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

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

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.
- For $p \in \mathbb{Z}$ a prime and $a \in Q$, $\mathrm{ord}_p(a) = \max\{k \in \mathbb{Z} \mid p^k | a\}$.

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.

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)

2.2.2 Global Fields

Frobenius substitution

2.2.3 Dirichlet Density

Definition 2.4 (Dirichlet's Density)**.**

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

Theorem 2.5 (Chebotarev's Density Theorem)**.**

2.2.4 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. Define $P_a = \{p \mid a \text{ is a primitive root}\}$.

We are interested in wether 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 -1 of a perfect square, then there are only finitely many primes for which it is a primitive root. Specifically $P_{-1} = \{2, 3\}$ and

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

This is conjectured also be sufficient.

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 p.r. in both cases. On the other hand, suppose $a = k^2$ has $\operatorname{ord}_{\mathbb{F}_p^*}(a) = p - 1$. Denote $r = \operatorname{ord}_{\mathbb{F}_p^*}(k)$. On one hand, $r \mid p-1$. On the other hand, $k^{2r} = 1 = a^r \mod p \implies p-1 \mid r$. Hence $r = p - 1$. But if $p > 2$, then $r = p - 1$ is even and $a^{r/2} = k^r = 1$, which contradicts $\operatorname{ord}_{\mathbb{F}_p^*}(a) = p - 1$ ∎

The previous lemma does not have an analogue for l-th powers, with $l > 2$. This has to do with the fact that $p - 1 \neq 0 \mod 2$ only happens at $p = 2$, yet $p - 1 \neq 0 \mod l$ happens for infinitely many primes, by Dirichlet's Theorem on primes in Arithmetic Progressions.

Remark 3.4. Note that $a \in \{-1, 0, 1\}$ do not follow the conjecture. We can exclude them from all our future attemps to prove that these conditions are sufficient. This resolves unrelevant corner cases in future lemmas.

Conjecture 3.5 (Artin's primitive root conjecture)**.** If $a \in \mathbb{Z}$ is not -1 or a square, the set P_a has positive density.

3.2 Probabilistic heuristic

I'm not sure if its worth to explain. The exposition is in Murty's survey paper

3.3 Artin's obervation

In the letter that proposed the conjecture, Artin gave a relevant observation that links the set P_a with the set of completely split primes over a explicit family of Kummer fields over $\mathbb{Q}$. 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 Hypthesis will play an important role.

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

Lemma 3.6. a is a p.r. mod p if and only if there isn't any $k \in \mathbb{Z}_{>1}$ such that

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

Proof. If the $\operatorname{ord}_{\mathbb{F}_p^*}(a) = r \neq p-1$, it must $r \mid p-1$. Take k any non-trivial factor of $\frac{p-1}{r} \neq 1$ and b such that $bk = \frac{p-1}{r}$. Then $k \mid \frac{p-1}{r} \mid p-1$ and $a^{\frac{p-1}{k}} = a^{rb} = 1 \mod p$. For the reciprocal, note that $\operatorname{ord}_{\mathbb{F}_p^*}(a) \leq \frac{p-1}{k} < p-1$. ∎

Lemma 3.7. Let $k \mid p-1$. Then $a^{\frac{p-1}{k}} = 1 \mod p$ is equivalent to $x^k = a \mod p$ 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 $\zeta^{i\frac{p-1}{k}} = 1 \mod p$. Hence $p-1 \mid i\frac{p-1}{k}$. There is a $b \in \mathbb{Z}$ such that $b(p-1) = i\frac{p-1}{k} \implies bk = i \implies k \mid i$. Then $u = \zeta^{\frac{i}{k}}$ is a solution of $x^k = a \mod p$.

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

Remark 3.8. Note that $x^k = a \mod p$ might have solutions when $k \nmid p-1$. In that case, all the elements in $\mathbb{F}_p^*$ are q-residues as the group homomorphism $x \mapsto x^q$ must have trivial kernel.

Lemma 3.9. Let s, t be two coprime integers. Then $x^{st} = a \mod p$ has a solution if and only if both $x^s = a \mod p$ and $x^t = a \mod p$ have solutions.

