Artin's primitive root conjecture: classically and over $\mathbb{F}_q[T]$

Ezra Waxman

University of Haifa

June 6^{th}, 2023

Decimal Expansion of Fractions

- In *Disquisitiones Arithmeticae* Gauss studied the decimal expansion of $\frac{1}{p}$, for prime p.
- Examples -
  - $\frac{1}{7} = 0.\overline{142857}$ has period 6
  - $\frac{1}{11} = 0.\overline{09}$ has period 2
  - $\frac{1}{13} = 0.\overline{076923}$ has period 6
  - $\frac{1}{17} = 0.\overline{0588235294117647}$ has period 16
- Are there any observable patterns to this behaviour?

Figure: Carl Friedrich Gauss (1777-1855)

Table:

Decimal expansion of $1/p$ for small primes $p \neq 2, 5$

p	$1/p$	decimal expansion	period	$p - 1$
3	1/3	$0.\overline{33}$	1	2
7	1/7	$0.\overline{142857}$	6	6
11	1/11	$0.\overline{09}$	2	10
13	1/13	$0.\overline{076923}$	6	12
17	1/17	$0.\overline{0588235294117647}$	16	16
19	1/19	$0.\overline{052631578947368421}$	18	18
23	1/23	$0.\overline{0434782608695652173913}$	22	22
29	1/29	$0.\overline{0344827586206896551724137931}$	28	28
31	1/31	$0.\overline{032258064516129}$	15	30
37	1/37	$0.\overline{027}$	3	36
41	1/41	$0.\overline{02439}$	5	40
43	1/43	$0.\overline{023255813953488372093}$	21	42
47	1/47	$0.\overline{0212765957446808510638297872340425531914893617}$	46	46

Decimal Expansion of Fractions

- We say that g is a **primitive root** mod p if $ord_g(p) = p - 1$, i.e. if g generates the group $(\mathbb{Z}/p\mathbb{Z})^\times$.
- Equivalently, g is said to be a primitive root mod p if

$$\frac{1}{p} = 0.\overline{a_1 \ldots a_{ord_g(p)}}$$

  has period $p - 1$ in base g.
- Gauss raised the question of how often 10 is a primitive root mod p, as p runs through the primes (but offered no precise conjecture).

Table:

Decimal expansion of $1/p$ for small primes $p \neq 2, 5$

p	$1/p$	decimal expansion	period	$p-1$
3	1/3	$0.\overline{33}$	1	2
7	1/7	$0.\overline{142857}$	6	6
11	1/11	$0.\overline{09}$	2	10
13	1/13	$0.\overline{076923}$	6	12
17	1/17	$0.\overline{0588235294117647}$	16	16
19	1/19	$0.\overline{052631578947368421}$	18	18
23	1/23	$0.\overline{0434782608695652173913}$	22	22
29	1/29	$0.\overline{0344827586206896551724137931}$	28	28
31	1/31	$0.\overline{032258064516129}$	15	30
37	1/37	$0.\overline{027}$	3	36
41	1/41	$0.\overline{02439}$	5	40
43	1/43	$0.\overline{023255813953488372093}$	21	42
46	1/47	$0.\overline{0212765957446808510638297872340425531914893617}$	46	46

Table:

Base 6 expansion of $1/p$ for small primes $p \neq 2$

p	$1/p$	base 6 expansion	period	p-1
5	1/5	$0.\overline{1}$	1	4
7	1/7	$0.\overline{05}$	2	6
11	1/11	$0.\overline{0313452421}$	10	10
13	1/13	$0.\overline{024340531215}$	12	12
17	1/17	$0.\overline{0.0204122453514331}$	16	16
19	1/19	$0.\overline{015211325015211325}$	18	18
23	1/23	$0.\overline{0132203044101322030441}$	22	22
29	1/29	$0.\overline{01124045443151}$	28	28
31	1/31	$0.\overline{010545}$	6	30
37	1/37	$0.\overline{0055}$	4	36
41	1/41	$0.\overline{0051335412440330234455042201431152253211}$	40	40
43	1/43	$0.\overline{005}$	3	42
46	1/47	$0.\overline{00433240302144201310521}$	23	46

