Theorem 4.2.3 (Erdos and Kac)**.** *For any fixed $\mathscr{B} \subseteq \mathbb{R}$ Borel set, we have*

$$\mathbb{P}\left(\frac{\omega - \log\log x}{\sqrt{\log\log x}} \in \mathscr{B}\right) \to \frac{1}{\sqrt{2\pi}} \int_{\mathscr{B}} e^{-t^2/2} dt \quad \text{as } x \to \infty.$$

The above theorem is in alignment with our observations in the previous sections that a typical integer $n \in [1,x]$ has roughly about $\log\log x$ prime factors. For instance the integer $10^9 + 3 = 23 \times 397 \times 141623$. Table 4.I (below) captures the growth of the average number of distinct prime factors of all natural numbers less than or equal to x for different values. [27] The second column displays the the number of digits in x which is $1 + \lfloor \log x / \log 10 \rfloor$. Clearly all the integers less than x will have at most $1 + \lfloor \log x / \log 10 \rfloor$ digits. The third column shows the expected number of distinct prime factors for a typical integer $n \in [1,x]$ chosen uniformly at random, which is about $\approx \log\log x$. The last column captures how much $\omega(n)$ deviates around the mean value on average which is approximately given by $\approx \sqrt{\log\log x}$.

x	Number of digits in x	Average number of distinct primes	Standard deviation
1000	4	2	1.4
10^9	10	3	1.7
10^{24}	25	4	2
10^{65}	66	5	2.2
10^{9566}	9567	10	3.2
$10^{210704568}$	210704569	20	4.5
$10^{10^{22}}$	$10^{22}+1$	50	7.1
$10^{10^{44}}$	$10^{44}+1$	100	10
$10^{10^{434}}$	$10^{434}+1$	1000	31.6

Table 4.I – Number of distinct prime factors of a typical integer $n \leqslant x$.

Before proving the Erdos-Kac theorem, let us mention a few interesting facts about in what ways the result can be interpreted and generalized. The same theorem also holds if one replaces

ω by Ω, and in fact, there is a vast generalization of the Erdos-Kac theorem for a certain class of additive functions that obey some regularity conditions. [4]

Theorem 4.2.4 (Generalized Erdos-Kac)**.** *Suppose that $\{f_n\}$ is a sequence of additive functions and let*

$$A_n = \sum_{p \leqslant n} \frac{f_n(p)}{p}$$

$$B_n = \sum_{p \leqslant n} \frac{f_n^2(p)}{p}.$$

Furthermore, suppose the two following conditions hold,

$$\lim_{n\to\infty} \frac{f_n(m)}{\sqrt{B_n}} = 0 \quad \text{for each fixed } m = 1,2,\ldots \tag{4.2.6}$$

$$\max_{p \leqslant n} \frac{|f_n(p)|}{\sqrt{B_n}} \to 0 \quad \text{as } n \to \infty. \tag{4.2.7}$$

Then for any fixed $\mathscr{B} \subseteq \mathbb{R}$ Borel set, we have

$$\mathbb{P}\left(\frac{f_n - A_n}{\sqrt{B_n}} \in \mathscr{B}\right) \to \frac{1}{\sqrt{2\pi}} \int_{\mathscr{B}} e^{-t^2/2} dt \quad \text{as } x \to \infty.$$

If f_n is identically equal to f for every n and the quantity $B_n \to \infty$ with n then condition (4.2.6) is automatically satisfied. Also, if, $\sup_p |f_n(p)| < \infty$ then condition (4.2.7) is guaranteed to hold. Therefore the above result is true when $f \equiv \omega$ or $f \equiv \Omega$. (In both cases, $B_n = \sqrt{\log\log n} + O(1)$) We also note for general completely additive functions (like Ω) condition (4.2.7) indeed implies condition (4.2.6). To see this, we first fix m and assume $m = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$. Therefore, if $n \geqslant m$ then

$$\begin{aligned} \frac{f_n(m)}{\sqrt{B_n}} &= \left(\frac{\alpha_1 f_n(p_1)}{\sqrt{B_n}} + \cdots + \frac{\alpha_\ell f_n(p_\ell)}{\sqrt{B_n}}\right) \\ &\leqslant \max(\alpha_1, \ldots, \alpha_\ell) \frac{\max_{p \leqslant n} |f_n(p)|}{\sqrt{B_n}}. \end{aligned}$$

The second step follows from the observation that if $n \geqslant m$ then all the prime factors of m must be less than n. Thus for each fixed $m \in \mathbb{N}$ we have

$$\lim_{n\to\infty} \frac{f_n(m)}{\sqrt{B_n}} = 0.$$

Rates of convergence: Berry-Esseen type bounds. Once can also ask for an estimate on the explicit error term in the convergence of distribution described in Theorem 4.2.2. Fix a real number $t \in \mathbb{R}$ and let us write

$$E(x) := \left| \mathbb{P}\left(\frac{\omega - \log\log x}{\sqrt{\log\log x}} \leqslant t \right) - \frac{1}{\sqrt{2\pi}} \int_0^t e^{-v^2/2} dv \right|.$$

What can we say about the function $E(x)$? Specifically, can we provide reasonable upper bounds? In the classical central limit theorem, the rate of convergence in the distribution is governed by the error function $E(x)$. The well-known Berry-Esseen bound [3] in probability theory states that the optimal size of $E(x)$ should be inversely proportional to the standard deviation of the random variables, i.e. of the order of $1/\sqrt{\log\log x}$.

— A. Renyi and P. Turan (1958) [21] proved the upper bound $E(x) \ll 1/\sqrt{\log\log x}$ holds .

— In a fairly recent work A. Harper (2009) [14] gave two new proofs of Erdos-Kac theorem using sophisticated probabilisitc tools like Stein's method. The advantage of using Stein's method is that, it always provides an estimate on the error term $E(x)$ unlike method of moments.
However, Harper's method yields a suboptimal upper bound $E(x) \ll \log\log\log x/\sqrt{\log\log x}$.

Below we give an outline of the proof of the Erdos-Kac theorem using Billingsley's ideas. We have closely followed the sketch given in [11].

Proof of Theorem 4.2.2. Much like Lemma 4.2.1, first, we first consider a truncation of ω defined by

$$\omega_y(n) := \sum_{p \leqslant y} 1_{p|n}.$$

The parameter y will be suitably chosen later. Second, we consider a sequence of **independent** random variables indexed by primes $\{X_p\}_{p \leqslant y}$ defined on the some probability space such that

$$\mathbb{P}(X_p = 1) = \frac{1}{p} \text{ and } \mathbb{P}(X_p = 0) = 1 - \frac{1}{p}.$$

Let us also define the summatory function of these random variables by

$$S_y := \sum_{p \leqslant y} X_p.$$

We note the mean and variance of the summatory function S_y is given by

$$\mu_y = \mathbb{E}S_y = \sum_{p \leqslant y} \frac{1}{p} = \log\log y + O(1).$$

$$\sigma_y^2 = \mathrm{Var}(S_y) = \sum_{p \leqslant y} \frac{1}{p}\left(1 - \frac{1}{p}\right) = \log\log y + O(1).$$

Since the summands in S_y are independent, the classical central theorem tells us that $(S_y - \mu_y)/\sigma_y$ converges to $N(0,1)$ in distribution. Our goal is to show that S_y is a good approximation of ω_y in the sense their moments asymptotically coincides.
We have the difference between the kth moment of ω_y and S_y

$$\frac{1}{x}\sum_{n \leqslant x} (\omega_y(n) - \mu_y)^k - \mathbb{E}(S_y - \mu_y)^k = \sum_{j=1}^{k} \binom{k}{j} (-\mu_y)^{k-j} \left(\frac{1}{x} \sum_{n \leqslant x} \omega_y(n)^j - \mathbb{E}(S_y^j) \right).$$

We call the inner expression L_j and upon expanding the sum inside L_j we get

$$\begin{aligned} L_j &= \sum_{p_1, p_2, \ldots, p_j \leqslant y} \left(\frac{1}{x} \sum_{n \leqslant x} 1_{p_1|n} 1_{p_2|n} \cdots 1_{p_j|n} - \mathbb{E}(X_{p_1} X_{p_2} \cdots X_{p_j}) \right) \\ &= \sum_{\substack{p_1, p_2, \ldots, p_j \leqslant y \\ \ell = \mathrm{lcm}[p_1, p_2, \ldots, p_j]}} \left(\frac{1}{x} \left\lfloor \frac{x}{\ell} \right\rfloor - \frac{1}{\ell} \right) \\ &\ll \sum_{p_1, p_2, \ldots, p_j \leqslant y} \frac{1}{x} \\ &= \frac{\pi(y)^j}{x}. \end{aligned}$$

At this point we set $y = x^{1/(\log\log x)^{1/3}}$.Therefore an upper bound on the difference of k th moment is given by

$$\ll \sum_{j=1}^{k} \binom{k}{j} \mu_y^{k-j} \frac{\pi(y)^j}{x} = \frac{(\mu_y + \pi(y))^k}{x} \leqslant \frac{(y + \log\log y + O(1))^k}{x} \ll \frac{y^k}{x} = x^{-1+k/(\log\log x)^{1/3}} \leqslant \frac{1}{\sqrt{x}},$$

since $y = x^{o(1)}$. Above chain of inequalities implies as $x, y \to \infty$

$$\frac{1}{x}\sum_{n\leqslant x}\left(\frac{\omega_y(n)-\mu_y}{\sigma_y}\right)^k \sim \mathbb{E}(Z^k),$$

where Z is a random variable distributed as $N(0,1)$.
Now $\omega(n)-\omega_y(n) \leqslant (\log\log x)^{1/3}$ since there can be at most $(\log\log x)^{1/3}$ primes $> y$ that can divide an integer $n \leqslant x$ and $\mu_y, \sigma_y^2 = \log\log x + O((\log\log x)^{1/3})$. Thus we have for all integers $n \leqslant x$

$$\frac{\omega(n)-\log\log x}{\sqrt{\log\log x}} = \frac{\omega_y(n)-\mu_y}{\sigma_y} + o(1),$$

which in turn implies

$$\frac{1}{x}\sum_{n\leqslant x}\left(\frac{\omega(n)-\log\log x}{\sqrt{\log\log x}}\right)^k \sim \mathbb{E}(Z^k).$$

□

4.2.3 Distribution of the function ω for polynomials

All the results discussed so far always had an intuitive counterpart for polynomials, and the Erdos-Kac theorem is not an exception as we are about to explore. The main goal of this section is to discuss a probabilistic framework so that we can talk about the distribution of various interesting arithmetic functions for polynomials which will finally lead to Billingsley's proof of the Erdos-Kac theorem. We call an arithmetic function $h : \mathscr{M} \to \mathbb{C}$ multiplicative if the relation $h(fg) = h(f)h(g)$ holds for every pair of monic coprime polynomials. Likewise, if h satisfies $h(fg) = h(f) + h(g)$, then it is called an additive function, and the values of multiplicative and additive functions are completely determined by its values on the powers of irreducible factors.

Example 4.2.5. *The Euler's phi function for polynomials $\Phi(f)$ introduced in chapter 2 is multiplicative, as can be concluded from corollary 4.2.1. Also, the functions $\Omega_q(f), \omega_q(f)$, which count the number of irreducible factors of a given polynomial f with or without multiplicity, can easily be checked to be additive functions. In accordance with the results in the previous section, we focus on studying the distribution of ω_q in the context of polynomials.*

4.2.4 Mean behaviour and variance of ω for polynomials

We consider $\mathscr{M}_n$, the set of all degree n monic polynomials of cardinality q^n. We wish to study the average behavior of arithmetic functions in the context of polynomials like we did for integers in the previous sections. Hence given a set, $\mathscr{A} \subset \mathscr{M}_n$, then we define the probability of the event that a randomly chosen polynomial from $\mathscr{M}_n$ will land inside $\mathscr{A}$ by the proportion that $\mathscr{A}$ occupies in $\mathscr{M}_n$. Therefore, we write

$$\mathbb{P}(\mathscr{A}) = \frac{\#\mathscr{A}}{\#\mathscr{M}_n} = \frac{1}{q^n}\#\mathscr{A}$$

In the polynomial setting, for an arithmetic function $h : \mathscr{M}_n \to \mathbb{C}$ we define the average of $h(f)$ in the following way

$$\mathbb{E}(h) := \frac{1}{q^n}\sum_{f\in\mathscr{M}_n} h(f).$$

Likewise the variance is given by

$$\mathrm{Var}(h) := \mathbb{E}(h-\mathbb{E}h)^2 = \frac{1}{q^n}\sum_{f\in\mathscr{M}_n} h^2(f) - \left(\frac{1}{q^n}\sum_{f\in\mathscr{M}_n} h(f)\right)^2.$$

Hence the average number of irreducible factors of a monic polynomial is given by

$$\begin{aligned}
\mathbb{E}\omega_q &:= \frac{1}{q^n}\sum_{f\in\mathscr{M}_n}\omega_q(f)\\
&= \frac{1}{q^n}\sum_{f\in\mathscr{M}_n}\sum_{\substack{I \text{ irreducible}\\ I|f}} 1\\
&= \frac{1}{q^n}\sum_{I\in\mathscr{P}_{\leqslant n}}\sum_{\substack{f\\ I|f}} 1 \qquad (\text{ Interchanging the summations})\\
&= \frac{1}{q^n}\sum_{d\leqslant n}\sum_{I\in\mathscr{P}_d} q^{n-d} \qquad (\text{ since } f=IG \text{ with } \deg(G)=n-d \text{ and } G \text{ has } q^{n-d} \text{ choices })\\
&= \sum_{d\leqslant n}\frac{\pi_q(d)}{q^d}\\
&= \sum_{d\leqslant n}\left(\frac{1}{d}+O(q^{-d/2})\right) \qquad (\text{ using PNT, (2.3.7)})\\
&= \log n + O(1). \qquad \left(\text{ since } \sum_{d\leqslant n} O(q^{-d/2}) = O\left(\frac{1-q^{-n/2}}{1-q^{-1/2}}\right) = O(1)\right)
\end{aligned}$$

It can be shown that $\mathrm{Var}(\omega_q)$ is bounded above by the mean in this case up to a constant.

Lemma 4.2.6. *We have the upper bound*

$$Var(\omega_q) = O(\log n).$$

Proof. We begin the task by estimating $\mathbb{E}(\omega_q^2)$.

$$\begin{aligned}
\mathbb{E}(\omega_q^2) &= \frac{1}{q^n} \sum_{f \in \mathscr{M}_n} \sum_{\substack{I, I' \text{ irreducibles} \\ I|f \\ I'|f}} 1 \\
&= \frac{1}{q^n} \sum_{f \in \mathscr{M}_n} \sum_{\substack{I \text{ irreducible} \\ I|f}} 1 + \frac{1}{q^n} \sum_{f \in \mathscr{M}_n} \sum_{\substack{I \neq I' \\ I|f \\ I'|f}} 1 \\
&= \mathbb{E}\omega_q + \frac{1}{q^n} \sum_{\substack{I \neq I' \\ deg(I)=d \\ deg(I')=d' \\ 0 \leqslant d+d' \leqslant n}} \sum_{\substack{f \in \mathscr{M}_n \\ f = II'G \\ deg(G)=n-(d+d')}} 1 \qquad (\text{ Interchanging the summations}) \\
&= \log n + \frac{1}{q^n} \sum_{\substack{2 \leqslant d+d' \leqslant n \\ d,d' \geqslant 1}} \sum_{\substack{I \in \mathscr{P}_d \\ I' \in \mathscr{P}_{d'}}} q^{n-(d+d')} + O(1) \\
&= \log n + \sum_{1 \leqslant d \leqslant n-1} \frac{\pi_q(d)}{q^d} \sum_{1 \leqslant d' \leqslant n-d} \frac{\pi_q(d')}{q^{d'}} + O(1) \\
&= \log n + \sum_{1 \leqslant d \leqslant n-1} \left(\frac{1}{d} + O\left(q^{-d/2}\right) \right) \sum_{1 \leqslant d' \leqslant n-d} \left(\frac{1}{d'} + O\left(q^{-d'/2}\right) \right) + O(1) \qquad (\text{ using PNT, (2.3.7)}) \\
&= \log n + \sum_{1 \leqslant d \leqslant n-1} \left(\frac{1}{d} + O\left(q^{-d/2}\right) \right) (\log(n-d) + O(1)) + O(1) \\
&= \log n + \sum_{1 \leqslant d \leqslant n-1} \frac{\log(n-d)}{d} + O\left(\sum_{1 \leqslant d \leqslant n-1} \frac{1}{d} \right) + O\left(1 + \sum_{1 \leqslant d \leqslant n-1} q^{-d/2} + \sum_{1 \leqslant d \leqslant n-1} \frac{\log(n-d)}{q^{d/2}} \right) \\
&= \log n + \sum_{1 \leqslant d \leqslant n-1} \frac{\log n}{d} + \sum_{1 \leqslant d \leqslant n-1} \frac{\log(1-\frac{d}{n})}{d} + O(\log n) + O\left(\log n \sum_{1 \leqslant d \leqslant n-1} \frac{1}{q^{d/2}} \right) + O(1) \\
&= \log n + \sum_{1 \leqslant d \leqslant n-1} \frac{\log n}{d} + \sum_{1 \leqslant d \leqslant n-1} \frac{1}{d} \left(\frac{d}{n} + O\left(\frac{d^2}{n^2} \right) \right) + O(\log n) \\
&= \log n + (\log n)^2 + O(\log n) + O(1) + O(\log n) \\
&= (\log n)^2 + O(\log n),
\end{aligned}$$

and hence

$$\mathrm{Var}(\omega_q) = \mathbb{E}(\omega_q^2) - (\mathbb{E}\omega_q)^2 = [(\log n)^2 + O(\log n)] - [\log n + O(1)]^2 = O(\log n).$$

□

It is possible to prove a more precise estimate by carefully analyzing the non-diagonal terms above and show $\mathrm{Var}(\omega_q) = \log n + O(1)$. This is what we will do in the proof of the Erdos Kac theorem in the next section. As a necessary intermediate step to establish the theorem, we will prove a stronger claim that, for every fixed natural number k, the difference of the k-th moment of the function ω_q and the k-th moment of a certain random variable whose mean and variance both are given by the value $(\log n + O(1))$, approaches to zero as $n \to \infty$. In particular when $k = 2$, this would mean $|\mathrm{Var}(\omega_q) - (\log n + O(1))| \to 0$. Therefore there exists $N_0 \in \mathbb{N}$ such that $|\mathrm{Var}(\omega_q) - (\log n + O(1))| \leqslant 1$ for all $n \geqslant N_0$. Also for $N < N_0$, we have from the previous lemma

$$|\mathrm{Var}(\omega_q) - (\log n + O(1))| \leqslant |\mathrm{Var}(\omega_q)| + |(\log n + O(1)| \leqslant O(\log N_0) + \log N_0 + O(1) = O(1).$$

The above observation implies $\mathrm{Var}(\omega_q) = \log n + O(1)$ holds for every $n \in \mathbb{N}$.
Having understood the mean and variance we can immediately prove a Hardy-Ramanujan type result for polynomials. The proof of the following result will be similar to Corollary 4.2.2 if we replace n by some monic polynomial $f \in \mathbb{F}_q[t]$ and $\log\log x$ by $\log n$.