Proof. By being coprime, there are integer coefficients c, d such that $cs + dt = 1$. Now, let u and v be solutions of $x^s = a$ and $x^t = a$ respectively and consider $w = u^d v^c$. Then, $w^{st} = u^{dst} v^{cst} = a^{dt+cs} = a$.

For the reciprocal, note that if u is a solution of $u^{st} = a$, then u^t and u^s are solutions of $x^s = a$ and $x^t = a$ respectively. ■

Definition 3.10 (Constants and fields relevant in Artin's observation)**.**
Let $h = \max\{h' \mid a \text{ is a perfect } h'\text{-power in } \mathbb{Z}\}$, which is well defined as $a \notin \{-1, 0, 1\}$. Let $k = q_1 \dots q_r$ be square-free integer coprime to a and $k_1 = \frac{k}{(k,h)}$. Denote $Z_k = \mathbb{Q}(\zeta_k)$, $L_k = \mathbb{Q}(\zeta_k, \sqrt[k_1]{a})$ and $n(k) = [L_k : \mathbb{Q}]$.

Remark 3.11. Note that h is odd, as a is not a perfect square. Also note that $\forall p$ and $\forall h' \mid h$, $x^{h'} = a \mod$ is always solvable.

Corollary 3.12. The following are equivalent.

1. $k \mid p-1$ and $x^{k_1} = a \mod p$ is solvable
2. $\forall i,\ q_i \mid p-1$ and $x^{q_i} = a \mod p$ is solvable

Proof. For the first direction, note that if $q_i \mid h$ then, by Remark 3.11, $x^{q_i} = a$ is solvable. For the reciprocal, apply the Chinese Remainder Theorem to see $k \mid p-1$ and Lemma 3.9 to see $x^{k_1} = a$ is solvable. ■

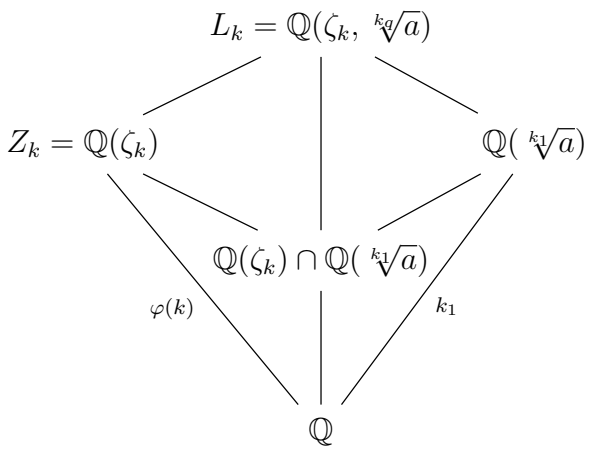
Lemma 3.13. A prime $p \in \mathbb{Z}$ splits completely in $\mathbb{Q}(\zeta_k)/\mathbb{Q}$ if and only if $k \mid p-1$.

Proof. p is completely split if and only if $\text{Frob}_p(\mathbb{Q}(\zeta_k)/\mathbb{Q}) = 1$. Now, $\zeta_k^p = \zeta_k \mod p \implies \zeta_k^{p-1} = 1 \mod p \implies k \mid p-1$. For the other direction, let $\text{Frob}_p(\mathbb{Q}(\zeta_k)/\mathbb{Q}) = a \in$

Gal $(\mathbb{Q}(\zeta_k)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\zeta_k \mapsto \zeta_k^a$. By the property of the Frobenius element on the residue field $\zeta_k^a = \zeta_k^p \mod p \implies \zeta_k^{p-a} = 1 \mod p \implies k \mid p-a$. As $k \mid p-1$ and $1 \leq a \leq k-1$, the only possible $a = 1$. Hence $\text{Frob}_p(\mathbb{Q}(\zeta_k)/\mathbb{Q}) = 1$, so p is completely split. ■

Lemma 3.14. All the primes $q_i \mid k$ follow conditions of Lemma 3.6 if and only if p is completely split over $L_k/\mathbb{Q}$. By Chebotarev's theorem, these primes p have density $\frac{1}{n(k)}$.

