Artin's conjecture on primes with prescribed primitive roots

Javier López-Contreras

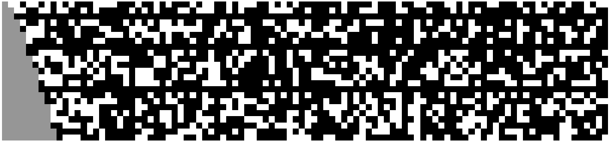
Supervised by Sug Woo Shin

April 27, 2023

Objective

Conjecture (Artin's Conjecture)

Given $a \in \mathbb{Z}$, $a \notin \{-1, 0, 1\} \cup \{k^2 \mid k \in \mathbb{Z}_{>1}\})$, there are infinitely many primes p such that a is a primitive root in $(\mathbb{Z}/p\mathbb{Z})^*$.



- Rows represent values of $a \in \mathbb{Z}$, increasing from top to bottom.
- Columns represent primes p, increasing from left to right.
- A cell is painted white if a is a primitive root $\mod p$

Structure of the talk

1. Overview of the conjecture
2. Artin's Observation. A precise conjectured density
3. Hooley's Theorem. The Riemann Hypothesis solves the problem

Part 1

Overview of the conjecture

Motivation. *Disquisitiones Arithmeticae* 314-317

Why does the decimal expression of $\frac{3}{7}$ have a period of length 6, while the expression of $\frac{1}{11}$ has a shorter period, of only 2 digits?

$$\frac{3}{7} = 0.428571\ 428571\ 428571\ldots \qquad \frac{1}{11} = 0.09\ 09\ 09\ldots$$

Remark

For p a prime and $a \in \mathbb{Z} \cap [1, p-1]$, the length of the decimal period of $\frac{a}{p}$ is $\mathrm{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(10)$.

$$\frac{a}{p} = \left(\frac{a_1}{10} + \cdots + \frac{a_s}{10^s}\right)\left(1 + \frac{1}{10^s} + \cdots\right) = \left(10^{s-1}a_1 + \cdots + a_s\right)\frac{1}{10^s - 1}$$

$$a(10^s - 1) = Mp \implies 10^s = 1 \mod p$$

Motivation II. *Disquisitiones Arithmeticae* 314-317

Remark

Given $a, b \in \mathbb{Z} \cap [1, p-1]$ such that $b = 10^\lambda a \mod p$ for some λ, then period of $\frac{b}{p}$ is a cyclic translation of the period of $\frac{a}{p}$.

$$b_i = \left\lfloor \frac{10^i b}{p} \right\rfloor \mod 10 = \left\lfloor \frac{10^i (10^\lambda a + Np)}{p} \right\rfloor \mod 10 = a_{i+\lambda}$$

Question

For which primes p are the periods of $\frac{a}{p}$ all translations of the period of $\frac{1}{p}$?

This is tantamount to asking for which primes is 10 a primitive root.

History

1927. In a letter to Helmut Hasse, Emil Artin proposes a precise density conjecture.

1937. Herbert Bilharz, a student of Hasse, solves the equivalent problem for $\mathbb{F}_q[x]$.

1957. With the aid of a computer, Emma and Derrick H. Lehmer observed that the conjectured density formula was not correct.

1967. Christopher Hooley proves that the Generalized Riemann Hypothesis implies Artin's conjecture.

1983. Rajiv Gupta and Ram Murty unconditionally prove that there is a set of 13 integers such that at least one of them follows Artin's conjecture. In 1985, this was improved by Heath-Brown to $a \in \{2, 3, 5\}$.

Part 2

Artin's Observation.

A precise conjectured density

Background. Dirichlet's Density

Inspired by Dirichlet's theorem about primes in arithmetic progressions.

$$\sum_{p=an+b \text{ prime}} \frac{1}{p}$$

Definition (Dirichlet's Density)

For $S \subseteq \operatorname{Spec} \mathcal{O}_K$, define

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

Good number theoretical density because it can often be related with special values of L-functions.

Artin's Observation

Conjecture (Artin's conjectured density)

Given a non-square integer $a \in \mathbb{Z}_{>1} \setminus \mathbb{Z}^2$, the density of primes where a is a primitive root is

$$A(a) = \delta(a) \prod_{l \text{ prime}} \left(1 - \frac{1}{l(l-1)}\right) \approx 0.3739558 \cdot \delta(a)$$

where $\delta(a)$ is an explicit correction factor that is 1 for most a.

Without loosing much flavor, we may assume $a = 2$, which makes $\delta(a) = 1$.

