Undergraduate Thesis
in Mathematics and Computer Science

Artin's Conjecture on primes with prescribed primitive roots

Universitat Politècnica de Catalunya[1]

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Centre de Formació Interdisciplinària Superior

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

University of California Berkeley[2]

Berkeley
UNIVERSITY OF CALIFORNIA

Author: Javier López-Contreras[1]

Supervisors: Sug Woo Shin[2]

Victor Rotger Cerdà[1]

Date: May 2022/2023

Abstract

English

Artin's Conjecture about primes with a prescribed primitive root is one of the simplest to state open questions in mathematics. In its most classical form it asks the following question: are there infinitely many primes p such that 2 is a primitive root modulo p? The purpose of this work is to introduce some of the most important results towards answering this and related questions. In particular, we give an in depth review of [LT65, Artin's Observation], [Bil37], [Hoo67], [W77] and [KR20; KM22]. In Section 4.2.3 and Section 5.2 the author has been able to make modest contributions about some open questions in the area.

Keywords: Analytical Number Theory, Artin's primitive root conjecture, Sieve Theory, Global Fields. **MSC Codes:** 11A07, 11N05, 11N35, 11N36

Català

La Conjectura d'Artin sobre la densitat del conjunt de nombres primers amb una arrel primitiva prescrita és un dels problemes matemàtics oberts més fàcils d'enunciar. En la seva versió més clàssica, es planteja la següent pregunta: hi ha infinits nombres primers p tal que 2 és una arrel primitiva mòdul p? El propósit d'aquest treball és introduir les tècniques més importants que s'han utilitzat per donar resultats parcials en aquesta àrea. En particular, fem una revisió detallada de [LT65, Artin's Observation], [Bil37], [Hoo67], [W77] i [KR20; KM22]. A la Secció 4.2.3 i a la Secció 5.2 l'autor ha pogut fer dues contribucions modestes a problemes oberts a l'area.

Paraules Clau: Teoria de Nombres Analítica, Conjectura d'Artin de les Arrels Primitives, Teoria de Garbells, Cossos Globals. **Codis MSC:** 11A07, 11N05, 11N35, 11N36

Español

La Conjetura de Artin sobre la densidad del conjunto de números primos con una raíz primitiva prescrita es uno de los problemas matemáticos abiertos más fáciles de enunciar. En su versión más clásica, plantea la siguiente pregunta: hay infinitos números primos p tal que 2 es una raíz primitiva módulo p? El propósito de este trabajo es introducir las técnicas más importantes que se han utilizado para dar resultados parciales en este área. En particular, hacemos una revisión detallada de [LT65, Artin's Observation], [Bil37], [Hoo67], [W77] y [KR20; KM22]. En la Sección 4.2.3 y en la Sección 5.2 el autor ha podido hacer dos contribuciones modestas a problemas abiertos en el área.

Palabras Clave: Teoría de Números Analítica, Conjetura de Artin de las Raíces Primitivas, Teoria de Cribas, Cuerpos Globales. **Códigos MSC:** 11A07, 11N05, 11N35, 11N36

Acknowledgements

I would like to express my most sincere gratitude to Professor Sug Woo Shin and to the *University of California Berkeley* for hosting me during the completion of this Undergraduate Thesis. I would also like to show a profound appreciation to Professor Victor Rotger for co-tutoring this thesis and for all the support he has provided during the start of my academic journey.

I would like to thank the Interdisciplinary *Center of Superior Formation (CFIS)* for the opportunity of developing my thesis abroad and to the *Cellex Foundation* and the *Polytechnic University of Catalonia (UPC)* for providing financial support.

Finally, I would like to thank my parents, Eva Gonzalez and Joaquín López-Contreras, my partner, Laura Arribas, and all of my friends and family, for their infinite support.

Contents

1. Introduction

As it often happens in Mathematics, the history of Artin's Conjecture can be traced back to the writtings of Carl Friedrich Gauss. In the articles 314-317 of his 1801 *Disquisitiones Arithmeticae* [GWC86], Gauss asks the following elementary question. Why does the decimal expression of $\frac{3}{7}$ have a period of length 6, while the expression of $\frac{1}{11}$ has a shorter period, of only 2 digits?

$$\frac{3}{7} = 0.428571\ 428571\ 428571\dots \qquad \frac{1}{11} = 0.09\ 09\ 09\dots \tag{1.1}$$

When p is a prime $\notin \{2,5\}$ and $a \in \mathbb{Z} \cap [1, p-1]$, it turns out that the length of the period of $\frac{a}{p}$ is exactly $\mathrm{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(10)$. To see this, note that

$$\frac{a}{p} = \left(\frac{a_1}{10} + \cdots + \frac{a_s}{10^s}\right)\left(1 + \frac{1}{10^s} + \cdots\right) = \left(10^{s-1}a_1 + \cdots + a_s\right)\frac{1}{10^s - 1} \tag{1.2}$$

This in turn implies that $10^s = 1 \mod p$. But for any $s' < s$ with $10^{s'} = 1 \mod p$, let $M \in \mathbb{Z}$ such that $a(10^s - 1) = pM$. Choosing the a_i to be the base 10 digits of M, we could give a shorter periodic expression of $\frac{a}{p}$.

The article continues with the following remark. If one had another $b \in \mathbb{Z} \cap [1, p-1]$ such that $b = 10^\lambda a \mod p$ for some λ, then period of $\frac{b}{p}$ would just be the period of $\frac{a}{p}$ translated λ decimal places to the right.

$$b_i = \left\lfloor \frac{10^i b}{p} \right\rfloor \mod 10 = \left\lfloor \frac{10^i(10^\lambda a + Np)}{p} \right\rfloor \mod 10 = \left\lfloor \frac{10^{i+\lambda} a}{p} \right\rfloor \mod 10 = a_{i+\lambda} \tag{1.3}$$

Therefore, if 10 was a primitive root modulo p, the periods of the $\frac{a}{p}$ would be in bijection with the possible translations of the period of $\frac{1}{p}$. The question of when is 10 a primitive root as we iterate p over the primes was not addressed by Gauss but will be the central topic of this Undergraduate Thesis.

In September of 1927, in a private conversation with Helmut Hasse, Emil Artin gave a precise conjecture about the density of primes with a prescribed primitive root [LT65, Pages vii-x]. Namely, he stated that given a non-square integer $a \in \mathbb{Z}_{>1} \setminus \mathbb{Z}^2$, the density of primes where a is a primitive root should be

$$A(a) = \prod_{l \text{ prime}} \left(1 - \frac{1}{l(l-1)}\right) \approx 0.3739558 \tag{1.4}$$

which has since become known as Artin's constant. To obtain such a precise conjecture, he used the Chebotarev's Density Theorem [Che26] over a certain family of Kummer Fields. This theorem had been proven in 1922 on the doctoral thesis of Nikolai Chebotarev and had just been published in 1926. With this powerful tool and assuming a certain *passing to the limit* argument, one reaches the conjectured density. Nonetheless, this limit argument is where the incredible difficulty of Artin's Conjecture lies. Since its conception in 1927, there have been many attempts at solving Artin's problem yet, so far, no mathematician has been able to give an unconditional proof.

In 1934, Hasse would propose Artin's problem to his doctoral student, Herbert Bilharz. After one year of work, they heard from Harold Davenport that Paul Erdős believed to have a proof. In April 5th 1935, Hasse wrote a letter to Erdős

> *"... My friend Davenport has told me that you believe to have solved a problem which is close to my heart: the problem of the density of those primes that have a given number as a primitive root... In case you have already dealt with this problem, I obviously have to find as quickly as possible a new PhD subject for Mr. Bilharz, who is working on this topic for already a year"*

Because of this, Bilharz was forced to develop his thesis about the equivalent conjecture over the Function Field $\mathbb{F}_q(x)$. In the end, Erdős' attempt ended up depending both on the Riemann Hypothesis and on an argument about the distribution of primes that he was unable to justify and was never published. To this day, Erdős argument remains a mystery from which we only know the few details that he wrote in a letter to Hasse [Coj02, Appendix II]. Nonetheless, the sudden change of topic in Bilharz' thesis had a happy ending. In 1937, he would publish a proof of Artin's Conjecture over $\mathbb{F}_q(x)$ [Bil37] that depended on the Riemann Hypothesis over Function Fields of Curves over $\mathbb{F}_q$. This version of the Riemann Hypothesis was settled by André Weil 1940 [Wei40].

In 1957, Emma and Derrick Lehmer computed some numerical estimates of Artin's constant with the aid of a computer. They realized that density of the set of primes with a prescribed primitive root at a didn't seem to be independent of a, as Artin had conjectured. After some correspondence, Artin realized that for certain values of a, his conjectured density formula missed a correction factor that could be given explicitly. This mistake came from a miss-calculation of the degree of a certain Kummer extension. As Artin sums it up in [Leh90]

> *"... So I was careless but the machine caught up with me.*
> *Cordially, E. Artin"*

The first major advancement towards a proof of the conjecture came in 1967, by Christopher Hooley [Hoo67]. He showed that the Generalized Riemann Hypothesis on a certain family of Kummer Fields would imply Artin's Conjecture. His proof is heavily inspired by the development of Sieve Theory in recent years. Hooley was able to reduce Artin's Conjecture to a problem about counting primes. Under the assumption of the Riemann Hypothesis, he proved a statement about the vertical distribution of the Riemann zeroes. With this, he gave a sufficiently fine estimation of the prime counting function which was enough to settle the conjecture.

Removing the Riemann Hypothesis condition has proven to be a hard problem on its own. In 1983, an important step in this direction was given by Rajiv Gupta and Ram Murty [Gup84]. They were able to give a set of 13 integers and proved unconditionally that at least one of these must follow Artin's Conjecture. In 1985, Heath-Brown [Hea86] refined their argument showing that at least one of $a \in \{2, 3, 5\}$ follows Artin's Conjecture.

Over the last century, Artin's Conjecture has remained one of the few elusive problems originated in Elementary Number Theory. As such, it has generated interest on a number of related problems, from which we give two notable examples. First, in 1976, J. P. Serre [Ser03] used a version of Hooley's argument to count the number of primes $p \leq x$ where the modulo p reduction of given Elliptic Curve is cyclic. Second, in 1977, H. W. Lenstra [W77] showed that Hooley's argument can be extended to settle a more general conjecture which has implications in the discovery of Euclidean Algorithms for certain rings of integers.

Note from the author: The historical introduction that you have just read has been pieced together from a number of sources that I would like to exhaustively list in the interest of full acknowledgement and proper book-keeping.

- The prologue of [LT65], written by two of Artin's doctoral students, John T. Tate and Serge Lang, gives a detailed accounting of the birth of the conjecture.
- The correspondence between Erdős, Davenport and Hasse seems to have been compiled and publicly published for the first time in 2002, in A. Cojocaru's PhD thesis [Coj02, Appendix II].
- The correspondence between the Lehmers and Artin was re-discovered in 2001 and is currently available in the Lehmer Archives [Leh90] of the Bancroft Library at U. C. Berkeley.
- A general overview of the history Artin's Conjecture can be found in Ram Murty's Survey [Mur88].
- A delightful historical exposition about the correction factor in Artin's constant is available in Stevenhagen's article [Ste03].

2. Notation and background

It is the author's aim to make the present document self-contained enough to be readable by any undergraduate in mathematics (and in particular, by his peers working in other areas of mathematics). Following this objective, this section introduces a series of classic results in Number Theory that may not be necessarily covered in the core courses of a Mathematics degree.

2.1 Notation

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denote the integer, rational, real and complex numbers respectively. To avoid confusion, we will use either $\mathbb{Z}_{>0}$ or $\mathbb{Z}_{\geq 0}$ instead of $\mathbb{N}$.
- The functions $\operatorname{Re}(z)$ and $\operatorname{Im}(z)$ give the real and imaginary part of a $z \in \mathbb{C}$, respectively.
- Unless otherwise stated, p will an arbitrary prime, $q = p^r$ and l will be a prime $l \neq p$.
- $\mathbb{F}_q$ denotes the finite field of q elements
- Given a group G and $a \in G$, $\operatorname{ord}_G(a)$ denotes the multiplicative order of a and $\operatorname{ind}_G(a) \coloneqq \frac{|G|}{\operatorname{ord}_G(a)}$ is the index.
- For $p \in \mathbb{Z}$ a prime and $a \in \mathbb{Q}$, $\operatorname{ord}_p(a) = \max\{k \in \mathbb{Z} \mid p^k \mid a\}$. *Warning!* Note that $\operatorname{ord}_{\mathbb{F}_p^*}$ and ord_p are different functions. This distinction could be a source of confusion.
- Given a group G, an element of $a \in G$ is called a primitive root if $G = \{a^n \mid n \in \mathbb{Z}_{\geq 0}\}$ or, equivalently, $\operatorname{ord}_G(a) = |G|$. A primitive root $\mod p$ is a primitive root of $\mathbb{F}_p^*$. Abusing notation, we also call a primitive root $\mod p$ to an element of $\mathbb{Z}$ or $\mathbb{Q}$ that has a well-defined image in $\mathbb{F}_p^*$ and whose image is a primitive root.
- For $a, b \in \mathbb{Z}$, we denote its greatest common divisor with (a, b) or $\gcd(a, b)$
- A function $f : \mathbb{Z} \to \mathbb{C}$ is weakly multiplicative if $f(ab) = f(a)f(b)\ \forall a, b \in \mathbb{Z}$ with

$(a, b) = 1$. The following functions are weakly multiplicative

- $\mu(n)$ denotes the Möebius Inversion function, namely

$$\begin{aligned} \mu : \mathbb{Z} &\longrightarrow \{-1, 0, 1\} \\ n &\mapsto \begin{cases} 0 & k^2 \mid n \\ (-1)^r & n = p_1 \dots p_r \end{cases} \end{aligned} \tag{2.1}$$

- $\phi(n)$ denotes Euler Totient function, namely

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \tag{2.2}$$

- $w(n)$ denotes the number of distinct prime divisors of n

- If L/K is a finite extension of Global or Local Fields with Dedekind Domains B/A, we denote
  - $\operatorname{Spec} A$ is the set of prime ideals of A
  - ΔL the discriminant over K
  - $\mathrm{Tr}, \mathcal{N} : L \to K$ the trace and norm respectively
  - $\mathrm{Spl}(L/K)$ or $\{L/K\}$ is the set of primes in L that split completely over K. When the base field is clear by context, we will write $\mathrm{Spl}(L)$ or $\{L\}$.
  - If $\mathfrak{p} \in \operatorname{Spec} K$ is unramified, we will denote the Frobenius conjugacy class as $\mathrm{Frob}_{\mathfrak{p}}(L/K)$ or by the Artin's symbol $(\mathfrak{p}, L/K)$.

2.2 Global Field Theory

One of the primary objectives of Algebraic Number Theory is to understand the solution set of a given polynomial equation in the rationals or in the integers. Nonetheless, a lot of insight can be extracted from studying the solution set over more general rings. This idea was initially explored by Ernst Kummer's on his work about Fermat's Last Theorem. Yet, the systematic study of Number Fields as we know it today was introduced by Richard Dedekind.

Definition 2.1 (Number Field)**.** A Number Field K is a finite (hence, algebraic) field extension of $\mathbb{Q}$. For example $\mathbb{Q}[i]$, called the Gaussian rationals.

The paper of the subring $\mathbb{Z} \subseteq \mathbb{Q}$ can also be generalized in the following way.

Definition 2.2 (Ring of integers)**.** Given a Number Field $K/\mathbb{Q}$, its ring of integers is the set $\mathcal{O}_K$ of elements $x \in K$ such that their minimal (monic) polynomial have coefficients in $\mathbb{Z} \subseteq \mathbb{Q}$. For example, the ring of integers of $\mathbb{Q}[i]$ is $\mathbb{Z}[i]$.

Remark 2.3. We call $\mathcal{O}_K$ a ring because it is indeed one, with the natural operations inherited by being a subset of K. [Neu99, Ch. 1.2]

At this point, it is necessary to remark that the paper of $\mathbb{Q}$ and $\mathbb{Z}$ in the constructions above can be seamlessly (at least for the moment) interchanged with $\mathbb{F}_q(x)$ and $\mathbb{F}_q[x]$, where $\mathbb{F}_q$ is the finite field of $q = p^r$ elements. The finite field extensions of $\mathbb{F}_q(x)$ are called Function Fields. The analogy between Number Fields and Function Fields is strong because $\mathbb{Z}$ and $\mathbb{F}_q[x]$ are both principal ideal domains with finite quotients. Function Fields take their name because they represent the meromorphic functions of a certain curve over $\mathbb{F}_q$. For example $\mathbb{F}_q(x)$ are the meromorphic functions from the projective line over $\mathbb{F}_q$. Number Fields and Function Fields are, together, called Global Fields.

Important distinctions between these classes of fields will appear during this thesis and are a central topic in Algebraic Number Theory. In general, problems over Function Fields are much better understood than their arithmetical counterparts because of the availability of geometric tools that often have no arithmetical parallel. For example, the Riemann Hypothesis, Langland's Functoriallity Conjecture, Artin's Conjecture are all theorems over Function Fields but extremely hard open problems over Number Fields.

2.2.1 Function Fields

Function Fields are much better understood that their arithmetical counterparts. A good reference for this material is M. Rosen's book *Number Theory in Function Fields* [Ros02]. For our purposes, it is worth to introduce an extra piece of structure which will be important in Section 4.1. This is the concept of the field of constants.

Note the difference between the following algebraic extensions of $\mathbb{F}_q(x)$.

Example 2.4. Let $K = \mathbb{F}_q(x)$ and $A = \mathbb{F}_q[x]$. Let $L = \mathrm{Frac}B$, where B will be specified in each case

1. $B = \mathbb{F}_{q^2}[x]$, Then L represents the meromorphic functions of the same abstract curve that K, namely the projective line. What has been extended is the "field of constants"
2. $B = \mathbb{F}_q[x, y]/(y^2 - x^3)$. In this case, L and K represent birationaly different curves.
3. $B = \mathbb{F}_{q^2}[x, y]/(y^2 - x^3)$ is a mix of the above

Definition 2.5 (Field of constants)**.** Let $L/\mathbb{F}_q(x)$ be a Function Field. The field of constants of L are the elements of L that are algebraic over $\mathbb{F}_q$, denote it by F. By definition, F is an algebraic extension of $\mathbb{F}_q$ and by being a subfield of L, it is a finite extension, hence a finite field.

Definition 2.6 (Constant Extension)**.** Let $K/\mathbb{F}_q(x)$ be a Function Field with field of constants F. Let L/K a Function Field extension, with extension of constants E/F. L/K is called a constant extension (or an extension of constants) if $L = EK$ (this is tantamount with the extension of constants accounting for the full degree of L/K).