Proof. By Corollary 3.12, the proof is reduced to proving that p is completely split in $L_k/\mathbb{Q}$ if and only if $k \mid p-1$ and $x^{k_1} = a \mod p$ is solvable. We will study ramification on the following tower of fields.



hard implication Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

For the other implication, note that p completely split over $L_k/\mathbb{Q}$ implies p completely split over both subextensions. By the Lemma 3.13, the first implies $k \mid p-1$. On the other hand, p completely split in $\mathbb{Q}(\sqrt[k_1]{a})/\mathbb{Q}$ implies that $x^{k_1} - a$ has $k_1 \geq 1$ unique solutions $\mod p$, hence it has at least one. ■

Remark 3.15. The fact that the restrictions of frobenius = 1 get transformed into modular restriction has to do with the fact that the two subextensions are abelian. Great way to introduce CFT!

Theorem 3.16 (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 $q|k$ following the conditions of Lemma 3.6 is

$$A_k(a) = \sum_{\substack{k'|k \\ k' \geq 1}} \frac{\mu(k')}{n(k')} \tag{3.1}$$

Proof. By Lemma 3.14, we know the density of primes such that all $q \mid k$ follow conditions of Lemma 3.6. Using the Inclusion-Exclusion Principle, yields the desired result. ∎

Remark 3.17. 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 a q following the conditions of Lemma 3.6 would need to be very large. Hence, one might expect the limit of $A_k(a)$ to be the density of of primes with a prescribed primitive root at a and this is precisely what Artin conjectured. Nonetheless, passing to the limit is where the difficulty in Artin's conjecture lies.

Hence, Artin arrived at the following specific conjecture.

Conjecture 3.18 (Artin primitive root Conjecture II)**.** Given $a \in \mathbb{Z}$ not -1 nor a perfect square. The set of P_a has Dirichlet density

$$A(a) = \sum_{k \geq 1} \frac{\mu(k)}{n(k)} \tag{3.2}$$

which is named Artin's constant.

Assuming this is true, one can compute the $n(k)$ and show $A(a) > 0$ conditionless. We do so in the following sections.

Remark 3.19. Over $\mathbb{Z}$ this computations can be carried explicitly. On generalizations, this will no longer be so easy. Nonetheless, this is solved by Lenstra, who proves a general result on positivity of these type of constants without using an explicit formula, evading the need to compute the degrees. Update I think this is false, review. I think lenstra needs to compute explicitly and separates the proof in FF and NF for that matter. He just presents it as a theorem in a general way.

3.3.1 Degree of $\mathbb{Q}(\zeta_k, \sqrt[k_1]{a})$

Following the identity $[L_k : \mathbb{Q}] = [L_k : Z_k][Z_k : \mathbb{Q}] = [L_k : Z_k]\varphi(k)$, we aim to compute $g = [L_k : Z_k]$, which is $[Z_k[\sqrt[k_1]{a}]/Z_k]$. When Artin proposed the conjecture, he assumed $g = k_1$. This was found to be incorrect by D.H. Lehmer and solved by Heilbronn. following the track of this citation is going to be tricky, it was a preprint at the time of Hooley's paper.

Lemma 3.20 (Degree correction, Heilbronn)**.** Let $a = a_1 a_2^2$ be the square free decomposition of a.Then, the degree $[L_k : Z_k]$ is

$$[L_k : Z_k] = \begin{cases} \frac{k_1}{2} & \text{if } 2a_1 | k \text{ and } a_1 = 1 \mod 4 \\ k_1 & \text{otherwise} \end{cases} \tag{3.3}$$

Remark 3.21. I'm using $a \in \mathbb{Z}$ how is it for $a \in \mathbb{Q}$?

Proof. TODO ∎

3.3.2 Positivity of Artin's constant

Todo

3.4 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.

3.4.1 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 $(\mathbb{Z}/(p))^*$. This same question can be naturally extended to general Dedekind Domains.

Problem 3.22 (A.C. over a Dedekind Domain)**.** Let D be a Dedekind Domain. Let $a \in D$, are there infinitely many prime ideals in $\mathfrak{p} \in \operatorname{Spec} D$ such that $a \mod \mathfrak{p}$ generates $(D/\mathfrak{p})^*$?