Corollary 4.2.7 (A large deviation result for polynomials)**.** *Almost all monic polynomials of degree n have* $(1 + o(1))\log n$ *distinct irreducible factors.*

4.3 Proof of Erdos-Kac theorem for polynomials

We now have all the necessary tools to establish the key result of this chapter which is to present a detailed proof of Erdos-Kac theorem for polynomials.

Theorem 4.3.1 (Erdos-Kac for polynomials)**.** *For any fixed* $\mathscr{B} \subseteq \mathbb{R}$ *Borel set, we have*

$$\mathbb{P}\left(\frac{\omega_q - \log n}{\sqrt{\log n}} \in \mathscr{B}\right) \to \frac{1}{\sqrt{2\pi}} \int_{\mathscr{B}} e^{-t^2/2} dt \quad \text{as } n \to \infty.$$

As we have discussed in earlier sections that, in the integer case the key idea was to closely approximate the function $\omega(n)$ with another function that is a sum of independent random variables. We follow a similar approach in this case.

Let $f \in \mathscr{M}_n$ be a given monic polynomial of degree n. We define the indicator function indexed by a monic irreducible polynomial $1_g(f)$ which detects the event whether f is divisible by g. The sequence of the indicator functions $\{1_g(f)\}$ will not be independent when f is chosen uniformly at random from the set $\mathscr{M}_n$, as we shall check shortly. If g is a monic irreducible with $\deg(g) = m \leqslant n$ then we first note that $1_g : \mathscr{M}_n \to \{0,1\}$ with

$$\mathbb{P}(1_g = 1) = \mathbb{P}(g|f) = \frac{q^{n-m}}{q^n} = \frac{1}{q^m} \quad \text{and} \quad \mathbb{P}(1_g = 0) = \mathbb{P}(g \nmid f) = \frac{q^n - q^{n-m}}{q^n} = 1 - \frac{1}{q^m}.$$

We now consider the space $\mathscr{M}_7$. Let f be a randomly selected monic polynomial from $\mathscr{M}_7$ and hence f has degree 7 and let g_1 be g_2 be monic irreducibles of degree 3 and 5 respectively. This clearly means $g_1 g_2 \nmid f$ but $\mathbb{P}(1_{g_1} = 1), \mathbb{P}(1_{g_2} = 1) \neq 0$ showing the 1_g's are not independent since

$$0 = \mathbb{P}(1_{g_1} = 1 \text{ and } 1_{g_2} = 1) \neq \mathbb{P}(1_{g_1} = 1)\mathbb{P}(1_{g_2} = 1).$$

We now return to the proof of Theorem 4.3.1.

Proof of Theorem 4.3.1. Let $f \in \mathscr{M}_n$ be a fixed monic polynomial of degree n. It is immediate that $1_g(f) = 0$ if $\deg(g) \geqslant n$. Inspired from the integer case, to prove a CLT for the function ω_q, our strategy will be decomposing ω_q into a sum of indicator functions and approximate the sum with an appropriate random model. We start with the following identity

$$\omega_q(f) = \sum_{g \in \mathscr{P}_{\leqslant n}} 1_g(f).$$

Our probabilistic model for ω_q will be the following sum of independent random variables $\{Y_g\}$ indexed by monic irreducibles and defined on some probability space

$$S_m := \sum_{g \in \mathscr{P}_{\leqslant m}} Y_g,$$

where Y_g has the following distribution, if g is a monic irreducible of degree $d \leqslant n$, then we

have

$$\mathbb{P}(Y_g = 1) = \frac{1}{q^d} \text{ and } \mathbb{P}(Y_g = 0) = 1 - \frac{1}{q^d}.$$

Due to independence, it is now straightforward to calculate the mean and variance of S_m,

$$\mu_m := \mathbb{E}(S_m) = \sum_{g \in \mathscr{P}_{\leqslant m}} \mathbb{E}Y_g = \sum_{1 \leqslant j \leqslant m} \frac{\pi_q(j)}{q^j} = \log m + O(1),$$

$$\sigma_m^2 := \mathrm{Var}(S_m) = \sum_{g \in \mathscr{P}_{\leqslant m}} \mathrm{Var}(Y_g) = \sum_{1 \leqslant j \leqslant m} \frac{\pi_q(j)}{q^j}\left(1 - \frac{1}{q^j}\right) = \log m + O(1).$$

The classical Central limit theorem (Theorem 3.4.1, [8]) thus tells us that the normalized variables $(S_m - \mathbb{E}S_m)/\sqrt{\mathrm{Var}(S_m)}$ approaches to standard normal distribution $N(0,1)$ as $m \to \infty$. Following the approach in the integer case, the next natural step is to show the difference between k-th moments of S_m and a truncated version ω_q is very small for every $k \in \mathbb{N}$.
Also, Billingsley's proof in the integer case suggests here we will have to get rid of the irreducible factors with large degree to maintain enough independence. Therefore we define the following truncated version of the function ω_q

$$\omega_q^{(m)}(f) = \sum_{g \in \mathscr{P}_{\leqslant m}} 1_g(f),$$

where the parameter m has to be chosen in terms of n which we shall optimize later. Therefore the difference between the k th moments of S_m and $\omega_q^{(m)}$ is given by

$$\frac{1}{q^n}\sum_{f \in \mathscr{M}_n} (\omega_q^{(m)}(f) - \mu_m)^k - \mathbb{E}(S_m - \mu_m)^k = \sum_{j=1}^{k} \binom{k}{j} (-\mu_m)^{k-j} \left(\frac{1}{q^n} \sum_{f \in \mathscr{M}_n} \omega_q^{(m)}(f)^j - \mathbb{E}(S_m^j) \right). \tag{4.3.1}$$

Before continuing with the proof we first make an observation. Let us write $\ell_0 := \mathrm{lcm}[I_1, I_2, \ldots, I_j]$ where $I_1, I_2, \ldots, I_j$ are some irreducible monic polynomials (not necessarily distinct). With this notation we now show that the relation $\mathbb{E}(Y_{I_1} Y_{I_2} \cdots Y_{I_j}) = 1/q^{deg(\ell_0)}$ holds due to independence of $\{Y_{I_j}\}$. We first note for a fixed irreducible monic polynomial $g \in \mathscr{P}_{\leqslant n}$ the identity $Y_g^2 = Y_g$ holds since Y_g is a $\{0,1\}$ valued random variable. Inductively it follows that $Y_g^k = Y_g$ for every $k \in \mathbb{N}$ and every monic irreducible g. Therefore, without loss of generality we can assume all the irreducible polynomials $I_1, I_2, \ldots, I_j$ are distinct. (otherwise we can collect the Y_I's corresponding to the repetitions and turn them into a single random variable) Assuming $I_1, I_2, \ldots, I_j$

are all distinct, we have $\ell_0 = I_1 I_2 \cdots I_j$ and therefore by the independence,

$$\mathbb{E}(Y_{I_1} Y_{I_2} \cdots Y_{I_j}) = \mathbb{E}(Y_{I_1})\mathbb{E}(Y_{I_2}) \cdots \mathbb{E}(Y_{I_j}) = \frac{1}{q^{deg(I_1)+deg(I_2)+\ldots+deg(I_j)}} = \frac{1}{q^{deg(\ell_0)}}.$$

In (4.3.1), we call the inner term in parenthesis L_j. Upon expanding the sum in L_j and interchanging summation we get

$$\begin{aligned} L_j &:= \sum_{I_1, I_2, \ldots I_j \in \mathscr{P}_{\leqslant m}} \left(\frac{1}{q^n} \sum_{f \in \mathscr{M}_n} 1_{I_1}(f) 1_{I_2}(f) \cdots 1_{I_j}(f) - \mathbb{E}\left(Y_{I_1} Y_{I_2} \cdots Y_{I_j}\right) \right) \\ &= \sum_{\substack{I_1, I_2, \ldots I_j \in \mathscr{P}_{\leqslant m} \\ \ell_0 = \mathrm{lcm}[I_1, I_2, \ldots, I_j] \\ deg(\ell_0) \leqslant n}} \left(\frac{1}{q^n} \sum_{\substack{f \in \mathscr{M}_n \\ \ell_0 | f}} 1 - \frac{1}{q^{deg(\ell_0)}} \right) - \sum_{\substack{I_1, I_2, \ldots I_j \in \mathscr{P}_{\leqslant m} \\ deg(\ell_0) > n}} \frac{1}{q^{deg(\ell_0)}} \qquad \left(\text{substituting } \mathbb{E}(Y_{I_1} Y_{I_2} \cdots Y_{I_j})\right) \end{aligned}$$

Now using the triangle inequality, we get

$$\begin{aligned} |L_j| &\leqslant \sum_{I_1, I_2, \ldots I_j \in \mathscr{P}_{\leqslant m}} \left(\frac{1}{q^n} \sum_{\substack{f \in \mathscr{M}_n \\ \ell_0 | f \\ deg(\ell_0) \leqslant n}} 1 - \frac{1}{q^{deg(\ell_0)}} \right) + \sum_{\substack{I_1, I_2, \ldots I_j \in \mathscr{P}_{\leqslant m} \\ deg(\ell_0) > n}} \frac{1}{q^{deg(\ell_0)}} \\ &\leqslant \sum_{I_1, I_2, \ldots I_j \in \mathscr{P}_{\leqslant m}} \left(\frac{q^{n - deg(\ell_0)}}{q^n} - \frac{1}{q^{deg(\ell_0)}} \right) + \frac{\pi_q(m)^j}{q^n} \\ &= \sum_{I_1, I_2, \ldots I_j \in \mathscr{P}_{\leqslant m}} \left(\frac{1}{q^{deg(\ell_0)}} - \frac{1}{q^{deg(\ell_0)}} \right) + \frac{\pi_q(m)^j}{q^n} \\ &= \frac{\pi_q(m)^j}{q^n}. \end{aligned}$$

Thus an upper bound on the difference of k-th moments of $\omega_q^{(m)}$ and S_m is given by

$$\ll \sum_{j=1}^{k} \binom{k}{j} \mu_m^{k-j} \frac{\pi_q(m)^j}{q^n} = \frac{(\mu_m + \pi_q(m))^k}{q^n} = \frac{(\log m + O(1) + \pi_q(m))^k}{q^n} \ll \frac{1}{q^n} \left(\frac{q^m}{m} \right)^k.$$

Inspired from the choice we made in the integer case, here we set $m = n/(\log n)^{1/3}$. We can

verify that as $m,n \to \infty$,

$$\frac{1}{q^n}\left(\frac{q^m}{m}\right)^k = \frac{q^{mk-n}}{m^k} = \frac{q^{\frac{kn}{(\log n)^{1/3}}-n}}{\left(n/(\log n)^{1/3}\right)^k} \to 0 \text{ for every fixed } k \in \mathbb{N}$$

as the numerator becomes bounded (in fact approaches 0) as n increases while the denominator approaches to infinity. The above observation implies for each fixed $k \in \mathbb{N}$

$$\mathbb{E}\left(\frac{\omega_q^{(m)} - \mu_m}{\sigma_m}\right)^k \to \mathbb{E}(Z^k) \qquad \text{as } n,m \to \infty,$$

where Z is distributed as a standard normal variable $N(0,1)$.

Desired convergence in distribution follows by the method of moments (see appendix C, [17]) and after we note $\omega_q(f) - \omega_q^{(m)}(f) \leqslant (\log n)^{1/3}$ since there can be at most $(\log n)^{1/3}$ irreducibles with degree $> m$ that divide $f \in \mathscr{M}_n$ and $\mu_m, \sigma_m^2 = \log n + O\left((\log n)^{1/3}\right)$. Thus we have

$$\frac{\omega_q(f) - \log n}{\sqrt{\log n}} - \frac{\omega_q^{(m)}(f) - \mu_m}{\sigma_m} = o(1) \qquad \text{as } m,n \to \infty.$$

□

Needless to mention that the Erdos-Kac theorem also holds for the completely additive function $\Omega_q(f)$ with mean and variance both $\log n$. Generalizations of this theorem also exist for various arithmetic functions in this context.

CHAPTER 5

ON A PROBLEM OF GAUSS, LANDAU, HARDY AND RAMANUJAN

In the previous chapter, we discussed the statistical properties of the functions ω, Ω. We now take the discussion one step further in this and the later chapter. We ask the fundamental question, how many integers are there up to 1000 billion (or any large number) with exactly 2022 (or any given integer) prime factors? This exciting question fascinated mathematicians for ages. Gauss initially started the investigation and the question was later pursued by several eminent mathematicians, including Landau, Hardy and Ramanujan.

5.1 The functions $\pi(x,k)$ and $\Pi(x,k)$

Let $m \leqslant x$ be positive integers. We begin with the following definitions.

$$\pi(x,k) := \#\Big\{ m \leqslant x : \omega(m) = k \Big\},$$

$$\Pi(x,k) := \#\Big\{ m \leqslant x : \Omega(m) = k \Big\}.$$

Using Chebyechev's estimate and mathematical induction one can establish an upper bound on $\pi(x,k)$. (see chapter 9 in [11])

Theorem 5.1.1 (Hardy-Ramanujan upper bound)**.** *There are two positive constants A_1, B_1 such that for any integer $x \geqslant 2$ the following upper bound holds*

$$\pi(x,k) \leqslant \frac{A_1 x}{\log x} \frac{(\log\log x + B_1)^{k-1}}{(k-1)!} \qquad \text{for each } k \in \mathbb{N}.$$

In the next section we prove an asymptotic result for $\pi(x,k)$ when k will be a fixed positive integer and then move onto discuss about the results when k grows uniformly with x to infinity for both $\pi(x,k)$, $\Pi(x,k)$ and their analogues in the polynomial setting.

5.1.1 Landau's theorem: an asymptotic for $\pi(x,k)$ and $\Pi(x,k)$ when $k \in \mathbb{N}$ fixed

The following result goes back to E. Landau. Below we present two proofs of Landau's theorem including the one due to E.M. Wright [29] with some minor modifications in the arguments.

Theorem 5.1.2. *For $k \in \mathbb{N}$ fixed we have*

$$\pi(x,k) \sim \Pi(x,k) \sim \frac{x}{\log x} \frac{(\log\log x)^{k-1}}{(k-1)!}.$$

Before proving the theorem, we need a technical lemma from analysis which will be helpful along the way.

Lemma 5.1.3. *Let $F(u,x)$ be a function $(2 \leqslant u \leqslant x)$ such that $F(u,x)$ is non negative. Let $F(u,x)/\log u$ be a decreasing function of u when x is fixed. We further assume the condition $F(2,x) = o(\int_2^x F(u,x)du/\log u)$ holds. Then we have that*

$$\sum_{p \leqslant x} F(p,x) \sim \int_2^x \frac{F(u,x)}{\log u} du.$$

A proof of the above lemma using Abel's partial summation can be found in [18] (see page 203).

