Undergraduate Thesis
in Mathematics and Computer Science

Artin's Conjecture on primes with prescribed primitive roots

Universitat Politècnica de Catalunya[1]

University of California Berkeley[2]

Author: Javier López-Contreras[1]

Supervisors: Sug Woo Shin[2]

Victor Rotger Cerdà[1]

Academic Year: 2022/2023

Acknowledgements

Nir Ember's Latex template

Abstract

TODO: Write Abstract

English version

Catalan version

Spanish version

Keywords

TODO: Keywords + I also need to add the AMS classification number

Contents

1. Introduction

TODO: Read sources and improve story

Gauss articles 315-317 of *Disquisitiones Arithmeticae*.

Emil Artin in 1927 during a conversation with H. Hasse. p.8-10. E.Artin Collected papers... Not avaliable in PDF from springer

Reread [Ste03], it shows letters. Great history prologue

2. Preliminaries

TODO: fill this section at the end, the decision of what to include is delicate and should be postponed until the very end, when the other sections are complete

2.1 Notation

We will use the following set of notation.

Notation 2.1 (Classical Number Theoretical Functions)**.**

- φ represents Euler's Totient function
- μ represents the Möebius function

Notation 2.2 (Order mod p and order at place p)**.**

- If G is a group and $a \in G$, $\mathrm{ord}_G(a)$ is the multiplicative order of a and $\mathrm{ind}_G(a) := \frac{|G|}{\mathrm{ord}_G(a)}$ is the index.
- For $p \in \mathbb{Z}$ a prime and $a \in Q$, $\mathrm{ord}_p(a) = \max\{k \in \mathbb{Z} \mid p^k \mid a\}$.

Warning 2.3. Note that $\mathrm{ord}_{\mathbb{F}_p^*}$ is not the same as ord_p, this distinction could be a source of confusion.

Notation 2.4 (Algebraic Number Theory)**.** If L/K is an extension of algebraic number fields with rings of integers B/A, we denote

- ΔL the discriminant over K
- Tr$, \mathcal{N} : L \to K$ the trace and norm respectively
- $\mathrm{Spl}(L/K)$ is the set of primes in L that split completely over K. When the base field is clear by context, we will write $\mathrm{Spl}(L)$.

2.2 Classical results

Aiming for this document to be as self contained as possible, we list a few results in the classical corpus of Algebraic Number Theory that will be central in the rest of the document.

2.2.1 Ramification Theory

Dedekind ramification theorem (p split if f(x) mod p splits)
Frobenius substitution. Completely split means frob = 1
Riemann Roch used

2.2.2 Dirichlet Density

Let K be a global field with ring of integers $\mathcal{O}_K$.

Definition 2.5 (Dirichlet's Density)**.** Let $S \subseteq \operatorname{Spec} \mathcal{O}_K$, define

$$\delta(S, s) = \frac{\sum_{\mathfrak{p} \in S} \frac{1}{(\mathcal{N}\mathfrak{p})^s}}{\sum_{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K} \frac{1}{(\mathcal{N}\mathfrak{p})^s}} \tag{2.1}$$

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

TODO: Generalization to global fields and saying that in those, it doesnt match the usual denisty, even though in $\mathbb{Q}$ it does

Theorem 2.6 (Chebotarev's Density Theorem)**.**

2.2.3 Sieving methods

Selberg Sieve

3. Artin's Conjecture

3.1 The original problem

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. There are some a for which the answer is negative, as shown in the following Lemma.

Lemma 3.3 (Necessary condition in A.C.)**.** 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. Specifically $P_{-1} = \{2, 3\}$ and, for $k \geq 0$,d

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

Proof. If $a = 0$, then $a \mod p = 0$ is not invertible, hence it can't be a primitive root. If $a = -1$, then $a \mod p$ always has order $\in \{1, 2\}$ as, $\forall p$, $(-1)^2 = 1 \mod p$. Hence, it can only be a primitive root for primes $p \in \{2, 3\}$, which is a finite list. Checking shows that -1 is a primitive root in both cases. On the other hand, suppose $a = k^2$ has $\text{ord}_{\mathbb{F}_p^*}(a) = p - 1$. Denote $r = \text{ord}_{\mathbb{F}_p^*}(k)$, which $r \mid p-1$ and $k^{2r} = 1 = a^r \mod p \implies p-1 \mid r$. Hence, $r = p-1$. 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.

3.2 Studied generalizations

This long-lasting conjecture has raised interest on a number of related problems. This section gives some of these generalizations, which will be studied in more detail in the rest of the document. These generalizations were explored and resolved (often conditionally to some version of the Riemann Hypothesis) in [W77]. Section 6.1 gives an exposition of this paper.

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

One could be interested in asking A.C. about $a \in \mathbb{Q}$ 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

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

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.

Remark 3.9. Conjecture 3.6 is not known to be true for any particular value of $a \in \mathbb{Z}$ nor $\mathbb{Q}$. Extending the domain is mainly a presentation convenience, as most of the arguments given in this text will work for the more general $a \in \mathbb{Q}$.

3.2.2 AC 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 $(\mathbb{Z}/(p))^*$. 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. Both of these are examples of Dedekind Domains with (1) infinitely many primes and (2) finite residue fields. Without both of these conditions the conjecture is trivially false. This excludes Local Fields and extensions of $\mathbb{R}(t)$ or $\mathbb{C}(t)$.