Restricting the choice of D discards unnecessary misbehaviours. For example, if D had finitely many prime ideals, the conjecture is trivially false. This excludes Local Fields. On the other hand, if the residue fields at primes were infinite, there would be two inconveniences. First, their multiplicative groups could be non-cyclic, hence a could never be a primitive root and second, there is no longer a well-defined norm $\mathcal{N}(\mathfrak{p}) = |D/\mathfrak{p}|$. For example, this excludes $\mathbb{C}(t)$, $\mathbb{R}(t)$ and their extensions.

The most canonical Dedekind Domains with infinitely many primes and finite residue fields are the rings of integers of Global Fields hence we restrict our choice of D to that set unless explicitly indicated.

Question 3.23. Is there a Dedekind Domain with infinitely many primes which have finite residue fields that is not listed bellow?

1. The ring of integers of a Global Field.
2. $D\left[\frac{1}{\mathfrak{N}}\right]$ with D following (1) and $\mathfrak{N} \subseteq D$ an ideal.

Note that we don't ask for the residue field to be finite at every prime, only at infinitely many of them.

For instance, rewritting Problem 3.22 for $\mathbb{F}_q[x]$ we obtain the following question.

Question 3.24 (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 $\mathbb{F}_q[x]/(v) \simeq \mathbb{F}_{q^{\deg v}}$?

The necessary and sufficient conditions for this version of the problem where found by Bilharz in 1937 [Bil37] conditional to the Riemann Hypothesis over Function Fields, one of

the famous Weil Conjectures. These conjectures where 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].

3.4.2 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 3.25. 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 3.26. 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 3.27. The sufficient conditions on a are now a bit trickier to hypothesize but a natural conjecture will arise from further study of the conjecture. Reference INITIAL CONDITION DISCUSSIOn

Remark 3.28. The same generalization can be performed for the general Dedekind Domain conjecture, one can choose the initial $a \in \mathrm{Frac}\ D$.

3.4.3 Bigger set of generators

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

Problem 3.29. 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 $p \in Z$ such that $\mathrm{ord}_p(w) = 0\ \forall w \in W$ and such that $\Gamma_p = \{\gamma \mod p \mid \gamma \in \Gamma\}$ is the full $\mathbb{F}_p^*$?

Remark 3.30. 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 and it is studied by Lenstra [Len]. How exaclty do they use this? $W = \mathcal{O}_K^*$ seems to matter

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

TODO

4. Function Field setting

This chapter focuses in the results and conjectures that have arisen from A.C in the Function Field setting. First, we give an exposition of the original proof of the A.C. over Function Fields by Bilharz. The original paper [Bil37] is in german, hence 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]. Cite chapter. Second, we give a second independent proof of the result found in 2020 by Kim-Murty [KR20; KM22].

Notation 4.1. For the remaining of this section K is a Function Field with field of constants $\mathbb{F}_q$. $a \in K$.

First, we give a formalized conjecture.

Proposition 4.2 (Necessary condition)**.** If $a(x)$ is a primitive root modulo infinitely many $v(x)$, then there cannot exist $d, i \in \mathbb{Z}$ with $d > 1$, $i \geq 1$ and

$$\text{(1)} \quad d \mid q^i - 1 \qquad \text{and} \qquad \text{(2)} \quad a(x) \text{ is a } d\text{-th power in } \mathbb{F}_q[x]$$

Theorem 4.3 (Artin's primitive root conjecture for $\mathbb{F}_q[x]$)**.** The necessary condition is also sufficient.

4.1 Original proof by Bilharz

Bilharz' proof begins with the same observation that Artin made for the original conjecture on $\mathbb{Z}$. Only at the end of this observation, Bilharz uses an adhoc argument only true in function fields.

4.1.1 Sketch of Artin's observation

We could write the following statements for a more general class of ring, which includes rings of integers of function fields and rings of integers number fields.