Artin's Observation II. Key Lemma

Lemma

a is a primitive root mod p if and only if there isn't any $l \in \mathbb{Z}$ prime such that

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

Lemma (Key Lemma)

A prime l follows the conditions (1) and (2) for $p > 2$ if and only if p is completely split over $L_l/\mathbb{Q}$, where $L_l = \mathbb{Q}(\zeta_l, a^{1/l})$.

This is a surprising link with Algebraic Number Theory.

Artin's Observation III. Chebotarev's theorem

Let k be square-free positive integer.

Lemma

All the primes $l \mid k$ follow the conditions (1) and (2) for $p > 2$ if and only if p is completely split over $L_k/\mathbb{Q}$, where $L_k = \prod_{l|k} L_l = \mathbb{Q}(\zeta_k, a^{1/k})$.

Chebotarev's theorem yields that the density of

$$\{p \mid p > 2 \text{ prime such that } \forall l \mid k \text{ conditions (1) and (2) are met}\}$$

is $\frac{1}{[L_k:\mathbb{Q}]}$.

Artin's Observation III. Computation of the degree

Lemma

For $a = 2$, the aforementioned degree equals $[L_k : \mathbb{Q}] = \varphi(k)k$.

This is where Artin's original statement was incorrect for some values of a.

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

Artin's Observation IV. Inclusion-Exclusion

Let k be square-free positive integer.

Theorem (Artin's observation)

The density of primes for which there is no $l \mid k$ following the conditions (1) and (2) is

$$A_k(a) = \sum_{\substack{k'|k \\ k' \geq 1}} \frac{\mu(k')}{[L_{k'} : \mathbb{Q}]} = \sum_{\substack{k'|k \\ k' \geq 1}} \frac{\mu(k')}{k'\varphi(k')} \underset{\textit{Euler Product}}{=} \prod_{l|k} \left(1 - \frac{1}{l(l-1)}\right)$$

where μ is the Möebius Inversion function.

As one makes k tend to infinity over the primordials, the primes counted by A_k are "closer" to being primitive roots. Yet, this *passing to limit* is where the difficulty in Artin's conjecture lies.

Part 3

Hooley's Theorem

The Riemann Hypothesis solves the problem

Hooley's Theorem

Theorem (Hooley, 1967)

The Generalized Riemann Hypothesis over the Number Fields $\mathbb{Q}(\zeta_k, a^{1/k})$ *imply Artin's Conjecture about the density of primes with a prescribed primitive root at* $a \in \mathbb{Z}_{>1} \setminus \mathbb{Z}^2$.

Sketch of the proof

- Sieve primes by intervals
- Reduce to the problem of counting primes
- Result on vertical distribution of Riemann Zeroes under GRH

Hooley's Theorem II. Prime counting functions

Definition (Prime counting functions)

1. $N_a(x) = \#\{p < x \mid a \text{ is a p.r.} \mod p\}$
2. $P_a(x, k) = \#\{p < x \mid \forall q \mid k,\ q \text{ follows } (1\ \&\ 2)\}$
3. $N_a(x, \xi) = \#\{p < x \mid \ \nexists\, q \text{ following } (1\ \&\ 2) \text{ in the range } q < \xi\}$
4. $M_a(x, \xi_1, \xi_2) =$
$$= \{p < x \mid \exists\, q \text{ following } (1\ \&\ 2) \text{ in the range } \xi_1 < q \leq \xi\}$$

Lemma (Artin's Observation)

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

as l' goes over square-free integers with all prime factors $\leq \xi$.

Hooley's Theorem III. Hooley's Sieve

Let $\xi_1 = \frac{1}{6}\log x, \xi_2 = x^{1/2}\log^{-2} x, \xi_3 = x^{1/2}\log x$.

Lemma

$$N_a(x) = \underbrace{N_a(x,\xi_1)}_{\sim A(a)\frac{x}{\log x}} + \underbrace{O(M_a(x,\xi_1,\xi_2))}_{\preccurlyeq \frac{x}{(\log x)^2}} + \underbrace{O(M_a(x,\xi_2,\xi_3))}_{\preccurlyeq \frac{x\log\log x}{(\log x)^2}} + \underbrace{O(M_a(x,\xi_3,x-1))}_{\preccurlyeq \frac{x}{(\log x)^2}}$$

1. Term 3 and 4 are easy to bound and don't require RH.
2. Both the bound on Term 2 and the estimation of Term 1 require RH

Hooley's Theorem IV. Reduction to counting primes

Definition (Prime counting function)

For $k \in \mathbb{Z}_{>0}^{\text{square-free}}$, let $L_k = \mathbb{Q}(\sqrt[k]{a}, \zeta_k)$ and $n(k) = [L_k : \mathbb{Q}]$. Then, define

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

Lemma

Then,

$$n(k)P_a(x,k) = \pi(x,k) + \underbrace{O(n(k)w(k))}_{e_p>1} + \underbrace{O(n(k)x^{1/2})}_{f_p>1}$$

where $w(k)$ is the number of unique prime factors of k.