Any Function Field extension can be separated into a constant extension and a fully geometrical extension. Because the underlying geometry is maintained, the theory of Constant Extensions is tightly related with the theory of Finite Field extensions, and hence, it is very well understood. A full account can be found in [Ros02, Chapter 8].

2.2.2 Dedekind Decomposition

An interesting, yet well understood, difficulty in the study of Global Fields comes from the fact that the concept of a prime element does not generalize neatly. In particular, the all important prime decomposition often stops being unique, as shown by the following notable example.

Example 2.7. In $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$, $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, even though $2, 3$ and $1 \pm \sqrt{-5}$ are all irreducible elements (namely, they cannot be expressed as $a \cdot b$, with $a, b \in \mathcal{O}$).

Nonetheless, Dedekind discovered that a uniqueness theorem can be given about the ideal decomposition into prime ideals.

Theorem 2.8 (Dedekind unique decomposition)**.** Given a Global Field K, its ring of integers $\mathcal{O}_K$ and an ideal $I \in \mathcal{O}_K$, there exists a tuple of prime ideals (with possible repetitions) $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $I = \prod \mathfrak{p}_i$. This tuple is unique up to permutations.

Remark 2.9. *Warning!* The product above is an ideal product, not a Cartesian product.

An important note is that Dedekind's theorem does not hold for all abstract commutative rings (nor for all integral domains). It is a remarkable property of the rings of integers of Global Fields. The integral domains that follow Dedekind's theorem are called Dedekind domains.

Going back to the example of $\mathbb{Z}[\sqrt{-5}]$, one can see that even though 2 is irreducible as an element, as an ideal (2) is not prime. Indeed, it decomposes as $(2) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})$, which are prime but not principal. Then, the ideal (6) has a unique prime decomposition, namely

$$(6) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \tag{2.3}$$

2.2.3 Hilbert's ramification theory

An important part of the study of the ring of integers of a Global Field is to understand how the primes in $\mathbb{Q}$ (or any other base field) lift through Dedekind ring extensions. Given a Number Field K and its ring of integers $\mathcal{O}$ and a rational prime $p \in \mathbb{Z}$, we know that the ideal $(p)_{\mathcal{O}} := p\mathcal{O}$ decomposes as some

$$p\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \tag{2.4}$$

We say $\mathfrak{p}_i$ are the primes above p. On the other hand, for each i, the ring extension $\mathcal{O}$ over $\mathbb{Z}$ quotients to give an extension of "residue" fields $\mathcal{O}/\mathfrak{p}_i$ over $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Denote $f_i = [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_p]$, called the residue field extension's degree.

Definition 2.10 (Inert, Ramified, Split)**.** A rational prime $p \in \mathbb{Z}$

1. is inert if and only if $p\mathcal{O}$ is prime in $\mathcal{O}$.

2. is ramified if and only if there is some $e_i > 1$. It is non-ramified if all $e_i = 1$.

3. is split or completely split if and only if all the $e_i = 1$ and all the $f_i = 1$.

These notations generalize to any extension of Dedekind Domains, we are only taking $\mathbb{Q}$ as the base field for simplicity.

The ramification theory of primes over Dedekind extensions is an extensive topic which can be found in most Algebraic Number Theory textbooks, for example [Neu99]. This section only states a few results that will make an appearance in this Undergraduate Thesis. All the proofs are excluded but can be found in [Neu99, Ch.1.1-1.7]

Theorem 2.11 (Hilbert's ramification theorem)**.** Given a Number Field $K/\mathbb{Q}$, let $n = [K : \mathbb{Q}]$. Given a $p \in \mathbb{Z}$, let e_i, f_i and g be the integers defined above. Then, the following equation holds

$$n = \sum_{i=1}^{g} e_i f_i \tag{2.5}$$

When the extension $K/\mathbb{Q}$ is Galois, even more can be said. If it is not, it will often be useful to consider it as a subextension of its Galois closure.

Theorem 2.12. Let K be a Number field such that $K/\mathbb{Q}$ is Galois and let $p \in \mathbb{Z}$ a prime. Then, the Galois group acts transitively on the set of primes above p. This implies $e_1 = e_2 = \cdots = e_g =: e$ and $f_1 = f_2 = \cdots = f_g =: f$. Hence, the previous theorem states

$$n = e \cdot f \cdot g \tag{2.6}$$

2.2.4 Frobenius elements

Another important piece of structure that can be studied in the Galois case are the so called Frobenius elements. These are special elements in the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ that come from lifts of the Frobenius automorphisms $x \mapsto x^p$ in the residue field extensions of each prime p. Because the Frobenius automorphism generates the Galois group of the residue extension, their lifts in $\mathrm{Gal}(K/\mathbb{Q})$ will "encode the information" of their residue extensions.

Definition 2.13 (Decomposition subgroups)**.** Let $K/\mathbb{Q}$ be a number field, p a prime and $\mathfrak{p}$ a prime ideal of K over p. The decomposition subgroup at $\mathfrak{p}$ is

$$D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) | \sigma(\mathfrak{p}) = \mathfrak{p}\} \subseteq \mathrm{Gal}(K/\mathbb{Q}) \tag{2.7}$$

Theorem 2.14. Let K be a Number Field such that $K/\mathbb{Q}$ is Galois and $p \in \mathbb{Z}$ an unramified prime. Let $\mathfrak{p}$ be a prime over p. Then the natural map

$$\kappa : D_{\mathfrak{p}} \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p) \tag{2.8}$$

is an isomorphism of groups. Hence, the Frobenius automorphism in the right has a unique anti-image in the left, which we denote $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}} \subseteq \mathrm{Gal}(K/\mathbb{Q})$.

Definition 2.15 (Frobenius conjugacy class)**.** Let K be a number field, $p \in \mathbb{Z}$ an unramified prime. Then the set

$$\{\mathrm{Frob}_{\mathfrak{p}} \mid \mathfrak{p} \text{ prime over } p\} \tag{2.9}$$

is a conjugacy class of the Galois Group, which we denote $\mathrm{Frob}_p(K/\mathbb{Q})$ or by the Artin's Symbol $(p, K/\mathbb{Q})$. By abuse of notation, it is sometimes called the Frobenius element at p.

The Frobenius element will have an important role in the study of Artin's conjecture. This will be explained in detail in Section 3.2.

2.3 Chebotarev's Density Theorem

As it was briefly explained in the Introduction (Section 1), Artin's conjecture about primes with a prescribed primitive root asks a question about the density of a certain set of primes. It is therefore imperative to discuss what we mean by "density over the primes".

The straight forward definition is the following

Definition 2.16 (Natural Density)**.** Let K be a Number Field and $\mathcal{O}_K$ its Dedekind Domain. Given an $S \subseteq \operatorname{Spec} \mathcal{O}_K$, define

$$\Delta(S, x) = \frac{\{\mathfrak{p} \in S | \mathcal{N}\mathfrak{p} < x\}}{\{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K | \mathcal{N}\mathfrak{p} < x\}} \tag{2.10}$$

We say S has natural Density $\Delta(S)$ if $\lim_{x\to\infty} \Delta(S, x)$ exists and is equal to $\Delta(S)$.

In 1837, Peter Gustav Lejeune Dirichlet was the first to realize that the natural notion of density is ill-behaved for number theoretical applications. He did so in his groundbreaking paper [Dir37, In German] about the infinitude of primes of the form $an+b$ when a and b are coprime. He proves that the sum $\sum_{p=an+b} \frac{1}{p}$ diverges by relating said quantity with a special value of a certain L-function. The gist of this remarkable result is precisely that the sum of reciprocals is a good notion of density. It is good for two reasons. On one hand, it is a "density" because its quantity gives information about the finitude of a certain set of primes. On the other hand, it has good number theoretical properties, as it will be possible to relate it with special values of certain L-functions.

This is essence that the following definition aims to capture. Let K be a Global Field with Dedekind Domain $\mathcal{O}_K$.

Definition 2.17 (Dirichlet's Density)**.** If $S \subseteq \operatorname{Spec} \mathcal{O}_K$, define

$$\delta(S,s) = \frac{\sum_{\mathfrak{p}\in S} \frac{1}{(\mathcal{N}\mathfrak{p})^s}}{\sum_{\mathfrak{p}\in \operatorname{Spec}\mathcal{O}_K} \frac{1}{(\mathcal{N}\mathfrak{p})^s}} \tag{2.11}$$

We say S has Dirichlet Density $\delta(S)$ if $\lim_{s\to 1}\delta(S,s)$ exists and is equal to $\delta(S)$. Define

$$\delta^+(S) = \limsup_{s\to 1}\delta(S,s) \quad \text{and} \quad \delta^-(S) = \liminf_{s\to 1}\delta(S,s) \tag{2.12}$$

These two notions of density are related in most cases, but one can give artificial counterexamples that set these definitions apart. A full discussion on these two settings can be found in the following exposition by P. Stevenhagen and H. W. Lenstra [SH94].[1] Unless otherwise stated, in this thesis the word "density" will always mean Dirichlet density.

Theorem 2.18 (Chebotarev's Density Theorem)**.** Let L/K be a finite Galois extension with $\operatorname{Gal}(L/K) = G$ and let $C \subseteq G$ formed as a union of conjugacy classes. The Dirichlet Density of the set S of primes $\mathfrak{p} \subseteq K$ that have $(\mathfrak{p}, L/K) \in C$ exists and equals $\delta(S) = \frac{|C|}{|G|}$.

An important particular case of the previous theorem if when $C = \{\mathrm{Id}\}$. In this case, the primes with $(\mathfrak{p}, L/K) = \mathrm{Id}$ are precisely the primes that split completely over the extension, as shown in the proof of Lemma 3.23. Chebotarev's theorem shows that their density is $\frac{1}{[L:K]}$.

[1] I encourage the reader to read both of Stevenhagen et. Lenstra's papers cited throughout this thesis. [Ste03] and [SH94] for their wonderful historical notes interwoven with distinctively well exposed mathematics.

3. Artin's Conjecture

In 1927, Emil Artin famously asked the following question pertaining to Elementary Number Theory.

Question 3.1. For a given $a \in \mathbb{Z}$, are there infinitely many primes $p \in \mathbb{Z}$ such that $a \mod p$ is a primitive root in $\mathbb{Z}/p\mathbb{Z}$?

Definition 3.2. We will denote $P(a) = \{p \in \mathbb{Z} \mid a \text{ is a primitive root } \mod p\}$.

We are interested in whether the cardinal of $P(a)$ is infinite or not. For certain values of $a \in \mathbb{Z}$, the question is easily answered in the negative.

Lemma 3.3 (Necessary condition in Artin's Conjecture)**.** If $a \in \mathbb{Z}$ is $\in \{-1, 0, 1\}$ or a perfect square, then there are only finitely many primes for which it is a primitive root. Namely, $P_{-1} = \{2, 3\}$ and, for $k \geq 0$,

$$P_{k^2} = \begin{cases} \emptyset & 2 \mid k \\ \{2\} & \text{otherwise} \end{cases} \tag{3.1}$$

Proof. If $a = 0$, then $a \mod p = 0$ is not invertible $\forall p$. If $a = -1$, then $a \mod p$ has order $\in \{1, 2\}$ as $(-1)^2 = 1 \mod p$. Hence, -1 can be, at most, a primitive root for primes $p \in \{2, 3\}$.

On the other hand, suppose $a = k^2$ with $k \geq 1$ has $\text{ord}_{\mathbb{F}_p^*}(a) = p - 1$. Denote $r = \text{ord}_{\mathbb{F}_p^*}(k)$. Then, $r \mid p - 1$ and $k^{2r} = 1 = a^r \mod p \implies p - 1 \mid r$ so $r = p - 1$. But if $p > 2$, then $r = p - 1$ is even and $a^{r/2} = k^r = 1$, which contradicts $\text{ord}_{\mathbb{F}_p^*}(a) = p - 1$ ■

Remark 3.4. The previous lemma does not have an analogue for l-th powers, with $l > 2$. This is because $p - 1 \neq 0 \mod 2$ only happens at $p = 2$, yet $p - 1 \neq 0 \mod l$ happens for infinitely many primes.

Remark 3.5. Note that $a \in \{-1, 0, 1\}$ do not follow the conjecture. We can exclude them from all our future attempts to prove that these conditions are sufficient. This resolves irrelevant corner cases in future lemmas.

Conjecture 3.6 (Artin's primitive root conjecture)**.** If $a \in \mathbb{Z}$ is not $\in \{-1, 0, 1\}$ or a square, the set $P(a)$ has positive density over the set of primes.

There are no values of a for which the conjecture has been proven to hold unconditional to the Riemann Hypothesis.

3.1 Studied generalizations

This long-lasting conjecture has raised interest in a number of related problems. This section describes some of these generalizations, which will be studied in more detail in the rest of the document. The generalizations listed here were explored and understood, albeit often conditionally to some version of the Riemann Hypothesis, in Lenstra's article [W77]. Section 6.1 of this thesis gives a detailed accounting of the results in this paper.

3.1.1 Prescribed root at $a \in \mathbb{Q}$

One could be interested in posing Artin's problem for $a \in \mathbb{Q}$ instead of restricting to only $a \in \mathbb{Z}$, which creates the following problem.

Problem 3.7. Let $a \in \mathbb{Q}^*$ and P_a the set of primes in $\mathbb{Z}$ following

$$(1)\ \mathrm{ord}_p(a) = 0 \qquad \text{and} \qquad (2)\ \mathrm{ord}_{\mathbb{F}_p^*}(a) = p - 1$$

Is P_a infinite?

Remark 3.8. Note that condition (1) is placed so that $a \mod p$ is well-defined and non-zero, which makes $\mathrm{ord}_{\mathbb{F}_p^*}(a)$ well-defined.

3.1.2 Artin's conjecture over Global Fields

The original conjecture studies the set of $p \in \mathbb{Z}$ for which $a \mod p$ generates the multiplicative group of the residue field $(\mathbb{Z}/p\mathbb{Z})^*$. The same question can be naturally extended to more general rings. We will be specially interested in the rings of integers of field extensions of $\mathbb{Q}$ and $\mathbb{F}_q(x)$, also known as Global Fields. The rings of integers of Global Fields are examples of Dedekind Domains with infinitely many primes and finite residue fields. Without both of these conditions the conjecture is trivially false. Note that this excludes Local Fields and extensions of $K(t)$ for any non-finite field K.

Problem 3.9 (Artin's Conjecture over Global Fields)**.** Let K be a Global Field, $\mathcal{O}_K$ its ring of integers and $a \in K^*$. Are there infinitely many prime ideals in $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ such that

$$(1)\ \operatorname{ord}_{\mathfrak{p}}(a) = 0 \qquad \text{and} \qquad (2)\ a \mod \mathfrak{p} \text{ generates } (\mathcal{O}_K/\mathfrak{p})^*?$$

For instance, writing Problem 3.9 for $\mathbb{F}_q(x)$ we obtain the following question.

Question 3.10 (Artin's Conjecture over $\mathbb{F}_q(x)$)**.** Given an $a(x) \in \mathbb{F}_q[x]$ monic, are there infinitely many $v(x) \in \mathbb{F}_q[x]$ monic and irreducible such that $\overline{a}(x)$ is a primitive root of $\mathbb{F}_q[x]/(v) \simeq \mathbb{F}_{q^{\deg v}}$?

Section 4.1 focuses on Artin's conjecture over Function Fields. In this case, the necessary and sufficient conditions were found by Bilharz in 1937 [Bil37] conditional to the Riemann Hypothesis over Function Fields of Curves, which was settled shortly after by André Weil [Wei40]. Note that Bilharz' result came three decades before significant progress was made on the original conjecture over $\mathbb{Q}$ by Hooley [Hoo67]. The main reason for this is that certain L-functions related to Artin's Conjecture have a multiplicative closed form over Function Fields.

Remark 3.11. By the same rationale exposed in Remark 3.5, the values $a \in \lambda(K) \cup \{0\}$ will never follow the conjecture, where $\lambda(K)$ are the roots of unity of the Global Field K. We will ignore these values in all further considerations.

3.1.3 Restricting $\mathrm{Frob}_{T/\mathbb{Q}}(p)$

One may be interested in imposing congruence conditions for the primes being counted. For example, one can show that there are no primes $p = \pm 1 \mod 8$ where 2 is a primitive root, as for those p, $\left(\frac{2}{p}\right) = 1$. A natural question would be to ask if there are infinitely many primes $p = 3 \mod 8$ such that 2 is a primitive root. For the general conjecture over a Global Field K, these modular restrictions are expressed as restrictions on the Frobenius element over an arbitrary Abelian extension T/K.

Problem 3.12. Let K be a Global Field, $a \in K^*$, T/K an Abelian field extension and $C \subseteq \mathrm{Gal}(T/K)$ a subset formed of conjugacy classes. Are there infinitely many prime ideals $\mathfrak{p} \in \mathrm{Spec}\, K$ such that

(1) $\mathrm{ord}_{\mathfrak{p}}(a) = 0$, (2) $\mathrm{ord}_{(K/\mathfrak{p})^*}(a) = \mathcal{N}\mathfrak{p} - 1$, (3) $\mathrm{Frob}_{\mathfrak{p}}(T/K) \in C$?

Remark 3.13. Note that $T = K$ and $C = \{1\}$ recovers the original problem.

3.1.4 Arbitrary set of generators

One more way Artin's Conjecture can be generalized is by choosing a more general set W to take the role of the prescribed primitive root a.

Problem 3.14. Let $W \subseteq \mathbb{Q}^*$ and let $\Gamma = \langle W \rangle$ be the multiplicative group $\Gamma \subseteq \mathbb{Q}$ generated by W. Are there infinitely many primes $p \in \mathbb{Z}$ such that the quotient $\Gamma \to F_p^*$ is well-defined and surjective?

Note that this is equivalent to $\mathrm{ord}_p(w) = 0\ \forall w \in W$ and $\Gamma_p = \{\gamma \mod p \mid \gamma \in \Gamma\} = \mathbb{F}_p^*$

Remark 3.15. Note that $W = \{a\}$ recovers the original conjecture.

This generalization comes up in applications of Artin's Conjecture in finding Euclidean Algorithms on Global Fields [CW75].

3.1.5 Primes with $\mathrm{ind}_{F_p^*}(a) \mid m, m \in \mathbb{Z}$

One can weaken the surjectivity condition of the quotient map $\langle a \rangle \to \mathbb{F}_p^*$. This results in the following problem.