Proposition 4.4. If $a(x)$ is not a p.r. modulo $v(x) \in \mathbb{F}_q[x]$, then there is a $l \in \mathbb{Z}$ prime that witnesses both

$$\text{(1)} \quad l \mid \deg v - 1 \qquad \text{and} \qquad \text{(2)} \quad a^{\frac{\deg v - 1}{l}} = 1 \text{ in } \mathbb{F}_q[x]/(v) \equiv \mathbb{F}_{q^{\deg v}}$$

Theorem 4.5 (Artin's observation for $\mathbb{F}_q[x]$)**.** l witnesses both (1) and (2) if and only if $v(x)$ is completely split on the extension E_l/K, where $K = \text{Frac } \mathbb{F}_q[x]$, $E_l = K(\sqrt[l]{a}, \zeta_l)$ and ζ_l is a primitive l-th root of unity. Also, $[E_l : K] = d_a f(d)$, where $d_a = \prod_{l'|d} l'$ is the product of the prime divisors of d such that $a(x)$ is not a l'-power and $f(d)$ is the order of q modulo d.

Then, using a simple version of Chebotarev Theorem and the principle of inclusion-exclusion, one can get to.

Proposition 4.6. Let P_n be the first n primes. Let $m_n = \prod_{l \in P_n} l$. A prime splits completely in all l if and only if it splits completely in their compositum $E_{m_n} = \prod E_l$. Hence, the density of primes $v \in K$ that do not split in any of the E_l is equal to

$$\sum_{d|m_n} \frac{\mu(d)}{d_a f(d)}$$

.

Making $n \to \infty$ one would get a formula for the density of primes where a is a p.r. Taking this limit is the crucial part of the proof, which Artin couldn't solve and which Bilharz studied in the function field case. Once one has that expression, a couple of Theorems by Romanoff and Heildelberg prove positivity.

4.1.2 Sketch of Bilharz contribution

TODO. Explain how to make $l \to \infty$. It ends up being bounding a series to see it is uniformly convergent and, to do so, Bilharz uses R.H.

4.2 Modern proof by Kim & Murty

The article [KR20] (and its corrigendum [KM22]) present a new proof of Theorem 4.3. Their proof doesn't depend on the Riemann Hypothesis over Function Fields, like the original proof did [Bil37]. well, actually

4.2.1 Overview of the paper

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

Lemma 4.7 (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 $a(x)$.

Sketch of proof of Lemma 4.7

Let φ be Euler's totient function.

Definition 4.8 (Sifting function)**.** Given a cyclic group G, define

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

where the last sum runs over all group characters of order exactly d. Note that the first term comes from the trivial character and $d = 1$.

We only separate the first term because it will be the asymptotically significant term.

Proposition 4.9. 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. TODO ■

Definition 4.10. Given a $a(x) \in \mathbb{F}_q[x]$ 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 will count irreducible v where a is a p.r. mod v but we will weight them with a multiplicity $\deg v$. This is analogous to the role that the function Name? Van magnold?

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

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

Proposition 4.11. For all $n \in \mathbb{Z}_{>0}$, the following equality holds.

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

Proposition 4.12. The set of upper bounds described in Lemma 4.7 imply that $\sum_{\theta \in \mathbb{F}_{q^n}^*} S(a(\theta))$ diverges as $n \to \infty$.

Proof. Use Definition 4.8 to fully expand the sum. Then, applying a triangular inequality and using the set of upper bounds in Lemma 4.7, the leading term is absolutely asymptotically bigger than all of the other combined. Hence the sum diverges. probably make more clear ■

Sketch of proof of character bounds

Objective 4.13. 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 4.14. 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 4.15. 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 relies on a paper by Davenport [Dav39] but only works for 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.

4.2.2 Potential error in the corrigendum

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

Definition 4.16. The second page of the corrigendum [KM22] introduces the following L-function. 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

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

with

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

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.

Definition 4.17. The L-function of the original paper is defined as follows. 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 4.17 with Definition 4.16, 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 4.17 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 4.17.

Question 4.18. Is $\mathcal{L} = \mathcal{L}'$?

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

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

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

For this to be equal to Definition 4.16, we would need the equality of all the coefficients. Namely, $\forall n\geq 1$

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

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 $\theta_1,\dots,\theta_m$ 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.

4.2.3 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 4.17 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 4.17. It only comes up as a coefficient in the Definition 4.16, which, a priori, is not a polynomial nor does it follow an equality similar to the one found by Davenport.