First proof of the asymptotic for $\pi(x,k)$. We proceed by strong induction on k. The case $k = 1$ is the prime number theorem. We observe the following identity holds for each positive integer k

$$\sum_{p \leqslant x} \pi\left(\frac{x}{p}, k\right) = (k+1)\pi(x,k+1) + \#\{m \leqslant x : \ m = p^2 m' \text{ with } \omega(m') = k-1 \text{ for some prime } p\}.$$

LHS counts all the integers of the form $p\ell \leqslant x$ where ℓ has k distinct prime factors and then we take a sum over all possible p and this is same as the RHS since if $p \nmid \ell$ then the integer $p\ell$ has $(k+1)$ distinct prime factors and hence contributes $(k+1)$ times in the sum and if $p \mid \ell$ then $p\ell$ can be split into two parts one of which is p^2 and the other part consists of $(k-1)$ different

prime factors. We show the latter is small using the strong induction hypothesis on k;

$$\begin{aligned}\#\{m \leqslant x:\ m = p^2 m' \text{ with } \omega(m') = k-1 \text{ for some prime } p\} &= O\left(\sum_{p \leqslant \sqrt{x/2}} \pi\left(\frac{x}{p^2}, k-1\right)\right) \\ &= O\left(\sum_{1 \leqslant n \leqslant \sqrt{x/2}} \pi\left(\frac{x}{n^2}, k-1\right)\right) \\ &= O\left(\sum_{n=1}^{\sqrt{x/2}} \frac{x}{n^2} \frac{(\log\log x)^{k-2}}{\log\left(\frac{x}{n^2}\right)}\right) \\ &= O\left(x(\log\log x)^{k-2} \sum_{n=1}^{\sqrt{x/2}} \frac{1}{n^2 \log\left(\frac{x}{n^2}\right)}\right).\end{aligned}$$

The sum inside the O-term is small once we note

$$\begin{aligned}\sum_{n=1}^{\sqrt{x/2}} \frac{1}{n^2 \log\left(\frac{x}{n^2}\right)} &= \sum_{n=1}^{x^{1/4}} \frac{1}{n^2 \log\left(\frac{x}{n^2}\right)} + \sum_{n=x^{1/4}+1}^{\sqrt{x/2}} \frac{1}{n^2 \log\left(\frac{x}{n^2}\right)} \\ &\leqslant \sum_{n=1}^{x^{1/4}} \frac{1}{n^2 \log\left(\frac{x}{\sqrt{x}}\right)} + \sum_{n=x^{1/4}+1}^{\sqrt{x/2}} \frac{1}{n^2 \log 2} \\ &= O\left(\frac{1}{\log x}\right) + O\left(\frac{1}{x^{1/4}}\right) \\ &= O\left(\frac{1}{\log x}\right).\end{aligned}$$

Thus we get that

$$\#\{m \leqslant x:\ m = p^2 m' \text{ with } \omega(m') = k-1 \text{ for some prime } p\} = O\left(\frac{x(\log\log x)^{k-2}}{\log x}\right).$$

Hence we obtain,

$$(k+1)\pi(x, k+1) + O\left(\frac{x(\log\log x)^{k-2}}{\log x}\right) = \sum_{p \leqslant x} \pi\left(\frac{x}{p}, k\right).$$

By induction hypothesis the leading term in the sum $\pi(x/2, k) \sim \frac{(x/2)(\log\log(x/2))^{k-1}}{\log(x/2)}$. Thus we

get

$$(k+1)\pi(x,k+1) \sim \sum_{p\leqslant x} \pi\left(\frac{x}{p},k\right). \tag{5.1.1}$$

Now we will use Lemma 5.1.3 to evaluate the sum on the right hand side. In the framework of Lemma 5.1.3 since k is fixed, it is convenient to set

$$F(u,x) := \pi\left(\frac{x}{u},k\right).$$

Using the induction hypothesis our aim is now to calculate the key integral $I_0 := \int_2^x F(x,u)du/\log u$ and show it satisfies the hypothesis of Lemma 5.1.3. Therefore we start with

$$\begin{aligned}
I_0 &= \int_2^x \frac{F(u,x)}{\log u}du \\
&= \int_2^{x/2} \frac{\pi\left(\frac{x}{u},k\right)}{\log u}du \qquad \left(\pi\left(\frac{x}{u},k\right) = 0 \text{ if } u \geqslant x/2\right) \\
&= x\int_{x/2}^2 \frac{\pi(v,k)}{\log x - \log v}\left(-\frac{dv}{v^2}\right) \qquad \left(\text{substituting } v = \frac{x}{u}\right) \\
&= x\int_2^{x/2} \frac{\pi(v,k)}{\log x - \log v}\frac{dv}{v^2} \\
&\sim x\int_2^{x/2} \frac{v(\log\log v)^{k-1}}{(k-1)!\log v}\frac{dv}{v^2(\log x - \log v)} \qquad \text{(induction hypothesis)}
\end{aligned} \tag{5.1.2}$$

To rigorously justify the above substitution we let $f(x,k) = \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}$ be a non negative function so that $\pi(x,k) \sim f(x,k)$ by the induction hypothesis. Therefore given $\varepsilon > 0$, there exists $x_0(\varepsilon)$ and a constant $C(\varepsilon)$ such that the following two inequalities hold

$$|\pi(x,k) - f(x,k)| \leqslant \varepsilon f(x,k) \text{ whenever } x > x_0(\varepsilon),$$

$$|\pi(x,k) - f(x,k)| \leqslant C(\varepsilon) f(x,k) \text{ whenever } 2 \leqslant x \leqslant x_0(\varepsilon).$$

The second claim is valid since $|\pi(x,k)/f(x,k) - 1| \leqslant \pi(x,k)/f(x,k) + 1 \leqslant \pi(x_0(\varepsilon),k)/f(2,k) + 1$ as both $\pi(x,k)$ and $f(x,k)$ are increasing functions in x. The error caused by the replacement of the integrals is defined by

$$E(x) := \left|\int_2^{x/2} \frac{\pi(v,k)}{\log x - \log v}\frac{dv}{v^2} - \int_2^{x/2} \frac{f(v,k)}{\log x - \log v}\frac{dv}{v^2}\right|.$$

Therefore when x sufficiently large and in particular when $x \geqslant \max\{2x_0(\varepsilon), x_0^4(\varepsilon)\}$ we can bound the error in the following way

$$\begin{aligned}
E(x) &\leqslant C(\varepsilon)\int_2^{x_0(\varepsilon)} \frac{f(v,k)dv}{v^2(\log x-\log v)} + \varepsilon\int_{x_0(\varepsilon)}^{x/2} \frac{f(v,k)}{\log x-\log v}\frac{dv}{v^2} \\
&\leqslant \frac{C(\varepsilon)}{(k-1)!}\int_2^{x_0(\varepsilon)} \frac{(\log\log v)^{k-1}dv}{v\log v(\log x-\log v)} + \frac{\varepsilon}{(k-1)!}\int_{x_0(\varepsilon)}^{x/2} \frac{f(v,k)}{\log x-\log v}\frac{dv}{v^2} \\
&\leqslant \frac{4C(\varepsilon)}{3(k-1)!\log x}\int_2^{x_0(\varepsilon)} \frac{(\log\log v)^{k-1}dv}{v\log v} + \varepsilon\int_2^{x/2} \frac{f(v,k)}{\log x-\log v}\frac{dv}{v^2}.
\end{aligned}$$

In the final step, for the first integral, we used $\log x-\log v \geqslant \log x-\log x_0(\varepsilon) \geqslant \log x-\log(x^{1/4}) = (3/4)\log x$. We also observe the first integral is a finite number depending only on ε. We thus obtain

$$E(x) = O_\varepsilon\left(\frac{1}{\log x}\right) + \varepsilon\int_2^{x/2} \frac{f(v,k)}{\log x-\log v}\frac{dv}{v^2}.$$

Since the first quantity decays, we have

$$\int_2^{x/2} \frac{\pi(v,k)}{\log x-\log v}\frac{dv}{v^2} \sim \int_2^{x/2} \frac{f(v,k)}{\log x-\log v}\frac{dv}{v^2}.$$

We continue our integral calculation from (5.1.2) and get

$$\begin{aligned}
\frac{(k-1)!I_0}{x} &\sim \int_2^{x/2} \frac{(\log\log v)^{k-1}}{v\log v}\frac{dv}{(\log x-\log v)} \\
&= \int_{\log 2}^{\log x-\log 2} \frac{\log^{k-1} w dw}{w(\log x-w)} \qquad (w=\log v) \\
&= \int_{\log 2}^{\log x-\log 2} \frac{\log^{k-1} w dw}{\log x}\left(\frac{1}{w}+\frac{1}{\log x-w}\right) \\
&= \int_{\log 2}^{\log x-\log 2} \frac{\log^{k-1} w dw}{w\log x} + \int_{\log 2}^{\log x-\log 2} \frac{\log^{k-1} w dw}{\log x(\log x-\log w)} \\
&= I_1+I_2. \qquad (5.1.3)
\end{aligned}$$

We can explicitly calculate I_1 and I_2. With the substitution $z=\log w$, I_1becomes

$$I_1 = \int_{\log\log 2}^{\log(\log x-\log 2)} \frac{z^{k-1}dz}{\log x} = \frac{\log^k(\log x-\log 2)-\log^k(\log 2)}{k\log x} \sim \frac{(\log\log x)^k}{k\log x}.$$

The estimation of I_2 a bit more involved;

$$\begin{aligned}
I_2 &= \int_{\log 2}^{\log x-\log 2} \frac{\log^{k-1} w dw}{\log x(\log x-\log w)} \\
&= \int_{\log 2}^{(\log x)/2} \frac{\log^{k-1} w dw}{\log x(\log x-\log w)} + \int_{(\log x)/2}^{\log x-\log 2} \frac{\log^{k-1} w dw}{\log x(\log x-\log w)} \\
&= O\left(\log x \frac{(\log\log x)^{k-1}}{\log^2 x}\right) + \int_{(\log x)/2}^{\log x-\log 2} \frac{\log^{k-1} w dw}{\log x(\log x-\log w)} \qquad \left(\frac{\log^{k-1} w}{\log x-\log w} \text{ is increasing in } w\right) \\
&= O\left(\frac{(\log\log x)^{k-1}}{\log x}\right) + \log^{k-1}\left(\log x-\log 2-\frac{\Theta}{2}\log x\right) \int_{(\log x)/2}^{\log x-\log 2} \frac{dw}{\log x(\log x-\log w)}
\end{aligned} \tag{5.1.4}$$

for some $0 < \Theta \leqslant 1$. This follows from generalized mean value theorem which we show now. Let $F_1(w) = \frac{\log^{k-1} w}{\log x(\log x-\log w)}$ and $F_2(w) = \frac{1}{\log x(\log x-\log w)}$. Then we consider the two following functions defined by

$$G_1(t) := \int_1^t F_1(w)dw \text{ and } G_2(t) := \int_1^t F_2(w)dw \text{ for } 1 \leqslant t \leqslant \log x.$$

By the fundamental theorem of calculus $G_1'(t) = F_1(t)$ and $G_2'(t) = F_2(t)$ for all $t \in (1, \log x)$. Therefore using generalized mean value theorem on the interval $[(\log x)/2, \log x - \log 2]$, we get

$$\frac{G_1(\log x-\log 2)-G_1((\log x)/2)}{G_2(\log x-\log 2)-G_2((\log x)/2)} = \frac{G_1'(c)}{G_2'(c)} = \frac{F_1(c)}{F_2(c)} = \log^{k-1} c$$

for some point $c \in (\log x/2, \log x - \log 2)$ and therefore we can select $0 < \Theta \leqslant 1$ such that $c = \log x - \log 2 - \frac{\Theta}{2}\log x$ holds. We first note that

$$\log^{k-1}\left(\log x-\log 2-\frac{\Theta}{2}\log x\right) \sim (\log\log x)^{k-1}.$$

Secondly,

$$\int_{(\log x)/2}^{\log x-\log 2} \frac{dw}{\log x(\log x-\log w)} = \frac{1}{\log x}\log\left(\frac{\log x-\frac{\log x}{2}}{\log x-(\log x-\log 2)}\right) = \frac{1}{\log x}\log\frac{\log x}{2\log 2} \sim \frac{\log\log x}{\log x}.$$

Combining the above observations with (5.1.4) we obtain

$$I_2 \sim \frac{(\log\log x)^k}{\log x}.$$

Finally we get from (5.1.3)

$$\frac{(k-1)!I_0}{x} \sim \left(1+\frac{1}{k}\right)\frac{(\log\log x)^k}{\log x}.$$

Thus

$$I_0 \sim \frac{x}{\log x}\frac{(k+1)(\log\log x)^k}{k!}.$$

We can now verify that $F(u,x)$ indeed satisfies the hypothesis described in Lemma 5.1.3. $F(u,x) = \pi(x/u,k)$ is clearly non negative and decreasing in u when x is fixed. Furthermore using the induction hypothesis

$$F(2,x) = \pi\left(\frac{x}{2},k\right) = \frac{(x/2)\log^{k-1}(\log(x/2))}{\log(x/2)(k-1)!} = o\left(I_0\right).$$

Hence from (5.1.1)

$$\begin{aligned}(k+1)\pi(x,k+1) &\sim \sum_{p\leqslant x}\pi\left(\frac{x}{p},k\right)\\ &= \sum_{p\leqslant x}F(p,x) \qquad \text{(definition of } F\text{)}\\ &\sim I_0 \qquad \text{(Lemma 5.1.3)}\\ &\sim \frac{x}{\log x}\frac{(k+1)(\log\log x)^k}{k!}.\end{aligned}$$

Therefore the induction step is complete as

$$\pi(x,k+1) \sim \frac{x}{\log x}\frac{(\log\log x)^k}{k!}.$$

□

5.1.2 Wright's proof of Landau's theorem

The proof due to E.M. Wright of Theorem 5.1.2 is fairly complicated and will require some auxiliary results. We begin the proof by introducing three different sums, and our final goal will be to connect these sums to extract the asymptotic information. Here $*$ above the summation symbol indicates the sum runs over all possible k tuples of primes $(p_1, p_2, \ldots, p_k)$ such that their product $p_1 p_2 \cdots p_k \leqslant x$. Note that we allow repetitions so that $p_i = p_j$ is possible in the tuple for $i \neq j$. Therefore different k tuples may correspond to the same product, and we let each of them contribute to the following sums.

We set

$$A(x,k) := \sideset{}{^*}\sum_{p_1\cdots p_k \leqslant x} \frac{1}{p_1 \cdots p_k}$$

$$B(x,k) := \sideset{}{^*}\sum_{p_1\cdots p_k \leqslant x} 1$$

$$C(x,k) := \sideset{}{^*}\sum_{p_1\cdots p_k \leqslant x} \log(p_1 \cdots p_k)$$

$$\pi(x,k) = \sum_{\substack{n \leqslant x \\ \omega(n)=k}} 1$$

$$\Pi(x,k) = \sum_{\substack{n \leqslant x \\ \Omega(n)=k}} 1$$

Clearly every square-free integer with k distinct prime factors, i.e. $m = q_1 q_2 \cdots q_k \leqslant x$ where q_i's are primes and $q_i \neq q_j$ for different i and j, that appears exactly once in $\pi(x,k)$ will appear $k!$ times in the sum $B(x,k)$. Also every integer $m \leqslant x$ with $\Omega(m) = k$ that appears once in the sum $\Pi(x,k)$ will appear at most $k!$ times in $B(x,k)$ since we allowed repetitions in the tuples. Hence we arrive at the inequality

$$\pi(k,x) \leqslant \frac{B(k,x)}{k!} \leqslant \Pi(k,x). \tag{5.1.5}$$

We also observe

$$\Pi(x,k) - \pi(x,k) \leqslant \sum_{\substack{p_1\cdots p_k \leqslant x \\ p_i = p_j, i \neq j}} 1 \leqslant \binom{k}{2} \sum_{p_1 \cdots p_{k-1} \leqslant x} 1 = \binom{k}{2} B(x, k-1). \tag{5.1.6}$$

At the second step, for a fixed i and j with $p_i = p_j$, the range of the summation is over $p_1 \cdots p_i \cdots p_k \leqslant x/p_j \leqslant x$ where the product is comprised of $k-1$ primes and there are $\binom{k}{2}$ different choices for i and j in total.

Lemma 5.1.4. *To establish the asymptotics of $\pi(x,k)$ and $\Pi(x,k)$ mentioned in the statement of the Theorem 5.1.2, It is enough to prove the following estimate*

$$B(x,k) \sim \frac{kx(\log\log x)^{k-1}}{\log x}.$$

Proof. Suppose the asymptotic for $B(x,k)$ described in the hypothesis holds. The inequality (5.1.6) implies

$$\begin{aligned}
1 - \frac{\pi(x,k)}{\Pi(x,k)} &\leqslant \frac{\binom{k}{2}B(x,k-1)}{\Pi(x,k)} \\
&\leqslant k! \frac{\binom{k}{2}B(x,k-1)}{B(x,k)} \qquad (\text{ Using the inequality (5.1.5)}) \\
&\ll k!\binom{k}{2}\frac{(k-1)}{k}\frac{1}{\log\log x} \qquad (\text{ Plugging in the asymptotic in hypothesis})
\end{aligned}$$

The above reasoning implies $\pi(x,k) \sim \Pi(x,k)$ since k is fixed.
Let $\varepsilon > 0$ be given. Therefore, the inequality

$$\pi(x,k) \geqslant \Pi(x,k)(1-\varepsilon/2) \tag{5.1.7}$$

holds for x sufficiently large. Also the two following inequalities in view of the assumption on the asymptotic of $B(x,k)$

$$\pi(x,k) \leqslant \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}(1+\varepsilon), \tag{5.1.8}$$

$$\Pi(x,k) \geqslant \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}\left(1-\frac{\varepsilon}{2}\right)$$

hold when x is sufficiently large. Hence we obtain from (5.1.7)

$$\pi(x,k) \geqslant \Pi(x,k)\left(1-\frac{\varepsilon}{2}\right) \geqslant \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}\left(1-\frac{\varepsilon}{2}\right)^2 \geqslant \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}(1-\varepsilon). \tag{5.1.9}$$

The claim follows from (5.1.8) and (5.1.9). □

We now prove two another auxiliary results.

Lemma 5.1.5. *We have*

$$A(x,k) \sim (\log\log x)^k$$

Proof. We note the inequality

$$\left(\sum_{p\leqslant x^{1/k}} \frac{1}{p}\right)^k \leqslant A(x,k) \leqslant \left(\sum_{p\leqslant x} \frac{1}{p}\right)^k. \tag{5.1.10}$$

Using Merten's estimate we see that

$$\begin{aligned}\left(\sum_{p\leqslant x^{1/k}} \frac{1}{p}\right)^k &\sim \left(\log\log\left(x^{1/k}\right)\right)^k \\ &\sim (\log\log x - \log k)^k \\ &\sim (\log\log x)^k.\end{aligned}$$

We also know that $(\sum_{p\leqslant x} 1/p)^k \sim (\log\log x)^k$ holds and the conclusion follows from (5.1.5). □

Lemma 5.1.6. *To establish the asymptotics of $\pi(x,k)$ and $\Pi(x,k)$ mentioned in the statement of the Theorem 5.1.2, It is enough to prove the following estimate*

$$C(x,k) \sim kx(\log\log x)^{k-1},$$

where

$$C(x,k) = \sideset{}{^*}\sum_{p_1\cdots p_k\leqslant x} \log(p_1\cdots p_k).$$

Proof. Let $d(n,k)$ denotes the number of tuples $(p_1,p_2,\ldots,p_k)$ of prime numbers (not necessarily distinct) such that $n = p_1\cdots p_k$. For instance, we have $d(n,k) = k!$ if n is a square-free integer with $\omega(n) = k$. We also note from the definition $C(x,k)$ can be re-written as

$$C(x,k) = \sum_{n\leqslant x} d(n,k)\log(n) = B(x,k)\log x - \int_1^x \frac{B(t,k)}{t}dt,$$

where the last step is obtained via partial summation and $B(x,k) = \sum_{n\leqslant x} d(n,k)$.