Problem 3.16. Given a $m \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Q}$, are there infinitely many primes such that $\mathrm{ord}_p(a) = 0$ and $\mathrm{ind}_{\mathbb{F}_p^*}(a) \mid m$?

Remark 3.17. $m = 1$ recovers de original conjecture.

3.2 Artin's observation

In the letter that proposed the conjecture, Artin gave a relevant observation that links the set $P(a)$ with the set of completely split rational primes over an explicit family of Kummer fields. This link with Algebraic Number Theory is a central piece in the attempts at solving the conjecture. It begins to explain why the Generalized Riemann Hypothesis will play an important role.

The work presented in this section can be generalized to the related conjectures described in Section 3.1. We have chosen to expose the classical setting first, as the general setting doesn't introduce any new ideas but complicates the notation. We will discuss a general version of Artin's Observation in Section 6.1.

Let $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ and $p > 2$ a prime with $p \nmid a$.

Remark 3.18. The prime $p = 2$ is a corner case in some of the following Lemmas. We explicitly exclude it from consideration as, in Artin's conjecture, we are only interested in density problems unaffected by finite exceptions.

Lemma 3.19. a is a primitive root mod p if and only if there isn't any $l \in \mathbb{Z}$ prime such that

$$(1)\ l \mid p-1 \qquad \text{and} \qquad (2)\ a^{\frac{p-1}{l}} = 1 \mod p$$

Proof. If the $\mathrm{ord}_{\mathbb{F}_p^*}(a) = r \neq p-1$, it must $r \mid p-1$. Take l any non-trivial prime factor of $\frac{p-1}{r} \neq 1$ and b such that $bl = \frac{p-1}{r}$. Then $l \mid \frac{p-1}{r} \mid p-1$ and $a^{\frac{p-1}{l}} = a^{rb} = 1 \mod p$.

For the reciprocal, note that $\operatorname{ord}_{\mathbb{F}_p^*}(a) \leq \frac{p-1}{l} < p-1$. ■

Lemma 3.20. Let l be a prime $l \mid p-1$. Then $a^{\frac{p-1}{l}} = 1 \mod p$ is equivalent to $x^l = a \mod p$ having a solution in $\mathbb{F}_p^*$.

Proof. Recall that $\mathbb{F}_p^*$ is a cyclic group, with some primitive root ζ. Let $a = \zeta^i$, so $\zeta^{i\frac{p-1}{l}} = 1 \mod p$. Hence, $p-1 \mid i\frac{p-1}{l}$. There is a $b \in \mathbb{Z}$ such that $b(p-1) = i\frac{p-1}{l} \implies bl = i \implies l \mid i$. Then $u = \zeta^{\frac{i}{l}}$ is a solution of $x^l = a \mod p$.

For the reciprocal, if $u \in \mathbb{F}_p^*$ is the solution to $u^l = a$, then $a^{\frac{p-1}{l}} = u^{p-1} = 1$. ■

Remark 3.21. Note that $x^l = a \mod p$ might have solutions when $l \nmid p-1$. In that case, all the elements in $\mathbb{F}_p^*$ are l-residues as the group endomorphism $x \mapsto x^l$ must have trivial kernel and, hence, full image.

Definition 3.22 (Kummer Fields relevant to Artin's Conjecture)**.** For l prime $l \nmid a$ and k square-free integer coprime with a, let $L_l = \mathbb{Q}(\zeta_q, \sqrt[l]{a})$ and $L_k = \prod_{\substack{l \mid k \\ \text{prime}}} L_l$ the compositum. Denote $C_k = \mathbb{Q}(\zeta_k)$.

Lemma 3.23. Let l be a prime. A prime $p \in \mathbb{Z}_{>2}$ splits completely in $C_l/\mathbb{Q}$ if and only if $l \mid p-1$.

Proof. For $l = 2$, $C_2 = \mathbb{Q}$ and the result is trivial. Otherwise, recall that the ring of integers of a cyclotomic field is $\mathbb{Z}[\zeta_l]$ [Lan94, Th. 4 Page 75], which is generated by the primitive element. By the classical theorem in Ramification Theory [Neu99, Ch 1 Prop. 8.3], the splitting behavior of p is equivalent to the splitting of the minimal polynomial of ζ_l, namely $\Phi_l(x) = \frac{x^l-1}{x-1}$, modulo p.

If $\Phi_l(x) \mod p$ splits completely, in particular it has one root $u \neq 1 \mod p$ which $u^l = 1 \underset{l \text{ prime}}{\implies} l \mid p-1$. For the reciprocal, let ζ be a primitive root of $\mathbb{F}_p^*$. Then, if $l \mid p-1$, $x^l = 1 \mod p$ has solutions $\{\zeta^{\frac{p-1}{l}}, \zeta^{2\frac{p-1}{l}}, \dots, \zeta^{l\frac{p-1}{l}} = 1\}$ which are all unique. Hence, $\Phi_l(x)$ splits completely.

■

Second proof (using Frobenius substitution). For $l = 2$, $C_2 = \mathbb{Q}$ and the result is trivial. Otherwise, recall that the discriminant of a prime cyclotomic field is $(-1)^{\frac{l-1}{2}} l^{l-2}$. Hence, p ramifies at $p = l$ which does not follow $l \mid p-1$. For p unramified, p is completely split if and only if $\mathrm{Frob}_p(C_l/\mathbb{Q}) = 1$. Now, $\zeta_l^p = \zeta_l \mod p \implies \zeta_l^{p-1} = 1 \mod p \implies l \mid p-1$ or $l = p = 2$.

For the other direction, let $\mathrm{Frob}_p(C_l/\mathbb{Q}) = a \in \mathrm{Gal}\,(C_l/\mathbb{Q}) = (\mathbb{Z}/l\mathbb{Z})^*$ such that $\zeta_l \mapsto \zeta_l^a$. By the property of the Frobenius element on the residue field $\zeta_l^a = \zeta_l^p \mod p \implies \zeta_l^{p-a} = 1 \mod p \implies l \mid p-a$. As $l \mid p-1$ and $1 \leq a \leq l-1$, the only possibility is $a = 1$. ■

The proofs of the following Lemmas 3.25 and 3.26 are taken from M. Rosen book *Number Theory in Function Fields*, where they are given for Function Fields [Ros02, Propositions 10.3-4]. A version of these Lemmas is true for general Dedekind Domains.

Remark 3.24. Recall, for l prime, $x^l - a$ is irreducible over K if and only if a is not an l-th power over K. [Lan05, Th. 9.1 Page 297]

Lemma 3.25. Let l be a prime. Let $\mathfrak{p}$ be a prime ideal of C_l with $(p) = \mathfrak{p} \cap \mathbb{Z}$, such that $p > 2$ and $l \mid p-1$. Then, $\mathfrak{p}$ ramifies over L_l/C_l if and only if $l \mid \mathrm{ord}_{\mathfrak{p}}(a)$

Proof. Let $O = \mathbb{Z}[\zeta_l]$ be the ring of integers of C_l and $O_{\mathfrak{p}}$ its localization ring at P and π a uniformizer element of $O_{\mathfrak{p}}$. Let $R_{\mathfrak{p}}$ be the integral closure of $O_{\mathfrak{p}}$ over L_l.

If $l \mid \mathrm{ord}_{\mathfrak{p}}(a)$, then $a = \pi^{lh} u$ with u a unit of $O_{\mathfrak{p}}$. Then $\mu := \frac{\sqrt[l]{a}}{\pi^h} \in L_l$. Clearly, $L_l = C_l(\mu)$. Now, $O_{\mathfrak{p}}[\mu]$ is a full rank free $O_{\mathfrak{p}}$-module under $R_{\mathfrak{p}}$. By a classical theorem in Algebraic Number Theory, if the discriminant of $O_{\mathfrak{p}}[\mu]$ is a unit in $O_{\mathfrak{p}}$ we must have $R_{\mathfrak{p}} = O_{\mathfrak{p}}[\mu]$.

Hence, let's compute $\mathrm{Disc}_{O_{\mathfrak{p}}[\mu]/O_{\mathfrak{p}}} = \mathrm{Det}((\mathrm{Tr}(\mu^i \mu^j))_{ij})$. If $l \nmid k$, then u^k cannot be an l-th power as u is not one and $l \nmid k$. Hence, the minimal polynomial of μ^k is $x^l - u^k$. On the other hand, if $l \mid k$, we must have $l = 0$ or $l = k$. In the first case, $\mathrm{Tr}(1) = l$

and in the second, $\mathrm{Tr}(\mu^l) = \mathrm{Tr}(u) = lu$. We conclude that

$$\mathrm{Tr}_{L_l/C_l}(\mu^k) = \begin{cases} l & k = 0 \\ lu & k = l \\ 0 & 0 \leq k \leq 2l - 1, k \notin \{0, l\} \end{cases} \tag{3.2}$$

From this, we can compute $\mathrm{Disc}_{O_\mathfrak{p}[\mu]/O_\mathfrak{p}} = \pm l^l u^{l-1}$. Indeed, this is a unit in $O_\mathfrak{p}$ as u is one by definition and $l \neq p$, hence $R_\mathfrak{p} = O_\mathfrak{p}[\mu]$. Furthermore, $\mathfrak{p} \nmid \mathrm{Disc}$ so $\mathfrak{p}$ is unramified.

For the other direction, suppose $l \nmid \mathrm{ord}_\mathfrak{p}(a)$. Let $\mathfrak{P}$ be a prime over $\mathfrak{p}$ in L_l/C_l. Since $(\sqrt[l]{a})^l = a$, we have

$$l \, \mathrm{ord}_\mathfrak{P}(\sqrt[l]{a}) = \mathrm{ord}_\mathfrak{P}(a) = e(\mathfrak{P}/\mathfrak{p}) \, \mathrm{ord}_\mathfrak{p}(a) \tag{3.3}$$

Hence, $l \mid e(\mathfrak{P}/\mathfrak{p})$. Because the extension has degree l, we know $e \leq l$ so $e = l$. This means that $\mathfrak{p}$ is totally ramified. ■

Lemma 3.26 (Key Lemma)**.** Let l be a prime. Let $\mathfrak{p}$ be a prime in C_l and $(p) = \mathfrak{p} \cap \mathbb{Z}$, such that $\mathrm{ord}_\mathfrak{p}(a) = \mathrm{ord}_p(a) = 0$, $p > 2$ and $l \mid p - 1$. $\mathfrak{p}$ splits completely over L_l/C_l if and only if $x^l = a \mod \mathfrak{p}$ has a solution.

Proof. Let $O_\mathfrak{p}$ be the localization of the ring of integers of C_l away from $\mathfrak{p}$ and let $R_\mathfrak{p}$ be its integral closure over L_l. The hypothesis $\mathrm{ord}_\mathfrak{p}(a) = 0$ implies that a is a unit over $O_\mathfrak{p}$ and, as shown in the proof of Lemma 3.25, $R_\mathfrak{p} = O_\mathfrak{p}[\sqrt[l]{a}]$. Note that, by Lemma 3.25, $\mathfrak{p}$ does not ramify over L_l/C_l as $l \mid 0 = \mathrm{ord}_\mathfrak{p}(a)$. Also note that $l \mid p - 1 \implies l \mid \mathcal{N}\mathfrak{p} - 1 = |O_\mathfrak{p}/\mathfrak{p}|$. Hence, the residue field contains some primitive l-root, $\zeta_l = \zeta^{\frac{\mathcal{N}\mathfrak{p}-1}{l}}$, where ζ is the generator of $(O_\mathfrak{p}/\mathfrak{p})^*$.

The case where a is an l-th power over C_l is trivial. Discard that case, which implies $x^l - a$ is irreducible over C_l. Now, the extension $R_\mathfrak{p}/O_\mathfrak{p}$ is generated by a power basis with minimal polynomial $x^l - a$. Hence, the ramification properties of $\mathfrak{p}$ are equal to the ramification of $x^l - a \mod \mathfrak{p}$. If $\mathfrak{p}$ is totally split, $x^l - a$ splits $\mod \mathfrak{p}$, so there is at least one solution. If $x^l = a \mod \mathfrak{p}$ has one solution, as $\zeta_l \in C_l$, all the solutions are $\{\zeta_l \sqrt[l]{a}, \zeta_l^2 \sqrt[l]{a}, \dots, \zeta_l^l \sqrt[l]{a} = \sqrt[l]{a}\}$ which are all distinct $\mod \mathfrak{p}$. Hence, $\mathfrak{p}$ totally splits. ■

Second proof (using Frobenius Substitution). See [Ros02, Proposition 10.4] ■

Lemma 3.27. A prime l follows the conditions of Lemma 3.19 for $p > 2$ if and only if p is completely split over $L_l/\mathbb{Q}$.

Proof. Application of Lemmas 3.23 and 3.26. Recall that $x^l = a \mod \mathfrak{P}$ has a solution if and only if $a^{\frac{\mathcal{N}\mathfrak{P}-1}{l}} = 1 \mod \mathfrak{P}$. As $\mathfrak{p}$ splits completely, $\mathcal{N}\mathfrak{P} = \mathcal{N}\mathfrak{p}$. Also, because both sides of the identity are in $O_\mathfrak{p}/\mathfrak{p} \subseteq R_\mathfrak{p}/\mathfrak{P}$, we can lower the modulo $a^{\frac{\mathcal{N}\mathfrak{p}-1}{l}} = 1 \mod \mathfrak{p} \iff x^l = a \mod \mathfrak{p}$ is solvable. ■

Lemma 3.28. For k square free, all the primes $l_i \mid k$ follow conditions of Lemma 3.19 if and only if p is completely split over $L_k/\mathbb{Q}$. By Chebotarev's theorem, these primes p have density $\frac{1}{[L_k:\mathbb{Q}]}$.

Proof. A prime splits completely in the compositum if and only if it splits completely in each factor. Using the previous Lemmas, we obtain the desired result. ■

Theorem 3.29 (Artin's observation)**.** Let $a \in \mathbb{Z}$ not -1 nor a square and k a square free integer coprime to a. The density of primes for which there is no $l \mid k$ following the conditions of Lemma 3.19 is

$$A_k(a) = \sum_{\substack{k'|k \\ k' \geq 1}} \frac{\mu(k')}{[L_{k'} : \mathbb{Q}]} \tag{3.4}$$

where μ is the Moebius Inversion function.

Proof. By Lemma 3.28, we know the density of primes such that all $l \mid k$ follow conditions of Lemma 3.19. The Inclusion-Exclusion Principle yields the desired result. ■

Remark 3.30. Note that taking $k \to \infty$ over the primorials coprime to a, the density $A_k(a)$ counts primes where a is "close" to being a primitive root, in the sense that an l following the conditions of Lemma 3.19 would need to be very large. Hence, one might expect the limit of $A_k(a)$ to be the density of primes with a prescribed primitive root at a. This is precisely what Artin conjectured. Nonetheless, the step of taking the limit is where the difficulty in Artin's conjecture lies. This is fundamentally a question pertaining to Sieve Theory and we will continue to see this strong relation in Section 5.1.

Hence, Artin arrived at the following specific conjecture.

Definition 3.31 (Artin's constant)**.** For $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$, we define Artin's constant as

$$A(a) = \sum_{k \geq 1} \frac{\mu(k)}{[L_k : \mathbb{Q}]} \tag{3.5}$$

Conjecture 3.32 (Artin primitive root Conjecture II)**.** Given $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$, the set of P_a has Dirichlet density $A(a)$. Furthermore, $A(a) > 0$ if and only if a is not a perfect square.

Assuming this conjecture was true, one can compute the $[L_k : \mathbb{Q}]$ and show positivity without using any version of the Riemann Hypothesis. We do so in the following sections.

3.2.1 Computation of the degree

Definition 3.33 (Constants relevant in Artin's observation)**.** Let $h = \max\{h' \mid a \text{ is an } h'\text{-perfect power in } \mathbb{Z}\}$, which is well-defined as $a \notin \{-1, 0, 1\}$. Let $k = l_1 \dots l_r$ be square-free integer coprime to a and $k_a = \frac{k}{(k,h)}$. Note that k_a is the product of the prime divisors l of k such that a is not a l-th power.

Definition 3.34 (Fields relevant to Artin's Conjecture II)**.** Denote $R_k = \mathbb{Q}(\sqrt[k_a]{a})$ and $I_k = C_k \cap R_k$.

Lemma 3.35. The field $L_k = \prod_{\substack{l|k \\ \text{prime}}} \mathbb{Q}(\zeta_q, \sqrt[l]{a})$ is precisely $\mathbb{Q}(\zeta_k, \sqrt[k_a]{a})$. It is also $\mathbb{Q}(\zeta_k, \sqrt[k]{a})$.

Proof. First we prove $\mathbb{Q}(\zeta_k, \sqrt[k_a]{a}) \subseteq L_k$. Let $x_i = \frac{k}{l_i} \in \mathbb{Z}$. The $\gcd(x_1, \ldots, x_r) = 1$ and Bézout's identity gives $a_i \in \mathbb{Z}$ such that $\sum a_i x_i = 1$. Now, $\prod_{\substack{l|k \\ \text{prime}}} (\zeta_q)^{a_i} = e^{2\pi i \cdot \sum \frac{a_i}{l}} = e^{2\pi i \frac{1}{k}} = \zeta_k$. By the same method that $\sqrt[k]{a} \in L_k$. The other inclusion holds because $\zeta_q = \zeta_k^{k/l}$ and

$$\sqrt[l]{a} = \begin{cases} \in \mathbb{Q} & \text{if } l|h \\ (\sqrt[k_a]{a})^{k_a/l} & \text{otherwise} \end{cases} \tag{3.6}$$

An analogous argument proves the second expression. ■

Remark 3.36. Even though the second expression might seem more canonical, in the computation of the degree, the first expression will be more useful. This is because the extension $\mathbb{Q}(\zeta_k, \sqrt[k]{a})/\mathbb{Q}(\zeta_k)$ could be trivial if, for example, a was a k-th power in $\mathbb{Z}$. This is accounted by substituting k by k_a.

$$\begin{tikzcd}
 & L_k = \mathbb{Q}(\zeta_k, \sqrt[k_q]{a}) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
C_k = \mathbb{Q}(\zeta_k) \arrow[dr, dash] \arrow[ddr, dash, "\varphi(k)"'] & & R_k = \mathbb{Q}(\sqrt[k_a]{a}) \arrow[dl, dash] \arrow[ddl, dash, "k_a"] \\
 & I_k = \mathbb{Q}(\zeta_k) \cap \mathbb{Q}(\sqrt[k_a]{a}) \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Following the identity $[L_k : \mathbb{Q}] = [L_k : C_k][C_k : \mathbb{Q}] = [L_k : C_k]\varphi(k)$, we aim to compute $[L_k : C_k]$. When Artin proposed the conjecture, he claimed $[L_k : C_k] = k_a$. This was found to be incorrect by D. H. and E. Lehmer and corrected in a private correspondence with Artin. Independently, Hooley [Hoo67] attributes this correction to Heilbronn. The full history of this correction is delightfully exposed in the first part of [Ste03], including the original letters from the Berkeley archives.

