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

English version

Catalan version

Spanish version

Keywords

I also need to add the AMS classification number

Contents

1. Preliminaries

1.1 Notation

1.2 Classical Results

Definition 1.2.1 (Dirichlet's Density)**.**

Introduction

Artin's Conjecture about primes with prescribed primitive roots is one of the oldest open problems in Number Theory. It was first observed by Gauss and formalized and conjectured by Artin in a letter to Hasse. Improve history of the problem

2. Artin's Conjecture

2.1 The original problem

Question. *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 $\mathbb{Z}/p\mathbb{Z}$?*

By the following Observation and Lemma, there are certain a for which questions has a negative answer.

Observation. *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.*

Lemma 2.1.1. *If $a = k^2 > 0$ is a perfect square, then there doesn't exist any prime $p > 2$ such that $a \mod p$ is a primitive root.*

Proof. Suppose the contrary, $\text{ord}_{\mathbb{F}_p^*}(a) = p - 1$. Denote $r = \text{ord}_{\mathbb{F}_p^*}(k)$. 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 $\text{ord}_{\mathbb{F}_p^*}(a) = p - 1$

Nonetheless, the previous lemma does not have an analogous 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.

Conjecture 2.1.1 (Artin's primitive root conjecture)**.** *If $a \in \mathbb{Z}$ is not -1 or a square, the set of primes $P_a = \{p \mid \text{ord}_{\mathbb{F}_p^*}(a) = p - 1\}$ is infinite.*

Artin's primitive root conjecture has been an open problem for more than a century. Hooley [2] managed to prove it conditional to the Generalized Riemann Hypothesis on number fields in 1965. The results without R.H. have been very limited. In particular, nobody has been able to proof that the conjecture stands for any particular value of a. It is known that at least one of 2, 3 and 5 follow the conjecture. The 2,3,5 result is from Murty et al and I should maybe read it because if feels similar to the conjecture I come up with in Section 5

2.2 A.P.R.C. over Global Fields

REDO This section, is not clear at all The same question can be posed on more general rings, which include the ring of integers of number fields and function fields. For the moment, we formulate the question on the ring $\mathbb{F}_q[x]$, the simplest of function fields.

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

Proposition 2.2.1 (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*

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

Theorem 2.2.1 (Artin's primitive root conjecture for $\mathbb{F}_q[x]$)**.** *The necessary condition is also sufficient.*

This was proven by Bilharz in 1937 [1] conditional to the Riemann Hypothesis over Function Fields, which was finally proven by Deligne in 1974.

Once the conjecture is defined over the basic global fields $\mathbb{Q}$ and $\mathbb{F}_q(x)$, it can be extended to their finite field extensions.

Problem 2.2.1 (A.P.R.C. over number fields)**.** *Let $K/\mathbb{Q}$ be a number field with ring of integers $\mathcal{O}_K$. For a given $a \in \mathcal{O}_K$, $a \notin O_K^\times$, are there infinitely many primes $\mathfrak{p} \subseteq \mathcal{O}_K$ such that a is a primitive root in $\mathcal{O}_K/\mathfrak{p}$?*

the statement below as is is incorrect

Problem 2.2.2 (A.P.R.C. over function fields)**.** *Let $K/\mathbb{F}_q$ be a function field with field of constants $\mathbb{F}_q$. Hence K is a finite extension of $\mathrm{Frac}\mathbb{F}_q[x]$ and we can consider $\mathcal{O}_K := Int(\mathbb{F}_q[x])$ the integral closure of $\mathbb{F}_q[x]$. For a given $a \in \mathcal{O}_K$, $a \notin O_K^\times$, are there infinitely many primes $\mathfrak{p} \subseteq \mathcal{O}_K$ such that $\overline{a}$ is a primitive root in $\mathcal{O}_K/\mathfrak{p}$?*

3. Function Field Setting

3.1 Original proof by Bilharz

Comment. *As M.Rosen exposes in Ch.10 [5], the original proof by Bilharz had a small flaw, at one point it assumed $a(x)$ geometric. For this note, we restrict to that case. Rosen refers to a preprint that states that can solve the general case.*

I have found the paper that formed from that preprint but I haven't looked into it yet. I suspect that issue is actually easy to fix, as it is just a slight change in the computation of a degree of a field extension. Via Chebotarev Theorem, this should only factor as a small term in the Dirichlet density of the set of primes where $a(x)$ is a p.r. The only thing to check is that the factor is non-zero.

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. Hooley's conditional proof also seems to start with Artin's observation.