Artin's Primitive Root Conjecture

- Suppose $g \in \mathbb{N}$ is not a perfect-square.
- Define

$$\mathcal{P}_g := \{p : ord_g(p) = p - 1\}$$

  to be the set of **Artin Primes** for g (i.e. primes p for which g is a primitive root mod p).
- **Artin Primitive Root Conjecture**: $\mathcal{P}_g$ *is infinite.*

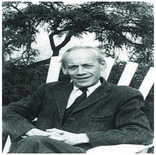

Figure: Emil Artin (1898 – 1962)

Artin's Primitive Root Conjecture

- The Primitive Root Conjecture is still unknown for any fixed g!
- Gupta and Murty (1983): There is a set S (consisting of 13 numbers) such that the Primitive Root Conjecture holds for some $g \in S$.
- Heath-Brown (1986): The Primitive Root Conjecture holds for either $g = 2$, $g = 3$, or $g = 5$.

Quantitative Primitive Root Conjecture

- Artin moreover wished to understand the asymptotic growth of $\mathcal{P}_g$.
- He conjectured that if $g \in \mathbb{N}$ is not a perfect power, then $\mathcal{P}_g$ has a natural density amongst the primes equal to

$$A := \prod_{q \text{ prime}} \frac{1}{1 - q(q-1)} \approx .3739558,$$

i.e. roughly 37% of primes are Artin primes.

Quantitative Primitive Root Conjecture

- In 1957, Derrick and Emma Lehmer set out to test Artin's conjecture using newly available computational methods.
- When studying the conjecture for $g = 5$, they noticed numerical deviations (roughly 5%) from Artin's predicted asymptotic.
- Indeed, it turns out that Artin's (quantitative) conjecture was imprecise for an infinite set of integers (not only $g = 5$).

Figure: Derrick and Emma Lehmer (August 21, 1974)

Artin Correction Factor

- Artin's conjecture had been built on the (false) heuristic assumption that any two field extensions of the form $\mathbb{Q}(\zeta_q, g^{1/q})$, q prime, are linearly disjoint over $\mathbb{Q}$.
- In response to the numerical data provided to him by the Lehmers, Artin put-forward a modified heuristic that corrects for subtle 'entanglements' between certain pairs of such field extensions.
- This modified heuristic provided a better match with the numerical data observed in the case $g = 5$.

Artin Correction Factor

- Lang and Tate (1965) eventually identified an analogous correction factor, c_g, for arbitrary (non-square) g.
- This modified heuristic was then proven to be correct by Hooley (1967), under the assumption of the **Generalized Riemann Hypothesis** (GRH).
- (**Hooley**, 1967): Suppose g is not a perfect power. Then under GRH,

$$\lim_{x\to\infty} \frac{\#\{p \in \mathcal{P}_g : p \leq x\}}{\#\{p \in \mathcal{P} : p \leq x\}} = c_g \cdot A,$$

  where $A \approx .3739558$ is **Artin's constant** (independent of g), and where $c_g \in \mathbb{Q}_{>0}$ is an explicit **correction factor** (depending on g).
  - Specifically, $c_g = 1$ if $\mathrm{disc}(\mathbb{Q}(\sqrt{g})) \not\equiv 1(4)$.

Artin Correction Factor

- In his letter to Artin, Derrick Lehmer assumes that Artin's conjecture was based on the following elementary heuristic:
- The group $(\mathbb{Z}/p\mathbb{Z})^\times$ has $p-1$ elements.
- The group $(\mathbb{Z}/p\mathbb{Z})^\times$ has $\varphi(p-1)$ generators, where

$$\varphi(n) := \{1 \leq k \leq n : gcd(k,n) = 1\}$$

  is Euler's totient function.
- The "probability" that g is a primitive root mod p may thus be approximated by $\varphi(p-1)/(p-1)$.
- Indeed,

$$\lim_{x \to \infty} \sum_{p \leq x} \frac{\varphi(p-1)}{p-1} \sim A \cdot \frac{x}{\log x}.$$

Probabilistic Interpretation

- We view each prime number as a "random event" (i.e. as a Bernoulli trial)
- To each prime number $p_i \in \mathbb{N}$ we assign a Bernoulli distributed random variable E_{p_i}, such that

$$E_{p_i} := \begin{cases} 1 & \text{with probability } \frac{\varphi(p_i - 1)}{p_i - 1}, \\ 0 & \text{with probability } 1 - \frac{\varphi(p_i - 1)}{p_i - 1}. \end{cases}$$

- We then consider the random variable

$$X_N := \sum_{p_i \le x} E_{p_i}$$

representing the number of successes amongst a sequence of N trials.