Lemma 3.37 (Degree correction, Heilbronn)**.** Let $a = a_1 a_2^2$ be the square free decomposition of a. Then, the degree $[L_k : C_k]$ is

$$[L_k : C_k] = \begin{cases} \frac{k_a}{2} & \text{if } 2a_1 | k \text{ and } a_1 = 1 \mod 4 \\ k_a & \text{otherwise} \end{cases} \tag{3.7}$$

Proof. $C_k/\mathbb{Q}$ is Galois. A classical proposition of Galois Theory [Mil22, Proposition 3.19] concerning the Galois group of a compositum states

$$[C_k : \mathbb{Q}][R_k : \mathbb{Q}] = [L_k : \mathbb{Q}][I_k : \mathbb{Q}] \implies k_a = [L_k : C_k][I_k : \mathbb{Q}] \tag{3.8}$$

If q is a prime factor of $[I_k : \mathbb{Q}]$, then $[C_k(\sqrt[q]{a}) : C_k]$ is either 1 or q and $[C_k(\sqrt[q]{a}) : C_k] \mid [L_k : C_k] = \frac{k_a}{[I_k:Q]}$. But q does not divide $\frac{k_a}{[I_k:\mathbb{Q}]}$ as k_a is square-free and $q \mid [I_k : \mathbb{Q}]$. Hence, $[C_k(\sqrt[q]{a}) : C_k] = 1 \implies \sqrt[q]{a} \in C_k$. Lastly, because $\mathbb{Q}(\zeta_q, \sqrt[q]{a}) \subseteq C_k$, the extension $\mathbb{Q}(\zeta_q, \sqrt[q]{a})/\mathbb{Q}$ must be an Abelian extension. Hence, q can only be an even prime and $[I_k : \mathbb{Q}]$ can only be either 1 or 2. It will be 2 precisely when k is even and $\sqrt{a} \in C_k \iff \sqrt{a_1} \in C_k$.

A classical application of Gauss Sums [Neu99, Ex. 4 Chapter 1.10] proves that the only quadratic subfields in the k-th cyclotomic field are of the form

$$\mathbb{Q}\left(\sqrt{\left(\frac{-1}{D}\right) D}\right) \subseteq \mathbb{Q}(\zeta_k) \tag{3.9}$$

where $D > 1$ is a square-free odd divisor of k. Hence, we need a_1 to be an odd divisor of k and $a_1 = 1 \mod 4 \iff \left(\frac{-1}{a_1}\right) = 1$. ■

Warning 3.38. This corner case is an inconvenience in further computations. Artin's conjecture is already an interesting and open problem for any particular value of $a \in \mathbb{Z}$. For the duration of this document, we will ignore these exceptional a and refer the reader to the precise bookkeeping in other references.

3.2.2 Positivity of Artin's constant

In Artin's conjecture over $\mathbb{Q}$, we end up having a conjectured density

$$A(a) = \sum_{k\geq 1} \frac{\mu(k)e(k)}{\phi(k)k_a}, \qquad \text{where } e(k) = \begin{cases} 2 & 2a_1|k \text{ and } a_1 = 1 \mod 4 \\ 1 & \text{otherwise} \end{cases} \tag{3.10}$$

Lemma 3.39 (Euler product of $A(a)$)**.** Let $a = a_1a_2^2$ be the square-free decomposition of a, and let h be the largest integer such that a is an h-power in $\mathbb{Z}$. The following identity is true.

$$A(a) = \delta_{a_1} \prod_{q|h \text{ prime}} \left(1 - \frac{1}{q-1}\right) \prod_{q\nmid h \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) \tag{3.11}$$

where, $\delta_{a_1} = 1$ if $a_1 \neq 1 \mod 4$ and

$$\delta_{a_1} = 1 - \mu(a_1) \prod_{\substack{q|a_1 \\ q|h \\ \text{prime}}} \frac{1}{q-2} \prod_{\substack{q|a_1 \\ q\nmid h \\ \text{prime}}} \frac{1}{q(q-1)-1} \tag{3.12}$$

otherwise.

Proof. When $a_1 \neq 1 \mod 4$, note that $e(k) = 1\ \forall k$ and the function $\psi(k) = \frac{\mu(k)}{\phi(k)k_a}$ is weakly multiplicative. Hence, it has a representation as an Euler Product.

$$A(a) = \sum_{k\geq 1} \frac{\mu(k)1}{\phi(k)k_a} = \prod_{q \text{ prime}} \left(1 - \frac{1}{q_a(q-1)}\right) \tag{3.13}$$

Now, q_a is either q or 1 precisely when a is a q-th power or not, respectively. Or equivalently, precisely when $q|h$ or not, respectively.

When $a_1 = 1 \mod 4$, this computation is more cumbersome. See [Hoo67, Eq. 31-32]. ■

Lemma 3.40 (Positivity of Artin's constant)**.** Let $a \notin \{-1, 0, 1\}$. Then, $A(a) > 0$ if and only if a is not perfect square.

Proof. If a is perfect square, h would be even and the term $1 - \frac{1}{2-1} = 0$. Hence, $A(a) = 0$. For the other direction, if $A(a) = 0$, either it has a 0 factor in its product expression or it tends to 0 in the limit. Yet the infinite product is

$$\prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) > \prod_{q \text{ prime}} \left(1 - \frac{1}{q^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} > 0 \tag{3.14}$$

Hence, if $A(a) = 0$, we must have a 0 term. The only possibility is $2 \mid h \iff a$ is a perfect square. ■

4. Function Field setting

This chapter focuses on Artin's Conjecture in the Function Field setting. First, we give an exposition of the original proof of Artin's Conjecture over Function Fields by Bilharz. The original paper [Bil37] is in German, so the main source for our exposition has been the translation of Bilharz' result found in the book *Number Theory in Function Fields* by M. Rosen [Ros02, Chapter 10]. On the other hand, we present a second independent proof of the result found in 2020 by Kim-Murty [KR20; KM22] developing on ideas of Davenport and Erdos [Dav39].

The abstract of [KR20] announces that their proof is independent of the Riemann Hypothesis on Function Fields. To the best of the author's knowledge, we have found a small technical error in their paper that invalidates this claim. The proof can be fixed assuming a weaker version of R. H. The author of the present document has been unable to find a condition-less fix.

Notation 4.1 (Relevant constants and fields in Artin's Conjecture over Function Fields)**.** For the remaining of this section, $q = p^r$ is an arbitrary prime power, K is a Function Field with field of constants $\mathbb{F}_q$ and let $a \in K^*$. To study Problem 3.9 over K, we will need to study the ramification properties of primes $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ over extensions L_l/K with l a rational prime and $L_l = K(\zeta_l, \sqrt[l]{a})$. Also, for $k \in \mathbb{Z}^+$ denote $C_k = K(\zeta_k)$.

Remark 4.2. If $a \in \mathbb{F}_q^* \subseteq K^*$, then $\operatorname{ord}_{K^*}(a) \mid q$, hence a can only be a primitive root for finitely many primes. We may assume $a \in K^* \setminus \mathbb{F}_q^*$.

$$\begin{tikzcd}
E_l = K(\zeta_l, \sqrt[l]{a}) \arrow[r, dash] \arrow[d, dash] & \mathcal{O}_{E_l} \arrow[dd, dash] & & \\
C_l = K(\zeta_l) \arrow[d, dash] & & \mathfrak{p} \arrow[dd, dash] & \\
a \in K \arrow[dd, dash] & \mathcal{O}_K \arrow[l, hook'] \arrow[ur, dashed, hook] \arrow[rr, two heads] \arrow[dd, dash] & & \mathcal{O}_K/\mathfrak{p} = \mathbb{F}_{q^{f_\mathfrak{p}}} \arrow[dd, dash] \\
& & x - c & \\
\mathbb{F}_q(x) & \mathbb{F}_q[x] \arrow[l, hook'] \arrow[ur, dashed, hook] \arrow[rr, two heads] & & \mathbb{F}_q[x]/(x-c) = \mathbb{F}_q
\end{tikzcd}$$

Remark 4.3. Note that we define the rings of integers of a Function Field as the integral closure of $\mathbb{F}_q[x]$. As discussed in [Neu99, Chapter 1.14], this decision is somewhat arbitrary and, for example, we could choose to center over $\mathbb{F}_q[1/x]$. Nonetheless, for Artin's Conjecture this makes no difference, as it only changes the behavior of the finitely many primes at infinity.

4.1 Bilharz' Theorem

An analogue of Artin's observation, presented in Section 3.2, can be given for general Global Fields, as will be discussed in Section 6.1. From this starting point, formalized by Theorem 4.6, Bilharz [Bil37] gave an argument to justify the *step to the limit* in the Function Field setting. This final step in his argument is remarkably ad-hoc and only valid for Function Fields. For the advancement of the conjecture over Number Fields, Hooley [Hoo67] was able to replace this ad-hoc argument by a more general solution, reducing the conjecture to problem of counting primes.

As discussed in Section 3.2.1, Artin's original conjecture had a small flaw in the density formula that came from a miss-computation of the degree $L_l/\mathbb{Q}$ for some values of a. Bilharz' proof contains a similar overlook but, in the Function Field case, the correction error doesn't appear. In the translation and exposition of Bilharz' result in M. Rosen's book [Ros02], this error is patched by assuming that the value of the prescribed primitive root a is a Geometric Element of K, as defined bellow. In the present document, we show that this condition is not necessary.

Definition 4.4 (Geometric Element)**.** Let K be a Function Field with constant field $\mathbb{F}_q$. An element $a \in K$ is said to be geometric at a prime $l \in \mathbb{Z}$ if and only if the integral closure of $\mathbb{F}_q$ over $K(\sqrt[l]{a})$ is $\mathbb{F}_q$, or, in order words, if $K(\sqrt[l]{a})/K$ is a geometric extension. An $a \in K$ is a Geometric Element if it is geometric at all primes.

Lemma 4.5. *$a \in K$ is a primitive root modulo $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ if and only if there is no $l \in \mathbb{Z}$ prime that follows both*

$$(1) \quad l \mid \mathcal{N}\mathfrak{p} - 1 \qquad \text{and} \qquad (2) \quad a^{\frac{\mathcal{N}\mathfrak{p}-1}{l}} = 1 \mod \mathfrak{p}$$

We can assume $l \neq p = \operatorname{char} K$ as condition 1 is never true for $l = p$.

Theorem 4.6 (Artin's observation for Function Fields)**.** *Let $a \in K$, and k square-free and $p = \operatorname{char}(K) \nmid k$. The density of primes such that there is no $l \mid k$ that follows conditions of Lemma 4.5 is*

$$A_k(a) = \sum_{k' \mid k} \frac{\mu(k')}{[L_{k'} : \mathbb{Q}]} \tag{4.1}$$

4.1.1 Computation of the degree

Definition 4.7. Given $k \in \mathbb{Z}$ square free $p \nmid k$, let $f(k) = \operatorname{ord}_{(\mathbb{Z}/k\mathbb{Z})^\times}(q)$, where $\mathbb{F}_q$ is the field of constants of K. This is well-defined as $(q, k) = (p^r, k) = 1$. Analogous to Definition 3.33, we denote k_a the product of all $l \mid k$ primes such that a is not an l-th power in K.

Lemma 4.8. *The extension $K(\zeta_k)/K$ is Galois and has degree $[K(\zeta_k) : K] = f(k)$.*

Proof. Notice that $K(\zeta_k) = K \cdot \mathbb{F}_q(\zeta_k)$. On one hand, $\mathbb{F}_q(\zeta_k)/\mathbb{F}_q$ is a finite field extension, so it is Galois and has a Galois group generated by $\phi_q : x \mapsto x^q$. Hence it has degree $[\mathbb{F}_q(\zeta_k) : \mathbb{F}_q] = f(k)$. On the other hand $\mathbb{F}_q(\zeta_k) \cap K = \mathbb{F}_q$ as we have chosen q such that $\mathbb{F}_q$ is the field of constants of K. A classical proposition of Galois Theory [Mil22, Proposition 3.19] concerning the Galois group of a compositum states that, with the given conditions, $K(\zeta_k)/K$ is Galois and its Galois group is isomorphic to $\mathrm{Gal}(\mathbb{F}_q(\zeta_k)/\mathbb{F}_q)$. This concludes $[K(\zeta_k) : K] = f(l)$. ∎

Lemma 4.9. If $a \in K^* \setminus (K^*)^2, a \notin \mathbb{F}_q$ is a non-constant non-square element, then a is a 2-geometric element of K. Namely, the extension $K(\sqrt{a})/K$ is geometric.

Proof. If a is not geometric at $l = 2$, then the extension $K(\sqrt{a})/K$ must be exactly $K \cdot \mathbb{F}_{q^2}/K$ as it is of degree 2 and must extend the constants. Nonetheless, if $a \in K^* \setminus (K^*)^2$, the extension $K(\sqrt{a})/K$ ramifies at $\mathfrak{p} \mid a$ but $K \cdot \mathbb{F}_{q^2}/K$ doesn't ramify anywhere. ∎

Lemma 4.10. If $a \in K^* \setminus (K^*)^2, a \notin \mathbb{F}_q$ is a non-constant non-square element, the degree $[L_k : K(\zeta_k)] = k_a$, where $L_k = K(\zeta_k, \sqrt[k]{a}) \underset{\text{Lemma 3.35}}{=} K(\zeta_k, \sqrt[k_a]{a})$.

Proof. Following the argument of Lemma 3.37, it is sufficient to see that $I_k := K(\sqrt[k_a]{a}) \cap K(\zeta_k)$ is $I_k = K$. Suppose not, then for some $l \mid k$, $K(\sqrt[l]{a}) \subseteq K(\zeta_k)$. If $l \neq 2$, we find a non-abelian extension $K(\zeta_l, \sqrt[l]{a})/K$ embedded in an abelian one $K(\zeta_k)/K$, which is a contradiction.

For $l = 2$, Lemma 4.9 shows that $a \in K$ is a Geometric Element at $l = 2$. A subextension of a constant extension must also be constant extension, which implies that the field of constants of $K(\sqrt{a})$ is $\mathbb{F}_{q^2}$. This precisely contracts the geometric condition. ∎

4.1.2 Bilharz' contribution

Notation 4.11. Let $\mathbb{P} = \{p_1 = 2, p_2 = 3, \ldots\}$ be the usual enumeration of the rational primes. Let $\mathrm{Pr}_n = \prod_{i \leq n} p_i$ be the n-th primorial.

To match our notation with the source [Ros02, Ch.10] we define $\mathcal{M}_k(a) := P_{\mathrm{Pr}_k}(a)$ and $\mathcal{M}(a) = P(a)$. The value a will remain constant throughout the section, so we drop the parenthesis and use $\mathcal{M}_k$ and $\mathcal{M}$.

The remaining step in Artin's conjecture is to relate the family $\mathcal{M}_k$ with the set $\mathcal{M}$.

$$\mathcal{M}_k = \{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K \mid \nexists\, l \leq k \text{ prime following the conditions of Lemma 4.5}\}$$

$$\begin{aligned}\mathcal{M} &= \{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K \mid a \text{ is a primitive root} \mod \mathfrak{p}\} = \\ &= \{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K \mid \nexists\, l \text{ prime following the conditions of Lemma 4.5}\}\end{aligned}$$

From Artin's observation, we compute the density $\delta(\mathcal{M}_k)$ as the finite sum found in Theorem 4.6. We aim to prove that the density of $\mathcal{M}$ is $\delta(\mathcal{M}) := \lim_k \delta(\mathcal{M}_k)$.

Remark 4.12. This is not trivial as the Dirichlet measure is not well-behaved with respect to infinite intersection of sets. For example, note that for $S_n = \{p \text{ prime} \mid p \geq n\}$, we have $0 = \delta(\cap_n S_n) \neq \lim_n \delta(S_n) = 1$. Weinberger [Wei72] found an example close to Artin's conjecture where this equality also fails.

We begin by introducing two preliminary theorems without proof.

Theorem 4.13 (Romanoff)**.** Let $q \in \mathbb{Z}_{>1}$ be a prime power, $m \in Z$ with $(q, m) = 1$ and $f(m) = \operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times}(q)$ which is well-defined as $(q, m) = 1$. Then the following sum converges.

$$\sum_{\substack{m \in \mathbb{Z}_{>0} \\ m \text{ square-free} \\ (m,q)=1}} \frac{1}{m \cdot f(m)} \tag{4.2}$$

Proof. See [Ros02, Theorem 10.8] ■

Lemma 4.14 (Upper bound on genus of L_l)**.** Let g_l be the genus of the field L_l. There exist constants $A, B \in \mathbb{R}$, $A > 0$ such that $\forall l$ prime $g_{L_l} = Al + B$. This implies there are $A_1, A_2 \in \mathbb{R}^+$ such that $\forall l$ prime, $A_1 l < g_l < A_2 l$.

Proof. Application of Riemann-Hurwitz Identity. See [Ros02, Proposition 10.4] ■

The next step of the proof uses a finer version of Chebotarev Theorem to upper bound the function $\delta(\mathcal{M}_n, s) - \delta(\mathcal{M}, s)$. Following Artin's observation, we can give the following properties of the sets $\mathcal{M}_n$ and $\mathcal{M}$.

Observation 4.15. The sets $\mathcal{M}_n$ and $\mathcal{M}$ follow

1. $\mathcal{M} \subseteq \mathcal{M}_m \subseteq \mathcal{M}_n$ for all $m > n$
2. $\cap_{n\geq 1}\mathcal{M}_n = \mathcal{M}$
3. $\mathcal{M}_n \setminus \mathcal{M} \subseteq \cup_{i\geq n+1} \operatorname{Spl}(L_{l_i})$

For $s \in \mathbb{R}$, these properties translate to Dirichlet Densities as

1. $\delta(\mathcal{M}, s) \leq \delta(\mathcal{M}_m, s) \leq \delta(\mathcal{M}_n, s)$ for all $m > n$
2. $\lim_n \delta(\mathcal{M}_n, s)$ exists and is $\geq \delta(\mathcal{M}, s)$.
3. $\delta(\mathcal{M}_n, s) - \delta(\mathcal{M}, s) \leq \sum_{i\geq n+1} \delta(\operatorname{Spl}(L_{l_i}), s)$

Lemma 4.16 (Fine version of Chebotarev's Theorem)**.** If L/K is Galois, and $s \in R$

$$\delta(\operatorname{Spl}(L), s) < \frac{1}{[L:K]} \frac{\log \zeta_L(s)}{\log \zeta_K(s)} \tag{4.3}$$

Proof. The classical proof of Chebotarev's Theorem 2.18 shows this finer result, before taking the limit $s \to 1$. ■

Lemma 4.17 (Main Lemma for Theorem 4.20)**.** There exists a real number $s_1 > 1$ such that

$$\sum_{i\geq 1} \frac{1}{[L_{l_i}:K]} \frac{\log \zeta_{L_{l_i}}(s)}{\log \zeta_K(s)} \tag{4.4}$$

converges uniformly on the interval $(1, s_1)$.