We have $B(x,k) \leqslant k!\Pi(x,k) \leqslant k!x = O(x)$ which in turn implies $C(x,k) = B(x,k)\log x + O(x)$. So if we are allowed to assume $C(x,k) \sim kx(\log\log x)^{k-1}$ then it would also imply

$$B(x,k) \sim \frac{kx(\log\log x)^{k-1}}{\log x}.$$

The conclusion now follows from Lemma 5.1.4. □

We have now set the stage for proving Theorem 5.1.2.

Second proof of Theorem 5.1.2. Using the previous lemma it is enough to show

$$C(x,k) \sim kx(\log\log x)^{k-1}.$$

We proceed by induction. The case $k = 1$ follows from PNT. To connect $C(x,k)$ with $C(x,k+1)$ we should look for a recurrence relation.
From Lemma 5.1.5 we conclude that

$$C(x,k+1) - (k+1)x(\log\log x)^k = C(x,k+1) - (k+1)xA(x,k) + o\left(x\,(\log\log x)^k\right). \quad (5.1.11)$$

We now build two recurrences that connect $C(x,k+1)$ to $C(x,k)$ and $A(x,k)$ to $A(x,k-1)$.

$$\begin{aligned} kC(x,k+1) &= \sideset{}{^*}\sum_{p_1\cdots p_{k+1}\leqslant x} \log\left(p_1^k p_2^k \cdots p_k^k\right) \\ &= \sideset{}{^*}\sum_{p_1\cdots p_{k+1}\leqslant x} [\log(p_2\cdots p_{k+1}) + \log(p_1p_3\cdots p_{k+1}) + \ldots + \log(p_1\cdots p_k)] \\ &= (k+1)\sum_{p_1\leqslant x} \sideset{}{^*}\sum_{p_2\cdots p_{k+1}\leqslant x/p_1} \log(p_2\cdots p_{k+1}) \\ &= (k+1)\sum_{p_1\leqslant x} C\left(\frac{x}{p_1},k\right). \end{aligned}$$

and likewise after letting $A(x,0) = 1$ we get

$$\begin{aligned} A(x,k) &= \sideset{}{^*}\sum_{p_1\cdots p_k\leqslant x} \frac{1}{p_1\cdots p_k} \\ &= \sum_{p_1\leqslant x} \frac{1}{p_1} A\left(\frac{x}{p_1},k-1\right). \end{aligned}$$

Combining these recurrences and plugging in (5.1.11), we obtain

$$C(x,k+1)-x(\log\log x)^k=\frac{(k+1)}{k}\sum_{p_1\leqslant x}\left(C\left(\frac{x}{p_1},k\right)-\frac{kx}{p_1}A\left(\frac{x}{p_1},k-1\right)\right). \tag{5.1.12}$$

Our induction hypothesis says that

$$C(x,k)-kxA(x,k-1)=o(x(\log\log x)^{k-1}).$$

The cake $k=1$ is PNT since $A(x,0)=1$ implies $C(x,1)\sim x$.
Let $\varepsilon>0$ be a given real number. The above equation implies the existence of an integer x_0 such that

$$|C(x,k)-kxA(x,k-1)|\leqslant \varepsilon x(\log\log x)^{k-1} \text{ holds whenever } x\geqslant x_0.$$

We pick a suitable constant $c>0$ such that the following inequality also holds

$$|C(x,k)-kxA(x,k-1)|\leqslant c \text{ whenever } x\leqslant x_0.$$

Thus from (5.1.12) we have for x sufficiently large,

$$\begin{aligned}\left|C(x,k+1)-x(\log\log x)^k\right| &\leqslant \left(1+\frac{1}{k}\right)\left(\sum_{x/x_0\leqslant p_1\leqslant x} c+\sum_{p_1\leqslant x/x_0}\frac{\varepsilon x}{p_1}\left(\log\log\left(\frac{x}{p_1}\right)\right)^{k-1}\right)\\ &\leqslant 2\left(cx+\varepsilon x(\log\log x)^{k-1}\sum_{p_1\leqslant x/x_0}\frac{1}{p_1}\right)\\ &\leqslant 2cx+4\varepsilon x(\log\log x)^k\\ &\ll \varepsilon x(\log\log x)^k.\end{aligned}$$

Hence it follows that

$$C(x,k+1)-x(\log\log x)^k=o(x(\log\log x)^k)$$

and the induction argument completes. □

Thus, from Theorem 5.1.2 we can conclude the functions $\pi(x,k)$ and $\Pi(x,k)$ are approximately

Poisson distributed with parameter $\log\log x$ for $k \in \mathbb{N}$ fixed, in the sense that we have

$$\mathbb{P}(\omega(n) = k) \sim \mathbb{P}(\Omega(n) = k) \sim \frac{1}{\log x} \frac{(\log\log x)^{k-1}}{(k-1)!} \qquad \text{as } x \to \infty.$$

However, the story becomes significantly different if we let k uniformly vary with x to infinity. It then becomes considerably harder to understand the asymptotic behaviour of $\pi(x,k)$ and $\Pi(x,k)$. It remained as an open problem for quite a long time.

In 1953, Sathe ingeniously showed that if $A > 0$ is given, then uniformly for $1 \leqslant k \leqslant A\log\log x$ and $x \geqslant 3$ we have

$$\pi(x,k) \sim \lambda\left(\frac{k-1}{\log\log x}\right) \frac{(\log\log x)^{k-1}}{(k-1)!} \frac{x}{\log x}, \tag{5.1.13}$$

where

$$\lambda(z) = \frac{1}{\Gamma(z+1)} \prod_p \left(1 - \frac{1}{p}\right)^z \left(1 + \frac{z}{p-1}\right).$$

Using his methods one can also show [23] that if $\varepsilon \in (0,2)$ is given, then uniformly for $1 \leqslant k \leqslant (2-\varepsilon)\log\log x$ we have

$$\Pi(x,k) \sim F\left(\frac{k}{\log\log x}\right) \frac{(\log\log x)^{k-1}}{(k-1)!} \frac{x}{\log x}, \tag{5.1.14}$$

where

$$F(z) = \frac{1}{\Gamma(z+1)} \prod_p \left(1 - \frac{1}{p}\right)^z \left(1 - \frac{z}{p}\right)^{-1} \qquad (|z| < 2).$$

This beautiful result then was further extended by Selberg [24] when k is a little larger and varies uniformly in a slightly wider range $(2+\varepsilon)\log\log x \leqslant k \leqslant B^*\log\log x$, where $B^* > 2$ is a real constant. In his paper Selberg only discussed the main ideas behind the proof. He observed a significant change in the asymptotic behaviour of $\Pi(x,k)$. He showed for this range we have

$$\Pi(x,k) \sim \frac{Cx\log(x/2^k)}{2^k}, \tag{5.1.15}$$

where C is an absolute constant.

The main ingredient of the attack of their method was to analyze the following sums

$$\sum_{n \leqslant x} z^{\omega(n)} \text{ and } \sum_{n \leqslant x} z^{\Omega(n)}$$

and then identifying the $\pi(x,k)$ and $\Pi(x,k)$ as the coefficient of z^k in those expressions, in the case of $\omega(n)$ and $\Omega(n)$ respectively. Therefore Cauchy's integral formula can be used to extract information about these coefficients. We do not discuss the Sathe-Selberg method over integers here, but we will provide a detailed sketch of this method in the function field setting and demonstrate two applications in the next chapter.

Finally Nicolas [19] settled this question for the entire range $(2+\varepsilon)\log\log x \leqslant k < \log x/\log 2$ by proving the same asymptotic result holds as (5.1.15) in this range. Unlike the previous attempts his main idea behind the proof was less analytic and more of combinatorial nature.

5.2 The functions $\pi_q(x,k)$ and $\Pi_q(n,k)$

The goal of this is section is to study the analogs of $\pi(x,k)$ and $\Pi(x,k)$ over $\mathbb{F}_q[t]$. We define

$$\pi_q(n,k) := \#\Big\{ f \in \mathscr{M}_n : \omega_q(f) = \Omega_q(f) = k \Big\},$$

$$\Pi_q(n,k) := \#\Big\{ f \in \mathscr{M}_n : \Omega_q(f) = k \Big\}.$$

Even though the main focus of the thesis is to derive asymptotic estimates for $\Pi_q(n,k)$ using the Sathe-Selberg's method for polynomials, we start the discussion with a brief interlude to mention some results on $\pi_q(n,k)$ first. We first notice $\pi_q(n,k)$ is slightly different from its integer analogue $\pi(x,k)$ since we are only considering the square-free monics. We have the following analogue of the classical Hardy-Ramanujan upper bound in the function field setting described in [10].

Theorem 5.2.1 (Gomez-Colunga–Kavaler–McNew–Zhu)**.** *Uniformly for all $k,n \geqslant 1$,*

$$\pi_q(n,k) \leqslant \frac{q^n}{n}\frac{(\log n + 2 - \log 2)^{k-1}}{(k-1)!}.$$

In a fairly recent work, Afshar and Porrit [1] proved an asymptotic estimate on $\pi_q(n,k)$ using the so-called Sathe-Selberg technique for function fields.

Theorem 5.2.2 (Afshar–Porritt). *Let $A > 1$. Uniformly for all $n \geqslant 2$ and $1 \leqslant k \leqslant A \log n$,*

$$\pi_q(n,k) \sim G\left(\frac{k-1}{\log n}\right) \frac{(\log n)^{k-1}}{(k-1)!} \frac{q^n}{n},$$

where

$$G(z) = \frac{1}{\Gamma(z+1)} \prod_{p \in \mathscr{P}} \left(1 + \frac{z}{q^{deg(p)}}\right) \left(1 - \frac{1}{q^{deg(p)}}\right)^z.$$

In the above result authors were also able to obtain an error term. As we have already mentioned the final goal of this thesis is to prove asymptotic estimates on the object $\Pi_q(n,k)$. Our main weapon to resolve this problem will be the Sathe-Selberg device developed in the context of polynomials in [20].

5.2.1 Review of notations

We remind the reader

$$\mathscr{M} := \left\{\text{set of all monics in } \mathbb{F}_q[T]\right\},$$

$$\widetilde{\mathscr{M}} := \left\{\text{set of all monics in } \mathbb{F}_q[T] \text{ having no root in } \mathbb{F}_q\right\},$$

$$\mathscr{P} := \left\{\text{set of all monic irreducibles in } \mathbb{F}_q[T]\right\}.$$

$\mathscr{M}_n$ consists of only those monics that have degree $= n$ and similarly we define $\widetilde{\mathscr{M}_n}$, $\mathscr{P}_n$. Let $\mathscr{P}_{\geqslant j}$ denotes the set of all monic irreducibles whose degree is at least j.

We also set

$$\Pi_q(n,k) := \#\left\{f \in \mathscr{M}_n : \Omega_q(f) = k\right\},$$

$$\Pi'_q(n,k) := \#\left\{f \in \widetilde{\mathscr{M}_n} : \Omega_q(f) = k\right\}.$$

As discussed initially, we are interested in understanding the object $\Pi_q(n,k)$ for different ranges of k. Surprisingly one of our main results reveals that the situation in $\mathbb{F}_q[t]$ is quite different than what one could naively guess from the knowledge in the integer case. This is remarkable since these two worlds are significantly different in only a few instances.

Our first result is fairly what one could speculate in light of (5.1.14). The following was proved by Warlimont [26] and also in Car [6].

Theorem 5.2.3. *Given $\varepsilon \in (0,q)$, then uniformly for $1 \leqslant k \leqslant (q-\varepsilon)\log n$ we have*

$$\Pi_q(n,k) \sim \frac{q^n}{n} H\left(\frac{k}{\log n}\right) \frac{(\log n)^{k-1}}{(k-1)!},$$

where

$$H(z) = \frac{1}{\Gamma(z+1)} \prod_{p \in \mathscr{P}} \left(1 - \frac{1}{q^{deg(p)}}\right)^z \left(1 - \frac{z}{q^{deg(p)}}\right)^{-1}$$

for $|z| < q$.

We may notice that the expression for the function H is quite similar to F in the integer case. The appearance of q^n/n is also no surprise as letting $q^n \approx x$ yields $q^n/n \approx x/\log x$ up to constant factors. The above theorem is more or less a straight forward application of the Selberg-Delange method developed in [20]. The object $\Pi_q(n,k)$ was extensively studied by Hwang [15] for the entire range $1 \leqslant k \leqslant n$. We recover the following simplified version of Hwang's asymptotic formula in a restricted range using a different set of techniques.

Theorem 5.2.4. *Let $B \geqslant 2$ be a real constant and $q > 2$ be a prime power. Let $\xi : \mathbb{N} \to \mathbb{R}$ be a function such that $\xi(n) \to \infty$ however slowly as $n \to \infty$. Then uniformly for $\xi(n)\log n \leqslant k \leqslant n/B$ we have*

$$\Pi_q(n,k) \sim C(q) \frac{q^n k^{q-1} (n-k)^{q-1}}{q^k},$$

where

$$C(q) = \frac{1}{((q-1)!)^2} \left(1 - \frac{1}{q}\right)^{q^2} \prod_{p \in \mathscr{P}_{\geqslant 2}} \left(1 - \frac{1}{q^{deg(p)-1}}\right)^{-1} \left(1 - \frac{1}{q^{deg(p)}}\right)^q,$$

an absolute constant that depends only on q.

Here "however slowly" means that $\xi(n)$ could be any function that grows to infinity with an additional constraint that ξ is sufficiently small so that the interval $[\xi(n)\log n, n/B]$ contains at least one integer for n large enough. As was expected, we remind the reader that $x/2^k$ is replaced by q^n/q^k. The appearance of $(n-k)$ is not also surprising in light of the main theorem proved in [19] and (5.1.15) where a factor of $\log\left(x/2^k\right)$ is present in the statement. However, the extra factor k^{q-1} and also the presence of higher powers of $(n-k)$ are what seem surprising at the moment, which shows $\Pi_q(n,k)$ grows at a much larger rate than what we would predict

from (5.1.15). The proofs of the above theorems are discussed in detail in the following sections.

We note Theorem 5.2.4 is valid for $q \neq 2$. Our methods do not cover the case $q = 2$ for technical reasons. We will discuss this technical restriction in the proof of Proposition 6.3.7. (See Remark 6.3.8) Also, there is a significant gap between the upper bound of k in Theorem 5.2.3 and the lower bound of k in Theorem 5.2.4. While it is fairly easy to prove an upper bound of the shape $\Pi_q(n,k) \ll q^{n-k}k^{q-1}(n-k)^{q-1}$ in the intermediate range $q\log n \leqslant k \ll \log n$ using the ideas in Proposition 6.3.7, it seems fairly difficult to obtain any non-trivial lower bound for that range. The proofs of the above theorems are discussed in detail in the following sections. The main ingredients of our proofs are the following two key propositions. The main ingredients of our proofs are the following two key propositions.

Proposition 5.2.5. *For all $\varepsilon \in (0,q)$ and uniformly for $|z| \leqslant q-\varepsilon$ we have*

$$M_n(z) := \sum_{f\in\mathscr{M}_n} z^{\Omega_q(f)} = q^n n^{z-1}\left\{ zH(z) + O_\varepsilon\left(\frac{1}{n}\right)\right\},$$

with $H(z)$ as described in Theorem 5.2.3.

Proposition 5.2.6. *For all $\delta \in (0,1)$ and uniformly for $|z| \leqslant q^2-\delta$ we have*

$$\widetilde{M_n}(z) := \sum_{f\in\widetilde{\mathscr{M}_n}} z^{\Omega_q(f)} = q^n n^{z-1}\left\{ zh(z) + O_\delta\left(\frac{1}{n}\right)\right\},$$

where $h(z) = \dfrac{1}{\Gamma(z+1)}\left(1-\dfrac{1}{q}\right)^{qz}\displaystyle\prod_{p\in\mathscr{P}_{\geqslant 2}}\left(1-\frac{z}{q^{deg(p)}}\right)^{-1}\left(1-\frac{1}{q^{deg(p)}}\right)^{z}$, an analytic function for $|z| < q^2$.

The connection between Theorem 5.2.3 and Proposition 5.2.5 becomes clear once we notice $\Pi_q(n,k)$ is precisely given by the coefficient of z^k in $M_n(z)$. In other words, if we could extract the information about $\Pi_q(n,k)$ from $M_n(z)$, we would have our result. Furthermore, we note that $M_n(z)$ is polynomial of degree at most n and therefore, we could hope to study the coefficients using Cauchy's integral formula. This is going to be our main strategy to attack Theorem 5.2.3. The connection between $\widetilde{M_n}(z)$ and Theorem 5.2.4 is not as immediate as the previous case since the coefficient of z^k in $\widetilde{M_n}(z)$ is $\Pi'_q(n,k)$ and not $\Pi_q(n,k)$. As we shall see, in Section 6.3 the two objects $\Pi_q(n,k)$ and $\Pi'_q(n,k)$ are intimately entangled, and information about one could

be transferred into another. We also note the relation $C(q) = qh(q)/(q-1)!$ holds.
In the later chapters, we will prove these claims in detail which is the main work we developed during this thesis.

CHAPTER 6

ON THE DISTRIBUTION OF POLYNOMIALS HAVING A GIVEN NUMBER OF IRREDUCIBLE FACTORS

In this chapter we present the detailed proof of every claim we made in the previous chapter about $\Pi_q(n,k)$ for different ranges of k.