- The number of Artin primes $p \le x$ looks like a "typical" instance of X_N.
- Hence, we say that Artin primes exhibit a **Poisson binomial distribution** amongst the ordinary primes.

Artin Correction Factor

- Artin was not a fan of such elementary heuristics:
- "Dear Professor Lehmer,

  [...] I would like to stress the fact that the root of these questions belongs to *algebraic number theory* and should be viewed from this point of view. Any interpretation in terms of elementary number theory hides very essential insights into the nature of the questions. If you have the patience to study the following explanations I should think that you will agree (Jan 6, 1958)
- Artin then proceeds to provide Lehmer with a crash course in algebraic number theory. In a follow-up letter (January 28, 1958), he then described his modified heuristic, accounting for the 'entanglement' of the corresponding splitting fields.

Artin Correction Factor

- Indeed, the "Lehmer model"

$$\lim_{x\to\infty} \sum_{p\leq x} \frac{\varphi(p-1)}{p-1} \sim A \cdot \frac{x}{\log x}$$

  fails to account for the correction factor first identified by Derrick and Emma Lehmer.

- Years later, however, Pieter Moree discovered that the appropriate correction factor may still indeed be obtained by elementary methods, specifically, by a refinement of the Lehmer model that takes into account "quadratic" interactions.

Moree's Improved Heuristic

- Let
$$\left(\frac{g}{p}\right) := g^{\frac{p-1}{2}} (\text{mod } p)$$
denote the Legendre symbol. Then
$$\left(\frac{g}{p}\right) = 1 \Leftrightarrow g^{\frac{p-1}{2}} \equiv 1 (\text{mod } p),$$
i.e. g is **not** a primitive root mod p.
- In other words, a necessary condition for g to be a primitive root mod p is for $\left(\frac{g}{p}\right) = -1$.

Moree's Improved Heuristic

Moree's Probabilistic Model:

- There are $\frac{(p-1)}{2}$ elements $1 \leq g \leq p-1$ such that $\left(\frac{g}{p}\right) = -1$.
- The group $(\mathbb{Z}/p\mathbb{Z})^{\times}$ has $\varphi(p-1)$ generators
- The likelihood that a "random" prime p lies in $\mathcal{P}_g$ may therefore be assigned the probability

$$w_g(p) := \begin{cases} \frac{\varphi(p-1)}{(p-1)/2} & \text{if } \left(\frac{g}{p}\right) = -1, \\ 0 & \text{if } \left(\frac{g}{p}\right) = 1. \end{cases}$$

- Indeed, we find that

$$\lim_{x\to\infty} \sum_{p\leq x} w_g(p) \sim c_g \cdot A \cdot \frac{x}{\log x},$$

as desired.

Moree's Improved Heuristic

Moree's Probabilistic Model:

- Moree's model can be used to accurately model a wide class of Artin-type problems. For example, it correctly counts the asymptotic number of Artin primes in an arithmetic progression up to x (including the appropriate correction factor).
- It arrives at the same heuristic predictions as the more "sophisticated" models using purely elementary models.
- It has a simple interpretation, namely it highlights the fact that the Artin primes exhibit a **Poisson binomial distribution** amongst the ordinary primes.

An Artin Twin Prime Conjecture

In our work, we consider **Twin Primes**.

- Let $\pi_d(x)$ count the number of primes $p \leq x$ such that p and $p + d$ are both prime.
  - Theorem (Zhang, 2013): There are infinitely many prime pairs $(p, p + d)$ for some $d \leq 70,000,000$.
  - Theorem (Maynard, 2013): There are infinitely many prime pairs $(p, p + d)$ for some $d \leq 600$.
  - Theorem (Polymath, 2014): There are infinitely many prime pairs $(p, p + d)$ for some $d \leq 246$.