Proof. For a geometric, $[L_l : K] = lf(l)$ for all but a finite amount of l. Hence, it suffices to prove

$$\sum_{\substack{l \text{ prime} \\ l\neq p \\ l\nmid h}} \frac{1}{lf(l)} \frac{\log \zeta_{L_l}(s)}{\log \zeta_K(s)} \tag{4.5}$$

is uniformly convergent in an interval $(1, s_1)$.

A classical theorem of Function Field extensions [Ros02, Theorem 3.5] states

$$\zeta_{L_l}(s) = \zeta_{R_l}(s) P_{L_l}(s) \tag{4.6}$$

where $P_{L_l}(s)$ is a polynomial in $q^{-f(l)s}$ of degree $2g_l$, where g_l is the genus of L_l. Substituting back, the sum in Equation 4.5 splits in two parts. It is sufficient to see that these two terms uniformly converge.

First we bound the ζ_{R_l} term. Note that the zeta function of a cyclotomic field has a closed formula

$$\zeta_{R_l}(s) = \frac{1}{(1-q^{-f(l)s})(1-q^{f(l)(1-s)})} \leq \frac{1}{(1-q^{-s})(1-q^{1-s})} = \zeta_R(s) \tag{4.7}$$

Hence, the term is bounded as follows. Note that order 1 pole in each ζ cancels out and the sum converges by Romanoff result 4.13.

$$\sum_{\substack{l \text{ prime} \\ l \neq p \\ l \nmid h}} \frac{1}{lf(l)} \frac{\log \zeta_{R_l}(s)}{\log \zeta_K(s)} \leq \frac{\log \zeta_R(s)}{\log \zeta_K(s)} \sum_{\substack{l \text{ prime} \\ l \neq p \\ l \nmid h}} \frac{1}{lf(l)} \tag{4.8}$$

Now we turn to the P_{L_l} term. If one writes the monomial factorization of P as

$$P_{L_l}(s) = \prod_{j=1}^{2g_l} \left(1 - \pi_j q^{-f(l)s}\right) \tag{4.9}$$

the Riemann Hypothesis on the Function Field L_l states that the π_j have absolute value $q^{f(l)/2}$. This, together with Lemma 4.14, gives the following bounds.

$$2A_1 l \log\left(1 - q^{-\frac{f(l)}{2}}\right) < \log P_{L_l}(s) < 2A_2 l \log\left(1 + q^{-\frac{f(l)}{2}}\right) \tag{4.10}$$

Using that for $x > 0$, $\log(1+x) < x$ and $-\log(1-x) = \sum_{k\geq 1} \frac{x^k}{k} < \sum_{k \geq 1} x^k = \frac{x}{1+x}$ and letting $r = \max(A_1, A_2)$, we conclude

$$\left|\log(P_{L_l}(s))\right| < rl \frac{\sqrt{q}}{\sqrt{q}-1} q^{-\frac{f(l)}{2}} \tag{4.11}$$

Because $|\log \zeta_K(s)|$ has a pole at 1, $\frac{1}{|\log \zeta_K(s)|} < C$ for s close to 1. Hence,

$$\sum_{l \neq p} \frac{|\log \zeta_{P_{L_l}}(s)|}{|\log \zeta_K(s)|} < rlC \frac{\sqrt{q}}{\sqrt{q}-1} \sum_{l \neq p} \frac{1}{f(l) q^{f(l)/2}} \tag{4.12}$$

■

Lemma 4.18. The sum $\sum_{l \neq p} \frac{1}{f(l) q^{f(l)/2}}$ converges

Proof. Separate the sum in two parts, regarding if $l \leq q^{f(l)/2}$ or not. The first term is now convergent by Romanoff's result 4.13.

$$\sum_{\substack{l \neq p \\ l \leq q^{f(l)/2}}} \frac{1}{f(l) q^{f(l)/2}} < \sum_{\substack{l \neq p \\ l \leq q^{f(l)/2}}} \frac{1}{f(l) l} \tag{4.13}$$

For the second term, we may use a sieving method. For a given $f \in \mathbb{Z}^+$, we can estimate how many primes $l > q^{f/2}$ will have $f(l) = f$. All such l will be prime divisors of $q^f - 1$, and since $l_1 l_2 > (q^{f/2})^2 > q^f - 1$, there can be at most 1. Hence

$$\sum_{\substack{l \neq p \\ l > q^{f(l)/2}}} \frac{1}{f(l) q^{f(l)/2}} < \sum_{f=1}^{\infty} \frac{1}{f q^{f/2}} = -\log(1 - q^{1/2}) < \infty \tag{4.14}$$

■

Remark 4.19. Note that the full Riemann Hypothesis is not needed for this result. A $\mathrm{Re}(z) > 1 - \epsilon$ zero-free region is enough as

$$\sum_{f=1}^{\infty} \frac{1}{f q^{(1-\epsilon) f}} = -\log(1 - q^{1-\epsilon}) < \infty \tag{4.15}$$

Theorem 4.20 (Bilharz)**.** Let K be a Function Field with field of constants $\mathbb{F}_q$. Let $a \in K$ an arbitrary element Geometric at $l = 2$. The Dirichlet density of the set $\mathcal{M}_a$ is

$$\delta(\mathcal{M}_a) = \sum_{\substack{k \geq 1 \\ p \nmid k}} \frac{\mu(k)}{[L_k : K]} = \sum_{\substack{k \geq 1 \\ p \nmid k}} \frac{\mu(k)}{k_a f(k)} \tag{4.16}$$

This sum converges by Theorem 4.13.

Proof. By Property 3 of Observation 4.15 and Lemma 4.16

$$0 \leq \delta(\mathcal{M}_n, s) - \delta(\mathcal{M}, s) \underset{4.15}{\leq} \sum_{i \geq n+1} \delta(\{L_{l_i}\}, s) \underset{4.16}{<} \sum_{i \geq n+1} \frac{1}{[L_{l_i} : K]} \frac{\log \zeta_{L_{l_i}}(s)}{\log \zeta_K(s)} \tag{4.17}$$

Fixing $s < s_1$, by Lemma 4.17, the right-hand side converges to 0 as $n \to \infty$. By a classical Lemma of Uniform Convergence [Ros02, Lemma 10.2], the limits $n \to \infty$ and $s \to 1$ can be swapped, which concludes

$$\delta(\mathcal{M}) = \lim_{n \to \infty} \delta(\mathcal{M}_n) \tag{4.18}$$

as desired. ■

4.1.3 Positivity conditions

In the previous section, we have concluded that when $a \in K$ is a Geometric Element at $l = 2$, then Artin's constant for the Function Field K is

$$\delta(\mathcal{M}) = \sum_{\substack{k \geq 1 \\ p \nmid k}} \frac{\mu(k)}{f(k) k_a} \tag{4.19}$$

Note that $f(k)$ is weakly multiplicative. If a, b are coprime integers, $f(ab) = \mathrm{ord}_{\mathbb{Z}/ab\mathbb{Z}}(q) = \mathrm{ord}_{\mathbb{Z}/a\mathbb{Z}}(q) \cdot \mathrm{ord}_{\mathbb{Z}/b\mathbb{Z}}(q) = f(a)f(b)$ by the Chinese Reminder Theorem. Hence, this series has an Euler Product.

Lemma 4.21 (Euler product)**.** Let K be a Function Field with field of constants $\mathbb{F}_q$ and $a \in K$ a Geometric Element at $l = 2$. Let S_a the finite set of primes l such that a is an l-th power. Then, Artin's Constant can be expressed as the following Euler Product.

$$\delta(\mathcal{M}) = \prod_{\substack{l \text{ prime} \\ l \in S_a}} \left(1 - \frac{1}{f(l)}\right) \prod_{\substack{l \text{ prime} \\ l \notin S_a}} \left(1 - \frac{1}{lf(l)}\right) \tag{4.20}$$

Proof. Perform the product expansion formally. Romanoff's Theorem 4.13 shows convergence. ■

Theorem 4.22 (Positivity conditions)**.** Let K be a Function Field with field of constants $\mathbb{F}_q$ and $a \in K$ a Geometric Element at $l = 2$. Then a follows Artin's Conjecture on K if and only if a is not an l-th power for a prime l with $f(l) = 1$. In order words, for a prime l such that $l \mid q - 1$.

Proof. If a is an l-th power with $l \mid q - 1$ then there is a 0-factor, so $\delta(\mathcal{M}) = 0$. For the other direction, if $\delta(\mathcal{M}) = 0$ it can either have a 0-factor or it can tend to 0 in the limit. If it has a 0-factor, it must be for some $l \in S_a$ with

$$1 - \frac{1}{f(l)} = 0 \implies f(l) = 1 \tag{4.21}$$

On the other hand, the infinite part of the product can be lower bounded using that $\log(1 - x) > -x$ for $0 < x \leq \frac{1}{2}$.

$$\prod_{l \text{ prime}} \left(1 - \frac{1}{lf(l)}\right) = \exp\left(\sum_{l \text{ prime}} \log\left(1 - \frac{1}{lf(l)}\right)\right) > \exp\left(\sum_{l \text{ prime}} \frac{1}{lf(l)}\right) \tag{4.22}$$

The exponent converges by Romanoff Theorem 4.13 which in turn implies that its exponential converges to a non-zero value. ■

4.2 Modern proof by Kim-Murty

The article [KR20] (and its corrigendum [KM22]) present a new proof of Theorem 4.20 only for the case of $K = \mathbb{F}_q(x)$. The paper's abstract claims that their proof doesn't depend on the Riemann Hypothesis over Function Fields, unlike the original [Bil37]. We believe that there is a small flaw in their argument that invalidates this claim.

We first give an exposition of the strategy followed by this paper. After this, we describe the technical error in their argument and how a reduced Riemann Hypothesis patches it. This proof with a reduced Riemann Hypothesis was already observed by Davenport [Dav39] without details. To this day, the author of the present document has not found a way to patch this proof without blackboxing the Riemann Hypothesis in Function Fields.

4.2.1 Proof Strategy

The paper aims to prove the conjecture by proving a series of bounds of polynomial character sums, following the next Lemma.

Lemma 4.23 (Sufficient condition)**.** Given $a(x) \in \mathbb{F}_q[x]$ monic. If there is some $c > \log_q(2)$ such that for all $n \in \mathbb{Z}_{\geq 1}$ and all non-trivial characters $\chi : \mathbb{F}_{q^n} \to \mathbb{C}$, we have

$$\left| \sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta)) \right| = o\left(\frac{q^{n\left(1 - \frac{c}{\log n}\right)}}{\log n} \right) \tag{4.23}$$

then, Artin's Conjecture holds for $a(x)$. In practice, we will try to prove that the character sum described is $\mathcal{O}(q^{nB})$ for $B < 1$.

Remark 4.24. This condition will not be necessary. We know from Theorem 4.22 that $a \in \mathbb{F}_q[x]$ will be a primitive root modulo infinitely many irreducible polynomials v if and only if a is not a d-th power for some $d \mid q - 1$.

But note that if a is a d-power for a $d \mid q^i - 1$ for any $i \geq 1$, then the character $\chi : \mathbb{F}_{q^{ni}} \to \mathbb{C}$ with $\chi(\gamma) = \zeta_{q^{ni}-1}^{(q^{ni}-1)/d}$ would make the character sum trivial for $m = ni$ arbitrarily large. Therefore, this proof will only show that a subset of the a in Theorem 4.22 follow Artin Conjecture over $\mathbb{F}_q(x)$.

In the rest of the section, we aim to give a sketch of the proof of Lemma 4.23.

Definition 4.25 (Sifting function)**.** Given a cyclic group G, define

$$\begin{aligned} S_G &: G \to \mathbb{C} \\ g &\mapsto \frac{\varphi(m)}{m}\left(1+\sum_{\substack{d\mid m\\ d>1}}\frac{\mu(d)}{\varphi(d)}\sum_{\operatorname{ord}\chi=d}\chi(g)\right) \end{aligned} \tag{4.24}$$

where φ is Euler's totient function and where the last sum runs over all group characters of order exactly d.

Remark 4.26. Note that the first term comes from the trivial character and $d = 1$. We only separate the first term as a presentation convenience, because it will be the asymptotically significant term.

Lemma 4.27. With the definition above, we have

$$S_G(g) = \begin{cases} 1, & g \text{ is a primitive root of } G \\ 0, & \text{otherwise} \end{cases} \tag{4.25}$$

Proof. Fixed a $g \in G$, the function

$$f(d) = \frac{\mu(d)}{\varphi(d)}\sum_{\substack{\chi:G\to\mathbb{C}\\ \operatorname{ord}\chi=d}}\chi(g) \tag{4.26}$$

is weakly multiplicative, so $S_G(g)$ has an Euler Product decomposition. Now, denote $G = \langle\lambda|\lambda^m = 1\rangle$ and $g = \lambda^k$, we have

$$S_G(g) = \frac{\varphi(m)}{m}\prod_{p\mid m}\left(1-\frac{1}{p-1}\sum_{\substack{\chi:G\to\mathbb{C}\\ \operatorname{ord}_G\chi=p}}\chi(g)\right) = \frac{\varphi(m)}{m}\prod_{p\mid m}\left(1-\frac{1}{p-1}\sum_{1\le i<p}\zeta_{p-1}^{ik}\right) \tag{4.27}$$

If a is not a primitive root, $(k, m) = a > 1$ and for any $p \mid a$, the p-th Euler Factor will be 0. Otherwise, $(k, m) = 1$ and each factor is

$$\sum_{1 \leq i < p} \zeta_{p-1}^{ik} = -1 \implies \Pi_p = \frac{p}{p-1} \implies = S_G(g) = 1 \tag{4.28}$$

■

Definition 4.28. Given an $a(x) \in \mathbb{F}_q[x]$ monic, define $W_a : \mathbb{F}_q[x]^{\text{irr}} \to \mathbb{Z}$,

$$W_a(v) = \begin{cases} \deg v, & a \text{ is a primitive root modulo } v \\ 0, & \text{otherwise} \end{cases} \tag{4.29}$$

We aim to count irreducible v where a is a primitive root modulo v, but we will find it easier to count them if we weight them with a multiplicity $\deg v$. This is analogous to the role that the Von Mangoldt function

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k \\ 0, & \text{otherwise} \end{cases} \tag{4.30}$$

takes in the original proof of the prime number theorem, by Hadamart and de la Vallée Poussin.

Lemma 4.29. For all $n \in \mathbb{Z}_{>0}$, the following equality holds.

$$\sum_{\substack{v \in \mathbb{F}_q[x]^{\text{monic, irr}} \\ \deg v | n}} W_a(v) = \sum_{\theta \in \mathbb{F}_{q^n}^*} S_{\mathbb{F}_{q^n}^*}(a(\theta)) \tag{4.31}$$

Proof. Let $v \in \mathbb{F}_q[x]^{\text{monic, irr}}$ with $\deg v = n$ and let $\theta_1, \ldots, \theta_n$ be the roots of v in $\mathbb{F}_{q^n}$. Then, each root gives a bijection $\mathbb{F}_q[x]/(v) \simeq \mathbb{F}_q[\theta_i] = \mathbb{F}_{q^n}$ where $a \mapsto a(\theta_i)$. Adding over all the possible v yield the desired equation. ■

Remark 4.30. Note that the definition of the sifting function and the linear sieve over primes can be effortlessly translated to Artin's problem over $\mathbb{Z}$. Nonetheless, this bijection between irreducible polynomials and their set of roots does not have an analogue over Number Fields. This greatly increases the difficulty of bounding the character sums that arise in the $\mathbb{Z}$ setting.

Lemma 4.31. The set of upper bounds described in Lemma 4.23 imply that $\sum_{\theta\in\mathbb{F}^*_{q^n}} S_{\mathbb{F}^*_{q^n}}(a(\theta))$ diverges as $n \to \infty$.

Proof. Use Definition 4.25 to fully expand the sum

$$\begin{aligned}\sum_{\theta\in\mathbb{F}_q^*} S_{\mathbb{F}^*_{q^n}}(a(\theta)) &= \sum_{\theta\in\mathbb{F}_q^*} \frac{\varphi(q^n-1)}{q^n-1}\left(1+\sum_{\substack{d\mid q^n-1\\ d>1}} \frac{\mu(d)}{\varphi(d)} \sum_{\substack{\chi:\mathbb{F}^*_{q^n}\to\mathbb{C}\\ \operatorname{ord}\chi=d}} \chi\left(a(\theta)\right)\right) = \\ &= \varphi(q^n-1) + \sum_{\substack{d\mid q^n-1\\ d>1}} \frac{\mu(d)}{\varphi(d)} \sum_{\substack{\chi:\mathbb{F}^*_{q^n}\to\mathbb{C}\\ \operatorname{ord}\chi=d}} \sum_{\theta\in\mathbb{F}_q^*} \chi\left(a(\theta)\right)\end{aligned} \tag{4.32}$$

Applying a triangular inequality and using the set of upper bounds in Lemma 4.23, the leading term is absolutely asymptotically bigger than all the other combined. Hence, the sum diverges.

$$\begin{aligned}\left|\sum_{\substack{d\mid q^n-1\\ d>1}} \frac{\mu(d)}{\varphi(d)} \sum_{\substack{\chi:\mathbb{F}^*_{q^n}\to\mathbb{C}\\ \operatorname{ord}\chi=d}} \sum_{\theta\in\mathbb{F}_q^*} \chi\left(a(\theta)\right)\right| &\leq \sum_{\substack{d\mid q^n-1\\ d>1\\ d \text{ sq-free}}} \frac{1}{\varphi(d)} \sum_{\substack{\chi:\mathbb{F}^*_{q^n}\to\mathbb{C}\\ \operatorname{ord}\chi=d}} \left|\sum_{\theta\in\mathbb{F}_q^*} \chi\left(a(\theta)\right)\right| = \\ &\underset{\text{Lemma 4.23}}{=} o\left(2^{w(q^n-1)}\frac{q^{n\left(1-\frac{c}{\log n}\right)}}{\log n}\right) = o\left(\varphi(q^n-1)\right)\end{aligned} \tag{4.33}$$

On the last step we have used that $w(N) < \frac{\log N}{\log\log N}$ and $\varphi(q^n-1) > \frac{q^n}{\log\log q^n}$. ■

4.2.2 Bound of the Polynomial Character Sums

> **Remark 4.32.** Bounding for each n independently is not enough, as we need the implicit constant to be independent on n. That's why proving the case $n = 1$ and then base changing from $\mathbb{F}_q$ to $\mathbb{F}_{q^n}$ doesn't work.