6.1 Set-up and the proof of Proposition 5.2.5

6.1.1 Preparatory results for Proposition 5.2.5

In this subsection we aim to develop the framework for a Selberg-Delange type argument that will be used to establish Proposition 5.2.5. As already discussed we are interested in the quantity

$$M_z(n) := \sum_{f\in\mathscr{M}_n} z^{\Omega_q(f)} = \sum_{k\geqslant 0} z^k \Pi_q(n,k).$$

We also want to introduce an auxiliary quantity

$$G_z(u) = \sum_{f\in\mathscr{M}} z^{\Omega_q(f)} u^{deg(f)} = \prod_{p\in\mathscr{P}} \left(1 - zu^{deg(p)}\right)^{-1}. \tag{6.1.1}$$

The function $G_z(u)$ defines an analytic function since the Euler product converges absolutely for $|u| < \min\left\{|z|^{-1}, q^{-1}\right\}$ which we argue now. We have that

$$|1 - zu^{deg(p)}| \geqslant 1 - |zu^{deg(p)}| \geqslant 1 - |zu| > 0,$$

showing there is no pole in the concerned region.

We now recall a well known result from complex analysis that says for a sequence of complex numbers $\{a_n\} \subset \mathbb{C}$ with $a_n \neq -1$ if $\sum_{n=1}^{\infty} |a_n| < \infty$, then

$$\prod_{n=1}^{\infty}(1+a_n) \text{ converges.}$$

Using this result we see the product in (6.1.1) converges whenever $0 < |u| < q^{-1}$. Indeed we have

$$\begin{aligned}\sum_{p\in\mathscr{P}}\left|zu^{deg(p)}\right| &\leqslant \sum_{p\in\mathscr{P}}|u|^{deg(p)-1} \qquad (|uz|<1)\\ &\leqslant q+\sum_{p\in\mathscr{P}_{\geqslant 2}}|u|^{deg(p)-1}\\ &\leqslant q+\sum_{n=2}^{\infty}q^n|u|^{n-1} \qquad (\text{ since } \#\mathscr{P}_n\leqslant q^n)\\ &\leqslant q+\frac{1}{|u|}\sum_{n=2}^{\infty}|qu|^n<\infty. \qquad (|qu|<1)\end{aligned}$$

Our job is to understand $M_z(n)$, which is precisely given by the coefficient of u^n in the power series of $G_z(u)$. Hence information about $M_z(n)$ can be obtained from $G_z(u)$ by applying Cauchy's integral formula. We took this leap from $M_z(n)$ to G_z because it seems to have a nicer arithmetic structure (i.e. an Euler product expansion), making it more amenable from the analytic point of view. Therefore it is natural to seek to meromorphically extend $G_z(u)$ beyond the region of absolute convergence discussed above to collect the contribution coming from the singularity of G_z in the extended domain. We do this job by introducing another function $F_z(u)$ via the Euler product

$$F_z(u)=\prod_{p\in\mathscr{P}}\left(1-zu^{deg(p)}\right)^{-1}\left(1-u^{deg(p)}\right)^{z}. \tag{6.1.2}$$

We intend to analyze the above Euler product in the following open region and show it is holomorphic.

$$\mathscr{R}:=\left\{(u,z)\in\mathbb{C}^2:|z|<q,|u|<|z|^{-1},|u|<q^{-1/2}\right\}\subset\mathbb{C}^2.$$

The following lemma shows $F_z(u)$ does converge absolutely in $\mathscr{R}$ which is what we wanted to establish.

Lemma 6.1.1. *We have that $F_z(u)$ defined in (6.1.2) is holomorphic in $\mathscr{R}$.*

Proof. We take the standard branch of complex logarithm defined over $\mathbb{C}\setminus(-\infty,0]$. Since

$|u|^n, |zu^n| < 1$ we could make use of their Taylor series and write for $|z| < q$,

$$\begin{aligned} z\log(1-u^n) - \log(1-zu^n) &= -zu^n + O\left(\left|zu^{2n}\right|\right) + zu^n + O\left(\left|z^2u^{2n}\right|\right) \\ &= O\left(\left|q^2u^{2n}\right|\right) \qquad \left(|u| < |z|^{-1} \text{ and } |u| < q^{-1/2}\right) \end{aligned} \tag{6.1.3}$$

and hence using $\exp(O(x)) = 1 + O(x)$ for $x = O(1)$ we get

$$(1-u^n)^z(1-zu^n)^{-1} = 1 + O\left(\left|q^2u^{2n}\right|\right).$$

We now observe the product in (6.1.2) converges absolutely in $\mathscr{R}$. Since $\#\mathscr{P}_n \leqslant q^n$, we have that

$$\sum_{p\in\mathscr{P}} |u|^{2n} \leqslant \sum_{n\geqslant 1} |qu^2|^n < \infty.$$

□

We recall the Riemann zeta function in the context of polynomials over finite field, defined for $|u| < q^{-1}$

$$\zeta(u) = \frac{1}{1-qu} = \prod_{p\in\mathscr{P}} \left(1-u^{deg(p)}\right)^{-1}.$$

As we can see $\zeta(u)$ can be continued mermorphically on $\mathbb{C}$ with a simple pole at $u = 1/q$. Furthermore considering the Euler products in (6.1.1) and (6.1.2) we can connect $G_z(u)$ and $F_z(u)$ in the following way whenever $|u| < \min\left\{|z|^{-1}, q^{-\frac{1}{2}}\right\}$

$$G_z(u) = \zeta(u)^z F_z(u). \tag{6.1.4}$$

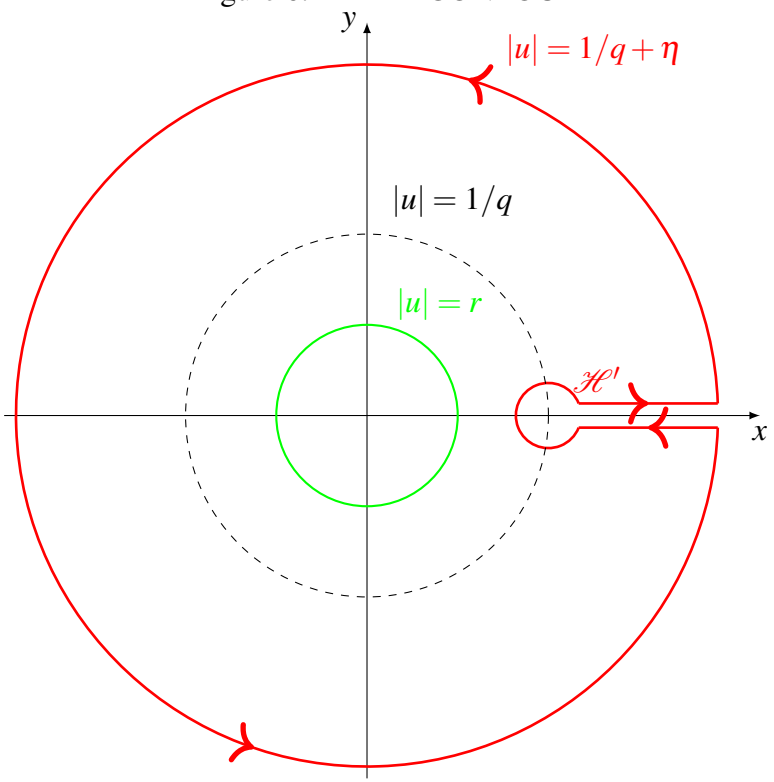
We are now in a position to prove our first Proposition. However, first, we want to record the following estimate [20], which is going to be helpful in the further calculation of the contribution that comes from the singularity of $G_z(u)$ at $u = 1/q$.

Lemma 6.1.2. *Let $A, \delta > 0$. Let $\mathscr{H}$ be the Hankel contour of radius 1 around 0 going in clockwise direction along the negative real axis to $-n\delta$. Then uniformly for $|z| \leqslant A$ we have*

that

$$\frac{1}{2\pi i}\int_{\mathscr{H}} w^z \frac{dw}{\left(1-\frac{w}{n}\right)^{n+1}} = -\frac{1}{\Gamma(-z)} + O_{\delta,A}\left(\frac{1}{n}\right).$$

Figure 6.1 – THE CONTOUR



6.1.2 Deduction of Proposition 5.2.5

Proof of Proposition 5.2.5. Let $|u| = r < q^{-1}$ (small green circle in Fig-6.1 above). Using Cauchy's integral formula on (6.1.1) we get for each fixed z satisfying the hypothesis $|z| \leqslant q-\varepsilon$,

$$M_z(n) = \frac{1}{2\pi i}\int\limits_{|u|=r} G_z(u)\frac{du}{u^{n+1}} = \frac{1}{2\pi i}\int\limits_{|u|=r} \zeta(u)^z F_z(u)\frac{du}{u^{n+1}}. \tag{6.1.5}$$

We wish to get past the point $u = 1/q$ so that we could collect the contribution coming from the singularity of $\zeta(u)$ there. We shift the smaller (green) circle $|u| = r$ to a bigger circle (red) $|u| = q^{-1}+\eta$ and a portion of Hankel contour around the point q^{-1} (Fig-6.1). Let $\mathscr{H}'$ be the contour that consists of a circle of radius $(qn)^{-1}$ traversed clockwise around q^{-1} and the two line segments on the ray 0 to q^{-1} joining this small circle to the bigger circle $|u| = q^{-1}+\eta$

where $\eta > 0$ is a fixed number. (to be specified shortly) However we must have $q^{-1}+\eta < q^{-\frac{1}{2}}$ as we cannot go beyond the region $\mathscr{R}$ in (6.1.4) where $G_z(u)$ makes sense. We recall that $|z| \leqslant (q-\varepsilon)$ inside $\mathscr{R}$ while performing the above integral. Keeping this in mind we get another constraint on η, $|uz| \leqslant (q^{-1}+\eta)(q-\varepsilon) \leqslant 1$. This shows taking any $0 < \eta < \min\{1/(q-\varepsilon) - 1/q, 1/\sqrt{q} - 1/q\}$ suffices. We then plan to use Lemma 6.1.2 to evaluate the integral in (6.1.5) with $\eta = \min\{1/(q-\varepsilon) - 1/q, 1/\sqrt{q} - 1/q\}/2$ for $|z| \leqslant q-\varepsilon$. We observe that for z fixed, $F_z(u)$ and $\zeta(u)$ are both analytic in an open neighbourhood containing the circle $|u| = q^{-1}+\eta$ which is compact. This implies $F_z(u), \zeta(u)$ and hence $G_z(u)$ are uniformly bounded (bound depends on q, η) on this circle. Thus we obtain

$$M_z(n) = \frac{1}{2\pi i}\int\limits_{\mathscr{H}'} G_z(u)\frac{du}{u^{n+1}} + O\left(\int\limits_{|u|=\frac{1}{q}+\eta}\left|G_z(u)\frac{du}{u^{n+1}}\right|\right) := I + O_{q,\varepsilon}\left(\frac{q^n}{(1+q\eta)^n}\right).$$

where at the last step we used the fact that, $\int_{|u|=R}|du/u^{n+1}| = \frac{1}{R^{n+1}}\int_{|u|=R}|du| = 2\pi/R^n$ and the big-O-uniform bound here depends only on q, η and η according our choice depends only on q and ε. Now we focus on the integral I.

Analyticity of F_z near q^{-1} allows us to consider the Taylor series around q^{-1} and write

$$F_z(u) = F_z(1/q) + a_1(u-1/q) + a_2(u-1/q)^2 + \dots$$

Hence we have that,

$$I = F_z\left(\frac{1}{q}\right)\frac{1}{2\pi i}\int_{\mathscr{H}'}\zeta(u)^z\frac{du}{u^{n+1}} + O\left(\int_{\mathscr{H}'}\left|\left(u-\frac{1}{q}\right)\zeta(u)^z\frac{du}{u^{n+1}}\right|\right).$$

We use a change of variable so that our contour $\mathscr{H}'$ transforms to $\mathscr{H}$ and we could then use our Lemma 6.1.2. The change of variable is given by, $w = n(1-uq) \implies u = 1/q\,(1-w/n)$. We can quickly check the transformation is indeed a valid one. If u is parameterized by $u = 1/q + (1/qn)e^{-it}, t \in [\varepsilon', 2\pi-\varepsilon']$ for some small enough $\varepsilon' > 0$ near the tiny circle around $1/q$ then $w = -e^{-it}$ is a circle revolving around 0 of radius 1 in the clockwise direction and similarly the horizontal ray part also gets reflected and $\mathscr{H}'$ indeed transforms into $\mathscr{H}$ and as $|u|$ goes up to $1/q+\eta$, we have w goes up to $-n\delta$ with $\delta = \eta q$. We note for this change of variable

$du = -dw/nq$. First we show the alleged error term is small. The O-term is

$$\begin{aligned}
\ll_q \int_{\mathscr{H}'} \left| \frac{(1-qu)du}{u^{n+1}(1-qu)^z} \right| &= \int_{\mathscr{H}} \left| \frac{1}{\left(\frac{w}{n}\right)^{z-1}} \frac{\frac{-dw}{nq}}{\frac{1}{q^{n+1}}\left(1-\frac{w}{n}\right)^{n+1}} \right| \\
&= \frac{q^n}{n} \int_{\mathscr{H}} \left| \frac{1}{\left(\frac{w}{n}\right)^{z-1}} \frac{dw}{\left(1-\frac{w}{n}\right)^{n+1}} \right| \qquad \text{(using Lemma 6.1.2)} \\
&\ll q^n n^{\Re(z)-2}.
\end{aligned}$$

Now, we evaluate the main term using Lemma 6.1.2

$$\begin{aligned}
F_z\left(\frac{1}{q}\right) \frac{1}{2\pi i} \int_{\mathscr{H}'} \zeta(u)^z \frac{du}{u^{n+1}} &= F_z\left(\frac{1}{q}\right) \frac{1}{2\pi i} \int_{\mathscr{H}'} \frac{1}{(1-qu)^z} \frac{du}{u^{n+1}} \\
&= F_z\left(\frac{1}{q}\right) \frac{q^n}{n} \frac{1}{2\pi i} \int_{\mathscr{H}} \frac{1}{\left(\frac{w}{n}\right)^z} \frac{-dw}{\left(1-\frac{w}{n}\right)^{n+1}} \\
&= F_z\left(\frac{1}{q}\right) q^n n^{z-1} \left(\frac{1}{\Gamma(z)} + O_\varepsilon\left(\frac{1}{n}\right) \right).
\end{aligned}$$

Hence we have that

$$M_z(n) = F_z\left(\frac{1}{q}\right) \frac{q^n n^{z-1}}{\Gamma(z)} + O\left(q^n n^{\Re(z)-2}\right) = q^n n^{z-1} \left\{ zH(z) + O_\varepsilon\left(\frac{1}{n}\right) \right\}, \tag{6.1.6}$$

where $H(z) = \frac{1}{\Gamma(z+1)} F_z\left(\frac{1}{q}\right)$ is an analytic function for $|z| < q$. □

6.2 Deduction of Theorem 5.2.3

With Proposition 5.2.5 at our disposal, we are now ready to prove Theorem 5.2.3. We also note three other straightforward results which will help us do so. We will verify the following claims in the appendix I.

Lemma 6.2.1. *For $t \in [-\pi, \pi]$ we have $\cos t - 1 \leqslant -\frac{t^2}{5}$ and $\left|1 - e^{it}\right|^2 \leqslant t^2$.*

Lemma 6.2.2. *We have the following upper bound*

$$\int_{|z|=r} \left| n^{z-r} \right| |dz| \ll \frac{r}{\sqrt{j}},$$

where $j = r\log n$.