4.2.4 Conditional fix

The character sum you want to bound would also come up in an L-series like the one in Definition 4.17 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 definind 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.

> **Remark 4.19.** The $Re(s) \geq 1 - \epsilon$ zero-free region is apparently a very hard problem on number fields. I am not sure if one can actually prove something like this for function fields without using R.H. but that would fix the flaw

Davenport bounds are enough!

5. Number Field Setting

TODO: rewrite as a chapter, not a note In this note, I will give a short summary of Hooley's conditional proof of Artin's Conjecture (AC) [Hoo67] and propose Conjecture 5.24, a new self-contained conjecture that, if proven, 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 A.C. conditional proof

In his 1967 paper[Hoo67], Hooley proves Artin's conjecture about primes with prescribed primitive roots conditioned to the Generalized Riemann Hypothesis for the zeta functions of a family of number fields.
The conjecture is the following.

Conjecture 5.1 (Artin's conjecture of primes with a prescribed primitive root)**.** Let $a \in \mathbb{Z}_{>1}$ not a perfect square. Then, there are infitely many primes $p \in \mathbb{Z}$ such that $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ is a primitive root. Moreover, the set of such primes has positive Dirichlet density, denoted $A(a)$.

An the paper proves the following statement

Theorem 5.2 (Hooley)**.** Given $a > 1$ not a square, let h be the maximum integer such that a is an h-th power. For a given k square free, let $k_1 = k/(h,k)$. If the Generalized Riemann Hypothesis is true for the Zeta-functions of the number fields $L_k = \mathbb{Q}(\sqrt[k_1]{a}, \zeta_k)$ for all k square free, then Artin's Conjecture is true for a.

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

5.1.1 Preparation

For the whole of this document, we fix the following notations. Let $a \in \mathbb{Z}$, $a > 1$ not a square, p, q distinct primes, k a square free integer, h the maximum integer such that a is an h-th power and $k_1 = k/(h,k)$. Also $w(N)$ is the number of distinct primes dividing N.

Proposition 5.3. a is a primitive root modulo p if and only if there are no primes q with both

1. $p = 1 \mod q$
2. $a^{\frac{p-1}{q}} = 1 \mod p$

In such case, we will say that q is a witness of a not being a p.r. modulo p.

Definition 5.4. We will use the following notations.

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

Proposition 5.5 (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. $M_a(x,\xi_1,\xi_2) \leq \sum_{\xi_1 < q \leq \xi_2} P_a(x,q)$

Proposition 5.6. $N_a(x,\xi) = \sum_{l'} \mu(l') P_a(x,l')$, 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.

Proposition 5.7. 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

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

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 5.8. 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 a 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

Proposition 5.9 (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 is a witness, in particular $a^{\frac{p-1}{q}} = 1 \mod p$. Hence, if there is a witness $q > \xi_3$, 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

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

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 5.10. 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.

Proposition 5.11 (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 Proposition 5.5, 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 is a witness, then in particular $p \equiv 1 \mod q$. By Brun's method, which is a inequality related to Dirichlet's Theorem, we have

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

From this we obtain the bound

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

■

Remark 5.12. This proposition 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 proposition 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 Artin's observation

When Artin proposed the conjecture, he had an intuition for what the Dirichlet density of the primes with a prescribed primitive root at a had to be. He developed this intuition by

translating the problem to an Algebraic Number Theory setting. This change in point of view is explained by the following proposition.

Proposition 5.13. Let $a > 1$ not a square, k as square-free integer and p a prime. All $q|k$ are witnesses if and only if p is completely split in the extension $L_k/\mathbb{Q}$, with $L_k = \mathbb{Q}(a^{1/k_1}, \zeta_k)$, with ζ_k a primitive k-root of unity.

Definition 5.14. We will use the notation $n(k) \coloneqq [L_k : \mathbb{Q}]$.

Remark 5.15. By Chebotarev's theorem, we get $P_a(x,k) = n(k)\frac{x}{\log x}$. The explicit value of $[L_k : \mathbb{Q}]$ is computed by Hooley [Hoo67] but it is not essential for the exposition on this note. Artin deduced what the constant in $N_a(x)$ should be by imagining an type of "infinite" inclusion-exclusion lemma but formalizing this lemma is the main difficulty in the conjecture.