> **Problem 3.10** (A.C. 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) $\operatorname{ord}_{\mathfrak{p}}(a) = 0$ and (2) $a \mod \mathfrak{p}$ generates $(D/\mathfrak{p})^*$?

For instance, writing Problem 3.10 for $\mathbb{F}_q(x)$ we obtain the following question.

> **Question 3.11** (A.C. 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 where found by Bilharz in 1937 [Bil37] conditional to the Riemann Hypothesis over Function Fields, one of the famous Weil Conjectures. These conjectures were settled by Deligne-Grothendieck-Weil in 1974. Bilharz's result came three decades before significant progress was made on the original conjecture over $\mathbb{Q}$ by Hooley [Hoo67].

> **Remark 3.12.** Note that, 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.

3.2.3 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 the

Global Field K, these modular restrictions are expressed as restrictions on the Frobenius element over an arbitrary Abelian extension T/K.

Problem 3.13. Let K be a Global Field, $a \in K^*$, T/K an Abelian field extension and $C \subseteq$ Gal(T/K) a subset formed of conjugacy classes. Are there infinitely many prime ideals $\mathfrak{p} \in \operatorname{Spec} K$ such that (1) $\operatorname{ord}_{\mathfrak{p}}(a) = 0$, (2) $\operatorname{ord}_{(K/\mathfrak{p})^*}(a) = \mathcal{N}\mathfrak{p} - 1$ and (3) Frob$_{\mathfrak{p}}(T/K) \in C$?

Remark 3.14. Note that $T = K$ and $C = \{1\}$ recovers the original problem.

3.2.4 Arbitrary set of generators

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

Problem 3.15. 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. This is equivalent to $\operatorname{ord}_p(w) = 0 \ \forall w \in W$ and $\Gamma_p = \{\gamma \mod p \mid \gamma \in \Gamma\} = \mathbb{F}_p^*$?

Remark 3.16. 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].

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

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

Problem 3.17. Given a $m \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Q}$, are there infinitely many primes such that $\operatorname{ord}_p(a) = 0$ and $\operatorname{ind}_{\mathbb{F}_p^*}(a) \mid m$.

Remark 3.18. $m = 1$ recovers de original conjecture.

3.3 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 3.2. 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 3.19. 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 3.20. 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 $\mathrm{ord}_{\mathbb{F}_p^*}(a) \leq \frac{p-1}{l} < p-1$. ∎

Lemma 3.21. 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 3.22. 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 3.23 (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 $L_k = \prod_{\substack{l|k \\ \text{prime}}} L_l$ the compositum. Denote $C_k = \mathbb{Q}(\zeta_k)$.

Lemma 3.24. 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 $u^l = 1 \underset{l \text{ prime}}{\Longrightarrow} l \mid p-1$. 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 $\{\zeta^{\frac{p-1}{l}}, \zeta^{2\frac{p-1}{l}}, \ldots, \zeta^{l\frac{p-1}{l}} = 1\}$ 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 $\text{Frob}_p(C_l/\mathbb{Q}) = 1$. 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 $\text{Frob}_p(C_l/\mathbb{Q}) = a \in \text{Gal}(C_l/\mathbb{Q}) = (\mathbb{Z}/l\mathbb{Z})^*$ 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 3.26 and 3.27 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 3.25. 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 3.26. 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 $l \mid \operatorname{ord}_{\mathfrak{p}}(a)$

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 $l \mid \operatorname{ord}_{\mathfrak{p}}(a)$, 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 $\text{Disc}_{O_{\mathfrak{p}}[\mu]/O_{\mathfrak{p}}} = \text{Det}((\text{Tr}(\mu^i\mu^j))_{ij})$. 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, $\text{Tr}(1) = l$ and in the second, $\text{Tr}(\mu^l) = \text{Tr}(u) = lu$. We conclude that

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

From this, we can compute $\text{Disc}_{O_{\mathfrak{p}}[\mu]/O_{\mathfrak{p}}} = \pm l^l u^{l-1}$. 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, $\mathfrak{p} \nmid$ Disc so $\mathfrak{p}$ is unramified.

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

$$l \operatorname{ord}_{\mathfrak{P}}(\sqrt[l]{a}) = \operatorname{ord}_{\mathfrak{P}}(a) = e(\mathfrak{P}/\mathfrak{p}) \operatorname{ord}_{\mathfrak{p}}(a) \tag{3.1}$$

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

Lemma 3.27 (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 $\operatorname{ord}_{\mathfrak{p}}(a) = \operatorname{ord}_p(a) = 0$, $p > 2$ 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 3.26, $R_{\mathfrak{p}} = O_{\mathfrak{p}}[\sqrt[l]{a}]$. Note that, by Lemma 3.26, $\mathfrak{p}$ 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 3.28. A prime l follows the conditions of Lemma 3.20 for $p > 2$ if and only if p is completely split over $L_l/\mathbb{Q}$.

Proof. Application of Lemmas 3.24 and 3.27. 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 3.29. For k square free, all the primes $l_i \mid k$ follow conditions of Lemma 3.20 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 3.30 (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 3.20 is

$$A_k(a) = \sum_{\substack{k'|k \\ k' \geq 1}} \frac{\mu(k')}{[L_{k'} : \mathbb{Q}]} \tag{3.2}$$

where μ is the Moebius Inversion function.