Lemma 6.2.3. *We have the following estimate*

$$\int_{-\infty}^{\infty} \theta^2 \exp\left(-\frac{k\theta^2}{5}\right) d\theta \ll k^{-\frac{3}{2}}.$$

Deduction of Theorem 5.2.3. We plan to recover $\Pi_q(n,k)$ with another application of Cauchy's integral formula,

$$\Pi_q(n,k) = \frac{1}{2\pi i} \int_{|z|=\frac{k}{\log n}} M_z(n) \frac{dz}{z^{k+1}}. \tag{6.2.1}$$

Given $\varepsilon \in (0,q)$ by the hypothesis of Theorem 5.2.3, from (6.1.6) we see the main term of $M_z(n)$ which is $F_z\left(\frac{1}{q}\right)\frac{q^n n^{z-1}}{\Gamma(z)}$ is analytic in the disk $|z| = r = k/\log n \leqslant (q-\varepsilon)$ since $F_z\left(\frac{1}{q}\right)$ is analytic for $|z| < q$ and $n^z, 1/\Gamma$ are entire functions. Now writing $M_z(n)/q^n = n^{z-1}\left(f(z) + O\left(1/n\right)\right)$ where $f(z) = zH(z) = F_z(1/q)\frac{1}{\Gamma(z)}$ and considering the Taylor expansion of $f(z)$ near $z = r$, $f(z) = f(r) + f'(r)(z-r) + O(|z-r|^2)$ we get

$$\frac{1}{q^n}\Pi_q(n,k) = \frac{1}{2\pi i}\int_{|z|=r} n^{z-1} f(z)\frac{dz}{z^{k+1}} + O(E), \tag{6.2.2}$$

where E is given by $\frac{1}{n}\int_{|z|=r}\left|\frac{n^{z-1}}{z^{k+1}}\right||dz|$. We see that

$$\frac{1}{2\pi i}\int_{|z|=r}(z-r)n^{z-1}\frac{dz}{z^{k+1}} = \frac{1}{n}\left\{\frac{(\log n)^{k-1}}{(k-1)!} - r\frac{(\log n)^k}{k!}\right\} = 0.$$

Hence

$$\begin{aligned}\frac{1}{q^n}\Pi_q(n,k) &= f(r)\frac{1}{2\pi i}\int_{|z|=r} n^{z-1}\frac{dz}{z^{k+1}} + O\left(r^{-k-1}\int_{|z|=r}|n^{z-1}(z-r)^2||dz| + E\right)\\ &= f(r)\frac{(\log n)^k}{k!n} + \text{Error term}.\end{aligned}$$

Here using Lemma 6.2.1 and Lemma 6.2.3 the integral in the Error term is bounded by

$$\frac{r^3}{n}\int_{-\pi}^{\pi}|1-e^{i\theta}|^2 e^{k\cos\theta}d\theta \ll \frac{r^3}{n}\int_{-\infty}^{\infty}\theta^2 e^{k(1-\frac{\theta^2}{5})}d\theta \ll \frac{r^3}{n}e^k k^{-\frac{3}{2}}.$$

Since there is a factor of r^{-k-1} outside, we have the above expression (final step by Stirling's formula)

$$\ll \frac{1}{n} r^{2-k} e^k k^{-\frac{3}{2}} \ll (\log n)^{k-2} \frac{e^k \sqrt{k}}{nk^k} \ll \frac{1}{n} \frac{(\log n)^{k-2}}{(k-1)!}.$$

Noting $e^k = n^r \iff k = r \log n$ and using Lemma 6.2.2, we also see the term E is bounded by

$$\ll \frac{r^{-k-1} e^k}{n^2} \int_{|z|=r} |n^{z-r}||dz| \ll \frac{r^{-k-1} e^k}{n^2} \left(\frac{r}{\sqrt{k}}\right) \ll \frac{1}{n^2} \frac{(e \log n)^k}{k^{k+\frac{1}{2}}} \ll \frac{1}{n^2} \frac{(\log n)^k}{k!},$$

where in the last step we have used Stirling. Thus we finally obtain

$$\Pi_q(n,k) \sim q^n f(r) \frac{(\log n)^k}{k! n} = \frac{q^n}{n} F_r\left(\frac{1}{q}\right) \frac{1}{\Gamma(r+1)} \frac{(\log n)^{k-1}}{(k-1)!}$$

and the proof follows once we recall $r = k/\log n$. The derived expression is identical to the integer case for $k \leqslant (2-\varepsilon)\log\log x$ as mentioned in [19] on the first page, a result due to Sathe(1953) [23].

□

6.3 Preparatory results and an odd-even decomposition

6.3.1 An odd-even decomposition for polynomials

We begin this subsection by introducing a decomposition for $\Pi(x,k)$ into k smaller parts used by Nicolas [19] to prove (5.1.15). We first note that any integer $n \leqslant x$ can be uniquely written as $n = 2^j \ell$ with ℓ odd. We note the following identity

$$\Pi(x,k) = \sum_{0 \leqslant j \leqslant k} \Pi'(x/2^{k-j}, j), \tag{6.3.1}$$

where

$$\Pi'(x,k) := \#\left\{ m \leqslant x : \ m \text{ odd and } \Omega_q(m) = k \right\}$$

holds. The key idea discussed in [19] says the major contribution in the former sum comes if we restrict $0 \leqslant j \leqslant \alpha \log\log x$ for some explicit constant $\alpha > 2$ whenever k ranges from $2\log\log x$ to $\log x/\log 2$.

Inspired from the idea above we wish to write $f = hg$ for any $f \in \mathscr{M}_n$, where the polynomials g and h are expected to play the role of "odd" and "even" respectively in some appropriate sense.

Let us define the set

$$\mathscr{S}(j) := \Big\{ h \in \mathscr{M}_j : h \text{ has only degree 1 irreducible factors } \Big\}.$$

Given $f \in \mathscr{M}_n$ with $\Omega_q(f) = k$, we can uniquely write $f = hg$ where $h \in \mathscr{S}(j)$ for some $0 \leqslant j \leqslant k$ and g has no degree 1 irreducible factor. Elements of the set $\mathscr{S}(j)$ mimic the even part while the odd part is mimicked by the polynomial g. Using this heuristic we could prove the following decomposition result for $\Pi_q(n,k)$.

Lemma 6.3.1. *We have*

$$\Pi_q(n,k) = \sum_{1 \leqslant j \leqslant k} \binom{k-j+q-1}{q-1} \Pi'_q(n+j-k, j)$$

for $k \geqslant 1$.

Proof. We observe that for any $h \in \mathscr{S}(j)$, one can find non negative integers $a_1, a_2, \ldots, a_q$ such that $h(t) = (t-\alpha_1)^{a_1}(t-\alpha_2)^{a_2}\ldots(t-\alpha_q)^{a_q}$ with $\Omega_q(h) = a_1 + a_2 + \ldots + a_q = j$. Here $\{\alpha_i\}_{1 \leqslant i \leqslant q}$ are the q-elements in $\mathbb{F}_q$. Counting the number of non negative integral solutions we readily see that, $\#\mathscr{S}(j) = \binom{j+q-1}{q-1}$. If we consider the unique decomposition $f = hg$ for some $f \in \mathscr{M}_n$ with $\Omega_q(f) = k$ then we note that $j \neq k$. For if $j = k$ then $f = hg$ will imply $f = h$ and hence they both have the same degree, a contradiction since $k \leqslant n/2$ by the hypothesis of Theorem 5.2.4. Therefore we obtain

$$\Pi_q(n,k) = \sum_{0 \leqslant j \leqslant k-1} \sum_{h \in \mathscr{S}(j)} \Pi'_q(n-j, k-j) = \sum_{0 \leqslant j \leqslant k-1} \binom{j+q-1}{q-1} \Pi'_q(n-j, k-j).$$

The statement of the lemma follows after we make the change of variable $j \mapsto k-j$. □

The rough sketch of our strategy to prove the Theorem 5.2.4 is: (a) In light of the approach discussed in (6.3.1) in the integer setting, we start by splitting the whole sum in the above decomposition up to $j \ll \log(n-k)$ and hence we end up with two parts so that we can write, $T_1 = \sum_{1 \leqslant j \ll \log(n-k)} \binom{k-j+q-1}{q-1} \Pi'_q(n+j-k, j)$ and $T_2 = \sum_{\log(n-k) \ll j \leqslant k} \binom{k-j+q-1}{q-1} \Pi'_q(n+j-k, j)$.

(b) We then show the main contribution comes from T_1 and is of order $q^{n-k}k^{q-1}(n-k)^{q-1}$ while the term T_2 is significantly smaller and is of order $q^{n-k}(n-k)^{q-2}$. Unlike the ideas dis-

cussed in the integer case, which is very combinatorial, our proof will be more analytical. The central idea to use a Selberg-Delange type argument followed by an application of residue theorem shall remain the same. The situation over $\mathbb{F}_q[t]$ is quite different due to the presence of many degree 1 irreducibles which is why an extra binomial term and other technical difficulties arise.

We begin our preparation with the easier task, a non-trivial upper bound on T_2. To do so, we would like an upper bound on each summand of T_2. The following result accomplishes this job.

Lemma 6.3.2. *Let $0 < \delta < 1, 0 < \eta \leqslant q^2 - q - \delta$ be given. We have the following upper bound*

$$\Pi'_q(n,j) \ll_\delta q^n n^{q+\eta-1} \left(\frac{1}{q+\eta}\right)^j.$$

Throughout our discussion, the implied constant solely depends on q, δ, which will be a fixed quantity. (the value of δ is soon to be decided in the following result) It is possible to show the above result as a direct application Proposition 5.2.6. The proof of Proposition 5.2.6 will roughly be in the same spirit as that of Proposition 5.2.5. We will present this proof followed by an argument leading to Lemma 6.3.2 in the section 6.4.1, 6.4.2. We now shift our attention to check that the term T_2 is small as claimed.

Proposition 6.3.3. *Let $q > 2$ be an integer and $Y = \log(n-k)$. We have the following upper bound*

$$T_2 = \sum_{eqY < j \leqslant k} \binom{q-1+k-j}{q-1} \Pi'_q(n+j-k, j) \ll_B q^{n-k}(n-k)^{q-2}.$$

Proof. We plan to use $\binom{\alpha}{\beta} \leqslant \alpha^\beta/\beta!$. We apply Lemma 6.3.2 with $\eta = (e-1)q$ and $\delta = 0.6$ so that $(q+\eta) = eq$. First we check this choice satisfies the hypothesis of Lemma 6.3.2. We see that $(e-1)q < q^2 - q - 0.6$ is true whenever $q \geqslant 3$. We now have that

$$\begin{aligned}
T_2 &\ll \sum_{j > (q+\eta)Y} \frac{(q-1+k-j)^{q-1}}{(q-1)!} q^{n-k+j}(n+j-k)^{q+\eta-1} \left(\frac{1}{q+\eta}\right)^j \\
&\ll q^{n-k} \sum_{j > (q+\eta)Y} (q-1+k-j)^{q-1}(n+j-k)^{q+\eta-1} \left(\frac{q}{q+\eta}\right)^j \\
&= q^{n-k} \sum_{j > eqY} (n-k)^{q-1} \left(\frac{q-1}{n-k} + \frac{k-j}{n-k}\right)^{q-1} (n-k)^{q+\eta-1} \left(1 + \frac{j}{n-k}\right)^{q+\eta-1} e^{-j}.
\end{aligned}$$

We used $q+\eta = eq$. Since $k \leqslant n/B$ we have $\left(\frac{q-1}{n-k} + \frac{k-j}{n-k}\right)^{q-1} \leqslant \left(q-1+\frac{k}{n-k}\right)^{q-1} \leqslant \left(q-1+\frac{1}{B-1}\right)^{q-1} \ll_B 1$. Also $k+j \leqslant 2k \leqslant n$ gives $\left(1+\frac{j}{n-k}\right)^{eq-1} \ll 1$. Recalling $Y = \log(n-k)$ and continuing from the previous step we get,

$$T_2 \ll_B q^{n-k}(n-k)^{eq+q-2} \sum_{j>eqY} e^{-j} \ll_B q^{n-k}(n-k)^{eq+q-2} e^{-eqY} = q^{n-k}(n-k)^{q-2}.$$

□

We are now only left to estimate T_1 and show it dominates in the asymptotic of $\Pi_q(n,k)$. For the ease of exploration, the calculation of T_1 is broken down into three smaller sub-parts. To have a good estimate for $T_1 = \sum_{1\leqslant j\ll \log(n-k)} \binom{k-j+q-1}{q-1} \Pi'_q(n+j-k,j)$, first it is natural to want to understand the terms $\Pi'_q(n+j-k,j)$ when the range for j is restricted to $\ll \log(n-k)$. With these observations in mind we could show the following result.

Lemma 6.3.4. *Let $Y = \log(n-k)$. We have uniformly for $j \leqslant eqY$,*

$$\Pi'_q(n+j-k,j) = \frac{q^{n+j-k}}{n-k}\left\{ Q_j(Y) + O\left(\frac{(\log(n-k))^{j+1}}{j!(n-k)}\right)\right\}$$

where

$$Q_j(X) := \sum_{m+\ell=j-1} \frac{1}{m!\ell!} h^{(m)}(0) X^{\ell}.$$

If we are given the above result in our toolbox, it is then evident that we are just a few steps away from proving an estimate for T_1 once we take care of what happens with the sum when the terms $\Pi'_q(n+j-k,j)$ are twisted by appropriate binomial coefficients for different j's. However, before we proceed to do that, we would like to mention a few words about what goes into the proof of Lemma 6.3.4. The proof of the above result rests on another two fairly technical auxiliary lemmas, which we shall state next. Details of these three claims are postponed till the section 6.4.3, 6.4.4, 6.4.5 and can be skipped at the moment as they do not offer many insights into our actual goal.

Lemma 6.3.5. *We have uniformly for $j \leqslant eq\log n$,*

$$\Pi'_q(n,j) = \frac{q^n}{n}\left\{ Q_j(\log n) + O\left(\frac{(\log n)^j}{j!n}\right)\right\}.$$

Lemma 6.3.6. *Let $m \geqslant 1$ be an integer. We have the following upper bounds*

$$h^{(m)}(0)/m! \ll \left(\frac{1}{2.9q}\right)^m,$$

$$Q_j(X) \ll \frac{X^{j-1}}{(j-1)!} \text{ and } Q_j'(X) \ll \frac{X^{j-2}}{(j-2)!},$$

for $1 \leqslant j \leqslant eqX$ uniformly, where X is a parameter that tends to ∞ with n.

We can now set up the stage for proving Theorem 5.2.4. As mentioned earlier we need to have a precise estimate for the twisted binomial sum appearing in T_1. Therefore the following Proposition plays a key role in establishing Theorem 5.2.4.

Proposition 6.3.7. *Let $Y = \log(n-k)$. We have the following estimate*

$$\sum_{j \leqslant eqY} \binom{q-1+k-j}{q-1} q^j Q_j(Y) = \frac{k^{q-1} q e^{qY}}{(q-1)!} h(q)\Big\{1+o(1)\Big\}.$$

Proof. We start with an observation first. By the hypothesis of Theorem 5.2.4 we have $k > \xi(n)\log n$ yielding $k-j \geqslant \xi(n)\log n - eq\log(n-k) \geqslant (\xi(n)-eq)\log n \to \infty$. Therefore using the standard fact $\binom{\alpha}{\beta} = (1+o(1))\frac{\alpha^\beta}{\beta!}$ where β is assumed to be fixed and $\alpha \to \infty$ we obtain

$$\begin{aligned}\sum_{j \leqslant eqY} \binom{q-1+k-j}{q-1} q^j Q_j(Y) &= \frac{1}{(q-1)!} \sum_{j \leqslant eqY} \Big\{q^j (q-1+k-j)^{q-1} Q_j(Y)\Big\}(1+o(1)) \\ &= \frac{k^{q-1}}{(q-1)!} \sum_{j \leqslant eqY} \Big\{q^j Q_j(Y)\Big\}(1+o(1)),\end{aligned}$$

where we used the the Taylor expansion of $(k+q-j-1)^{q-1} = k^{q-1}(1+o(1))$ since $j = o(k)$.

We now evaluate the sum

$$\begin{aligned}\sum_{j\leqslant eqY} q^j Q_j(Y) &= \left(\sum_{j\geqslant 1} q^j \sum_{\substack{m+\ell=j-1\\ m,\ell\geqslant 0}} \frac{h^m(0)}{m!\ell!}Y^\ell\right) - R\\ &= \left(q\sum_{\ell\geqslant 0}\frac{(qY)^\ell}{\ell!}\sum_{j-m=\ell+1}\frac{h^m(0)}{m!}q^{j-\ell-1}\right) - R \qquad \text{(after interchanging the sum)}\\ &= \left(q\sum_{\ell\geqslant 0}\frac{(qY)^\ell}{\ell!}\sum_{m\geqslant 0}\frac{h^m(0)}{m!}q^m\right) - R \qquad \text{(since } m=j-\ell-1 \text{ and } j\geqslant \ell+1)\\ &= qe^{qY}h(q) - R, \qquad (h(z) \text{ is analytic for } |z|<q^2)\end{aligned}$$

where

$$\begin{aligned}R &= \sum_{j>\lfloor eqY\rfloor} q^j Q_j(Y) \quad (\text{where } \lfloor x\rfloor \text{ denotes the greatest integer } \leqslant x)\\ &= \sum_{j\geqslant\lfloor eqY\rfloor+1} q^j \sum_{\substack{m+\ell=j-1\\ m,\ell\geqslant 0}} \frac{h^m(0)}{m!\ell!}Y^\ell\\ &= q\left(\sum_{0\leqslant\ell\leqslant\lfloor eqY\rfloor}\frac{(qY)^\ell}{\ell!}\sum_{m\geqslant\lfloor eqY\rfloor-\ell}\frac{h^m(0)}{m!}q^m\right) + q\left(\sum_{\ell\geqslant\lfloor eqY\rfloor}\frac{(qY)^\ell}{\ell!}\sum_{m\geqslant 0}\frac{h^m(0)}{m!}q^m\right)\\ &\ll_q S_1 + S_2. \quad (\text{say})\end{aligned}$$

We have the following estimates,

$$\begin{aligned}S_1 &\leqslant \sum_{0\leqslant\ell\leqslant\lfloor eqY\rfloor}\frac{(qY)^\ell}{\ell!}\sum_{m\geqslant\lfloor eqY\rfloor-\ell}\left(\frac{1}{2}\right)^m \quad \left(\text{using } h^{(m)}(0)/m! < (1/2q)^m \text{ from Lemma 6.3.6}\right)\\ &= \sum_{0\leqslant\ell\leqslant\lfloor eqY\rfloor}\frac{(qY)^\ell}{\ell!}\left(\frac{1}{2}\right)^{\lfloor eqY\rfloor-\ell}\\ &= \left(\frac{1}{2}\right)^{\lfloor eqY\rfloor}\sum_{0\leqslant\ell\leqslant\lfloor eqY\rfloor}\frac{(2qY)^\ell}{\ell!}\\ &\leqslant e^{0.12qY}. \quad \left(\text{since } \left(\frac{1}{2}\right)^{\lfloor eqY\rfloor} = e^{-1.88qY} \text{ and the rest is bounded by the complete sum } e^{2qY}\right)\end{aligned}$$

Similarly

$$\begin{aligned}
S_2 &= h(q) \sum_{\ell \geqslant \lfloor eqY \rfloor} \frac{(qY)^\ell}{\ell!} \\
&\ll (qY)^{\lfloor eqY \rfloor} \sum_{\ell \geqslant 0} \frac{(qY)^\ell}{(\ell + \lfloor eqY \rfloor)!} \quad \text{(dropping } h(q) \text{and using a change of variable } \ell \mapsto \ell - \lfloor eqY \rfloor) \\
&\leqslant \frac{(qY)^{\lfloor eqY \rfloor}}{\lfloor eqY \rfloor!} \sum_{\ell \geqslant 0} \frac{(qY)^\ell}{\ell!} \left(\text{since } \binom{\ell + \lfloor eqY \rfloor}{\ell} \geqslant 1 \text{ so that } \frac{1}{(\ell + \lfloor eqY \rfloor)!} \leqslant \frac{1}{\ell! \lfloor eqY \rfloor!} \right) \\
&\ll \frac{1}{\sqrt{\lfloor eqY \rfloor}} e^{qY},
\end{aligned}$$

where at the last step we used Stirling. Indeed letting $p = eqY$, we have

$$\frac{(qY)^{\lfloor eqY \rfloor}}{\lfloor eqY \rfloor!} \ll \frac{\left(\frac{p}{e}\right)^{\lfloor p \rfloor}}{\left(\frac{\lfloor p \rfloor}{e}\right)^{\lfloor p \rfloor} \sqrt{\lfloor p \rfloor}} = \left(\frac{p}{\lfloor p \rfloor}\right)^{\lfloor p \rfloor} \frac{1}{\sqrt{\lfloor p \rfloor}} \leqslant \left(1 + \frac{1}{\lfloor p \rfloor}\right)^{\lfloor p \rfloor} \frac{1}{\sqrt{\lfloor p \rfloor}} \leqslant \frac{e}{\sqrt{\lfloor p \rfloor}}.$$

□

Remark 6.3.8. *In the hypothesis of the above proposition, the factor e in the parameter eqY was chosen carefully. The final application of Stirling will not work if we choose a factor strictly smaller than e. This choice induces a restriction in the hypothesis of the Lemma 6.3.5. The proof of Lemma 6.4.3 crucially uses the technical condition $q > e$. This is why our methods do not cover the case $q = 2$.*

Proof of Theorem 5.2.4. We have that

$$\begin{aligned}
\Pi_q(n,k) &= \sum_{1 \leqslant j \leqslant eqY} \binom{k-j+q-1}{q-1} \Pi'_q(n+j-k, j) + \sum_{j > eqY} \binom{k-j+q-1}{q-1} \Pi'_q(n+j-k, j) \\
&= T_1 + T_2.
\end{aligned}$$

Proposition 6.3.3 shows the tail T_2 is small and is $\ll q^{n-k}(n-k)^{q-2}$.

