ARTIN'S PRIMITIVE ROOT CONJECTURE

VIVAAN DAGA

EULER CIRCLE

Abstract. In 1927, Emil Artin [Art66, pp. viii-x] conjectured that if an integer a is neither a perfect square nor -1, then it is a primitive root mod p for infinitely many primes p. Further, if $\mathcal{P}_a(x)$ denotes the number of such primes up to x, he conjectured that

$$\mathcal{P}_a(x) \sim \delta(a)\frac{x}{\log(x)},$$

where $\delta(a)$ is a specific positive function of a. This conjecture, now known as *Artin's Primitive Root Conjecture*, is still open to date. In this article, we shall look at several results related to this conjecture, including a positive answer assuming the Generalized Riemann Hypothesis(GRH). This article has been heavily inspired by [Mur88] and [Mor12].

1. Introduction

The notion of a primitive root was first introduced by Gauss in the context of periodicity in decimal expansions. Specifically, Gauss was considering the period of the decimal expansion of $\frac{1}{p}$ for prime $p \neq 2, 5$. He showed that the period is the least positive k such that $10^k = 1 \mod p$. So if we have a prime p, for which the decimal expansion of $\frac{1}{p}$ has period $p-1$, the maximum possible, then $p-1$ must the least positive k for which $10^k = 1 \mod p$ holds. In such a case, we say that 10 is a primitive root mod p. For example, 10 is a primitive root mod 23, and so the period of the decimal expansion of $\frac{1}{23}$ is 22. Indeed,

$$\frac{1}{23} = 0.\overline{0434782608695652173913}.$$

More generally, given a prime p, an integer a is said to be a primitive root mod p if $p-1$ is the least positive integer k such that $a^k = 1 \mod p$. In more modern terms, an integer a[1] is a primitive root mod p if the order of a in the cyclic[2] group $(\mathbb{Z}/p\mathbb{Z})^\times$ is $p-1$, or, phrased differently, if the subgroup generated by a is the whole group. Now, it is not unnatural to ask if given an integer a, we can always find infinitely primes p, for which a is a primitive root. Of course, this is trivially false when $a = -1$ and also when a is a perfect square[3], but other than these trivial cases, this question is very difficult to answer. During a conversation with Hasse in 1927, motivated by some heuristics, Artin made the following conjectures:

Date: June 9, 2024.

[1] Of course, p must not divide a, but if p divides a, then we do not have a primitive root mod p.

[2] The cyclicity of $\mathbb{Z}/p\mathbb{Z}^\times$ implies that given a prime p there is an integer a such that a is a primitive root mod p. As might be expected, the cyclicity was first proven by Gauss. A plethora of proofs exist for this fact, see [Con] for a collection of many.

[3] Since 2 always divides the order of $\mathbb{Z}/p\mathbb{Z}^\times$, $p > 2$.

Conjecture 1.1 (Artin's Primitive Root Conjecture Qualitative Form)**.** *Given an integer a other than -1 or a perfect square, there exist infinitely many primes p for which a is a primitive root mod p.*

Conjecture 1.2 (Artin's Primitive Root Conjecture Quantitative Form)**.** *Given an integer a other than -1 or a perfect square, if $\mathcal{P}_a(x)$ denotes the number of primes less than or equal to x for which a is a primitive root, then we have that $\mathcal{P}_a(x) \sim \delta(a)\frac{x}{\log x}$, where $\delta(a)$ is a specific positive function of a.*

Since $\frac{x}{\log(x)} \sim \pi(x)$, in the quantitative form of Artin's conjecture, the number $\delta(a)$ is the density of primes for which a is a primitive root. In other words,

$$\delta(a) = \lim_{x\to\infty} \frac{|\{p \text{ prime} : a \text{ is a primitive root mod } p \text{ and } p \leq x\}|}{|\{p \text{ prime} : p \leq x\}|}.$$

Of course, since $\delta(a)$ is postulated to be positive in the quantitative form, the quantitative form of Artin's conjecture implies the qualitative form. Artin's original motivation for these conjectures came from algebraic number theory, and several results have been proven in support of the conjectures. Hooley's conditional proof assuming GRH in [Hoo67] being perhaps the most noteworthy of these. In the next section, we shall look at the connection to algebraic number theory. Next, we shall give a heuristic for $\delta(a)$. Then we shall look at Hooley's conditional proof assuming GRH. Finally, in the last section, we shall mention some other interesting results related to Artin's Primitive Root Conjecture.