Proof. By Lemma 3.29, we know the density of primes such that all $l \mid k$ follow conditions of Lemma 3.20. The Inclusion-Exclusion Principle yields the desired result. ■

Remark 3.31. Note that taking $k \to \infty$ over the primordials 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 3.20 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.

Hence, Artin arrived at the following specific conjecture.

Definition 3.32 (Artin's constant)**.** For $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$, we define Artin's constant as

$$A(a) = \sum_{k \geq 1} \frac{\mu(k)}{[L_k : \mathbb{Q}]} \tag{3.3}$$

Conjecture 3.33 (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.

3.3.1 Computation of the degree

Definition 3.34 (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 3.35 (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 3.36. 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 $\gcd(x_1, \dots, x_r) = 1$ 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

$$\sqrt[l]{a} = \begin{cases} \in \mathbb{Q} & \text{if } l|h \\ (\sqrt[k_a]{a})^{k_a/l} & \text{otherwise} \end{cases} \tag{3.4}$$

An analogous argument proves the second expression. ∎

Remark 3.37. 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.

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

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 3.38 (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

$$[L_k : C_k] = \begin{cases} \frac{k_a}{2} & \text{if } 2a_1 | k \text{ and } a_1 = 1 \mod 4 \\ k_a & \text{otherwise} \end{cases} \tag{3.5}$$

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

$$[C_k : \mathbb{Q}][R_k : \mathbb{Q}] = [L_k : \mathbb{Q}][I_k : \mathbb{Q}] \implies k_a = [L_k : C_k][I_k : \mathbb{Q}] \tag{3.6}$$

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

$$\mathbb{Q}\left(\sqrt{\left(\frac{-1}{D}\right) D}\right) \subseteq \mathbb{Q}(\zeta_k) \tag{3.7}$$

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 3.39. 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.

3.3.2 Positivity of Artin's constant

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

$$A(a) = \sum_{k\geq 1} \frac{\mu(k)e(k)}{\phi(k)k_a}, \qquad \text{where } e(k) = \begin{cases} 2 & 2a_1 | k \text{ and } a_1 = 1 \mod 4 \\ 1 & \text{otherwise} \end{cases} \tag{3.8}$$

Lemma 3.40 (Euler product of $A(a)$)**.** Let $a = a_1 a_2^2$ 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.

$$A(a) = \delta_{a_1} \prod_{q|h \text{ prime}} \left(1 - \frac{1}{q-1}\right) \prod_{q\nmid h \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) \tag{3.9}$$

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

$$\delta_{a_1} = 1 - \mu(a_1) \prod_{\substack{q|a_1 \\ q|h \\ \text{prime}}} \frac{1}{q-2} \prod_{\substack{q|a_1 \\ q\nmid h \\ \text{prime}}} \frac{1}{q(q-1)-1} \tag{3.10}$$

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.

$$A(a) = \sum_{k\geq 1} \frac{\mu(k)1}{\phi(k)k_a} = \prod_{q \text{ prime}} \left(1 - \frac{1}{q_a(q-1)}\right) \tag{3.11}$$

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 3.41 (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

$$\prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) > \prod_{q \text{ prime}} \left(1 - \frac{1}{q^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} > 0 \tag{3.12}$$

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 in A.C in the Function Field setting. First, we give an exposition of the original proof of A.C. 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's 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 [Dav39].

The abstract of [KR20] announces that their proof is independent of the Riemann Hypothesis on Function Fields. Yet 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 3.10 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 $a \in K^* \setminus \mathbb{F}_q^*$.

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

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 on $\mathbb{F}_q[1/x]$. Nonetheless, for the topic of Artin's Conjecture this makes no difference, as it only changes the behavior of the finitely many primes at infinity, which is unimportant in problems regarding the density of primes.

4.1 Original proof by Bilharz

An analogue of Artin's observation, presented in Section 3.3, 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.

As discussed in Section 3.3.1, 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 original proof contains a similar error. When a follows Definition 4.4 over K, Bilharz's proof is correct as is. By the same rationale exposed in the Warning 3.39, this document will limit the exposition to that case.

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 element $a \in K$ is geometric if and only if it is geometric over all primes $l \in \mathbb{Z}$.

Most a are geometric. Prove it!

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 $p = \mathrm{char}(K) \nmid k$. The density of primes such that there is no $l \mid k$ that follows conditions of Lemma 4.5 is

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

4.1.1 Computation of the degree

Definition 4.7. Given $k \in \mathbb{Z}$ square free $p \nmid k$, let $f(k) = \mathrm{ord}_{(\mathbb{Z}/k\mathbb{Z})^\times}(q)$, 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 3.34, 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 Gal$(\mathbb{F}_q(\zeta_k)/\mathbb{F}_q)$. This concludes $[K(\zeta_k) : K] = f(l)$. ∎

Lemma 4.9. Let $a \in K$ be a Geometric Element. Then, the degree $[L_k : K(\zeta_k)] = k_a$, where $L_k = K(\zeta_k, \sqrt[k]{a}) \underset{\text{Lemma 3.36}}{=} K(\zeta_k, \sqrt[k_a]{a})$.