- L_k is Galois $\implies p\mathcal{O}_{L_k} = \mathfrak{p}_1^{e_p} \dots \mathfrak{p}_{g_p}^{e_p}$ with $f_p = [\mathcal{O}_{L_k}/\mathfrak{p}_i : \mathbb{F}_p]$
- $\mathcal{N}(\mathfrak{p}_i) = p^{f_p}$
- Almost all primes counted are totally split

Hooley's Theorem V. Prime counting estimation

Theorem (Main Theorem)

Assuming the Generalized Riemann Hypothesis for $\zeta_{L_k}(z)$, we have the estimate

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

- $\pi(x,k)$ can be computed from the Riemann Zeroes
- Hooley's estimation follows from a theorem about the vertical distribution of Riemann Zeroes under GRH.
- The $1/2$ error term cannot be lowered

Thank you for your attention

jlopezcontreras10@gmail.com

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Centre de Formació Interdisciplinària Superior

Berkeley
UNIVERSITY OF CALIFORNIA

Annex

Extra Slides

Background I. Number Fields

A Number Field K is a finite field extension of $\mathbb{Q}$.

Given a Number Field, one can define its ring of integers $\mathcal{O}_K$, which is a generalization of $\mathbb{Z} \subseteq \mathbb{Q}$.

$$\begin{tikzcd}
K \arrow[d, dash] & \mathcal{O}_K \arrow[l, hook'] \arrow[d, dash] \\
\mathbb{Q} & \mathbb{Z} \arrow[l, hook']
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
p\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_n \arrow[d, dash] \\
p
\end{tikzcd}$$

In these rings, factorization of ideals as a product of prime ideals is unique.

Definition (Completely split prime)

A prime p is called completely split over K if $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$ and the residue fields $(\mathcal{O}_K/\mathfrak{p}_i) \simeq \mathbb{F}_p$

Background III. Chebotarev's Theorem

Theorem (Chebotarev's Density Theorem. Simplified Version)

Let $K/\mathbb{Q}$ be a finite Galois extension. The Dirichlet Density of the set S of primes $\mathfrak{p} \subseteq \mathbb{Q}$ that are totally split over K is

$$\delta(S) = \frac{1}{[K : \mathbb{Q}]}$$

For example, when $K = \mathbb{Q}(\zeta_n)$ a prime splits completely if and only if $p = 1 \mod n$. They have density $\frac{1}{\varphi(n)}$.

Estimation of term 1

Lemma (Estimation of the 1st term)

$$N_a(x,\xi_1) = \sum_{l'} \mu(l') \left(\frac{x}{\log x \cdot n(l')} + O(x^f \log x) \right) =$$

$$\underset{l'<e^{2\xi_1}}{=} \frac{x}{\log x} \sum_{l'} \frac{\mu(l')}{n(l')} + O\left(\sum_{l<e^{2\xi_1}} x^f \log x \right) =$$

$$= A(a)\frac{x}{\log x} + O(e^{2\xi_1} x^f \log x) =$$

$$= A(a)\frac{x}{\log x} + O(x^{f+1/3} \log x)$$

Bound of term 2

Lemma (Bound of the 2nd term)

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

Bound of term 3

Lemma (Bound of the 3rd term)

Let $\xi_2 = x^{1/2}\log^{-2} x$ *and* $\xi_3 = x^{1/2}\log x$. *Then* $M_a(x, \xi_2, \xi_3) = O\left(\frac{x}{\log^2 x}\right)$.

In particular $p \equiv 1 \mod q$. By Brun's method, which is an inequality related to Dirichlet's Theorem, we have

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

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

Bound of term 4

Lemma (Bound of the 4th term)

Let $\xi_3 = x^{1/2}\log x$, *then*

$$M_a(x, \xi_3, x-1) = O\left(\frac{x}{\log^2 x}\right) \tag{3}$$

In particular $a^{\frac{p-1}{q}} = 1 \mod p$. Hence, if there is a $q > \xi_3$ that follows the Lemma, there will be an $m < \frac{x}{\xi_3}$ such that $p|a^m - 1$. All the primes counted on $M_a(x, \xi_3, x-1)$ need to be divisors of

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