Artin's primitive root Conjecture

Javier López-Contreras

November 2022

Contents

1 Introduction

This is an informal note describing the readings, considerations and findings of the research I'm doing for the development of my Undergraduate Thesis.

Originally, the project was to read *Artin's primitivie root conjecture for function fields revisited*, by Kim & Murty [5] (and its corrigendum [4]) and generalize their proof to a wider setting. They describe a new elementary proof of result that was proven in 1937 by Bilharz [1], a student of Hasse. To the best of my understanding, I found a flaw on the main proof of the paper. I got in contact with the authors, which have not responded the emails yet.

Aiming to fill the flaw, I read Bilharz original proof, not from the original paper [1] (in german!), but from the exposition found in Chapter 10 of M.Rosen's book *Number Theory on Function Fields* [7]. The original proof takes a very different path and I don't think one can use it to fill the flaw without using the Riemann Hypothesis.

Lastly, I have been considering a more general problem that seems to be a common factor between the Conjecture over Function Fields and the Conjecture over $\mathbb{Z}$. From this setting, new natural problems arise.

2 Artin's primitive root Conjecture

Question. *Given an integer $a \in \mathbb{Z}$, are there infinitely many primes $p \in \mathbb{Z}$ such that $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ is a primitive root?*

The conjecture is that this happens if and only if $a \notin \{-1, 0, 1\}$. Artin's primitive root conjecture has been an open problem for more than a century. Hooley [3] 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

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 2.1 (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 2.1 (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.

3 Paper by Kim & Murty

The article [5] (and its corrigendum [4]) present a new proof of Theorem 2.1. Their proof doesn't depend on the Riemann Hypothesis over Function Fields, like the original proof did [1].

3.1 Overview of the paper

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

Lemma 3.1 (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 $a(x)$.

3.1.1 Sketch of proof of Lemma 3.1

Let φ be Euler's totient function.

Definition 3.1. *Given a cyclic group G, define*

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

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 when we bound, it will be the asymptotically important term.

Proposition 3.1. *With the definition above, we have*

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

Definition 3.2. *Given a $a(x) \in \mathbb{F}_q[x]$ monic, define $W_a : \mathbb{F}_q[x]^{irr} \to \mathbb{Z}$,*

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

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

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

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

Proposition 3.2. *For all $n \in \mathbb{Z}_{>0}$, the following equality holds.*

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

Proposition 3.3. *The set of upper bounds described in Lemma 3.1 imply that $\sum_{\theta \in \mathbb{F}_{q^n}^*} S(a(\theta))$ diverges as $n \to \infty$.*

Expanding the sum, one can see that, thanks to the set of upper bounds in Lemma 3.1, the leading term is absolutely asymptotically bigger than all of the other combined. Hence the sum diverges.

3.1.2 Sketch of proof of character bounds

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

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

Comment. *Here is where the necessary condition is needed. If a was a d-th power for some $d | q^i - 1$ 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}.*

Comment. *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 [2] 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.

3.2 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 3.3. *The second page of the corrigendum [4] 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*

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

with

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

The next paragraph states that this L-function is another form of the L-function given in the original paper [5]. I believe the error is in this equality of L-functions.

Definition 3.4. *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*

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

To equalize Definition 3.4 with Definition 3.3, 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 3.4 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 3.4.

Question. *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 3.3, we would need the equality of all the coefficients. Namely, $\forall n \geq 1$

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

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.

3.3 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 [2] proves that the L-function on Definition 3.4 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 3.4. It only comes up as a coefficient in the Definition 3.3, which, a priori, is not a polynomial nor does it follow an equality similar to the one found by Davenport.

It would also come up in an L-series like the one in Definition 3.4 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 necessarily $\leq B$. Hence, one should 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. (For instance, assuming the Riemann Hypothesis). This looks similar to Theorem 4 in [5] 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.

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

4 Original proof by Bilharz

Comment. *As M.Rosen exposes in Ch.10 [7], 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.

4.1 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 4.1. *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*

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

Theorem 4.1 (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 $K =$ 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 4.2. *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.

4.2 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.

5 Hooley's conditional proof

The project wasn't going to go into Artin's conjecture over $\mathbb{Z}$ because it looked too hard but, after the observations made in the next section I expect this proof to be important.

The proof starts with Artin's observation but the $n \to \infty$ is adhoc. I haven't read the adhoc part yet. TODO. Read the details

6 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.

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

Proposition 6.1. 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 $V((x)) \simeq \text{Spec } \mathbb{Z}[x]/x = \text{Spec } \mathbb{Z}$.

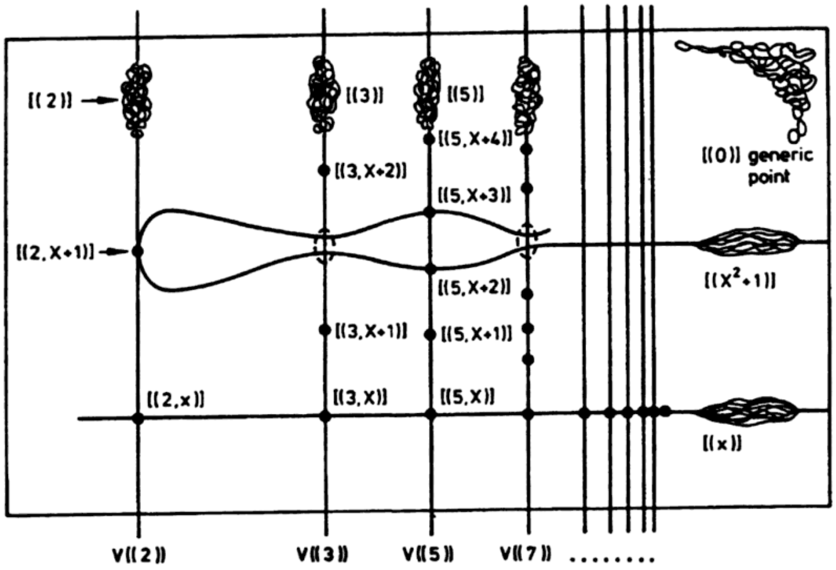

Figure 1: 2D Geometry of Spec $\mathbb{Z}[x]$. Picture taken from [6]

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 6.2 (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*

(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 $\mathrm{Frob}_{\mathbb{Q}_f/\mathbb{Q}}(p)$ 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 $\mathcal{F} = \{f_1, \ldots, \}$, $f_i \in \mathbb{Z}[x]$ 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. *Let $a \in \mathbb{Z}[x]$ and $\mathcal{F} = \{f_1, \ldots\}$. Then a follows Artin's conjecture on at least one of the number fields $\mathbb{Z}[x]/f_i$*

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 6.1. *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.

6.2 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 6.1, 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.

6.3 Schemes

Proposition 6.3. *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 $\operatorname{Spec}\mathbb{Z}[x_1,\ldots,x_n]/I$ + 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.

References

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.