Proof. Following the argument of Lemma 3.38, 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 $l \mid k$, $K(\sqrt[l]{a}) \subseteq K(\zeta_k)$. A subextension of a constant extension must also be constant extension, which would imply that the field of constants of $K(\sqrt[l]{a})$ is $\mathbb{F}_q(\sqrt[l]{a})$. But by a geometric, the field of constants must be $\mathbb{F}_q$, which is a contradiction. ∎

4.1.2 Bilharz's contribution

Notation 4.10. 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 primordial.

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 4.11. 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 fails.

We begin by introducing two preliminary theorems without proof. The first will serve to prove the convergence of a number of related sums. The second gives us an upper bound on the genus of L_l.

Theorem 4.12 (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 4.13 (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 $\delta(\mathcal{M}_n, s) - \delta(\mathcal{M}, s)$.

Observation 4.14. 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. $\mathcal{M}_n \setminus \mathcal{M} \subseteq \cup_{i \geq n+1} \mathrm{Spl}(L_{l_i})$

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. $\delta(\mathcal{M}_n, s) - \delta(\mathcal{M}, s) \leq \sum_{i \geq n+1} \delta(\mathrm{Spl}(L_{l_i}), s)$

Lemma 4.15 (Fine version of Chebotarev's Theorem)**.** If L/K is Galois, and $s \in R$

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

Proof. The classical proof of Chebotarev's Theorem 2.6 shows this finer result, before taking the limit $s \to 1$. ■

Lemma 4.16 (Main Lemma for Theorem 4.18)**.** 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 4.12.

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

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 4.13, 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

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

As $|\log \zeta_K(s)|$ 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 4.17. The sum $\sum_{l \neq p} \frac{1}{f(l)q^{f(l)/2}}$ converges

Proof. Todo. Look for if /2 can be reduced ■

Theorem 4.18 (Bilharz)**.** The Dirichlet density of the set $\mathcal{M}$ is

$$A(a) = \sum_{\substack{m \geq 1 \\ p \nmid m}} \frac{\mu(m)}{[L_m : K]} \tag{4.13}$$

This sum converges by Theorem 4.12.

Proof. By Property 3 of Observation 4.14 and Lemma 4.15

$$0 \leq \delta(\mathcal{M}_n, s) - \delta(\mathcal{M}, s) \underset{4.14}{\leq} \sum_{i \geq n+1} \delta(\{L_{l_i}\}, s) \underset{4.15}{<} \sum_{i \geq n+1} \frac{1}{[L_{l_i} : K]} \frac{\log \zeta_{L_{l_i}}(s)}{\log \zeta_K(s)} \tag{4.14}$$

Fixing $s < s_1$, by Lemma 4.16, the right-hand side converges to 0 as $n \to \infty$. By a classical theorem of Uniform Convergence reference, the limits $n \to \infty$ and $s \to 1$ can be swapped, which concludes

$$\delta(\mathcal{M}) = \lim_{n \to \infty} \delta(\mathcal{M}_n) \tag{4.15}$$

as desired. ■

4.1.3 Positivity

todo. discus necessary condition

4.2 Modern proof by Kim-Murty

The article [KR20] (and its corrigendum [KM22]) present a new proof of Theorem 4.18 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 R.H. was already observed by Davenport [Dav39] without details and was the main motivator for [KR20; KM22].

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 4.19 (Sufficient condition)**.** Given $a(x) \in \mathbb{F}_q[x]$ monic. If there is a constant $B \in \mathbb{R}$ with $B < 1$ such that for all $n \in \mathbb{Z}_{>0}$ and for all non-trivial characters $\chi : \mathbb{F}_{q^n} \to \mathbb{C}$, we have

$$\left| \sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta)) \right| < q^{nB}$$

then, Artin's conjecture holds for $a(x)$.

In the rest of the section, we aim to give a sketch of the proof of Lemma 4.19.

Definition 4.20 (Sifting function)**.** Given a cyclic group G, define

$$S : G \to \mathbb{C}$$
$$g \mapsto \frac{\varphi(m)}{m} \left(1 + \sum_{\substack{d|m \\ d>1}} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}\,\chi = d} \chi(g) \right)$$

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

Remark 4.21. Note that the first term comes from the trivial character and $d = 1$. We only separate the first term as a presentation convenience, as it will be the asymptotically significant term.

Lemma 4.22. With the definition above, we have

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

Proof. To-do ■

Definition 4.23. Given an $a(x) \in \mathbb{F}_q[x]$ monic, define $W_a : \mathbb{F}_q[x]^{\text{irr}} \to \mathbb{Z}$,

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

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

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

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

Lemma 4.24. For all $n \in \mathbb{Z}_{>0}$, the following equality holds.

$$\sum_{\substack{v \in \mathbb{F}_q[x]^{\text{irr}} \\ \deg v \mid n}} W_a(v) = \sum_{\theta \in \mathbb{F}_{q^n}^*} S(a(\theta))$$

Proof. To-do ■

Lemma 4.25. The set of upper bounds described in Lemma 4.19 imply that $\sum_{\theta\in\mathbb{F}_{q^n}^*} S(a(\theta))$ diverges as $n\to\infty$.