Lemma 6.3.4 and Proposition 6.3.7 implies,

$$\begin{aligned}
T_1 &= \sum_{j\leqslant eqY}\binom{k-j+q-1}{q-1}\frac{q^{n+j-k}}{n-k}Q_j(Y)+O\left(\sum_{j\leqslant eqY}\binom{k-j+q-1}{q-1}\frac{(\log(n-k))^{j+1}}{j!(n-k)}\right)\\
&= \frac{q^{n-k}}{n-k}\sum_{j\leqslant eqY}\binom{k-j+q-1}{q-1}q^jQ_j(Y)+O\left(\sum_{j\leqslant eqY}\binom{k-j+q-1}{q-1}\frac{(\log(n-k))^{j+1}}{j!(n-k)}\right)\\
&= \frac{q^{n-k+1}k^{q-1}e^{qY}}{(q-1)!(n-k)}h(q)\Big\{1+o(1)\Big\}+O\left((1+o(1))\frac{k^{q-1}}{(q-1)!}\sum_{j=1}^{\infty}\frac{(\log(n-k))^{j+1}}{j!(n-k)}\right)\\
&= \frac{q^{n-k+1}k^{q-1}e^{qY}}{(q-1)!(n-k)}h(q)\Big\{1+o(1)\Big\}+O\left(k^{q-1}\frac{\log(n-k)e^{\log(n-k)}}{n-k}\right)\\
&= \frac{q^{n-k+1}k^{q-1}e^{qY}}{(q-1)!(n-k)}h(q)\Big\{1+o(1)\Big\}+O\left(k^{q-1}\log(n-k)\right).
\end{aligned}$$

Thus we obtain

$$T_1 \sim \frac{q^{n-k}k^{q-1}e^{qY}}{(n-k)}\frac{qh(q)}{(q-1)!}\sim C(q)\frac{q^nk^{q-1}(n-k)^{q-1}}{q^k},$$

where we used $e^{qY}/(n-k)=(n-k)^{q-1}$ when $Y=\log(n-k)$ and

$$C(q)=\frac{qh(q)}{(q-1)!}=\frac{1}{((q-1)!)^2}\left(1-\frac{1}{q}\right)^{q^2}\prod_{p\in\mathscr{P}_{\geqslant 2}}\left(1-\frac{1}{q^{deg(p)-1}}\right)^{-1}\left(1-\frac{1}{q^{deg(p)}}\right)^{q},$$

an absolute constant that only depends on q. □

6.4 Towards Proposition 5.2.6 and auxiliary results for theorem 5.2.4

6.4.1 A Selberg-Delange style argument for $\widetilde{M_z}(n)$

Proof of Proposition 5.2.6. We recall some definitions for convenience,

$$\widetilde{\mathscr{M}} := \Big\{\textit{set of all monics in } \mathbb{F}_q[T] \textit{ having no root in } \mathbb{F}_q\Big\},$$

$$\widetilde{\mathscr{M}_n} := \Big\{\textit{set of all of degree } n \textit{ monics in } \mathbb{F}_q[T] \textit{ having no root in } \mathbb{F}_q\Big\},$$

$$\Pi'_q(n,k) := \#\Big\{f\in\widetilde{\mathscr{M}_n} : \Omega_q(f)=k\Big\}.$$

We proceed as the proof of Theorem 5.2.3 by first defining the following quantities,

$$\widetilde{M}_z(n) = \sum_{f \in \widetilde{\mathscr{M}_n}} z^{\Omega_q(f)} = \sum_{k \geqslant 0} z^k \Pi'_q(n,k) \text{ and } \widetilde{G}_z(u) = \sum_{f \in \widetilde{\mathscr{M}}} z^{\Omega_q(f)} u^{deg(f)}.$$

Our Euler product decomposition for $\widetilde{G}_z(u)$ now becomes

$$\widetilde{G_z}(u) = \prod_{p \in \mathscr{P}_{\geqslant 2}} \left(1 - zu^{deg(p)}\right)^{-1}.$$

Following the same spirit we now have

$$\widetilde{G}_z(u) = \zeta(u)^z \widetilde{F}_z(u),$$

where $\widetilde{F}_z$ is given by the Euler product below

$$\widetilde{F}_z(u) = (1-u)^{qz} \prod_{p \in \mathscr{P}_{\geqslant 2}} \left(1 - zu^{deg(p)}\right)^{-1} \left(1 - u^{deg(p)}\right)^{z}.$$

We first show the above Euler product converges absolutely in the region defined by,

$$\widetilde{\mathscr{R}} := \left\{(u,z) \in \mathbb{C}^2 : |z| < q^2, |u|^2 < |z|^{-1}, |u| < q^{-1/2}\right\} \subset \mathbb{C}^2.$$

Since $|1 - zu^{deg(p)}| \geqslant 1 - |zu^{deg(p)}| \geqslant 1 - |zu^2| > 0$, we have none of the $\left(1 - zu^{deg(p)}\right)^{-1}$ factors contribute to a pole in $\widetilde{\mathscr{R}}$.

We take the standard branch of complex logarithm defined over $\mathbb{C} \setminus (-\infty, 0]$ and get for each integer $n \geqslant 2$, $\left(|u|^n < 1, |zu^n| \leqslant |zu^2| < 1\right)$

$$\begin{aligned} z\log(1-u^n) - \log(1-zu^n) &= -zu^n + O\left(\left|zu^{2n}\right|\right) + zu^n + O\left(\left|z^2u^{2n}\right|\right) \\ &= O\left(\left|q^4u^{2n}\right|\right) \qquad \left(|z| < q^2\right). \end{aligned} \tag{6.4.1}$$

and hence using $\exp(O(x)) = 1 + O(x)$ for $x = O(1)$ we get,

$$(1-u^n)^z(1-zu^n)^{-1} = 1 + O\left(\left|q^4u^{2n}\right|\right).$$

We now observe the Euler product for $\widetilde{F_z}$ converges absolutely in $\widetilde{\mathscr{R}}$ as,

$$\sum_{p\in\mathscr{P}_{\geqslant 2}} |u|^{2n} \leqslant \sum_{n\geqslant 2} |qu^2|^n < \infty. \qquad \text{(where we used, } \#\mathscr{P}_n \leqslant q^n\text{)}$$

Also $(1-u)^{qz}$ is holomorphic in $\widetilde{\mathscr{R}}$ and this proves $\widetilde{F_z}(u)$ is holomorphic inside $\widetilde{\mathscr{R}}$. We determine the coefficient of u^n in $\widetilde{G_z}(u)$ using Cauchy's integral formula and recover $\widetilde{M_z}(n)$ exactly as in the proof of Theorem 5.2.3. We have that, if $|u| = r < q^{-1}$ (refer to the small green circle in the same Fig-6.1), then using Cauchy's residue formula on (6.1.1) gives

$$\widetilde{M_z}(n) = \frac{1}{2\pi i}\int\limits_{|u|=r} \widetilde{G_z}(u)\frac{du}{u^{n+1}} = \frac{1}{2\pi i}\int\limits_{|u|=r} \zeta(u)^z\widetilde{F_z}(u)\frac{du}{u^{n+1}}. \tag{6.4.2}$$

Now we again want to collect the contribution coming from the singularity of $\zeta(u)^z$ at $u = 1/q$ to evaluate the above integral. We shift the contour $|u| = r$ to a bigger circle $|u| = 1/q + \widetilde{\eta}$ with a different choice of $\widetilde{\eta}$ here (not the same choice for η in Proposition 5.2.5) and with $|z| \leqslant q^2 - \delta$. (the same δ in the hypothesis of this lemma) Since the region of absolute convergence for $\widetilde{F_z}(u)$ here is $\widetilde{\mathscr{R}}$, we have a different set of constraints on $\widetilde{\eta}$ than before. Here we get for $\widetilde{\eta}$, $|zu^2| \leqslant (q^{-1}+\widetilde{\eta})^2(q^2-\delta) \leqslant 1$ and $|u| = 1/q + \widetilde{\eta} < q^{-\frac{1}{2}}$. This shows taking any $0 < \widetilde{\eta} < \min\{1/\sqrt{q^2-\delta} - 1/q, 1/\sqrt{q} - 1/q\}$ suffices. We then plan to use Lemma 6.1.2 to evaluate the integral in (6.4.2) with, $\widetilde{\eta} = \min\{1/\sqrt{q^2-\delta} - 1/q, 1/\sqrt{q} - 1/q\}/2$ for $|z| \leqslant q^2 - \delta$ just as we did in the proof of Proposition 5.2.5.

Remark 6.4.1. *$F_z(u)$ was absolutely convergent in $\mathscr{R}$ which gave us the appropriate choice for η. All the calculations are identical here with $\widetilde{F_z}$ instead of F_z. The main difference is, here we have $|z| \leqslant q^2 - \delta$ instead of $|z| \leqslant q - \varepsilon$. Earlier $F_z\left(\frac{1}{q}\right)$ had a pole at $z = q, q^2, \ldots$ but we got rid of the $z = q$ pole here. This is what essentially allowing us to take $|z| \leqslant q^2 - \delta$.*

We therefore get

$$\begin{aligned}\widetilde{M}_z(n) &= \frac{1}{2\pi i}\int\limits_{\{|u|=\frac{1}{q}+\widetilde{\eta}\}\cup\mathscr{H}'} \zeta(u)^z\widetilde{F}_z(u)\frac{du}{u^{n+1}}\\ &= \widetilde{F}_z\left(\frac{1}{q}\right)q^n n^{z-1}\left(\frac{1}{\Gamma(z)}+O_\delta\left(\frac{1}{n}\right)\right)\\ &= q^n n^{z-1}\left(zh(z)+O_\delta\left(\frac{1}{n}\right)\right),\end{aligned}$$

where

$$h(z)=\frac{1}{z}\widetilde{F}_z\left(\frac{1}{q}\right)\frac{1}{\Gamma(z)}=\frac{1}{\Gamma(z+1)}\left(1-\frac{1}{q}\right)^{qz}\prod_{p\in\mathscr{P}_{\geqslant 2}}\left(1-\frac{z}{q^{deg(p)}}\right)^{-1}\left(1-\frac{1}{q^{deg(p)}}\right)^{z}.$$

Also we have $h(z)=\frac{1}{\Gamma(z+1)}\widetilde{F}_z\left(\frac{1}{q}\right)$. Since, $\widetilde{F}_z\left(\frac{1}{q}\right)$ is analytic in $|z|<q^2$, so is h. □

6.4.2 An useful upper bound for $\Pi'_q(n,j)$.

Proof of Lemma 6.3.2. We use Proposition 5.2.6 with $z=q+\eta$ and if $a_j(f)$ denotes the indicator function of polynomials in $\widetilde{M_n}$ with $\Omega_q(f)=j$ then, we see that every time $a_j=1$ occurs, it contributes an amount of $(q+\eta)^j$ on the left hand side of the sum of Proposition 5.2.6 and all the other terms are positive. We have by the previous lemma $h(z)$ is analytic in an open set containing the disc $|z|\leqslant q^2-\delta$. Since the disk is compact and h is continuous there, we have $h(z)\ll_{q,\delta}1$ for every $|z|\leqslant q^2-\delta$. Consequently for every $|z|\leqslant q^2-\delta$, $|zh(z)|\leqslant|(q+\eta)h(q+\eta)|\ll_{q,\delta}1$. This observation leads to an upper bound $\Pi'_q(n,j)\ll_{q,\delta}q^n n^{q+\eta-1}\left(\frac{1}{q+\eta}\right)^j$. □

6.4.3 An uniform estimate for $\Pi'_q(n,j)$ when $j\leqslant eq\log n$

Proof of Lemma 6.3.5. We use Proposition 5.2.6. The coefficient of z^j in $\widetilde{M}_z(n)$ is what we want to evaluate. We have for $r<q^2$,

$$\Pi'_q(n,j)=\frac{1}{2\pi i}\int\limits_{|z|=r}\widetilde{M}_z(n)\frac{dz}{z^{j+1}}.$$

We recall from Proposition 5.2.6 $\widetilde{M}_z(n) = \frac{q^n}{n}\left\{ zh(z)n^z + O\left(n^{z-1}\right)\right\}$. Plugging this back in the integral we get that

$$\frac{n}{q^n}\Pi'_q(n,j) = \frac{1}{2\pi i}\int_{|z|=r} zh(z)n^z\frac{dz}{z^{j+1}} + O(E_0),$$

where E_0 is given by, $\displaystyle\int_{|z|=r}\left|\frac{n^{z-1}}{z^{j+1}}\right||dz|$. At this point we choose $r = \frac{j}{\log n} \leqslant eq < q^2$ since by hypothesis $j \leqslant eq\log n$ and $q \geqslant 3$.

Noting $e^j = n^r \iff j = r\log n$ and using Lemma 6.2.2, we get the term E_0 is bounded by

$$\ll \frac{r^{-j-1}e^j}{n}\int_{|z|=r}|n^{z-r}||dz| \ll \frac{r^{-j-1}e^j}{n}\frac{r}{j^{\frac{1}{2}}} \ll \frac{1}{n}\frac{(e\log n)^j}{j^{j+\frac{1}{2}}} \ll \frac{1}{n}\frac{(\log n)^j}{j!},$$

where the final step of bounding follows by Stirling. This is the same trick that we used while bounding above E on page 68 in the proof of Theorem 5.2.3. Now now return to the main term

$$M_0 = \frac{1}{2\pi i}\int_{|z|=r} zh(z)n^z\frac{dz}{z^{j+1}} = \frac{1}{2\pi i}\int_{|z|=r} h(z)n^z\frac{dz}{z^j},$$

where $h(z)$ is an analytic function in the region $|z| < q^2$, so the integrand has a pole at $z = 0$ of order j. We evaluate this integral using residue theorem and obtain

$$M_0 = \lim_{z\to 0}\frac{1}{(j-1)!}\frac{d^{j-1}}{dz^{j-1}}h(z)n^z.$$

Using binomial theorem for higher order differentiation of products of two complex functions

$$\begin{aligned}\frac{1}{(j-1)!}\frac{d^{j-1}}{dz^{j-1}}h(z)n^z\Big|_{z=0} &= \frac{1}{(j-1)!}\sum_{m+\ell=j-1}\frac{(j-1)!}{m!\ell!}h^{(m)}(z)(n^z)^{(\ell)}\Big|_{z=0}\\ &= \sum_{m+\ell=j-1}\frac{1}{m!\ell!}h^{(m)}(0)(\log n)^\ell.\end{aligned}$$

where we have taken the limits inside the argument of the higher order derivatives which is allowed because all the functions here are analytic and hence infinitely differentiable. Plugging everything back we obtain the desired result. □

6.4.4 A technical upper bound for $h(z)$, $Q_j(X)$ and their derivatives.

Proof of Lemma 6.3.6. From Proposition 5.2.6 we have that $h(z)$ is holomorphic for $|z| < q^2$ which in particular implies $h(z) \ll_q 1$ for $|z| \leqslant 2.9q$. Therefore we have by Cauchy's integral formula,

$$h^{(m)}(0)/m! = \left| \int\limits_{|z|=2.9q} h(z) \frac{dz}{z^{m+1}} \right| \ll \left(\frac{1}{2.9q}\right)^m \quad \left(2.9q < q^2 \text{ whenever } q \geqslant 3\right).$$

We have from Lemma 6.3.4

$$Q_j(X) = \sum_{m+\ell=j-1} \frac{1}{m!\ell!} h^{(m)}(0) X^\ell \ll \sum_{m+\ell=j-1} \left(\frac{1}{2.9q}\right)^m \frac{X^\ell}{\ell!}$$