5.1.4 Reduction to counting primes

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

Definition 5.16 (Prime counting function)**.**

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

Proposition 5.17.

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

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

5.1.5 Prime counting theorem

By Proposition 5.17, 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 Propositions 5.5 and 5.6. The final part of Hooley's article deduces a good enough prime counting theorem.

Theorem 5.18. 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, we is able to deduce the desired bound. ■

Remark 5.19. 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.

5.1.6 Bounds for the 1st and 2nd term

By Proposition 5.17, one gets an estimate of P_a and unrolling Propositions 5.5 and 5.6 one gets estimates of the first and second term in Equation 5.1. They are explained in the following propositions.

Proposition 5.20 (Estimation of the 1st term)**.**

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

Remark 5.21. 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 a $R(s) \geq 2/3$ zero-free region.

Proposition 5.22 (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 5.23. 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 5.24. Let $S_a(n):=\prod_{m<n}(a^m-1)$. Let $w(N)=\#\{\text{distinct primes } p|N\}$. Is is 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 a a $R(s)\geq 2/3$ 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 a $R(s)\geq 1/2+\epsilon/3$ 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 $\text{ord}_p(a)=p-1$ it asks for primes with low $\text{ord}_p(a)$.

Conjecture 5.25. Let $P(n)=\#\{p \text{ prime} \mid \text{ord}_p(a)<n\}$, is $P(n)=O(n\cdot \text{ poly-log})$?

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

Remark 5.26. 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 5.27. The polylogarithmic part will take no paper in the application to AC, can be taken as large as one wants.

Remark 5.28. 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 $a = 2$.

The limitation of these numerical computations is the number of primes can be saved in a computer in practice. The current program, foudn 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 the 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 5.24 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 5.24 and, to simplify the computations, we let the polylogarithmic part be trivial $L(n) = 1$. Hence, suppose $w(S_a(n)) \leq C_a \cdot n$

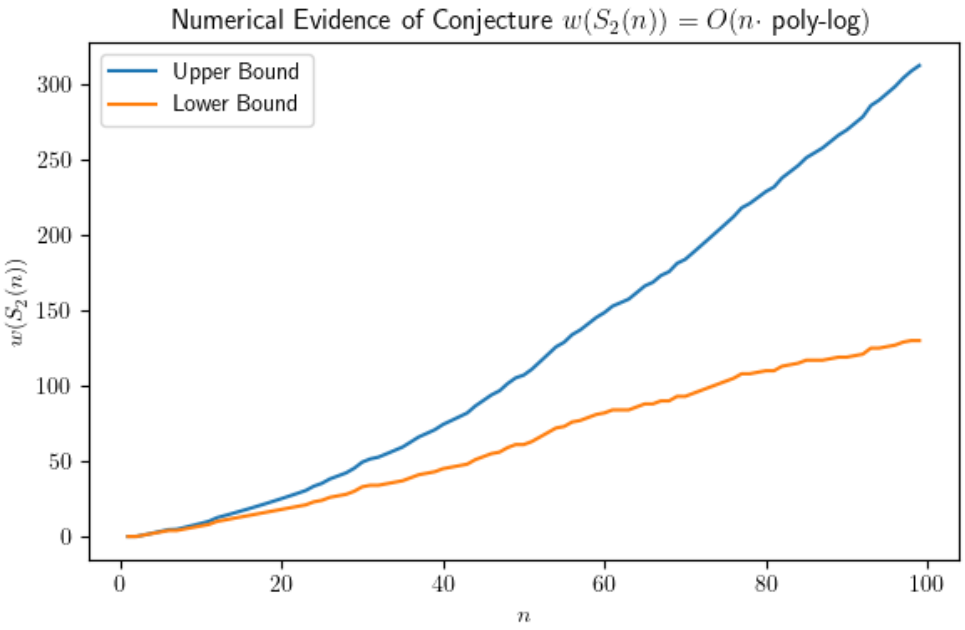


Figure 5.1: Numerical Evidence of Conjecture 5.24. The lower bound w' is the number of distinct primes in $S_2(n)$ in the range $< 10^8$. The upper bound has an extra correction term of $\frac{n(n-1)}{2} \log_{10^8}(2)$ which over counts the number of primes that $S_2(n)$ can have on the range $\geq 10^8$.