Proof. Use Definition 4.20 to fully expand the sum. Then, applying a triangular inequality and using the set of upper bounds in Lemma 4.19, the leading term is absolutely asymptotically bigger than all the other combined. Hence, the sum diverges. Probably make more clear ■

4.2.2 Bound of the Polynomial Character Sums

Objective 4.26. We would like to find a $B<1$ such that, for all n and all non-trivial character $\chi:\mathbb{F}_{q^n}\to\mathbb{C}$

$$\left|\sum_{\theta\in\mathbb{F}_{q^n}}\chi(a(\theta))\right|<q^{nB}$$

Remark 4.27. Here is where the necessary condition is needed. If a was a d-th power for some $d\mid q^i-1$ for some i, there would be a character in $\mathbb{F}_{q^i}$ for which the character sum was trivial, hence it would sum to q^i, not q^{iB}.

Remark 4.28. Bounding for each n independently is not enough, as we need the B 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.

Here is where the paper makes its initial mistake, which is, a priori, fixed in the corrigendum. Their method only works for characters of $\mathbb{F}_{q^n}$ that are lifts of characters of $\mathbb{F}_q$. By "lifts" we mean that $\chi:\mathbb{F}_{q^n}\to\mathbb{C}$ decomposes as $\chi=\chi'\circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}:\mathbb{F}_{q^n}\to\mathbb{F}_q\to\mathbb{C}$, where $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is the norm of the field extension and χ' is a character of $\mathbb{F}_q$

Apart from this error, which is supposedly fixed in the corrigendum, I have found another flaw that I think invalidates the proof. The details are described in the next section.

4.2.3 Potential error in the corrigendum

These are the details of a potential error in the corrigendum that would invalidate the proof of Artin's conjecture.

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

Definition 4.29. 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

$$L(s, \chi) := \exp\left(\sum_{n \geq 1} N_n(\chi) \frac{q^{-sn}}{n}\right)$$

with

$$N_n(\chi) := \sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta))$$

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

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

Definition 4.30. 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

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

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

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

To equalize Definition 4.30 with Definition 4.29, 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 4.30 to include characters of $\overline{F}_q$, 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 $\overline{F}_q$, 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 4.30.

Question 4.31. Is $\mathcal{L} = \mathcal{L}'$?

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

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

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

For this to be equal to Definition 4.29, we would need the equality of all the coefficients. Namely, $\forall n \geq 1$

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

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

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

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

But, given an arbitrary $\chi : \overline{F}_q \to \mathbb{C}$ 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 4.30 is a polynomial. Only in the case $\chi = \chi' \circ N$ he uses this to find an equality of the character sum with a sum over the zeroes of the L-function. Because there are only finitely many characters on the base field, one can take the $B = \max |s_i|$ of all the finitely many zeroes (as Davenport has seen $\mathcal{L}$ is a polynomial) of all the finitely many L-series. This will be a uniform bound on all the infinitely many lifts and $B < 1$ by the result analogous to the classical argument by Hadamart and de la Vallée Poussin.

For $\chi \neq \chi' \circ N$, the character sum that one needs to bound doesn't even come up as a coefficient in the L-series of Definition 4.30. It only comes up as a coefficient in the Definition 4.29, 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

The character sum you want to bound would also come up in an L-series like the one in Definition 4.30 via base change from $\mathbb{F}_q$ to $\mathbb{F}_{q'}$ with $q' = q^n$. But in this case, the zeroes of this L series are not linked in any way to the family of L-series 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.

This would be solved if you knew that the zeroes of all the L series are in the region $Re(s) < 1 - \epsilon$ for some ϵ independent of n and χ. This looks similar to Theorem 4 in [KR20] but the bound given in the paper isn't enough. Under base change, it seems to be

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

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

5. Number Field Setting

In this chapter, we give a short summary of Hooley's conditional proof of Artin's Conjecture [Hoo67] over $\mathbb{Q}$ and propose a new Conjecture 5.18. This self-contained conjecture would reduce the strength of the Riemann Hypothesis (RH) assumed by Hooley. There is strong numerical evidence that the conjecture holds, as shown in Figure 5.1.

5.1 Hooley's conditional result

In his 1967 paper [Hoo67], Hooley proved Artin's conjecture about primes with prescribed primitive roots (Conjecture 3.33) conditioned to the Generalized Riemann Hypothesis for the zeta functions of a family of number fields.

This section will give a sketch of the strategy used in this paper, needed to understand the small improvement that we propose in the second part of the chapter.

5.1.1 Preparation

For this chapter, we return to the notations of Definition 3.34. To match the notations used in Hooley's paper [Hoo67], we introduce the following functions.

Definition 5.1 (Prime counting functions in [Hoo67])**.**

1. $R_a(q,p) = \begin{cases} 1 & q \text{ follows Lemma 3.20} \\ 0 & \text{otherwise} \end{cases}$
2. $N_a(x) = \#\{p < x \mid a \text{ is a primitive root } \mod p\}$
3. $N_a(x,\xi) = \#\{p < x \mid \nexists\, q \text{ following Lemma 3.20 in the range } q < \xi\}$
4. $M_a(x,\xi_1,\xi_2) = \#\{p < x \mid \exists\, q \text{ following Lemma 3.20 in the range } \xi_1 < q \leq \xi\}$
5. $P_a(x,k) = \#\{p < x \mid \forall q|k, q \text{ follows Lemma 3.20}\}$

Lemma 5.2 (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 5.3. $N_a(x, \xi) = \sum_{l'} \mu(l') P_a(x, l')$, where the second sum is over all l' square free with factors $\leq \xi$. Note that

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

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

Lemma 5.4. 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

$$\begin{aligned} N_a(x) = N_a(x, \xi_1) + O(M_a(x, \xi_1, \xi_2)) + \\ + O(M_a(x, \xi_2, \xi_3)) + O(M_a(x, \xi_3, x-1)) \end{aligned} \tag{5.1}$$

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.