An Artin Twin Prime Conjecture

- **Quantitative Twin Prime Conjecture** (Hardy, Littlewood):

$$\pi_d(x) \sim C_d \cdot \frac{x}{\log^2 x},$$

  where

$$C_d := 2 \cdot \prod_{p \text{ prime}} \left(\frac{p(p-2)}{(p-1)^2} \right) \prod_{p \mid d} \left(\frac{p-1}{p-2} \right).$$

- In particular,

$$C_2 \approx 0.6601618158$$

  is referred to as the **twin prime constant**.

An Artin Twin Prime Conjecture

- In our work we consider **Artin Twin Primes**.
- Let

$$\pi_{d,g}(x) : \#\{p \leq x : p, p + d \in \mathcal{P}_g\}$$

  count such pairs for which p and $p + d$ are both **Artin** primes in base g.
- What is the asymptotic behavior of $\pi_{d,g}(x)$, in the limit as $x \to \infty$?

A Twin Artin Prime Conjecture

- Conjecture (Tinková, EW, Zindulka):

$$\lim_{x\to\infty} \frac{\pi_{d,g}(x)}{\pi_d(x)} = \mathbf{c}_g(d)\mathbf{A}(d).$$

- In other words, the **density** of Twin Artin primes amongst ordinary twin prime pairs is $\mathbf{c}_g(d)\mathbf{A}(d)$.
- $\mathbf{A}(d)$ is a constant that comes from the "naive" model.
- $\mathbf{c}_g(d)$ is a correction factor, that comes from applying Moree's improved heuristic.

A Twin Artin Prime Conjecture

- Conjecture (Tinková, EW, Zindulka, 2020):

$$\pi_{d,g}(x) \sim \mathbf{c}_g(d)\mathbf{A}(d)\mathfrak{S}(d)\frac{x}{(\log x)^2} \qquad (1)$$

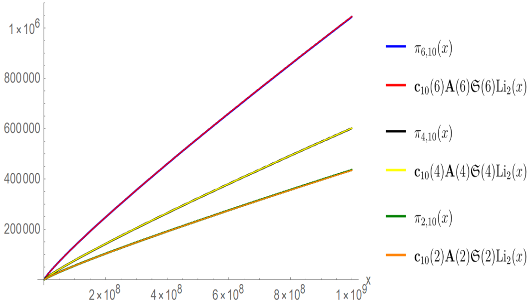

Figure: Twin, Cousin, and Sexy Artin primes up to $x = 10^9$ (g = 10)

Twin Artin Primes: prime pairs (p,p+2) both of which are Artin primes (with root g)

Cousin Artin Primes: prime pairs (p,p+4) both of which are Artin primes (with root g)

Sexy Artin Primes: prime pairs (p,p+6) both of which are Artin primes (with root g)

Twin Prime Conjecture

- Slightly more generally: let

$$\pi_{d_1,\ldots,d_k}(x) := \#\{p \le x : p, p+d_1, p+d_2, \cdots, p_{d_k} \text{ are all prime}\}$$

  denote the number of primes $p \le x$ such that $(p, p+d_1, \ldots, p+d_k)$ are all prime.

- **Hardy Littlewood Conjecture** (1922):

$$\pi_{d_1,\ldots,d_k}(x) \sim C_2 \cdot \frac{x}{\log^2 x},$$

  where

$$C_{d_1,\ldots,d_k} := \prod_{p \text{ prime}} \left(\frac{1-\omega_d(p)/p}{(1-1/p)^k} \right)$$

  is referred to as the **singular series**.