	Proportion $\delta(a)$ of primes p for which a is a primitive root mod p
$a = -1$ or b^2	$\delta(a) = 0$
$a = b^k$	$\delta(a) = v(k)\delta(b)$ Where v is multiplicative, and $v(q^n) = \frac{q(q-2)}{q^2-q-1}$, for prime q.
$\text{sf}(a) = 1 \mod 4$ Where $\text{sf}(a)$ is the square free part of a.	$\delta(a) = \left(1 - \prod_q \frac{1}{1+q-q^2}\right) \prod_q \left(1 - \frac{1}{q(q-1)}\right)$, q prime
Otherwise	$\delta(a) = \prod_q \left(1 - \frac{1}{q(q-1)}\right)$, q prime

Table 1. Conjectural values for $\delta(a)$ for a in order of earliest applicable case

2. A Very Näive Heuristic for Artin's Primitive Root Conjecture

Recall that Artin conjectured

$$\mathcal{P}_a(x) \sim \delta(a)\frac{x}{\log(x)} \tag{2.1}$$

Why should we expect this to be true? By the Prime Number Theorem for Arithmetic Progressions, we have

$$\pi(x;d,a) := \sum_{\substack{p\leq x \\ p\equiv a \mod d}} 1 \sim \frac{x}{\phi(d)\log x}, \tag{2.2}$$

where $(d,a)=1$. In light of the Prime Number Theorem, this implies that the primes are roughly uniformly distributed in the $\phi(d)$ primitive congruence classes mod d. Fix an integer a, and a prime q. Let us estimate the density of primes p such that $p\equiv 1 \mod q$ and $a^{\frac{p-1}{q}} \equiv 1 \mod p$. By the Prime Number Theorem for Arithmetic Progressions, we have that probability that $p \equiv 1 \mod q$ is roughly $\frac{1}{\phi(q)} = \frac{1}{q-1}$. Further the probability that $a^{\frac{p-1}{q}} \equiv 1 \mod p$ is roughly $1/q$. Assuming independence, we can take the product over all primes to get $\delta(a)$ is equal to the product

$$\prod_q \left(1-\frac{1}{q(q-1)}\right),$$

where q ranges over the primes. The value $\prod_q(1-\frac{1}{q(q-1)})$ is known as Artin's constant. We know it's non-zero since $\sum_{k=1}^{\infty}\frac{1}{k(k-1)}$ converges.

3. The Connection to Algebraic Number Theory

It is the tools of algebraic number theory that will allow us to make progress on Artin's Primitive Root Conjecture. Before we continue, let us fix some notation: let a denote an integer other than -1 or a square, a_1 denote the square free part of a, and h denote the largest integer for which a is a perfect h-th power. The connection with algebraic number theory is seen from the following theorem, which follows from a principle of Dedekind:

Theorem 3.1. *Let p and q be primes, then $p=1 \mod q$ and $a^{\frac{p-1}{q}}=1 \mod p$ if and only if p splits completely in the number field $K_q=\mathbb{Q}(\zeta_q, a^{\frac{1}{q}})$*[4].

Proof. We can assume that p does not divide a since then both sides of the equivalence would be false. Now, the condition $p=1 \mod q$ and $a^{\frac{p-1}{q}}=1 \mod p$ is equivalent to the assertion that $x^p=a \mod p$ has exactly q roots. By the Dedekind-Kummer theorem, the assertion that $x^p=a \mod p$ has exactly q roots is equivalent to p factorise in F as the product of q linear prime ideals and p factorise in G as a product of $\phi(q)$ linear prime ideals which is equivalent to p splitting completely in K_q. ■

An easy of corollary of this theorem is

Corollary 3.2. *Given a prime p, a is a primitive root mod p if and only if p does not split completely in any K_q, where q is prime.*

Now, the reason the reformulation in 3.2 is useful is because of Chebotarev's Density Theorem[5], which implies that the density of primes which split in K_k[6] is $\frac{1}{n(k)}$, where $n(k)$

[4] Note that it does not matter which q-th root we take since we always end up in the same field.