Remark 5.5. The bounds of terms 3 and 4 use elementary techniques. For terms 1 and 2, the R.H. 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 $1/2$ R.H.

The conjecture that we propose gives an equally good bound for term 2 using less strength of the R.H. 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 R.H.

The estimation of the first term still needs the $2/3$ R.H., 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

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

Proof. If q follows Lemma 3.20, 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

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

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 5.2, we may express $M_a(x,\xi_2,\xi_3) \le \sum_{\xi_2<q\le\xi_3} P_a(x,q)$.

Now, if q follows Lemma 3.20, then in particular $p \equiv 1 \mod q$. By Brun's method, which is an inequality related to Dirichlet's Theorem, we have

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

From this we obtain the bound

$$\begin{aligned} M_a(x,\xi_2,\xi_3) &= O\left(\frac{x}{\log x}\sum_{\xi_2<q\le\xi_3}\frac{1}{q}\right) = \\ &= O\left(\frac{x}{\log^2 x}\left(\log\frac{\xi_3}{\xi_2} + O(1)\right)\right) = O\left(\frac{x\log\log x}{\log^2 x}\right) \end{aligned} \tag{5.2}$$

■

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

The point of view found by Artin's observation gives a clearer line of attack to the conjecture. This is exemplified by the following lemmas, linking the prime counting function to the sums we are interested in computing.

Definition 5.10 (Prime counting function)**.**

$$\pi(x,k) := \#\{\mathfrak{p} \text{ prime ideal of } L_k | N\mathfrak{p} \le x\}$$

Lemma 5.11.

$$n(k)P_a(x,k) = \pi(x,k) + O(n(k)w(k)) + O(n(k)x^{1/2}) \tag{5.3}$$

Proof. This is an implication of elementary ramification theory applied to L_k, check the article [Hoo67] for the details. Maybe add? ■

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 5.1, by Lemmas 5.2 and 5.3. The final part of Hooley's article deduces a good enough prime counting theorem.

Theorem 5.12. Assuming the GRH for ζ_{L_k}, we have the estimate

$$\pi(x,k) = \frac{x}{\log x} + O(n(k)x^{1/2}\log kx) \tag{5.4}$$

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. ■

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

$$\pi(x,k) = \frac{x}{\log x} + O(n(k)x^{f}\log kx) \tag{5.5}$$

From the rest of the document, f will note the value up to which the RH 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 5.2 and 5.3 one gets estimates of the first and second term in Equation 5.1. They are explained in the following lemmas.

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

$$
\begin{aligned}
N_a(x,\xi_1) = \sum_{l'} \mu(l') \left(\frac{x}{\log x \cdot n(l')} + O(x^f \log x) \right) = \\
\underset{l'<e^{2\xi_1} \text{ by Prop. 5.3}}{=} \frac{x}{\log x} \sum_{l'} \frac{\mu(l')}{n(l')} + O\left(\sum_{l<e^{2\xi_1}} x^f \log x \right) = \\
= A(a)\frac{x}{\log x} + O(e^{2\xi_1} x^f \log x) = \\
= A(a)\frac{x}{\log x} + O(x^{f+1/3} \log x)
\end{aligned}
\tag{5.6}
$$

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)**.**

$$
\begin{aligned}
M_a(x,\xi_2,\xi_3) \leq \sum_{\xi_1<q\leq\xi_2} \left(\frac{x}{\log x \cdot q(q-1)} + O(x^f \log x) \right) = \\
= O\left(\frac{x}{\log x} \sum_{q>\xi_2} \frac{1}{q^2} \right) + O\left(x^f \log x \sum_{q\leq\xi_2} 1 \right) = \\
= O\left(\frac{x}{\xi_1 \log x} \right) + O\left(\frac{x^f \xi_2 \log x}{\log \xi_2} \right) = O\left(\frac{x}{\log^2 x} \right)
\end{aligned}
\tag{5.7}
$$

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

We state 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 $w(S_a(n)) = O(n^{2-\epsilon} \cdot$

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 AC but instead of asking for primes with high $\mathrm{ord}_p(a) = p - 1$ it asks for primes with low $\mathrm{ord}_p(a)$.

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

Seems like the conjecture is as hard as Artin's conjecture

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

Remark 5.21. The polylogarithmic part will take no paper in the application to AC, 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 primordials.

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 $a = 2$.