Artin Hardy-Littlewood Conjecture

- One may then consider an **Artin-HLW Conjecture**.
- Let

$$\pi_{d_1,\ldots,d_k,\mathrm{g}}(x) := \#\{p \leq x : p, p+d_1 \ldots p+d_k \in \mathcal{P}_g\}$$

  count the number of prime k-tuples less than x, all of which lie in $\mathcal{P}_g$.
- Conjecture (Liu, EW, 2022):

$$\pi_{d_1,\ldots,d_k,\mathrm{g}}(x) \sim \mathbf{c}_{\mathrm{g}}(\mathbf{d})\mathbf{A}(\mathbf{d})\mathfrak{S}(\mathbf{d})\frac{x}{(\log x)^k}$$

Artin Hardy-Littlewood Conjecture

- Conjecture (Liu, EW, 2022):

$$\pi_{d_1,\dots,d_k,\mathrm{g}}(x) \sim \mathbf{c}_{\mathrm{g}}(\mathbf{d})\mathbf{A}(\mathbf{d})\mathfrak{S}(\mathbf{d})\frac{x}{(\log x)^k}$$

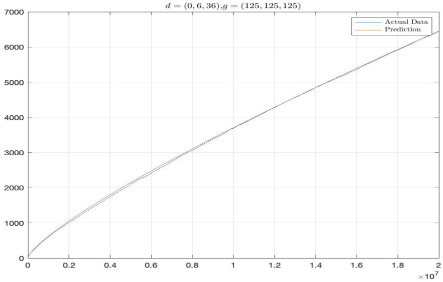

Figure: Artin Prime three-tuples: prime triples $(p, p+6, p+36)$ all of which are Artin primes (with root $g = 125$)

Artin Hardy-Littlewood Conjecture

Proof Concept: The above conjectures are composed from a synthesis of two different probabilistic models, namely:

- **Moree's Model**: primitive roots mod p are uniformly distributed over permissible residue classes $[1, \cdots, p-1]$.
- **Hardy Littlewood Conjecture**: primes mod q are uniformly distributed across residue classes $[1, \ldots, q-1]$

Artin over Global Function Fields

Artin's primitive root conjecture may also be viewed geometrically:

- Instead of primes $p \in \mathbb{Z}$, we now count *closed points* $\mathfrak{p} \in X$, where X denotes a (geometrically integral) projective variety over $\mathbb{F}_q$.
- Instead of $(\mathbb{Z}/p\mathbb{Z})^\times$, we now ask about $\kappa_\mathfrak{p}^*$, where $\kappa_\mathfrak{p}$ denotes the *residue field* attached to a closed point $\mathfrak{p} \in X$.
- We say that g is a *primitive root* modulo $\mathfrak{p}$ if g generates $\kappa_\mathfrak{p}^*$, where g now lies in the *function field* $\mathbb{F}_q(X)$.

Artin over $\mathbb{F}_q[t]$

- For example, let $\mathbb{F}_q[t]$ denote the ring of polynomials with coefficients in $\mathbb{F}_q$, and $\mathcal{P}_n \subset \mathbb{F}_q[t]$ the subset of prime monic polynomials of degree n.
- For a polynomial $g(t) \in \mathbb{F}_q[t]$, let $\mathrm{ord}_P(g(t))$ denote the order of $g(t)$ in the multiplicative group $(\mathbb{F}_q[t]/(P))^\times$, where $(P) \subseteq \mathbb{F}_q[t]$ denotes some prime ideal.
- We then study the size of the set

$$\mathcal{P}_g(n) = \#\{P \in \mathcal{P}_n : ord_P(g) = q^n - 1\},$$

i.e. we ask how often $g(t)$ generates the group $(\mathbb{F}_q[t]/(P))^\times$ (as $n \to \infty$).

- Primitive polynomials are of practical interest for engineering applications concerning sequences and LFSRs (linear feedback shift registers)

Artin over Global Function Fields

- **Artin's Primitive Root Conjecture for $\mathbb{F}_q(X)$:** *Suppose $g \in \mathbb{F}_q(X) \setminus \mathbb{F}_q$ is not an ℓ^{th} power for any prime $\ell \mid q-1$. Then g is a primitive root mod $\mathfrak{p}$, for infinitely many closed points $\mathfrak{p} \in X$.*
- The special case in which X is a (non-singular) projective curve was solved by Hasse's student Bilharz (1937). His result was conditional on the Riemann Hypothesis for global function fields - a theorem subsequently established by Andre Weil (1948).
- However, his proof contains a gap (first identified by Yu) for cases in which $g \in \mathbb{F}_q(X)$ is **non-geometric**.
- As in the classical set-up, Bilharz's proof fails to account for a relevant correction factor $\rho_g(n)$, which emerges for non-geometric $g \in \mathbb{F}_q(X)$.