3.1.1 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 3.1.1. *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*

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

Theorem 3.1.1 (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 $K = \operatorname{Frac} \mathbb{F}_q[x]$, $E_l = K(\sqrt[l]{a}, \zeta_l)$ and ζ_l is a primitive l-th root of unity. Also, $[E_l : K] = d_a f(d)$, where $d_a = \prod_{l' \mid d} l'$ 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 3.1.2. *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.

3.1.2 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.

3.2 Original proof by Bilharz

Comment. *As M.Rosen exposes in Ch.10 [5], the original proof by Bilharz had a small flaw, at one point it assumed $a(x)$ geometric. For this note, we restrict to that case. Rosen refers to a preprint that states that can solve the general case.*

I have found the paper that formed from that preprint but I haven't looked into it yet. I suspect that issue is actually easy to fix, as it is just a slight change in the computation of a degree of a field extension. Via Chebotarev Theorem, this should only factor as a small term in the Dirichlet density of the set of primes where $a(x)$ is a p.r. The only thing to check is that the factor is non-zero.

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. Hooley's conditional proof also seems to start with Artin's observation.

3.2.1 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 3.2.1. *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*

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

Theorem 3.2.1 (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 $K = \operatorname{Frac} \mathbb{F}_q[x]$, $E_l = K(\sqrt[l]{a}, \zeta_l)$ and ζ_l is a primitive l-th root of unity. Also, $[E_l : K] = d_a f(d)$, where $d_a = \prod_{l' \mid d} l'$ 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 3.2.2. *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*

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

.

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.

3.2.2 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. Number Field Setting

In this note, I will give a short summary of Hooley's conditional proof of Artin's Conjecture (AC) [2] and propose Conjecture 4.2.1, 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 4.1.

4.1 Proof of AC conditioned to RH

In his 1967 paper[2], 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 4.1.1 (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 4.1.1 (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.

4.1.1 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 4.1.1. *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 4.1.1. *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. $N_a(x) = \#\{p < x \,|a \text{ is a p.r. } \mod p\}$

3. $N_a(x,\xi) = \#\{p < x \mid \nexists\, q \text{ witness in the range } q < \xi\}$

4. $M_a(x,\xi_1,\xi_2) = \#\{p < x \,|\exists\, q \text{ witness in the range } \xi_1 < q \leq \xi\}$

5. $P_a(x,k) = \#\{p < x \mid \forall q|k, q \text{ is a witness}\}$

Proposition 4.1.2 (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. $M_a(x,\xi_1,\xi_2) \leq \sum_{\xi_1 < q \leq \xi_2} P_a(x,q)$

Proposition 4.1.3. *$N_a(x,\xi) = \sum_{l'} \mu(l') P_a(x,l')$, 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.

Proposition 4.1.4. *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*

$$\begin{aligned} N_a(x) = N_a(x,\xi_1) + O(M_a(x,\xi_1,\xi_2)) + \\ + O(M_a(x,\xi_2,\xi_3)) + O(M_a(x,\xi_3,x-1)) \end{aligned} \tag{4.1}$$

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.

Comment. *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.*

4.1.2 Bounds on the 3rd and 4th term

Proposition 4.1.5 (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 $M_a(x, \xi_3, x-1) < \log S_a(x/\xi_3) < \log a \sum_{m<x/\xi_3} m = O\left((x/\xi_3)^2\right) = O\left(\frac{x}{\log^2 x}\right)$.

Comment. *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 4.1.6 (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 4.1.2, 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

$$\begin{aligned} M_a(x,\xi_2,\xi_3) &= O\left(\frac{x}{\log x}\sum_{\xi_2 < q \leq \xi_3}\frac{1}{q}\right) = \\ &= O\left(\frac{x}{\log^2 x}\left(\log\frac{\xi_3}{\xi_2} + O(1)\right)\right) = O\left(\frac{x\log\log x}{\log^2 x}\right) \end{aligned} \tag{4.2}$$

Comment. *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.*

4.1.3 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 4.1.7. *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 4.1.2. *We will use the notation $n(k) := [L_k : \mathbb{Q}]$.*

Comment. *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 [2] 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.*

4.1.4 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 4.1.3 (Prime counting function)**.**

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

Proposition 4.1.8.

$$n(k)P_a(x,k) = \pi(x,k) + O(n(k)w(k)) + O(n(k)x^{1/2}) \tag{4.3}$$

Proof. This is an implication of elementary ramification theory applied to L_k, check the article[2] for the details.