In this part of the proof, the initial paper [KR20] has an error which, a priori, is fixed in the corrigendum [KM22]. Initially, their method only works for characters of $\mathbb{F}_{q^n}$ that are lifts of characters of $\mathbb{F}_q$, meaning that $\chi : \mathbb{F}_{q^n} \to \mathbb{C}$ factorizes as $\chi = \chi' \circ \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q \to \mathbb{C}$, where $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is the norm of the field extension and χ' is a character of $\mathbb{F}_q$.

In theory, this error is corrected in the corrigendum, but we have found a flaw in the correction that we believe invalidates the proof of Artin's Conjecture. The details are described in the next section.

4.2.3 Potential error in the corrigendum [KM22]

The second page of the corrigendum [KM22] introduces the following L-function.

> **Definition 4.33.** Given a fix $a \in \mathbb{F}_q[x]$ monic of degree K and an arbitrary character of the algebraic closure $\chi : \overline{\mathbb{F}_q} \to \mathbb{C}$, define
>
> $$L(s,\chi) := \exp\left(\sum_{n\geq 1} N_n(\chi)\frac{q^{-sn}}{n}\right) \tag{4.34}$$
>
> with
>
> $$N_n(\chi) := \sum_{\theta\in\mathbb{F}_{q^n}} \chi(a(\theta)) \tag{4.35}$$

The next paragraph states that this L-function is another form of the L-function given in the original paper [KR20]. We believe the error is in this equality of L-functions.

The L-function of the original paper is defined as follows.

Definition 4.34. Given an r-tuple of characters $\chi'_i : \mathbb{F}_q \to \mathbb{C}$ and an r-tuple of monic irreducible polynomials $f_i \in \mathbb{F}_q[x]$, define

$$\begin{aligned} \widehat{\chi} : \mathbb{F}_q[x] &\to \mathbb{C} \\ g &\mapsto \prod_{i=1}^{r} \chi'_i(\ (f_i, g)\ ) \end{aligned} \tag{4.36}$$

where (f_i, g) indicates the resultant. Then, define

$$\mathcal{L}'(s, \widehat{\chi}) = \sum_{\substack{g \in \mathbb{F}_q[x] \\ \text{monic}}} \frac{\widehat{\chi}(g)}{(q^{\deg g})^s} \tag{4.37}$$

To equalize Definition 4.34 with Definition 4.33, I understand that the natural choice is to take $r = \#$irreducible factors of a, $(f_1, \ldots, f_r)$ the irreducible components of a.

Setting the $\chi'_i = \chi$ doesn't work as, to start, the χ_i should be characters of $\mathbb{F}_q$ and χ is a character of $\overline{\mathbb{F}}_q$. Even if we stretch the Definition 4.34 to include characters of $\overline{\mathbb{F}}_q$, this choice of χ_i will still not work, as I will show in a moment. For now, let's just set them all equal to each other $\chi'_i = \chi'$, letting χ' be an arbitrary character of $\mathbb{F}_q$ (possibly a character of $\overline{\mathbb{F}}_q$, if we need to stretch the definition).

Note that we have $\widehat{\chi}(g) = \chi'(\ (a, g)\ )$ as $a = \prod f_i$. We have split a into irreducible components just to match the conditions of the Definition 4.34.

Question 4.35. Is $\mathcal{L} = \mathcal{L}'$?

Taking the logarithm of the Euler product of second L-function, we get

$$\begin{aligned} \log \mathcal{L}'(s, \widehat{\chi}) &= \sum_{\substack{v \in \mathbb{F}_q[x] \\ \text{monic irreducible}}} -\log\left(1 - \frac{\widehat{\chi}(v)}{q^{\deg v s}}\right) \\ &= \sum_{\substack{v \in \mathbb{F}_q[x] \\ \text{monic irreducible}}} \sum_{k \geq 1} \frac{1}{k} \cdot \left(\frac{\widehat{\chi}(v)}{q^{\deg v s}}\right)^k \end{aligned} \tag{4.38}$$

$$\begin{aligned}
&= \sum_{m\geq 1} \sum_{\substack{v\in\mathbb{F}_q[x] \\ \text{monic irreducible} \\ \deg v = m}} \sum_{k\geq 1} \frac{1}{k} \cdot \widehat{\chi}(v)^k q^{-mk\cdot s} \\
&= \sum_{n\geq 1} \left(\sum_{m|n} \sum_{\substack{v\in\mathbb{F}_q[x] \\ \text{monic irreducible} \\ \deg v = m}} m \cdot \widehat{\chi}(v)^{n/m} \right) \frac{q^{-sn}}{n}
\end{aligned} \tag{4.39}$$

where, in the last equality, we have set $n = mk$

For this to be equal to Definition 4.33, we would need the equality of all the coefficients. Namely, $\forall n \geq 1$

$$N_n(\chi) = \sum_{\theta\in\mathbb{F}_{q^n}} \chi(a(\theta)) \overset{?}{=} \sum_{m|n} \sum_{\substack{v\in\mathbb{F}_q[x] \\ \text{monic irreducible} \\ \deg v = m}} m \cdot \chi'(\ (a,v)\ )^{n/m} \tag{4.40}$$

If $\chi = \chi' \circ N_{\mathbb{F}_q^n/\mathbb{F}_q}$, this is true. For any $v \in \mathbb{F}_q[x]$ irreducible polynomial of degree m, let $\theta_1, \ldots, \theta_m$ be its roots. Now

$$\begin{aligned}
\chi(a(\theta_1)) + \cdots + \chi(a(\theta_m)) &= \chi'(N(a(\theta_1))) + \cdots + \chi'(N(a(\theta_m))) \\
&= \sum_i \chi' \left(\left(\prod_j a(\theta_j) \right)^{n/m} \right) \\
&= m \cdot \chi' \left(\prod_i a(\theta_i) \right)^{n/m} \\
&= m \cdot \chi'(\ (a,v)\ )^{n/m}
\end{aligned} \tag{4.41}$$

Adding over all conjugation classes, we get the desired identity.

But, given an arbitrary $\chi : \overline{\mathbb{F}_q} \to \mathbb{C}$ which is not the lift of any character on the base field, there doesn't seem to be a natural choice of χ' that makes the identity true.

4.2.4 Flaw in the proof of Artin's conjecture

The equality of the two L-functions is not merely a presentation problem. It is logically used in the proof of Artin's conjecture.

Davenport [Dav39] proves that the L-function on Definition 4.34 is a polynomial. Only in the case $\chi = \chi' \circ N$ he uses this to find an equality of the character sum with an exponential sum over the zeroes of the L-function, named s_i.

$$\sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta)) = \sum q^{ns_i} \tag{4.42}$$

Because there are only finitely many characters on the base field and each L-function gives rise to finitely many zeros, one can take the $B = \max |s_i|$. Then, $B < 1$ by a result analogous to the classical argument of the proof of the Prime Number Theorem by Hadamart and de la Vallée Poussin. Hence, we have the following uniform bound for the character sums coming from lifts of base characters.

$$\left| \sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta)) \right| = \mathcal{O}(q^{nB}) \tag{4.43}$$

For the $\chi \neq \chi' \circ N$, the character sum that one needs to bound doesn't even come up as a coefficient in the L-series of Definition 4.34. It only comes up as a coefficient in the Definition 4.33, which, a priori, is not a polynomial nor does it follow an equality similar to the one found by Davenport.

4.2.5 Conditional fix

Given a $\chi : \mathbb{F}_{q^n} \to \mathbb{C}$ that is not a lift, its character sum comes up in an L-series like the one in Definition 4.34 via base change from $\mathbb{F}_q$ to $\mathbb{F}_{q'}$ with $q' = q^n$. In this case, the zeroes of this its L-series are not linked in any explicit way to the family of L-series of the base field characters, considered when defining B. Hence, the zeros of this L-function are not necessarily $\leq B$. So one would have to take $B' = \sup |s_i|$ which, a priori, can be 1.

Assuming a $1 - \epsilon$ Riemann Hypothesis, which, in Function Fields is a theorem, would be sufficient to see $B' < 1$. This looks similar to the bound given in [KR20, Theorem 4] but that upper bound isn't enough. Under base change, it gives

$$1 - \frac{c}{(K-1)\log(q^n)} = 1 - \frac{c}{n(K-1)\log q} \tag{4.44}$$

which is not enough as, when $n \to \infty$ it tends to 1.

5. Number Field Setting

This chapter focuses on Artin's conjecture over Number Fields where the problem remains open. In Section 5.1, we give an exposition of Hooley's conditional proof of Artin's Conjecture [Hoo67] over $\mathbb{Q}$. Following that, in Section 5.2, we propose a new Conjecture 5.18. This self-contained conjecture would reduce the strength of the Riemann Hypothesis assumed in Hooley's result. There is strong numerical evidence that the conjecture holds, as shown in Figure 5.1.

Before that, we can reproduce the computation of Lemma 3.40 to find the conjecture necessary condition of Artin's conjecture over Number Fields, albeit purposely ignoring the values from Warning 3.38. If one wants to include the values from Warning 3.38, the extra "entanglement" term in the Euler Product has been studied in [Ste03].

Lemma 5.1 (Necessary condition in Number Fields)**.** Given a Number Field $K/\mathbb{Q}$, let $\lambda(K)$ be the roots of unity of K and $h_{-1} = |\lambda(K)|$. Choose a generic element (namely one missing the corner case described in Warning 3.38) $a \in \mathcal{O}_K \setminus \lambda(K)$. Then, let $h_a = \max\{r \mid a = z^r \text{ for some } z \in K\}$. Artin conjecture does not hold for a if and only if

1. $\gcd(h_{-1}, h_a) \neq 1$
2. $2 \mid h_a \iff a$ is a "perfect square" on $\mathcal{O}_K$

This is summed up as a follows Artin's Conjecture if and only if $(2h_{-1}, h_a) \neq 1$.

In the classical setting, only Condition 2 can be met as $h_{-1} = 2$. Nonetheless, for general Number Fields, Condition 1 is necessary and has full meaning (namely, it is not implied by condition 2).

Proof. Ignoring the values of a for which $K(\zeta_k) \cap K(a^{1/k}) \neq K$, we have that the expression for Artin's Conjecture has an Euler Product form, as shown in 3.39. For a given square-free k, define $k_{-1} = \frac{k}{(k,h_{-1})}$ and $k_a = \frac{k}{(k,h_a)}$. Then, by the argument used in Lemma 3.37, the degree $[L_k : K] = \frac{\phi(k)}{\phi((h_{-1},k))} k_a = \phi(k_{-1}) k_a$.

For a prime l, we have

$$[L_l : K] = [K(\zeta_l, a^{1/l}) : K] = \begin{cases} 1 & l \mid h_{-1} \text{ and } l \mid h_a \\ l & l \mid h_{-1} \text{ and } l \nmid h_a \\ l-1 & l \nmid h_{-1} \text{ and } l \mid h_a \\ l(l-1) & l \nmid h_{-1} \text{ and } l \nmid h_a \end{cases} \tag{5.1}$$

And the conjecture density by Conjecture 6.10 is

$$A(a) = \prod_l \left(1 - \frac{1}{[L_l : K]}\right) \tag{5.2}$$

The tail of product converges to a non-zero value by the argument used in Lemma 3.40. Hence, for $A(a) = 0$, one of the two cases has to be met. ■

5.1 Hooley's Theorem

In his 1967 paper [Hoo67], Hooley published a conditional proof of Artin's conjecture 3.32 under the assumption that the Generalized Riemann Hypothesis holds for an explicit family of Kummer fields. His proof follows a structure classically pertaining to Sieve Theory. Namely, there will be a certain sum to be asymptotically approximated which will be separated into segments and attacked by different methods.

Hooley's proof is given for the original problem over $\mathbb{Z}$ but, as we will see in Section 6.1, it is not hard to generalize the argument for general Number Fields. Another relevant takeaway of his proof is that it reduces Artin's Conjecture to the problem of counting primes over certain Kummer Fields. The assumption of the Riemann Hypothesis is used to give an extremely fine estimate of the prime counting function.

5.1.1 Preparation

For this chapter, we return to the notations of Definition 3.33. To match the notations used in Hooley's paper [Hoo67], we introduce the following functions.

Definition 5.2 (Prime counting functions in [Hoo67])**.**

1. $R_a(q,p) = \begin{cases} 1 & q \text{ follows Lemma 3.19} \\ 0 & \text{otherwise} \end{cases}$
2. $N_a(x) = \#\{p < x \mid a \text{ is a primitive root } \mod p\}$
3. $N_a(x,\xi) = \#\{p < x \mid \nexists\, q \text{ following Lemma 3.19 in the range } q < \xi\}$
4. $M_a(x,\xi_1,\xi_2) = \#\{p < x \mid \exists\, q \text{ following Lemma 3.19 in the range } \xi_1 < q \leq \xi\}$
5. $P_a(x,k) = \#\{p < x \mid \forall q | k, q \text{ follows Lemma 3.19}\}$

Lemma 5.3 (Basic observations of the newly defined functions)**.**

1. $N_a(x) = N_a(x, x-1)$
2. $N_a(x) \leq N_a(x,\xi)$
3. $N_a(x) \geq N_a(x,\xi) - M_a(x,\xi,x-1)$
4. $M_a(x,\xi_1,\xi_2) \leq \sum_{\xi_1 < q \leq \xi_2} P_a(x,q)$

Lemma 5.4. $N_a(x,\xi) = \sum_{l'} \mu(l') P_a(x,l')$, where the sum is over all l' square free with factors $\leq \xi$. Note that

$$l' \leq \prod_{q \leq \xi} q = e^{\sum_{q\leq\xi} \log q} \leq e^{2\xi} \tag{5.3}$$

where in the last inequality we have used the prime number theorem.

Lemma 5.5. Let $\xi_1 = \frac{1}{6}\log x, \xi_2 = x^{1/2}\log^{-2} x, \xi_3 = x^{1/2}\log x$. From the previous observations, we get

$$\begin{aligned} N_a(x) = N_a(x,\xi_1) + O(M_a(x,\xi_1,\xi_2)) + \\ + O(M_a(x,\xi_2,\xi_3)) + O(M_a(x,\xi_3,x-1)) \end{aligned} \tag{5.4}$$

Hooley proves that the first is the leading term, being $\sim A(a)\frac{x}{\log x}$ for an explicit constant $A(a)$. Moreover, he proves that, the other 3 terms will be asymptotically smaller, upper bounded by $O\left(\frac{x}{\log^2 x}\right)$. This concludes that $N_a(x) \sim A(a)\frac{x}{\log x}$, which is precisely Artin's conjecture. The choice of ξ_i is taken carefully to fulfill the estimates.

The bounds of terms 3 and 4 use elementary techniques. For terms 1 and 2, the Riemann Hypothesis is needed. As we will detail in the following section, the estimation of term 1 only needs the 2/3-zero free region but the upper bounding of term 2 will need the full 1/2 Riemann Hypothesis. The Conjecture 5.18 that we propose gives an equally good bound for term 2 using less strength of the Riemann Hypothesis We do so by improving the bound on term 4, which makes it possible to choose a lower ξ_3, which at its turn makes it possible to choose lower ξ_2 without disrupting the bound of term 3. Having a lower ξ_2 gives the possibility of conserving the bound of the second term but using less strength of the Riemann Hypothesis.

The estimation of the first term still needs the 2/3 Riemann Hypothesis, so the best this possible improvement can hope to do is lower the conditions, but not give a condition-less proof.

5.1.2 Bounds on the 3rd and 4th term

Lemma 5.6 (Bound of the 4th term)**.** Let $\xi_3 = x^{1/2}\log x$, then

$$M_a(x, \xi_3, x-1) = O\left(\frac{x}{\log^2 x}\right) \tag{5.5}$$

Proof. If q follows Lemma 3.19, in particular $a^{\frac{p-1}{q}} = 1 \mod p$. Hence, if there is a $q > \xi_3$ that follows the Lemma, there will be an $m < \frac{x}{\xi_3}$ such that $p|a^m - 1$. All the primes counted on $M_a(x, \xi_3, x-1)$ need to be divisors of

$$S_a(x/\xi_3) \coloneqq \prod_{m<x/\xi_3} (a^m - 1) \tag{5.6}$$

Hence, $2^{M_a(x,\xi_3,x-1)} < S_a(x/\xi_3)$ which implies $M_a(x, \xi_3, x-1) < \log S_a(x/\xi_3) < \log a \sum_{m<x/\xi_3} m = O\left((x/\xi_3)^2\right) = O\left(\frac{x}{\log^2 x}\right)$. ■

Remark 5.7. One is forced to choose $\xi_3 = x^{1/2}\log x$ for the last equality to be true. Yet, in this document we conjecture a refined upper bound for the number of primes diving $S_a(n) = \prod_{m<n}(a^m - 1)$. Using our conjecture, one will be able to choose a lower ξ_3.

Lemma 5.8 (Bound of the 3rd term)**.** Let $\xi_2 = x^{1/2}\log^{-2} x$ and $\xi_3 = x^{1/2}\log x$. Then $M_a(x, \xi_2, \xi_3) = O\left(\frac{x}{\log^2 x}\right)$.

Proof. By Lemma 5.3, we may express $M_a(x, \xi_2, \xi_3) \leq \sum_{\xi_2 < q \leq \xi_3} P_a(x, q)$.

Now, if q follows Lemma 3.19, then in particular $p \equiv 1 \mod q$. By Brun's method, which is an inequality related to Dirichlet's Theorem, we have

$$P_a(x, q) \leq \sum_{\substack{p \leq x \\ p \equiv 1 \mod q}} 1 \leq \frac{A_1 x}{(q-1)\log(x/q)} \tag{5.7}$$

From this we obtain the bound

$$\begin{aligned} M_a(x, \xi_2, \xi_3) &= O\left(\frac{x}{\log x} \sum_{\xi_2 < q \leq \xi_3} \frac{1}{q}\right) = \\ &= O\left(\frac{x}{\log^2 x}\left(\log \frac{\xi_3}{\xi_2} + O(1)\right)\right) = O\left(\frac{x \log\log x}{\log^2 x}\right) \end{aligned} \tag{5.8}$$

■

Remark 5.9. This lemma forces to choose the polynomial degree of ξ_2 to be the same as ξ_3, a priori $1/2$. Yet a key takeaway from this lemma is that the bound only depends on the ratio ξ_3/ξ_2. If we manage to lower ξ_3, we can automatically lower ξ_2 without disturbing this bound.