We now take out the top term $\frac{X^{j-1}}{(j-1)!}$ to bound the sum from above and observe for each $m \geqslant 1$, $\frac{X^\ell}{\ell!} = \frac{X^{j-m-1}}{(j-m-1)!} \leqslant (eq)^m \frac{X^{j-1}}{(j-1)!}$ which is true after cross multiplying whenever $j \leqslant eqX$ since $(j-1)(j-2)\cdots(j-m) \leqslant j^m \leqslant (eqX)^m$. Hence we arrive at the following upper bound,

$$Q_j(X) \ll \frac{X^{j-1}}{(j-1)!} \sum_{0 \leqslant m \leqslant j-1} \left(\frac{eq}{2.9q}\right)^m \ll \frac{X^{j-1}}{(j-1)!}.$$

Likewise when $j \leqslant eqX$,

$$\begin{aligned} Q_j'(X) &= \sum_{m+\ell=j-1} \frac{1}{m!(\ell-1)!} h^{(m)}(0) X^{\ell-1} \\ &\ll \sum_{m+\ell=j-1} \left(\frac{1}{2.9q}\right)^m \frac{X^{\ell-1}}{(\ell-1)!} \\ &\ll \frac{X^{j-2}}{(j-2)!} \sum_{0 \leqslant m \leqslant j-1} \left(\frac{eq}{2.9q}\right)^m \\ &\ll \frac{X^{j-2}}{(j-2)!}. \end{aligned}$$

□

6.4.5 One of the main ingredients of Proposition 6.3.7 and Theorem 5.2.4

Proof of Lemma 6.3.4. By Lemma 6.3.5 we have that

$$\Pi'_q(n+j-k,j) = \frac{q^{n+j-k}}{n+j-k}\left\{Q_j(\log(n+j-k)) + O\left(\frac{(\log(n+j-k))^j}{j!(n+j-k)}\right)\right\}.$$

We observe $n-k \geqslant n\left(1-\frac{1}{B}\right) \to \infty$ as $n \to \infty$. We also note if $E_1 = \frac{(\log(n-k))^{j+1}}{j!(n-k)^2}$ and $E_2 = \frac{(\log(n+j-k))^j}{j!(n+j-k)^2}$ then as $n \to \infty$

$$\begin{aligned}\frac{E_2}{E_1} &= \frac{1}{(\log(n-k))}\left(\frac{\log(n+j-k)}{\log(n-k)}\right)^j \frac{(n-k)^2}{(n+j-k)^2}\\ &\leqslant \left(1+\frac{\log\left(1+\frac{j}{n-k}\right)}{\log(n-k)}\right)^j \frac{1}{(\log(n-k))} \to 0\\ &\implies E_2 = o(E_1),\end{aligned}$$

where we have at the second step the term inside the bracket is bounded, because $\frac{j}{n-k} \leqslant \frac{eq\log(n-k)}{(n-k)} \to 0$ and hence for n large enough it is bounded by $(1+\log 2/\log(n-k))^{eq\log(n-k)} \leqslant e^{eq\log 2} = 2^{eq}$.

We show at a small cost it is possible to replace $\frac{Q_j(\log(n+j-k))}{n+j-k}$ by $\frac{Q_j(\log(n-k))}{n-k}$. We use mean value theorem to study the error. Let $F(x) := \frac{Q_j(\log x)}{x}$ which is a regular function if $x > 0$. The difference caused by this replacement

$$D = \frac{Q_j(\log(n+j-k))}{n+j-k} - \frac{Q_j(\log(n-k)}{n-k} = F(n+j-k) - F(n-k).$$

By mean value theorem one can pick $y \in (n-k, n+j-k)$ such that

$$D = jF'(y) = j\frac{Q'_j(\log y) - Q_j(\log y)}{y^2} = \frac{j}{y^2}Q'_j(\log y) - \frac{j}{y^2}Q_j(\log y) = F_1 + F_2.$$

We apply Lemma 6.3.6 with the choice $X = \log y$. We note from the hypothesis that $j \leqslant eqY \leqslant eq\log y$ and $y > n-k$, so that we must have $X = \log y \to \infty$ with n. Using this observation, we upper bound the first term of F_1 which gives $F_1 = \frac{j}{y^2}Q'_j(\log y) \ll \frac{j}{y^2}\frac{(\log(n+j-k))^{j-2}}{(j-2)!}$. Thus we obtain

$$\begin{aligned}\frac{F_1}{E_1} &= \frac{(n-k)^2 j!}{(\log(n-k))^{j+1}} \frac{j}{y^2} \frac{(\log(n+j-k))^{j-2}}{(j-2)!} \\ &\leqslant \left(\frac{\log(n+j-k)}{\log(n-k)}\right)^{j-2} \frac{j^2(j-1)}{(\log(n-k))^3} \\ &\ll 1,\end{aligned}$$

since $j \leqslant eq\log(n-k)$ and $y > n-k$. Hence $F_1 = O(E_1)$ and likewise from Lemma 6.3.6 one can show $|F_2| = \frac{j}{y^2} Q_j(\log y) \ll \frac{j(\log(n+j-k))^{j-1}}{y^2(j-1)!}$, leading to

$$\begin{aligned}\frac{|F_2|}{E_1} &= \frac{j!(n-k)^2}{(\log(n-k))^{j+1}} \frac{j(\log(n+j-k))^{j-1}}{y^2(j-1)!} \\ &\leqslant \left(\frac{\log(n+j-k)}{\log(n-k)}\right)^{j-1} \frac{j^2}{(\log(n-k))^2} \\ &\ll 1.\end{aligned}$$

Thus we infer $F_2 = O(E_1)$, which completes the proof of Lemma 6.3.4. □

CHAPTER 7

CONCLUSION

This thesis explored the similarities between integers and polynomials over finite fields with respect to several fundamental results of analytic and probabilistic number theory. We started our exploration with results from elementary number theory like the Chinese remainder theorem, Euler's theorem, and Fermat's little theorem and then took the discussion to advanced analytic tools like the Sathe-Selberg formula in the function field setting.

On the way, we introduced the reader to one of the key important functions, the Riemann zeta function, whose presence is ubiquitous in analytic number theory and discussed its' connection with the prime numbers. The main goal of thesis was to study the set $\{f \in \mathscr{M}_n : \Pi_q(f) = k\}$ for various ranges of k. To motivate our interest in this problem, we introduced the reader to some famous arithmetic functions including ω and Ω that frequently appear in number theoretic results and discussed several important aspects concerning the distributions of these functions, one of which is notably a central limit theorem due Erdos and Kac. We compared the two worlds, integers and polynomials for every result we investigated throughout the work.

In the final two chapters, we talked about the main tool used that lies in the heart of the thesis, i.e., the Sathe-Selberg formula in the function field setting and proved two applications of the formula. Although the main results concerning the object $\Pi_q(n,k)$ for different ranges of k are not new, our proof techniques for reproducing Hwang's asymptotic of $\Pi_q(n,k)$ when k is a bit larger than $\log n$ is new. From the existing work in the integer setting, we observed a significant difference in the asymptotic behaviour of $\pi(x,k)$ and $\Pi(x,k)$ when k exceeds the $2\log\log x$ barrier. Identical "difference of asymptotic phenomenon" is also observed in the function setting for the functions $\pi_q(n,k)$ and $\Pi_q(n,k)$ when k is a bit larger than $q\log n$. However, the asymptotic result that we established when k is larger than $q\log n$ had some major differences than what we expected from the behaviour of $\Pi(x,k)$ when $k > 2\log\log x$. This was perhaps the only instance where we could exhibit integers and the polynomials were behaving differently.

BIBLIOGRAPHY

[1] Ardavan Afshar and Sam Porritt. The function field Sathe-Selberg formula in arithmetic progressions and 'short intervals'. *Acta Arith.*, 187(2):101–124, 2019. ISSN 0065-1036. doi: 10.4064/aa170726-24-4. URL https://doi.org/10.4064/aa170726-24-4.

[2] Michael Artin. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991. ISBN 0-13-004763-5.

[3] Andrew C. Berry. The accuracy of the Gaussian approximation to the sum of independent variates. *Trans. Amer. Math. Soc.*, 49:122–136, 1941. ISSN 0002-9947. doi: 10.2307/1990053. URL https://doi.org/10.2307/1990053.

[4] Patrick Billingsley. The probability theory of additive arithmetic functions. *Ann. Probability*, 2:749–791, 1974. ISSN 0091-1798. doi: 10.1214/aop/1176996547. URL https://doi.org/10.1214/aop/1176996547.

[5] Patrick Billingsley. *Probability and measure*. Wiley Series in Probability and Statistics. John Wiley & Sons, Inc., Hoboken, NJ, 2012. ISBN 978-1-118-12237-2. Anniversary edition [of MR1324786], With a foreword by Steve Lalley and a brief biography of Billingsley by Steve Koppes.

[6] Mireille Car. Factorisation dans $F_q[X]$. *C. R. Acad. Sci. Paris Sér. I Math.*, 294(4):147–150, 1982. ISSN 0249-6291.

[7] C. J. de la Vallée Poussin. Recherches analytiques sur la théorie des nombres premiers. *Ann. Soc. Sci. Bruxelles*, 20:183–256, 1896.

[8] Rick Durrett. *Probability: theory and examples*, volume 31 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, Cambridge, fourth edition, 2010. ISBN 978-0-521-76539-8. doi: 10.1017/CBO9780511779398. URL https://doi.org/10.1017/CBO9780511779398.

[9] C.F. Gauss. *Werke*. 1863. 2d ed.

[10] Andrés Gómez-Colunga, Charlotte Kavaler, Nathan McNew, and Mirilla Zhu. On the size of primitive sets in function fields. *Finite Fields Appl.*, 64:101658, 23, 2020. ISSN 1071-5797. doi: 10.1016/j.ffa.2020.101658. URL https://doi.org/10.1016/j.ffa.2020.101658.

[11] Andrew Granville. *Analytic number theory revealed: The distribution of prime numbers.*

[12] J. Hadamard. Étude sur les proprietés des fonctions entiéres et en particulier d'une fonction considérée par riemann. *J. de Math. Pures Appl.*, (4) **9**:171–215, 1893.

[13] J. Hadamard. Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bull. Soc. Math. France*, 24:199–220, 1896. ISSN 0037-9484. URL http://www.numdam.org/item?id=BSMF_1896__24__199_1.

[14] Adam J. Harper. Two new proofs of the Erdos-Kac theorem, with bound on the rate of convergence, by Stein's method for distributional approximations. *Math. Proc. Cambridge Philos. Soc.*, 147(1):95–114, 2009. ISSN 0305-0041. doi: 10.1017/S0305004109002412. URL https://doi.org/10.1017/S0305004109002412.

[15] Hsien-Kuei Hwang. A poisson $*$ negative binomial convolution law for random polynomials over finite fields. *Random Structures Algorithms*, 13(1):17–47, 1998.

[16] Mark Kac. *Statistical independence in probability, analysis and number theory*. The Carus Mathematical Monographs, No. 12. Mathematical Association of America; distributed by John Wiley and Sons, Inc., New York, 1959.

[17] Dimitris Koukoulopoulos. *The distribution of prime numbers*, volume 203 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2019. ISBN 978-1-4704-4754-0; 978-1-4704-6285-7. URL https://doi.org/10.1090/gsm/203.

[18] Edmund Landau. *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände*. Chelsea Publishing Co., New York, 1953. 2d ed, With an appendix by Paul T. Bateman.

[19] Jean-Louis Nicolas. Sur la distribution des nombres entiers ayant une quantité fixée de facteurs premiers. *Acta Arith.*, 44(3):191–200, 1984. ISSN 0065-1036. doi: 10.4064/aa-44-3-191-200. URL https://doi.org/10.4064/aa-44-3-191-200.

[20] Samuel Porrit. Character sums over products of prime polynomials. 2020. URL https://doi.org/10.48550/arXiv.2003.12002.

[21] A. Rényi and P. Turán. On a theorem of Erdos-Kac. *Acta Arith.*, 4:71–84, 1958. ISSN 0065-1036. doi: 10.4064/aa-4-1-71-84. URL https://doi.org/10.4064/aa-4-1-71-84.

[22] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. ISBN 0-387-95335-3. doi: 10.1007/978-1-4757-6046-0. URL https://doi.org/10.1007/978-1-4757-6046-0.

[23] L. G. Sathe. On a problem of Hardy on the distribution of integers having a given number of prime factors. I. *J. Indian Math. Soc. (N.S.)*, 17:63–82, 1953. ISSN 0019-5839.

[24] Atle Selberg. Note on a paper by L. G. Sathe. *J. Indian Math. Soc. (N.S.)*, 18:83–87, 1954. ISSN 0019-5839.

[25] Elias M. Stein and Rami Shakarchi. *Complex analysis*, volume 2 of *Princeton Lectures in Analysis*. Princeton University Press, Princeton, NJ, 2003. ISBN 0-691-11385-8.

[26] R. Warlimont. Arithmetical semigroups. IV. Selberg's analysis. *Arch. Math. (Basel)*, 60 (1):58–72, 1993. ISSN 0003-889X. doi: 10.1007/BF01194240. URL https://doi.org/10.1007/BF01194240.

[27] Wikipedia contributors. Erdős–kac theorem — Wikipedia, the free encyclopedia, 2022. URL https://en.wikipedia.org/w/index.php?title=Erd%C5%91s%E2%80%93Kac_theorem&oldid=1087229591. [Online; accessed 19-July-2022].

[28] Wikipedia contributors. Prime number theorem — Wikipedia, the free encyclopedia, 2022. URL https://en.wikipedia.org/w/index.php?title=Prime_number_theorem&oldid=1097753524. [Online; accessed 19-July-2022].

[29] E. M. Wright. A simple proof of a theorem of Landau. *Proc. Edinburgh Math. Soc. (2)*, 9:87–90, 1954. ISSN 0013-0915. doi: 10.1017/S0013091500021349. URL https://doi.org/10.1017/S0013091500021349.

Appendix I

First Appendix

I.1 Auxiliary results towards Theorem 5.2.3

We establish the technical Lemmas 6.2.1, 6.2.2 and 6.2.3, used in the proofs of Theorem 5.2.3 and will again be used in showing Proposition 5.2.6.

Proof of Lemma 6.2.1. In this result we need to show For $t \in [-\pi, \pi]$ we have

$$\cos t - 1 \leqslant -\frac{t^2}{5} \text{ and } \left|1 - e^{it}\right|^2 \leqslant t^2.$$

We define the function $f(t) := 1 - \frac{t^2}{5} - \cos t$ for $t \in [0, \pi]$ and observe that $f'(t) = 0 \implies \sin t = \frac{2t}{5}$. A quick graph plot or plugging this equation into a computer reveals that it has only two solutions in the interval $[0, \pi]$, namely $t = 0, 2.125$. Checking that $f''(0) = -\frac{2}{5} + \cos 0 = \frac{3}{5} > 0$ and hence $t = 0$ is the global minima in the interval $[0, \pi]$ since $0 = f(0) < f(2.125)$ which can also be checked on a computer. Finally since $\cos t$ and t^2 are both even functions we have for all $t \in [-\pi, \pi]$ the following inequality,

$$f(t) \geqslant 0 \implies 1 - \frac{t^2}{5} - \cos t \geqslant 0 \implies \cos t - 1 \leqslant -\frac{t^2}{5}.$$

For $0 \leqslant x, t \leqslant \pi$ it is well known that,

$$\sin x \leqslant x \implies \int_0^t \sin x dx \leqslant \int_0^t x dx \implies 1 - \cos t \leqslant \frac{t^2}{2}.$$

Again the above inequality is true for $-\pi \leqslant t \leqslant \pi$ since cos and t^2 are both even functions. Finally we observe $\left|1 - e^{it}\right|^2 = (1 - \cos t)^2 + \sin^2 t = 2(1 - \cos t) \leqslant t^2$ and the claim follows. □

Proof of Lemma 6.2.2. We need to establish the following upper bound

$$\int_{|z|=r} \left|n^{z-r}\right| |dz| \ll \frac{r}{\sqrt{j}},$$

where $j = r\log n$.

We let $I_0 = \int_{|z|=r} \left|n^{z-r}\right| |dz|$. After substituting $z = re^{2\pi it}$ where $t \in \left[-\frac{1}{2}, \frac{1}{2}\right)$ we get

$$\begin{aligned}
I_0 &\ll \int_{-\frac{1}{2}}^{\frac{1}{2}} \left|n^{re^{2\pi it}-r}\right| r dt \\
&= r\int_{-\frac{1}{2}}^{\frac{1}{2}} \left|n^{r(\cos 2\pi t - 1)}\right| dt \qquad \left(\left|n^{ir\sin 2\pi t}\right| = 1\right) \\
&\ll r\int_{-\frac{1}{2}}^{\frac{1}{2}} n^{-\frac{4\pi^2 rt^2}{5}} dt \qquad (\text{ by Lemma 6.2.1}) \\
&\ll r\int_{-\infty}^{\infty} e^{-t^2} \frac{dt}{\sqrt{r\log n}} \qquad \left(t \mapsto 2\pi t\sqrt{\frac{r\log n}{5}}\right) \\
&\ll r\frac{1}{\sqrt{r\log n}} = \frac{r}{\sqrt{j}}. \qquad (j = r\log n)
\end{aligned}$$

□

Proof of Lemma 6.2.3. We need to check the following estimate holds

$$\int_{-\infty}^{\infty} \theta^2 \exp\left(-\frac{k\theta^2}{5}\right) d\theta \ll k^{-\frac{3}{2}}.$$

We observe

$$\begin{aligned}
\int_{-\infty}^{\infty} \theta^2 \exp\left(-\frac{k\theta^2}{5}\right) d\theta &= \frac{5\sqrt{5}}{k^{\frac{3}{2}}} \int_0^{\infty} \sqrt{z} e^{-z} dz \qquad \left(z = \frac{k\theta^2}{5}\right) \\
&\ll k^{-\frac{3}{2}}. \qquad \left(\text{ since } \int_0^{\infty} \sqrt{z} e^{-z} dz \text{ is convergent}\right)
\end{aligned}$$

□