- (Hochfilzer, EW - 2023) Let X denote a projective variety of dimension r, and let $N_X(g, n)$ count the number of closed points $\mathfrak{p} \in X$ of degree n such that $g \in \mathbb{F}_q(X)$ generates $\kappa_{\mathfrak{p}}^*$. Then

$$N_X(g,n) = \rho_g(n)\left(\frac{\varphi(q^n-1)q^{n(r-1)}}{n} + O_\epsilon\left(q^{n(r-1/2)+\epsilon}\right)\right),$$

where $\rho_g(n)$ is an explicit *correction factor*.

- In particular, $\rho_g(n) = 1$ whenever $g \in \mathbb{F}_q(X)$ is **geometric**.
- The special case in which X is a projective curve (i.e. $r = 1$) and $g \in \mathbb{F}_q(X)$ is geometric, was previously worked out by Pappalardi and Shparlinski.
- As a corollary, we conclude that Artin's primitive root conjecture holds for any algebraic function field over $\mathbb{F}_q$.

Proof Idea

For any $g \in (\mathbb{Z}/p\mathbb{Z})^\times$, we define

$$f_p(g) := \begin{cases} 1 & \text{if } ord_p(g) = p-1 \\ 0 & \text{otherwise.} \end{cases}$$

One may decompose $f_p(g)$ into a sum over *sifting functions*

$$f_p(g) = \sum_{k|p-1} \mathcal{S}_k(p),$$

where

$$\mathcal{S}_k(p) := \frac{\varphi(p-1)}{p-1} \sum_{k|p-1} \frac{\mu(k)}{\varphi(k)} \sum_{\mathrm{ord}\,\chi = k} \chi(g).$$

Here μ is the Möbius function, and the inner sum runs over the multiplicative characters of $(\mathbb{Z}/p\mathbb{Z})^\times$ with order precisely k.

Proof Idea

- The *linear* contribution comes from the sifting function
$$\mathcal{S}_1(p) = \frac{\varphi(p-1)}{p-1},$$
while the *quadratic* contribution comes from the sifting function
$$\mathcal{S}_2(p) = -\frac{\varphi(p-1)}{p-1}\left(\frac{g}{p}\right)$$
- We then find that
$$\mathcal{S}_1(p) + \mathcal{S}_2(p) = w_g(p) = \begin{cases} \frac{\varphi(p-1)}{(p-1)/2} & \text{if } \left(\frac{g}{p}\right) = -1 \\ 0 & \text{if } \left(\frac{g}{p}\right) = 1. \end{cases}$$
- Moree's model amounts to the conjecture that the asymptotic contribution of $\mathcal{S}_k(p)$ is negligible for all $k > 2$.
- The Artin HLW conjecture is obtained via a similar construction, alongside an application of the Hardly Littlewood Conjecture.

Proof Idea

- Over $\mathbb{F}_q(X)$, the following proposition may be used to **prove** that the asymptotic contribution of $\mathcal{S}_k(p)$ is negligible for all $k > 1$.
- **Proposition** (Weil; Hochfilzer, EW): Let X be a projective variety of dimension r, and let $\chi \in \widehat{\mathbb{F}_q^\times}$ denote a non-trivial character. Let $\mathcal{R}_g \subset X(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points on X that are neither zeroes nor poles of an appropriately chosen $g \in \mathbb{F}_q(X)$. Then

$$\sum_{\rho \in \mathcal{R}_g} \chi(g(\rho)) \ll_X q^{r-1/2}. \tag{2}$$

Further Exploration

- One long-term goal of these results is to better understand how the sifting function perspective relates to the more "traditional" heuristic of Artin (i.e. Hooley's approach).
- In particular, it would be nice to identity the family of L-functions hidden behind our application of Weil's result with those in Hooley's conditional proof (HRH).
- An end-goal would be to see if the sifting approach (i.e. Moree's model) can be transformed into a new (conditional) proof of Artin's Primitive Root Conjecture, in the classical setting.

Thank You!