# Artin's conjecture on primes with prescribed primitive roots

Javier López-Contreras

Supervised by Sug Woo Shin

April 29, 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: $a \in \mathbb{Z}$, increasing from top to bottom.

- Columns: primes $p$, increasing from left to right.

- A cell is white if $a$ is a primitive root $\mod p$

# History

1927. Emil Artin proposes a precise density conjecture.

1937. Herbert Bilharz solves the equivalent problem for $\mathbb{F}_q[x]$.

1957. Emma and Derrick H. Lehmer observe that the conjectured density is incorrect.

1967. Christopher Hooley proves AC under GRH.

1983. Rajiv Gupta and Ram Murty give a set of 13 integers such that at least one of them follows AC.

1985. Heath-Brown improves their argument to $\{2, 3, 5\}$.

# History

1927. **Emil Artin proposes a precise density conjecture.**

1937. Herbert Bilharz solves the equivalent problem for $\mathbb{F}_q[x]$.

1957. Emma and Derrick H. Lehmer observe that the conjectured density is incorrect.

1967. **Christopher Hooley proves AC under GRH.**

1983. Rajiv Gupta and Ram Murty give a set of 13 integers such that at least one of them follows AC.

1985. Heath-Brown improves their argument to $\{2, 3, 5\}$.

Part 1

# Artin's Observation

A precise conjectured density

# 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 $\delta(a) = 1$.

# 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

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

## Lemma (Key Lemma)

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

- By Chebotarev's Density Theorem, they have density $\frac{1}{[\mathbb{Q}(\zeta_l, a^{1/l}):\mathbb{Q}]}$

# 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*

$$A_k(a) = \sum_{d \mid k} \frac{\mu(d)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]}$$

*where $\mu$ is the Möebius Inversion function.*

- Conjecture:

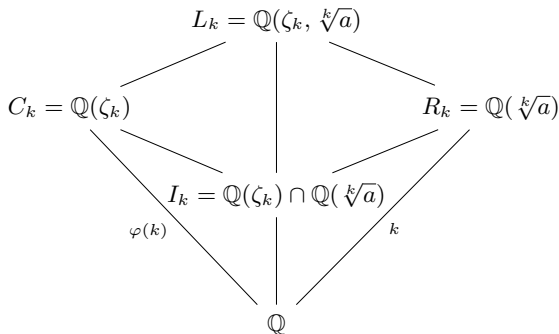$$\lim_{k \text{ primordial}} A_k(a) = A(a)$$

- This *passing to limit* is where the difficulty lies.

# Computation of the degree

> **Lemma**
>
> For $a = 2$, $[\mathbb{Q}(\zeta_k, a^{1/k}) : \mathbb{Q}] = \varphi(k)k$.

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



$$L_k = \mathbb{Q}(\zeta_k, \sqrt[k]{a})$$

$$C_k = \mathbb{Q}(\zeta_k) \qquad\qquad R_k = \mathbb{Q}(\sqrt[k]{a})$$

$$I_k = \mathbb{Q}(\zeta_k) \cap \mathbb{Q}(\sqrt[k]{a})$$

$\varphi(k)$ $\qquad\qquad$ $k$

$$\mathbb{Q}$$

Part 2

# 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 prime ideals with bounded norm
- Result on vertical distribution of Riemann Zeroes under GRH

# 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

# 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

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

Almost all prime ideals come from totally split primes in $\mathbb{Q}$

### Lemma

*Then,*

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

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

- $L_k$ is Galois $\implies p\mathcal{O}_{L_k} = \mathfrak{p}_1^{e_p} \ldots \mathfrak{p}_{g_p}^{e_p}$ with $f_p = [\mathcal{O}_{L_k}/\mathfrak{p}_i : \mathbb{F}_p]$
- $\mathcal{N}(\mathfrak{p}_i) = p^{f_p} \leq x \implies p \leq x^{1/f_p}$

# Effective prime counting estimate

## Theorem (Main Theorem)

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

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

- $\pi(x, k)$ can be computed from the Riemann Zeroes
- Result about the vertical distribution of Riemann Zeroes under GRH.

# Thank you for your attention

jlopezcontreras10@gmail.com

Annex

# Extra Slides

## 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 $\operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^{\times}}(10)$.*

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

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

# 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 $\lambda$, 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.

# Gauss' Party Trick

| | | | |
|---|---|---|---|
| $\frac{1}{7}$ | 0.142857 | 142857 | ... |
| $\frac{2}{7}$ | 0.2857 | 142857 | ... |
| $\frac{3}{7}$ | 0.42857 | 142857 | ... |
| $\frac{4}{7}$ | 0.57 | 142857 | ... |
| $\frac{5}{7}$ | 0.7 | 142857 | ... |
| $\frac{6}{7}$ | 0.857 | 142857 | ... |

# 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 $\mathbb{Z} \subseteq \mathbb{Q}$.

$$
\begin{array}{ccc}
K & \longleftrightarrow & \mathcal{O}_K \\
\big| & & \big| \\
\mathbb{Q} & \longleftrightarrow & \mathbb{Z}
\end{array}
\qquad\qquad
\begin{array}{c}
p\mathcal{O}_K = \mathfrak{p}_1 \ldots \mathfrak{p}_n \\
\big| \\
p
\end{array}
$$

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. 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

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

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

# 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 $\frac{1}{\varphi(n)}$.

# 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 $L_k = \prod_{l \mid k} L_l = \mathbb{Q}(\zeta_k, a^{1/k})$.*

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

# 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. $N_a(x, \xi) = \#\{p < x \mid \ \nexists q \text{ following (1 \& 2) in the range } q < \xi\}$
4. $M_a(x, \xi_1, \xi_2) =$
   $= \{p < x \mid \exists q \text{ following (1 \& 2) in the range } \xi_1 < q \leq \xi\}$

## 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 $\leq \xi$.*

# 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)**

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

$$= O\left( \frac{x}{\log x} \sum_{q > \xi_2} \frac{1}{q^2} \right) + O\left( x^f \log x \sum_{q \leq \xi_2} 1 \right) =$$

$$= O\left( \frac{x}{\xi_1 \log x} \right) + O\left( \frac{x^f \xi_2 \log x}{\log \xi_2} \right) = O\left( \frac{x}{\log^2 x} \right)$$

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

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

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