4.1.5 Prime counting theorem

By Proposition 4.1.8, 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 4.1, by Propositions 4.1.2 and 4.1.3. The final part of Hooley's article deduces a good enough prime counting theorem.

Theorem 4.1.2. *Assuming the GRH for ζ_{L_k}, we have the estimate*

$$\pi(x,k) = \frac{x}{\log x} + O(n(k)x^{1/2}\log kx) \tag{4.4}$$

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.

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

$$\pi(x,k) = \frac{x}{\log x} + O(n(k)x^{f}\log kx) \tag{4.5}$$

From the rest of the document, f will note the value up to which the RH is assumed.

4.1.6 Bounds for the 1st and 2nd term

By Proposition 4.1.8, one gets an estimate of P_a and unrolling Propositions 4.1.2 and 4.1.3 one gets estimates of the first and second term in Equation 4.1. They are explained in the following propositions.

Proposition 4.1.9 (Estimation of the 1st term)**.**

$$\begin{aligned} N_a(x,\xi_1) &= \sum_{l'} \mu(l') \left(\frac{x}{\log x \cdot n(l')} + O(x^f \log x) \right) = \\ &\underset{l'<e^{2\xi_1} \text{ by Prop. 4.1.3}}{=} \frac{x}{\log x} \sum_{l'} \frac{\mu(l')}{n(l')} + O\left(\sum_{l<e^{2\xi_1}} x^f \log x \right) = \\ &= A(a)\frac{x}{\log x} + O(e^{2\xi_1} x^f \log x) = \\ &= A(a)\frac{x}{\log x} + O(x^{f+1/3} \log x) \end{aligned} \tag{4.6}$$

Comment. *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 4.1.10 (Bound of the 2nd term)**.**

$$\begin{aligned} M_a(x,\xi_2,\xi_3) &\leq \sum_{\xi_1<q\leq\xi_2} \left(\frac{x}{\log x \cdot q(q-1)} + O(x^f \log x) \right) = \\ &= O\left(\frac{x}{\log x} \sum_{q>\xi_2} \frac{1}{q^2} \right) + O\left(x^f \log x \sum_{q\leq\xi_2} 1 \right) = \\ &= O\left(\frac{x}{\xi_1 \log x} \right) + O\left(\frac{x^f \xi_2 \log x}{\log \xi_2} \right) = O\left(\frac{x}{\log^2 x} \right) \end{aligned} \tag{4.7}$$

Comment. *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.*

4.2 Proposed improvement

We propose the following self-contained conjecture.

Conjecture 4.2.1. *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 $\mathrm{ord}_p(a) = p - 1$ it asks for primes with low $\mathrm{ord}_p(a)$.

Conjecture 4.2.2. *Let $P(n) = \#\{p \text{ prime} \mid \mathrm{ord}_p(a) < n\}$, is $P(n) = O(n \cdot \text{ poly-log})$?*

Comment. *For the application on AC, the value of a can be asked to be a non-square. Yet, numerical evidence in Figure 3 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.*

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

Comment. *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 [4] on $P(\Phi(a))$, the largest prime divisor which has a very similar flavor.*

4.2.1 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.

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

A trivial application of Zsigmondy's theorem[6] shows $w(S_a(n)) = \Omega(n)$.

4.2.3 Numerical evidence

We believe that the strong conjecture is true. Numerical evidence is shown in Figure 4.1, for $a = 2$.