5.1.3 Reduction to counting primes

Using basic facts of Ramification Theory, the following lemmas link the prime counting function over certain Kummer Fields to the sums we are interested in estimating

Definition 5.10 (Prime counting function)**.** For $k \in \mathbb{Z}_{>0}^{\text{square-free}}$, let $L_k = \mathbb{Q}(\sqrt[ka]{a}, \zeta_k)$ the Kummer Field relevant in Artin's conjecture and $n(k) = [L_k : \mathbb{Q}]$. Then, define

$$\pi(x,k) \coloneqq \#\{\mathfrak{p} \text{ prime ideal of } L_k \mid \mathcal{N}\mathfrak{p} \leq x\} \tag{5.9}$$

Lemma 5.11.

$$n(k)P_a(x,k) = \pi(x,k) + O(n(k)w(k)) + O(n(k)x^{1/2}) \tag{5.10}$$

Proof. This is a Corollary of Theorem 2.11. ■

5.1.4 Prime counting theorem

By Lemma 5.11, an estimate of $\pi(x,k)$ will give an estimate of $P_a(x,k)$ and which in turn will give an estimate of the first and second term in Equation 5.4, by Lemmas 5.3 and 5.4. The final part of Hooley's article deduces a good enough prime counting theorem.

Theorem 5.12. Assuming the Generalized Riemann Hypothesis for ζ_{L_k}, we have the estimate

$$\pi(x,k) = \frac{x}{\log x} + O(n(k)x^{1/2}\log kx) \tag{5.11}$$

Sketch of the proof. Hooley starts from the classical idea that π can be expressed in terms of the zeroes of ζ_{L_k}. He deduces a theorem about the vertical distribution of zeroes and, together with the assumption that the zeroes are in the 1/2 line, he is able to deduce the desired bound.

The key Lemma in Hooley's paper is the result on the vertical distribution of the Riemann zeros under the Generalized Riemann Hypothesis[Hoo67, Page 215-216]. [1] ■

[1] The proof of this Lemma is too technical for the present author to be able to give an exposition that is any better than the original. We have hence chosen not to include it in the text.

Remark 5.13. If you follow Hooley's proof only assuming the zero-free region $Re(s) > f$, you get the estimate

$$\pi(x,k) = \frac{x}{\log x} + O(n(k)x^f \log kx) \tag{5.12}$$

From the rest of the Section, f will note the value up to which the Riemann Hypothesis is assumed.

5.1.5 Bounds for the 1st and 2nd term

By Lemma 5.11, one gets an estimate of P_a and unrolling Lemmas 5.3 and 5.4 one gets estimates of the first and second term in Equation 5.4. They are explained in the following lemmas.

Lemma 5.14 (Estimation of the 1st term)**.**

$$\begin{aligned} N_a(x,\xi_1) = \sum_{l'} \mu(l') \left(\frac{x}{\log x \cdot n(l')} + O(x^f \log x)\right) = \\ \underset{l'<e^{2\xi_1} \text{by Prop. } 5.4}{=} \frac{x}{\log x} \sum_{l'} \frac{\mu(l')}{n(l')} + O\left(\sum_{l<e^{2\xi_1}} x^f \log x\right) = \\ = A(a)\frac{x}{\log x} + O(e^{2\xi_1} x^f \log x) = \\ = A(a)\frac{x}{\log x} + O(x^{f+1/3} \log x) \end{aligned} \tag{5.13}$$

Remark 5.15. Very significantly, note that for the extra term to be irrelevant, we only need f to be $f < 2/3$. For this, it is sufficient to assume an $R(s) \geq 2/3$ zero-free region.

Lemma 5.16 (Bound of the 2nd term)**.**

$$
\begin{aligned}
M_a(x,\xi_2,\xi_3) \leq \sum_{\xi_1<q\leq\xi_2}\left(\frac{x}{\log x\cdot q(q-1)}+O(x^f\log x)\right) = \\
= O\left(\frac{x}{\log x}\sum_{q>\xi_2}\frac{1}{q^2}\right)+O\left(x^f\log x\sum_{q\leq\xi_2}1\right) = \qquad (5.14)\\
= O\left(\frac{x}{\xi_1\log x}\right)+O\left(\frac{x^f\xi_2\log x}{\log\xi_2}\right) = O\left(\frac{x}{\log^2 x}\right)
\end{aligned}
$$

Remark 5.17. Note that in the last equality we did need $f = 1/2$ because $\xi_2 = x^{1/2}\log^{-2} x$. If we manage to lower the polynomial degree of ξ_2, we would be able to conserve the bound using a higher f, hence reducing the conditions in Hooley's proof.

5.2 Proposed improvement

We propose the following self-contained conjecture.

Conjecture 5.18. Let $S_a(n) \coloneqq \prod_{m<n}(a^m-1)$. Let $w(N) = \#\{\text{distinct primes } p|N\}$. Is it true that $w(S_a(n)) = O(n\cdot\text{poly-log})$?

We claim that this would reduce the conditions on Hooley's conditional proof from the full R. H. to an $R(s)\geq 2/3$ zero free region. The weaker conjecture $w(S_a(n)) = O(n^{2-\epsilon}\cdot\text{poly-log})$ for $\epsilon>0$ would already improve the conditions to an $R(s)\geq 1/2+\epsilon/3$ zero-free region.

The conjecture can be reformulated as follows. Note that it is asking a similar question to the original Artin's conjecture but instead of asking for the density of primes with high $\text{ord}_p(a) = p-1$ it asks for primes with low $\text{ord}_p(a)$.

Conjecture 5.19. Let $P(n) = \#\{p \text{ prime} \mid \text{ord}_p(a) < n\}$, is $P(n) = O(n\cdot$ poly-log$)$?

Remark 5.20. For the application on Artin's Conjecture, the value of a can be asked to be a non-square. Yet, numerical evidence in Figure 5.1 seems to imply that the conjecture is true regardless. This doesn't contradict the necessary condition in Artin's Conjecture as a being a non-square is still necessary for Artin's observation.

Remark 5.21. The polylogarithmic part will take no paper in the application to Artin's Conjecture, can be taken as large as one wants.

Remark 5.22. Note that, following the factorization $a^m - 1 = \prod_{d|m} \Phi_d(a)$, the conjecture is very related to the values of $w(\Phi_d(a))$, where Φ_d is the d-th cyclotomic polynomial. There seems to be a conjecture by Erdós [MS19] on $P(\Phi(a))$, the largest prime divisor which has a very similar flavor.

5.2.1 Upper bound $w(S_a(n)) = O(n^2)$

It is not hard to prove $w(S_a(n)) = O(n^2)$. For example, $2^{w(S_a(n))} < S_a(n)$, from which the desired bound follows. This bound can be improved by logarithmic factors in a number of ways. For instance using the well-known bound $w(N) = O\left(\frac{\log N}{\log\log N}\right)$, which can be proven by looking at $N = \prod_{p<n} p$ the primorials.

5.2.2 Lower bound $w(S_a(n)) = \Omega(n)$

A trivial application of Zsigmondy's theorem[Zsi92] shows $w(S_a(n)) = \Omega(n)$.

5.2.3 Numerical evidence

We believe that the strong conjecture is true. Numerical evidence is shown in Figure 5.1, for $a = 2$.

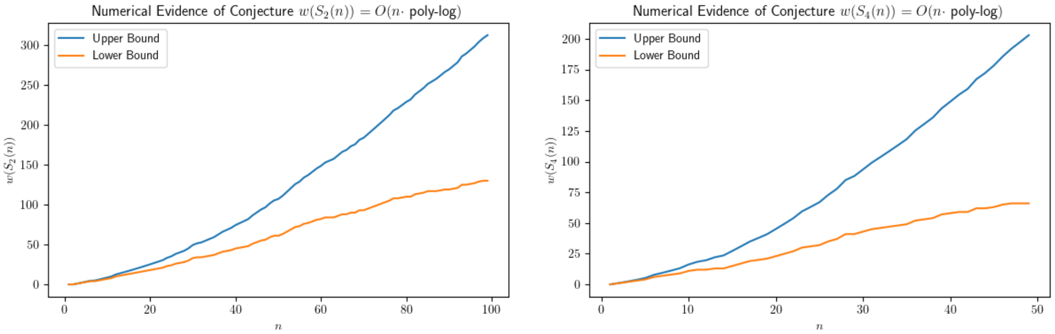

Figure 5.1: Numerical Evidence of Conjecture 5.18. The lower bound w' is the number of distinct primes in $S_2(n)$ in the range $< 10^8$. The upper bound has an extra correction term of $\frac{n(n-1)}{2}\log_{10^8}(2)$ which over counts the number of primes that $S_2(n)$ can have on the range $\geq 10^8$.

The limitation of these numerical computations is the number of primes can be saved in a computer in practice. The current program, found in the Appendix, checks for primes up to $L = 10^8$ through an Eratosthenes Sieve. Yet $S_2(n)$ grows very quickly so, a priori, it could start having prime factors larger than our range. We can only give an exact value of $w(S_a(n))$ for n relatively small (~ 10). For higher values, we compute a lower and higher bound for $w(S_2(n))$.

The lower bound $w'(S_2(n))$ is just the number of distinct primes dividing $S_2(n)$ that are in the range $p < L$ which we compute by counting. The upper bound is $w' + \frac{n(n-1)}{2}\log_L(2)$. This is an upper bound because any extra prime of $S_2(n)$ not in our range is at least $\geq L$, hence there can only be, at most, $\log_L(S_2(n)) \leq \log_L(2^{\sum_{m<n} m}) = \frac{n(n-1)}{2}\log_L(2)$.

5.2.4 Improvement on Artin's conjecture

Conjecture 5.18 gives a finer upper bound for the 4th term in Equation 5.4. This will let us choose a smaller ξ_3'. For this section, we assume Conjecture 5.18 and, to simplify the computations, we let the polylogarithmic part be trivial $L(n) = 1$. Hence, suppose $w(S_a(n)) \leq C_a \cdot n$

Lemma 5.23 (New Bound of the 4th Term)**.** Let $\xi_3' = \log^2 x$, then

$$M_a(x, \xi_3', x-1) = O\left(\frac{x}{\log^2 x}\right) \tag{5.15}$$

Proof. As seen in the original proof $M_a(x, \xi_3, x-1) \leq w(S_a(x/\xi_3))$. Now Hooley uses the trivial bound $w(S_a(n)) = O(n^2)$ and concludes that $M_a(x, \xi_3, x-1) = O\left((x^2/\xi_3^2)\right) = O\left(\frac{x}{\log^2 x}\right)$. In the new case, $M_a(x, \xi_3', x-1) = O(w(S_a(x/\xi_3'))) = O(x/\xi_3') = O\left(\frac{x}{\log^2 x}\right)$. ■

Now let $\xi_2' = \log^{-3} x$, which makes the ratio $\xi_3'/\xi_2' = \log^5 x$. Lemma 5.8 still holds with these new brackets. But now, having $\xi_2' = \log^{-3} x$ makes the bound of the 2 term condition-free. This can be seen in the last equality of Lemma 5.16.

Hence, the only condition that remains is the $R(s) \geq 2/3$ zero-free region used for estimation the first term.

6. Common Factor

6.1 Lenstra's Theorem

In 1977, Lenstra published a paper [W77] where he fully settled a generalization of Artin's conjecture that had arisen in relation to the discovery of Euclidean Algorithms in Global Fields. The applications of this theorem to Euclidean Algorithms are not of principal importance for this thesis. Lenstra's article is interesting because it is a prime example of an algebraic generalization of Hooley's Sieve. In particular, his paper settles all the generalizations we defined in Section 3.1, often conditional to some version of the Riemann Hypothesis.

Question 6.1. Let K be a global field with Dedekind Domain $\mathcal{O}_K$. Let F/K a finite abelian extension and $C \subseteq \mathrm{Gal}(F/K)$ a subset formed as a union of conjugacy classes. Let $W = \langle w_1, \ldots, w_r \rangle \subseteq K^*$ a finitely generated subgroup of rank $r \geq 1$ and let $k \in \mathbb{Z}_{\geq 1}$. Let $M = M(K, F, C, W, k)$ be the set of non-archimedean primes of K such that

1. The Frobenius Element $(\mathfrak{p}, F/K) \in C$
2. $\mathrm{ord}_{\mathfrak{p}}(w_i) = 0$
3. The quotient map $\psi : W \to (O_K/\mathfrak{p})^*$ has index $[(O_K/\mathfrak{p})^* : \psi(W)] \mid k$

Does M have positive density?

Following Artin's observation, one arrives at the following conjecture

Definition 6.2. Let $l \neq p$ a prime number and define $q(l) = \min\{l^a \mid l^a \nmid k\}$. Then, let $L_l = K(\zeta_{q(l)}, W^{1/q(l)})$. For $n \in \mathbb{Z}_{>0}$, let $L_n = \prod_{l|n} L_l$ and $q(n) = \prod_{l|n} q(l)$. Note that $q(l) = l$ for almost all the l primes.

Definition 6.3. Define $C_n \subseteq \mathrm{Gal}(F \cdot L_n/K)$ as

$$C_n = \{\sigma \in \mathrm{Gal}(F \cdot L_n/K) \mid \sigma_{|F} \in C \text{ and } \sigma_{|L_l} \neq \mathrm{Id}\,\forall l \mid n\} \tag{6.1}$$

and let $a_n = \frac{|C_n|}{|\mathrm{Gal}(F \cdot L_n/K)|}$.

Remark 6.4. Note that for $n \mid m$, $a_n \geq a_m \geq 0$ as any $\sigma \in C_m$ must have $\sigma_{|L_n} \in C_n$ and for every $\sigma' \in C_n$, there are at most m/n extensions to $C_m \subseteq \mathrm{Gal}(F \cdot L_m/K)$. Hence, the series a_n has a limit, when n is iterated over the square-free integers.

Conjecture 6.5. The density $\delta(M) = \lim_n a_n$

Lenstra's main contribution is given by the following theorem

Theorem 6.6. If h is the product of the primes l such that $W \subseteq (K^*)^{q(l)}$, the following are equivalent

1. $\lim_n a_n = 0$
2. There is some n such that $a_n = 0$
3. There exists some $\sigma \in \mathrm{Gal}(F(\zeta_h)/K)$ such that
   - $(\sigma_{|F}) \in C$
   - $(\sigma_{|L_l}) \neq \mathrm{Id}_{L_l}$ for all l with $L_l \subseteq F(\zeta_h)$

By the previous Remark, 2 $\implies$ 1 is trivial. This following sections will discuss the implication 1 $\implies$ 2. The implications 2 $\iff$ 3 are a useful characterization of the necessary conditions but will not be explained in this dissertation.

6.1.1 Artin's observation revisited

In this section, we will sketch how the Lemmas of Artin's observation, described in Section 3.2, generalize to the problem studied by Lenstra.

Lemma 6.7 (Lemma 2.5 of [W77])**.** Let $\mathfrak{p} \subseteq K$ such that

1. $\mathrm{ord}_{\mathfrak{p}}(w) = 0 \ \ \forall w \in W$
2. $\mathrm{ord}_{\mathfrak{p}}(2\Delta_K) = 0$ if K is a number field

Then, $[(K/\mathfrak{p})^* : \psi(W)] \mid k$ if and only if for all $l \neq p$, $(\mathfrak{p}, L_l/K) \neq \mathrm{Id}_{L_l}$

Sketch of the proof. This Lemma is a generalization of Lemma 3.26. Condition 1 needs to be added for ψ to be a well-defined group homomorphism. Condition 2 is asking for the prime $\mathfrak{p}/p$ to be non-ramified, as the Frobenius Element needs to be well-defined, and not above $p = 2$. The corner case at $p = 2$ also appeared in Section 3.2 and can be ignored, because we are only interested in density questions. Also, note that the dependency of k in the right-hand side of the double implication is hidden in the definition of L_l.

We refer to the details of this proof to the original source [W77, Lemma 2.5] ■

Definition 6.8. Let M_n be the set of primes $\mathfrak{p} \subseteq$ with $(\mathfrak{p}, F/K) \in C$ and $(\mathfrak{p}, L_l/K) \neq \mathrm{Id}_{L_l}$ for all $l|n$

Theorem 6.9 (Generalized Artin's observation)**.** The density $\delta(M_n) = a_n$. One may express it as $a_n = \sum_{d|n} \frac{\mu(d)c(d)}{[F \cdot L_d : K]}$, where $c(d) = |C \cap \mathrm{Gal}(F/F \cap L_d)|$.

Proof. Chebotarev's theorem directly states that $\delta(M_n) = a_n$. It suffices to see that the equality with the sum on the right hand side holds.

Let $D_n = \{\sigma \in \mathrm{Gal}(F \cdot L_n/K) \ \mid \sigma_{|F} \in C \text{ and } \sigma_{|L_l} = \mathrm{Id}_{L_l} \forall l \mid n\}$. The Inclusion-Exclusion lemma implies $|C_n| = \sum_{d|n} \mu(d)|D_d|$. Furthermore, any $\sigma' \in \mathrm{Gal}(F/F \cap L_d)$ can be extended to a $\sigma \in D_d$ in $[F \cdot L_n : F \cdot L_d]$ ways, so $|D_d| = [F \cdot L_n : F \cdot L_d]c(d)$. This again uses [Mil22, Proposition 3.19] about the Galois Groups in a compositum tower where one of the side extensions is Galois.

$$\begin{tikzcd}
& & F \cdot L_n \arrow[dl, dash] \arrow[dr, dash] & \\
& F \cdot L_d \arrow[dl, dash] \arrow[dr, dash] & & L_n \arrow[dl, dash] \\
F \arrow[dr, dash] \arrow[ddr, dash] & & L_d \arrow[dl, dash] & \\
& F \cap L_d \arrow[d, dash] & & \\
& K & &
\end{tikzcd}$$

Putting all together results in the desired identity. ■

Conjecture 6.10. $\delta(M) = \delta(\cap M_n) = a$ equals $\lim_n \delta(M_n) = \lim_n a_n$.

One side of the conjecture trivially holds.

Lemma 6.11. With the notations from Question 6.1, $\delta_+(M) \leq a$.