Proposition 5.29 (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 $\xi_3'/\xi_2' = \log^5 x$. Proposition 5.11 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 Proposotion 5.22.
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

6. Common Factor

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 $\mathbb{F}_p$-points of an elliptic curve and a scheme-theoretic residue field? I would expect the answer to be no.

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

Proposition 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 $V((x)) \simeq \operatorname{Spec} \mathbb{Z}[x]/x = \operatorname{Spec} \mathbb{Z}$.

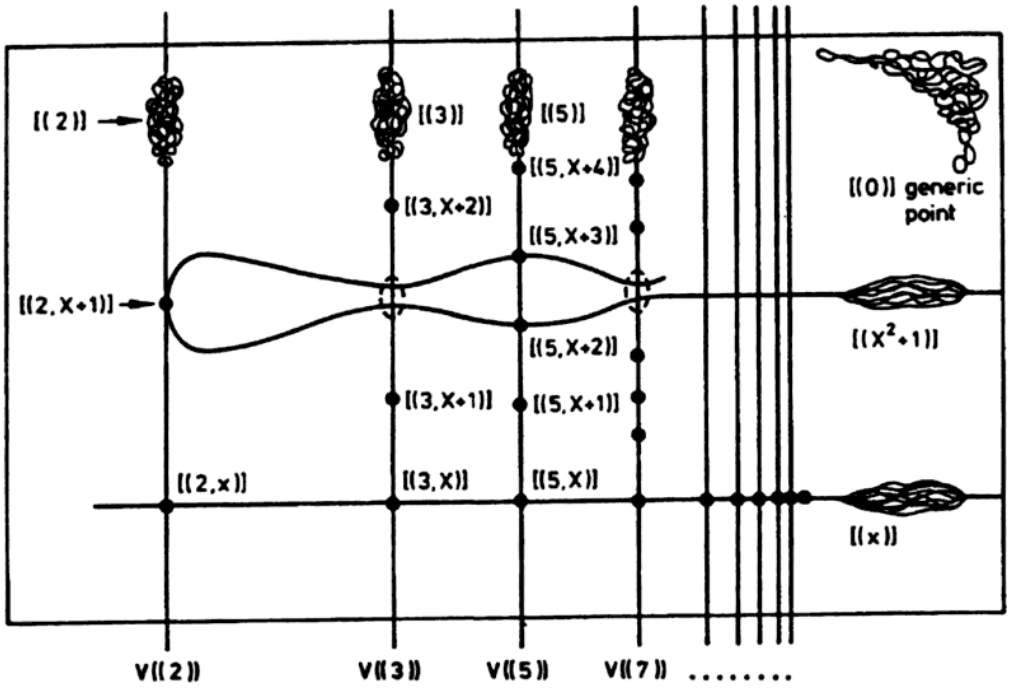


Figure 6.1: 2D Geometry of $\operatorname{Spec} \mathbb{Z}[x]$. Picture taken from [MM04]

Remark 6.2. We have a geometric object for which the open conjecture is a statement on a horizontal line $x = 0$ and all of 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 existance of infinitely many closed points in a subscheme 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 proposition

Proposition 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 p.r. 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 iff 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 $\mathcal{F} = \{f_1, \dots, \}$, $f_i \in \mathbb{Z}[x]$ irreducible such that there are infitely many rational primes $p \in \mathbb{Z}$ such that for some i, we have

(1) f_i is irreducile modulo p and (2) a is a p.r. 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 $\mathbb{Z}[x]/f$. This 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 p.r. in $\mathbb{F}_p$
2. $p \equiv 3 \mod 4$ and $\zeta(i) \mod p$ is a p.r. in $\mathbb{F}_p[i]$

TODO. 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

This 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.

TODO. 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

Proposition 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?

TODO. 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.

[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.

[MM04] David Mumford and David B. 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.

[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.

[Len] Lenstra. "LOOK UP REFERENCE WHEN YOU HAVE INTERNET ACCESS". In: ().

List of Definitions