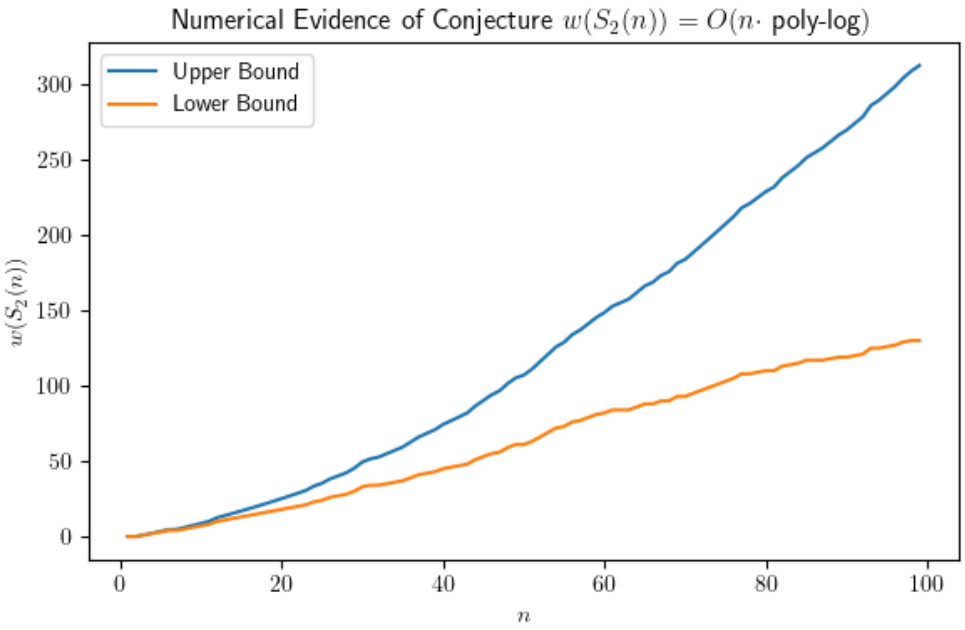

Figure 4.1: Numerical Evidence of Conjecture 4.2.1. The lower bound w' is the number of distinct primes in $S_2(n)$ in the range $< 10^8$. The upper bound has an extra correction term of $\frac{n(n-1)}{2} \log_{10^8}(2)$ which over counts the number of primes that $S_2(n)$ can have on the range $\geq 10^8$.

The limitation of these numerical computations is the number of primes can be saved in a computer in practice. The current program, 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, $\log_L(S_2(n)) \leq \log_L(2^{\sum_{m<n} m}) = \frac{n(n-1)}{2} \log_L(2)$.

4.2.4 Improvement on Artin's conjecture

Conjecture 4.2.1 gives a finer upper bound for the 4th term in Equation 4.1. This will let us choose a smaller ξ_3'. For this section, we assume Conjecture 4.2.1 and, to simplify the computations, we let the polylogarithmic part be trivial $L(n) = 1$. Hence, suppose

$w(S_a(n)) \leq C_a \cdot n$

Proposition 4.2.1 (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 4.1.6 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 4.1.10.

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

5. Common Factor

5.1 Lenstra's paper

5.2 General setting

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.

5.2.1 Spec $\mathbb{Z}[x]$

Proposition 5.2.1. 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 $V(p) \simeq \text{Spec } \mathbb{Z}[x]/(p) = \text{Spec } \mathbb{F}_p[x]$. The horizontal line at $x = 0$ is $V((x)) \simeq \text{Spec } \mathbb{Z}[x]/x = \text{Spec } \mathbb{Z}$.

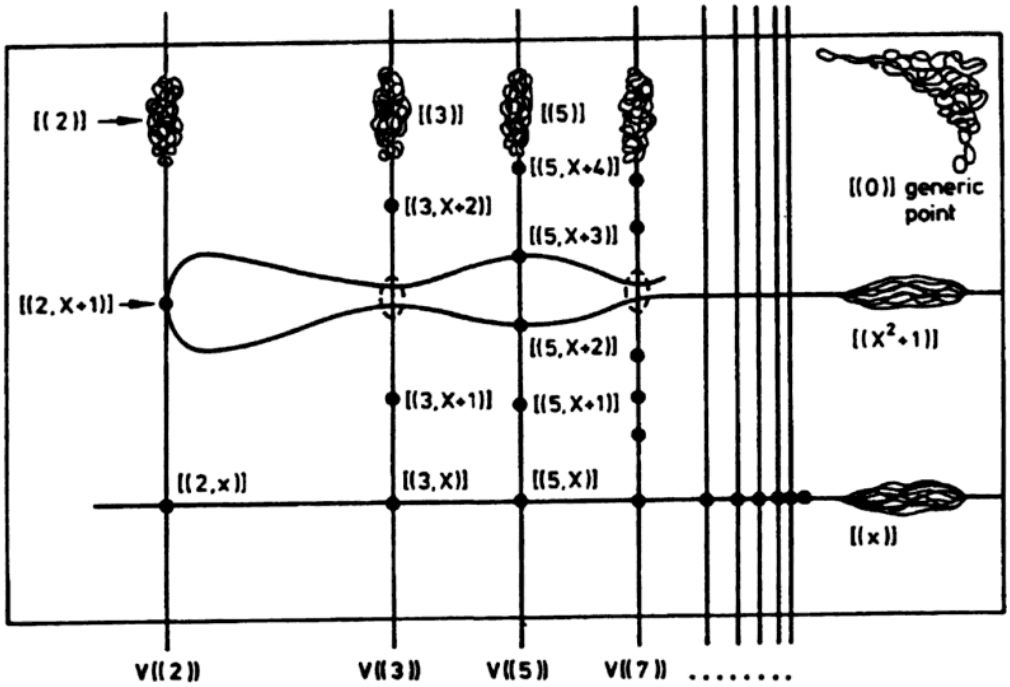

Figure 5.1: 2D Geometry of Spec $\mathbb{Z}[x]$. Picture taken from [3]