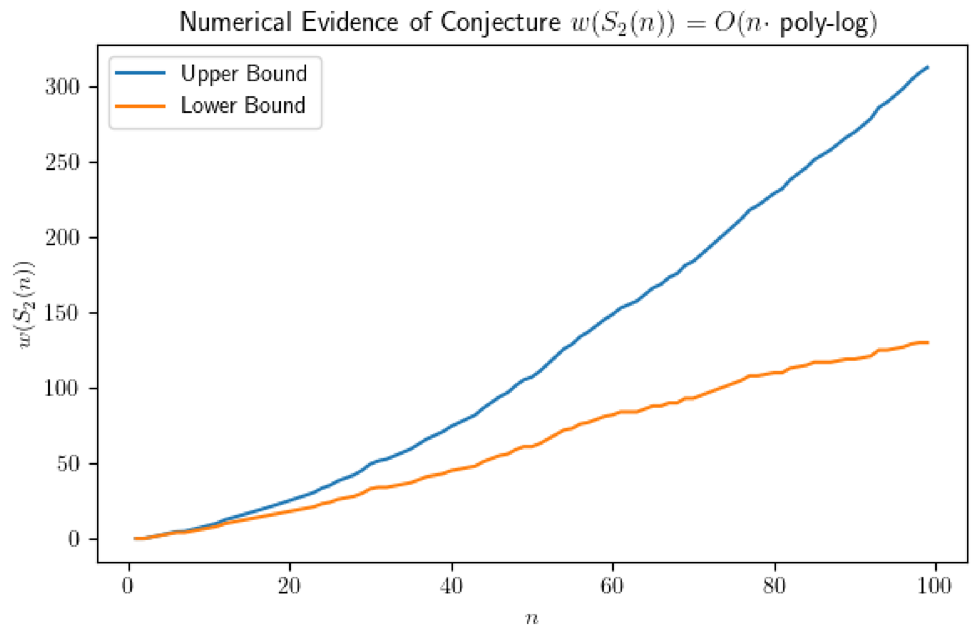

Figure 5.1: Numerical Evidence of Conjecture 5.18. The lower bound w' is the number of distinct primes in $S_2(n)$ in the range $< 10^8$. The upper bound has an extra correction term of $\frac{n(n-1)}{2}\log_{10^8}(2)$ which over counts the number of primes that $S_2(n)$ can have on the range $\geq 10^8$.

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 5.1. 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

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

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.

5.3 Quasi-resolution by Gupta-Murty

Add full chapter

6. Common Factor

Write almost from scratch again

6.1 Lenstra's paper

6.1.1 Artin's observation revisited

6.2 Higher generalizations

As we introduced at the beginning, one can pose the problem on more general algebraic objects. To the best of my 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. They instead talk about primitive roots of the group structure on the points of over $\mathbb{F}_p$. I have not thought about these yet. The generalizations I give in this section have (as far as I know) nothing to do with these.

Is there a relation between the Fp-points of an elliptic curve and a scheme-theoretic residue field? I would expect the answer to be no.

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

Lemma 6.1. $\operatorname{Spec} \mathbb{Z}[x]$ 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 can be visualized as a "2D plane" (2D affine scheme) with primes in the abscissa and x

in the coordinate axis. The vertical lines at each p are the subschemes $V(p) \simeq \operatorname{Spec} \mathbb{Z}[x]/(p) = \operatorname{Spec} \mathbb{F}_p[x]$. The horizontal line at $x = 0$ is $V((x)) \simeq \operatorname{Spec} \mathbb{Z}[x]/x = \operatorname{Spec} \mathbb{Z}$.

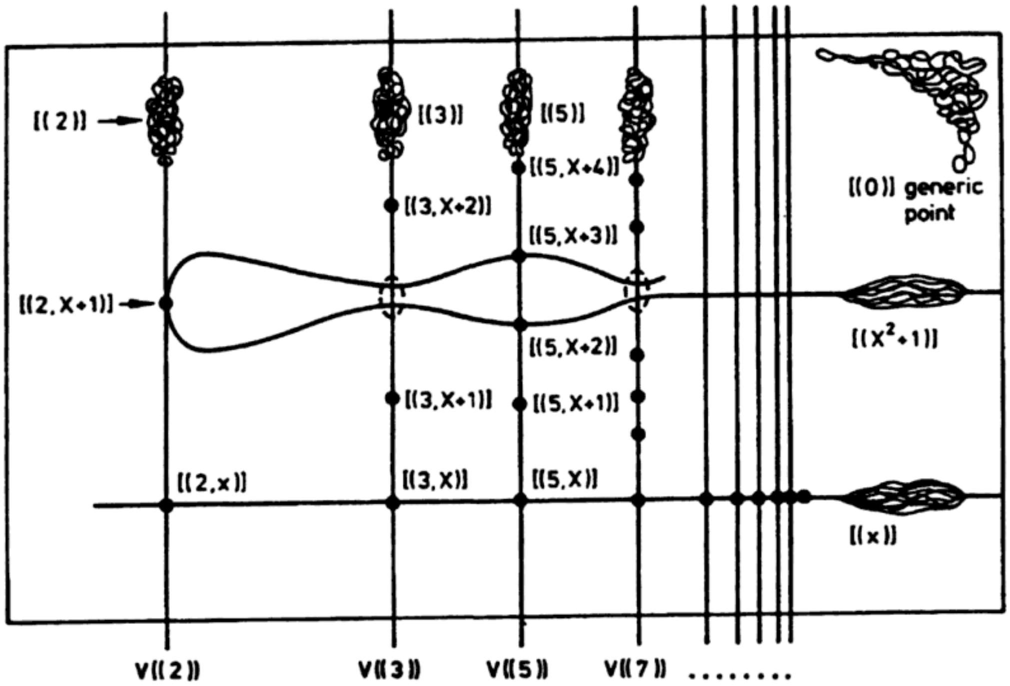

Figure 6.1: 2D Geometry of $\operatorname{Spec} \mathbb{Z}[x]$. Picture taken from [Mum04]

Remark 6.2. We have a geometric object for which the open conjecture is a statement on a horizontal line $x = 0$ and all the conjectures over function fields appear as statements over vertical lines.