[5] For a motivating account of Chebotarev's Density Theorem, see [SL96].

[6] Here k need not be prime, and we will require the result for square free k.

is the degree of $K_k/\mathbb{Q}$. We have the following formula for the degree $n(k)$ when k is square free, which will allow us to get a heuristic for $\delta(a)$:

Theorem 3.3. *For square free k, we have*

$$n(k) = \frac{k\phi(k)}{(h,k)\varepsilon(k)},$$

where

$$\varepsilon(k) = \begin{cases} 2 & \text{if } 2a_1|k \text{ and } a_1 = 1 \mod 4 \\ 1 & \text{otherwise} \end{cases}$$

4. A Heuristic for the Function $\delta(a)$

By 3.2, $\delta(a)$ is the density of primes which do not split completely in any K_q, where q ranges over the primes. Using Chebotarev's Density Theorem and the fact that a prime p splits completely in K_k and K_l if and only if it splits completely in $K_{\mathrm{lcm}(k,l)}$, we can find a heuristic for $\delta(a)$ using the inclusion-exclusion principle: $\delta(a)$ gives us the density of primes which split in none of the K_q, for prime q. To "compute" this density subtract the density for each prime:

$$1 - \frac{1}{n(2)} - \frac{1}{n(3)} - \frac{1}{n(3)} - \cdots$$

Then add the densities for product of two primes:

$$+\frac{1}{n(6)} + \frac{1}{n(10)} + \frac{1}{n(14)} + \cdots$$

And so on. In this way, we get the heuristic

$$\delta(a) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)},$$

where μ is the Möbius function. The following theorem evaluates the sum $\delta(a) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}$:

Theorem 4.1. *Let $A(h) = \prod_{q\nmid h}\left(1 - \frac{1}{q(q-1)}\right)\prod_{q|h}\left(1 - \frac{1}{q-1}\right)$, where q is prime. Then we have that*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} = \begin{cases} A(h) & \text{if } a_1 \neq 1 \mod 4 \\ \left(1 - \mu(|a_1|)\prod_{q|a_1,q|h}\frac{1}{q-2}\prod_{q|a_1,q\nmid h}\frac{1}{q^2-q-1}\right)A(h) & \text{if } a_1 = 1 \mod 4 \end{cases}$$

Note that since $A(h)$ is positive the sum is also positive.

5. Hooley's Conditional Proof

Subject to the truth of the Generalized Riemann Hypothesis Cristopher Hooley [Hoo67] proved that our heuristic value for $\delta(a)$ is indeed correct.

Intuitively, the Generalized Riemann Hypothesis gives us an effective version of Chebatorev's Density Theorem, which allows us to make the inclusion-exclusion argument rigorous. Except not quite since the error term ends up being two large. Nevertheless, Hooley was

able to introduce some intermediate quantities that made everything work.
Hooley proved:

Theorem 5.1.

$$\mathcal{P}_a(x) = \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}\right) \frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

6. Acknowledgements

The author would like to thank Simon Rubinstein-Salzedo for several helpful comments and for organizing the Euler Circle Analytic Number Theory class for which this paper was written.

References

[Art66] E. Artin. *Collected Papers.* Addison Wesley, 1966.
[Con] K. Conrad. Cyclicity of $(\mathbf{Z}/(p))^{\times}$. https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicmodp.pdf.
[Hoo67] C. Hooley. Artin's conjecture for primitive roots. *J. Reine Angew. Math.*, 1967.
[Mor12] P. Moree. Artin's primitive root conjecture -a survey -. https://arxiv.org/pdf/math/0412262, 2012.
[Mur88] M. Ram Murty. Artin's conjecture for primitive roots. *The Mathematical Intelligencer*, 1988.
[SL96] P. Stevenhagen and H.W. Lenstra. Chebotarev and his density theorem. *The Mathematical Intelligencer*, 1996.

Email address: vivaandaga@gmail.com