Proof.

$$\delta_+(M) = \delta_+(\cap M_n) \leq \delta_+(M_n) = a_n \implies \delta_+(M) \leq \lim a_n = a \tag{6.2}$$

■

For the case $F = K$, $C = \{\mathrm{Id}_K\}$, this conjecture has already been fully explored by Bilharz [Bil37] and Cooke-Weinberger [CW75] (extending Hooley's argument) in Function Fields and Number Fields respectively. Hence, to deal with the full conjecture, only the following Lemma is needed.

Lemma 6.12 (Lemma 3.2 in [W77])**.** Conjecture 6.10 is true if and only if it is true for the case, $F = K$, $C = \{\mathrm{Id}_K\}$.

Proof. Let $M = M(K, F, C, W, k)$, $M' = M(K, F, C', W, k)$ and $N = M(K, K, \{\mathrm{Id}_K\}, W, k)$, where C' is the complementary of C in $\mathrm{Gal}(F/K)$. Then, let a, a' and b, be each of their conjectured densities. Clearly, $a + a' = b$. We claim that if $\delta(N) = b$, then $\delta(M) = a$.

Now, note that N only differs by a finite set from $M \cup M'$ (at most, they differ by the set of ramified primes over F/K). Hence $b = \delta_-(N) \leq \delta_-(M) + \delta_+(M') \leq \delta_-(M) + a'$, so $\delta_-(M) \geq a$. Together with Lemma 6.11, this completes the proof. ■

6.2 Other generalizations

One might be interested in investigating what is the most general type of algebraic object where Artin's problem can be posed. To the best of the author's knowledge, the only cases where Artin's conjecture has been studied are Number Fields and Function Fields. There is a class of generalizations of Artin's conjecture to Elliptic Curves and Abelian Varieties but these no longer talk about primitive roots of the residue fields, but instead they talk about primitive roots of the geometric group structure on the points of over $\mathbb{F}_p$.

6.2.1 Geometric setting in $\operatorname{Spec} \mathbb{Z}[x]$

The conjectures over Function Fields and Number Fields tie together as statements in the following geometric object.

Lemma 6.13. $\operatorname{Spec} \mathbb{Z}[x]$ has exactly the following elements

1. Height 0. (0)
2. Height 1. (p) for $p \in \mathbb{Z}$ prime
3. Height 1. $(f(x))$ for $f(x) \in \mathbb{Z}[x]$ irreducible
4. Height 2. $(p, f(x))$ for $f(x)$ irreducible, p prime and $\overline{f}(x)$ irreducible in $\mathbb{F}_p$. These are maximal, with residue field $\mathbb{F}_p[x]/(\overline{f}) \simeq \mathbb{F}_{p^{\deg \overline{f}}}$

This scheme is visualized in Figure 6.1 as a 2D plane with primes in the abscissa and irreducible polynomials of $\mathbb{Z}[x]$ in the coordinate axis. The vertical lines at each p are the sub-schemes $V(p) \simeq \operatorname{Spec} \mathbb{Z}[x]/(p) = \operatorname{Spec} \mathbb{F}_p[x]$. The horizontal lines are $V((f)) \simeq \operatorname{Spec} \mathbb{Z}[x]/f$. In particular, the horizontal line at $f(x) = x$ is $V((f)) = \mathbb{Z}[x]/x = \mathbb{Z}$. We have defined a geometric object for which the open conjecture is a statement on a horizontal line $x = 0$ and the solved conjectures over Function Fields appear as statements over vertical lines.

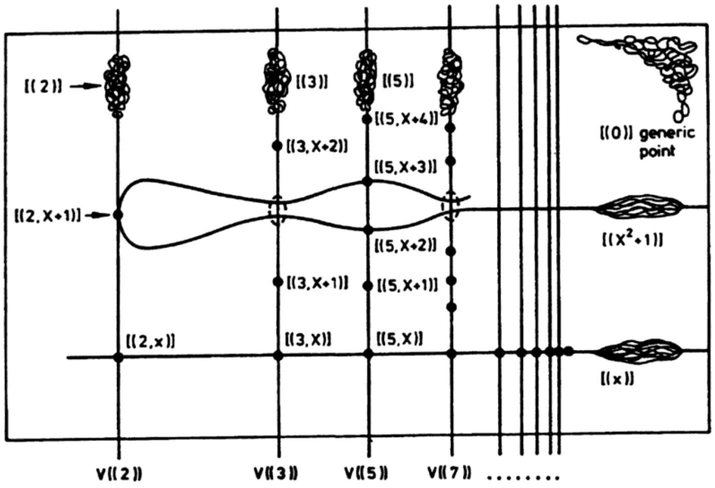

Figure 6.1: 2D Geometry of Spec $\mathbb{Z}[x]$. Picture taken from [Mum04]

In this setting, Artin's problem can be restated as follows.

> **Question 6.14.** Given $a \in \mathbb{Z}[x]$ and a closed subscheme $V \subseteq \operatorname{Spec} \mathbb{Z}[x]$, are there infinitely many closed points $\mathfrak{m}$ in of V where $a \mod \mathfrak{m}$ is a primitive root of the residue field?

6.2.2 Horizontal Lines and Orders of Number Fields

> **Question 6.15.** What happens on other horizontal lines?

This question can be solved completely. If $f \in \mathbb{Z}[x]$ is a monic irreducible polynomial, the conjecture over the sub-scheme $V(f) \simeq \operatorname{Spec} Z[x]/f$ is equivalent to the conjecture over the ring $Z[x]/f$. This ring may not be the ring of integers of a number field, for example for $f(x) = x^2 - 5$, but it is always an Order, i.e. a maximal rank free $\mathbb{Z}$-submodule of a Number Field.

Even though orders are not Dedekind Domains, one can normalize via the following construction. Given an order O, let $\overline{O}$ be the integral closure of O over its field of fractions. Then, $\overline{O}$ is the ring of Integers of Frac$O$. The theory of orders [Neu99, Chapter 1.12] shows that the set of prime ideals in the ring $\overline{O}$ and O differ only by a finite amount, the divisors of the conductor of $\overline{O}/O$. Because Artin's conjecture can ignore finite exceptions, Artin's problem over an order is equivalent to solve it over its normalization. Conditioned to the Riemann Hypothesis, we have shown in Section 6.1 that one can solve Artin's problem over the rings of integers of Number Fields.

6.2.3 Multiple base fields conjecture

Even though the question over a specific horizontal line is solved, the geometric setting of Figure 6.1 inspires a related question. It is practically the same as before, but you allow the wiggle room of changing between a "simple" set of horizontal lines for each p.

> **Question 6.16.** For a given $a \in \mathbb{Z}[x]$, can we find a "simple" family of $\mathcal{F} = \{f_1, \ldots, \}$, $f_i \in \mathbb{Z}[x]$ irreducible such that there are infinitely many rational primes $p \in \mathbb{Z}$ such that there exists an index i for which
>
> (1) f_i is irreducible modulo p and (2) a is a primitive root modulo (f_i, p)

If we managed to prove this problem unconditionally for a family of size 1 $\mathcal{F} = \{f\}$, we would have proven Artin's conjecture over a Number Field $\mathbb{Q}[x]/f$. This is a hard open problem that we don't expect to be able to solve.

Nonetheless, the question as is posed gives more wiggle room as we can play with choosing families of polynomials of size > 1. For example, if we let $\mathcal{F}$ be all the irreducible polynomials in $\mathbb{Z}[x]$, the problem follows from Artin's conjecture over Function Fields (vertical lines). This gives an interesting intermediate conjecture. If one chooses a finite $\mathcal{F}$, the infinite amount of primes required by the conjecture implies that at least one of (finitely many) associated Number Field would follow Artin's conjecture. Possibly, by not pinning which f, one could give an existence result.

The conjecture would prove a theorem of the following type.

> **Objective 6.17.** Let $a \in \mathbb{Z}[x]$ and $\mathcal{F} = \{f_1, \ldots\}$. Then a follows Artin's conjecture on at least one of the Number Fields $\mathbb{Q}[x]/f_i$

Choosing $\mathcal{F} = \{x, x^2 + 1\}$ already gives a conjecture that, to the best of my knowledge, is new. It reads as follows

Conjecture 6.18. Given $\zeta(x) \in \mathbb{Z}[x]$, are there infinitely many primes $p \in \mathbb{Z}$ such that either

1. $\zeta(0) \mod p$ is a primitive root in $\mathbb{F}_p$
2. $p \equiv 3 \mod 4$ and $\zeta(i) \mod p$ is a primitive root in $\mathbb{F}_p[i]$

Proving a conjecture of this type could be an indirect way of proving the existence of some Number Field and some value where Artin's conjecture is true.

Bibliography

[Dir37] P. G. L. Dirichlet. "Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält". In: (1837).

[Zsi92] K. Zsigmondy. "Zur Theorie der Potenzreste". In: *Monatshefte für Mathematik und Physik* 3 (1892), pp. 265–284. DOI: https://doi.org/10.1007/BF01692444. URL: https://link.springer.com/article/10.1007/BF01692444#citeas.

[Che26] N. Chebotarev. "Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören". In: *Mathematische Annalen* 95 (1926).

[Bil37] Herbert Bilharz. "Primdivisoren mit vorgegebener Primitivwurzel". In: *Mathematische Annalen* 114.1 (1937). Cited by: 20, pp. 476–492. DOI: 10.1007/BF01594189.

[Dav39] H Davenport. "On character sums in finite fields". In: *Acta Math.* 71 (1939), pp. 99–121.

[Wei40] André Weil. "Sur les fonctions algebriques á corps de constantes fini." In: *C. R. Acad. Sci. Paris* 210 (1940), pp. 592–594.

[LT65] Artin Emil Serge Lang and John Torrence Tate. *The Collected Papers of Emil Artin*. Springer-Verlang, 1965.

[Hoo67] Christopher Hooley. "On Artin's conjecture." In: *Journal für die reine und angewandte Mathematik* 225 (1967), pp. 209–220. URL: http://eudml.org/doc/150785.

[Wei72] Peter J. Weinberger. "A counterexample to an analogue of Artin's conjecture". In: 1972.

[CW75] George Cooke and Peter J. Weinberger. "On the construction of division chains in algebraic number rings,with applications to SL2". In: *Communications in Algebra* 3.6 (1975), pp. 481–524. DOI: 10.1080/00927877508822057. eprint: https://doi.org/10.1080/00927877508822057. URL: https://doi.org/10.1080/00927877508822057.

[W77] Lenstra H. W. “On Artin’s conjecture and Euclid’s algorithm in global fields”. In: *Inventiones mathematicae* (1977). DOI: 10.1007/BF01389788.

[Gup84] Murty M. R. Gupta R. “A remark on Artin’s conjecture”. In: *Inventiones mathematicae* 78 (1984).

[GWC86] C.F. Gauss, W.C. Waterhouse, and A.A. Clarke. *Disquisitiones Arithmeticae*. Springer-Verlag, 1986. ISBN: 9783540962540. URL: https://books.google.com/books?id=Y-49PgAACAAJ.

[Hea86] D. R. Heath-Brown. “Artin’s conjecture for primitive roots”. In: *The Quarterly Journal of Mathematics* 37 (1986).

[Mur88] M. Ram Murty. “Artin’s conjecture for primitive roots”. In: *The Mathematical Intelligencer* 10 (1988).

[Lan94] S. Lang. *Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 1994. ISBN: 9780387942254. URL: https://books.google.es/books?id=u5eGtA0YalgC.

[SH94] P. Stevenhagen and Jr. H. W. Lenstra. “Chebotarëv and his density theorem”. In: *Commemoration of the centenary of the birth of Chebotarëv at the University of Amsertdamm. Lecture notes* (1994).

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. Grundlehren der mathematischen Wissenschaften. Berlin: Springer, 1999.

[Coj02] Alina Carmen Cojocaru. “Cyclicity of Elliptic Curves Modulo p”. PhD thesis. Queen’s University, 2002.

[Ros02] M. Rosen. *Number Theory in Function Fields*. Graduate Texts in Mathematics. Springer New York, 2002. ISBN: 9780387953359. URL: https://books.google.com/books?id=vDpa%5C_C5DIbkC.

[Ser03] Jean-Pierre Serre. “Résumé des cours de 1977–1978”. In: 2003.

[Ste03] Peter Stevenhagen. “The correction factor in Artin’s primitive root conjecture”. en. In: *Journal de théorie des nombres de Bordeaux* 15.1 (2003), pp. 383–391. URL: http://www.numdam.org/item/JTNB_2003__15_1_383_0/.

[Mum04] David Mumford. *The Red Book of Varieties and Schemes*. Vol. 1358. Lecture Notes in Mathematics. Springer Berlin / Heidelberg, 2004. DOI: 10.1007/978-3-540-46021-3.

[Lan05] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005. ISBN: 9780387953854. URL: https://books.google.es/books?id=Fge-BwqhqIYC.

[MS19] M. Ram Murty and François Séguin. "Prime divisors of sparse values of cyclotomic polynomials and Wieferich primes". In: *Journal of Number Theory* 201 (2019), pp. 1–22. ISSN: 0022-314X. DOI: https://doi.org/10.1016/j.jnt.2019.02.016. URL: https://www.sciencedirect.com/science/article/pii/S0022314X19300927.

[KR20] Seoyoung Kim and M. Ram Murty. "Artin's primitive root conjecture for Function Fields revisited". In: *Finite Fields and Their Applications* 67 (2020), p. 101713. ISSN: 1071-5797. DOI: https://doi.org/10.1016/j.ffa.2020.101713. URL: https://www.sciencedirect.com/science/article/pii/S1071579720300824.

[KM22] Seoyoung Kim and M. Ram Murty. "Corrigendum to "Artin's primitive root conjecture for Function Fields revisited" [Finite Fields Appl. 67 (2020) 101713]". In: *Finite Fields and Their Applications* 78 (2022), p. 101963. ISSN: 1071-5797. DOI: https://doi.org/10.1016/j.ffa.2021.101963. URL: https://www.sciencedirect.com/science/article/pii/S107157972100157X.

[Mil22] J. S. Milne. *Fields and Galois Theory.* Ann Arbor, MI: Kea Books, 2022.

[Leh90] Derrick Lehmer. *Lehmer Papers, Approximately 1926-1990.* University Archives, The Bancroft Library, University of California, Berkeley, 1926-1990.

A. More numerics for Conjecture 5.18

A.1 Estimates for $a \in \{3, 4, 5, 6\}$

Estimates for $a = 2$ are given in Figure 5.1. For $a \in \{3, 4, 5, 6\}$, they are given below. These values include a square and a composite number. A detailed explanation of the lower and upper bounds can be found in Figure 5.1.

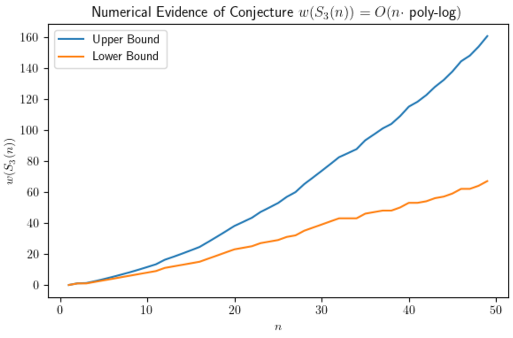

Figure A.1: Computations $w(S_3(n))$

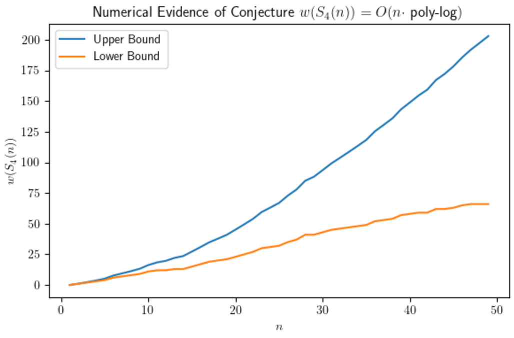

Figure A.2: Computations $w(S_4(n))$

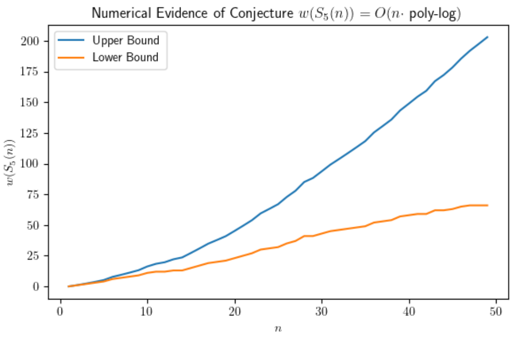

Figure A.3: Computations $w(S_5(n))$

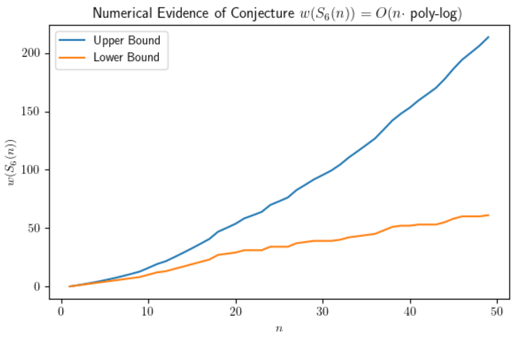

Figure A.4: Computations $w(S_6(n))$

A.2 Program computing estimations of $w(S_a(n))$

This is the exact version of the program used to compute the data in Figure 5.1.

```
#include <bits/stdc++.h>
using namespace std;

typedef long long ll;

ll L = 1e8;

// Eratosthenes Sieve
vector<ll> sieve(ll n) {
  vector<ll> primes;
  vector<bool> prime(n, true);
    for (ll i=2; i<n; i++) {
    if (prime[i]) {
      primes.push_back(i);
      for (ll m=2*i; m < n; m += i) prime[m] = false;
    }
  }
  return primes;
}

// Fast exponentiation
ll poww(ll a, ll n, ll p) {
  if (n == 0) return 1LL;
  ll mid = poww(a, n/2, p);
  ll twomid = (mid*mid)%p;
  if (n%2 == 0) return twomid;
  else return (a * twomid)%p;
}

int main() {
  vector<ll> primes = sieve(L);
  ll a = 2;
  ll N = 100;

  for (ll n=1; n<N; n++) {
    cerr << n << endl;
    ll count = 0;
    for (ll p : primes) {
      ll num = 1;
      for (ll m=1; m<n; m++) {
        num *= (poww(a, m, p) + p - 1) % p;
        num %= p;
      }
      if (num == 0) count += 1;
    }
    long double logVal = 0;
    for (ll m=1; m<n; m++) logVal += m*log(a);
    cout << n << "," << count << "," << count + logVal / log(L) << endl;
  }
}
```