But in both cases, the statement posed by Artin conjecture is the same. Namely, it asks for the existence of infinitely many closed points in a sub-scheme of $\operatorname{Spec} \mathbb{Z}[x]$ where $a \in \mathbb{Z}[x]$ is a primitive root of the residue field.

From this setting two new problems arise.

Question 6.3. What happens on other horizontal lines?

This question can be answered completely. Stating the conjecture on polynomial lines gives two cases. One trivial and one equivalent to the original conjecture on number fields. We sketch the result on the following lemma

Lemma 6.4 (Artin's conjecture over the subscheme $V(f)$)**.** Let $f \in \mathbb{Z}[x]$ irreducible and $a \in \mathbb{Z}[x]$. If the splitting field $\mathbb{Q}_f/\mathbb{Q}$ is cyclic, Artin's conjecture over the function field $\mathbb{Z}[x]/f$ is equivalent to asking for the existence of infinitely many primes p where both

(1) f is irreducible modulo p and (2) a is a primitive root modulo (f, p)

If $\mathbb{Q}_f/\mathbb{Q}$ is not cyclic, there are no such primes, as condition (1) is never met.

This comes from the fact that f irreducible modulo p if and only if p is inert in $\mathbb{Q}_f/\mathbb{Q}$. The existence of an inert prime implies $\text{Frob}_{\mathbb{Q}_f/\mathbb{Q}}(p)$ generates the whole Galois group, so the extension $\mathbb{Q}_f/\mathbb{Q}$ must be cyclic.

Nonetheless, the previous question inspires the following version. It is practically the same question, but you allow the wiggle room of changing between a "simple" set of horizontal lines for each p.

Question 6.5. 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 for some i, we have

(1) f_i is irreducible modulo p and (2) a is a primitive root modulo (f_i, p)

This problem is particularly interesting. If we managed to prove it for the family $\mathcal{F} = \{x\}$, we would have proven Artin's conjecture over $\mathbb{Z}$. If we manage to prove it for $\mathcal{F} = \{f\}$ we would have proven Artin's conjecture over the number field $\mathbb{Z}[x]/f$. These are both hard problems that have been open for a century and 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.

For finite $\mathcal{F}$ there still will be one of the f_i with infinitely many such primes and hence the conjecture over that number field would be solved. But hopefully by not pinning which f, we can give an existence result. Very similar to the 2,3,5-theorem. Apparently, working with sets of L-functions is easier than working with specific ones. This is why I believe this might be a workable problem.

The conjecture would prove a theorem of the following type.

Objective 6.6. Let $a \in \mathbb{Z}[x]$ and $\mathcal{F} = \{f_1, \dots\}$. Then a follows Artin's conjecture on at least one of the number fields $\mathbb{Z}[x]/f_i$

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 6.7. 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 $\mathbb{F}_p[i]$

To-do. One interesting thing is: why is the necessary condition different on $\mathbb{F}_q$ and $\mathbb{Z}$. What was the necessary condition on general function fields and number fields? I believe one can express it as a factorization property of a over the E_l on Artin's observation. This might point to other rings where the conjecture is well posed.

Example 6.8.

6.2.2 Affine Schemes

These are very new/unripe ideas. I still haven't dedicated enough time to think about them.

The aim is to look for a common factor between the conjecture over function fields and over number fields. A natural question is the following.

Question 6.9. What properties does a ring R have to follow so that Artin conjecture is well posed on $\operatorname{Spec} R$.

The following set of conditions is general enough to be a common factor between the two cases we would like to study.

- R Dedekind Domain
- R contains infinitely many prime ideals
- The residue fields of R at any prime must be finite.

Question 6.10. Do I know any example of a ring R that follows this but is neither the ring of integers of a number field nor the ring of integers of a function field? I would be specially interested in an example where Artin's conjecture is not true, which would imply the need for more conditions.

To-do. Think about this. To formalize "Artin's conjecture is not followed" I would need to understand the necessary conditions in each ring.

In Conjecture 6.7, the ring $Z[x]/(x(x^2+1))$ appears naturally and is no longer an integral domain. This exemplifies the possibility of considering the conjecture on rings that are not Dedekind Domains. We can go one step further and take a general scheme.

6.2.3 Schemes

Lemma 6.11. Given a scheme S of finite type (over $\operatorname{Spec}\mathbb{Z}$), the residue fields at all closed points are finite.

It has an affine open cover of the type $\operatorname{Spec}\mathbb{Z}[x_1,\dots,x_n]/I$ + Nullstellensatz. Solved exercise in Hartshorne

Question 6.12. Can I construct a (possibly non-affine) scheme where Artin's conjecture is false for non-obvious reasons?

To-do. Think about this. Again this question is not well posed as I need to understand the necessary condition.

Bibliography

[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.

[Bil37] Herbert Bilharz. “Primdivisoren mit vorgegebener Primitivwurzel”. In: *Mathematische Annalen* 114.1 (1937). Cited by: 20, pp. 476–492. doi: 10.1007/BF01594189. url: https://www.scopus.com/inward/record.uri?eid=2-s2.0-0007014593&doi=10.1007%2fBF01594189&partnerID=40&md5=d8e876a9bae38fe7311a4d9cfe417aaf.

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

[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.

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

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

[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.

[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.