Comment. *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 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. *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 5.2.2 (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*

$$\textit{(1) } f \textit{ is irreducible modulo } p \qquad \textit{and} \qquad \textit{(2) } a \textit{ is a p.r. modulo } (f, p)$$

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. *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*

$$\textit{(1) } f_i \textit{ is irreducile modulo } p \qquad \textit{and} \qquad \textit{(2) } a \textit{ is a p.r. modulo } (f_i, p)$$

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. *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 5.2.1. *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 5.2.1.

5.2.2 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. *What properties does a ring R have to follow so that Artin conjecture is well posed on* 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. *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 5.2.1, 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.

5.2.3 Schemes

Proposition 5.2.3. *Given a scheme S of finite type (over* Spec $\mathbb{Z}$*), the residue fields at all closed points are finite.*

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

Question. *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

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

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

Estimates for $a = 2$ are given in Figure 4.1. For $a \in \{3, 4, 5, 6\}$, they are given below. These values include a square and a composite number. A detailed explanation of the lower and upper bounds can be found in Figure 4.1.

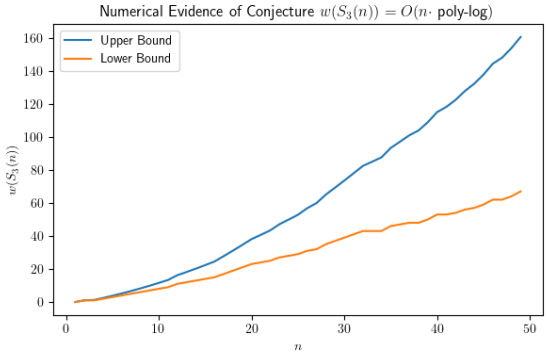

Figure 2: Computations $w(S_3(n))$

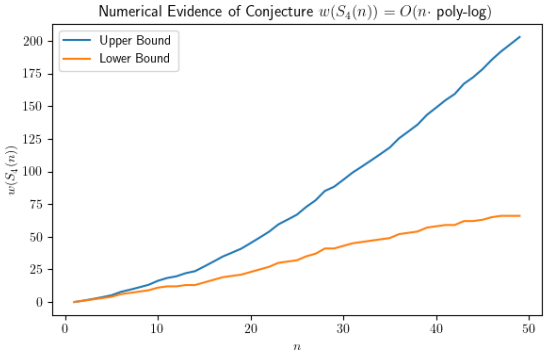

Figure 3: Computations $w(S_4(n))$

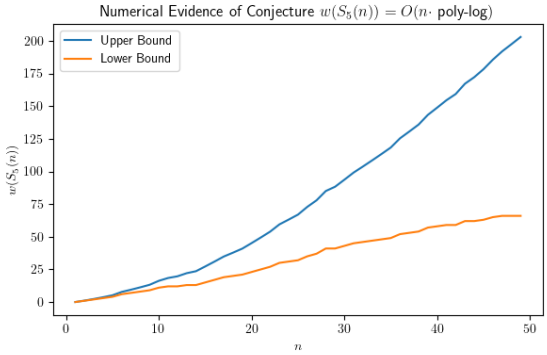

Figure 4: Computations $w(S_5(n))$

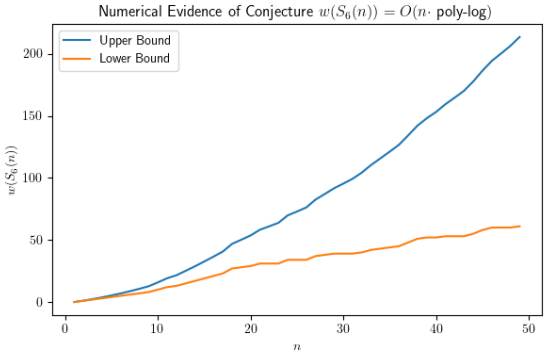

Figure 5: Computations $w(S_6(n))$

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

This is the exact version of the program used to compute the data in Figure 4.1.

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

typedef long long ll;

ll L = 1e8;

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

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

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

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