On an Extension of Artin's Conjecture on Primitive Roots

Neil Kolekar

June 2024

Abstract

The question of whether or not there are infinitely many primes p for which 2 is a primitive root modulo p is of much interest in the subject of analytic number theory. This is a (currently unresolved) conjecture by Artin, which, however, does hold under the assumption of the generalized Riemann Hypothesis (GRH), as shown by Hooley. In this paper, we discuss how we can take a generalized version of Hooley's work to the next level by giving a conditional asymptotic approximation for the number of primes p in an interval $[2, x]$ for which 2 is a primitive root modulo p.

1 Introduction and Preliminary Results

1.1 The Work of Artin and Hooley

To begin with, we state Artin's conjecture on primitive roots:

Conjecture 1.1 (Artin, 1927)**.** *There is an infinitude of primes p with the property that 2 is a primitive root modulo p.*

Although Conjecture 1.1 is unresolved as of the writing of this paper, there has been substantial progress on it that is worth noting. Alongside several useful density results, it has been shown by Hooley that under the assumption of the generalized Riemann Hypothesis (GRH), Artin's conjecture holds true. In particular, the following quantitative statement has been proven:

Theorem 1.2. *Assume that GRH holds. Let $N_2(x)$ denote the number of primes $p \leq x$ for which 2 is a primitive root modulo p. Then, if we let C denote Artin's constant (to be defined later), then*

$$N_2(x) = C \cdot \frac{x}{\log x} + O\left(\frac{x \log\log x}{(\log x)^2}\right)$$

as x approaches ∞.

Our goal is to prove an analogous result for a similar function $N(x)$ that instead counts the number of *positive integers* $n \leq x$ for which 2 is a primitive root modulo n.

1.2 Preliminary Results

As for preliminary results, we are required to introduce the *Carmichael totient function* λ, as it will be required to make our definition of "primitive root modulo n" more rigorous.

Definition 1.3. For a positive integer n, we say that the *Carmichael function* $\lambda(n)$ of n is the smallest positive integer m such that for all a relatively prime to n, $a^m \equiv 1 \pmod{n}$.

Now, we can define primitive roots modulo composite numbers.

Definition 1.4 (Primitive root modulo n)**.** We say that g is a *primitive root modulo* n if and only if $g^{\lambda(n)} \equiv 1 \pmod{n}$.

Essentially, we can break down the condition of being a primitive root modulo n to that of prime powers.

Lemma 1.5 (Breaking down into prime powers)**.** *Let n be an odd positive integer. Then g is a primitive root modulo n if and only if g is a primitive root modulo p^k for each prime power p^k such that $p^k \mid n$.*

2 Wirsing's Formula

2.1 The Formula

Wirsing's formula is a useful approximation theorem that utilizes the Euler product in summations running over a finite interval $[1, x]$. In particular, we can improve our results from sums running over primes in $[1, x]$ to those of sums running over all integers in $[1, x]$. Later, we will define the characteristic function, to which we will apply this formula.

Theorem 2.1 (Wirsing's Formula)**.** *Let f be an arithmetic function with codomain $\mathbb{R}$ such that $f(n) \geq 0$ always and for each prime p and integer $k > 0$, $f(p^k) \leq c^k$ for some constant $c < 2$. Furthermore, suppose that there exists a constant α for which*

$$\sum_{p \leq x} f(p) = (\alpha + o(1)) \cdot \frac{x}{\log x}$$

as x approaches ∞. Then,

$$\sum_{n \leq x} f(n) = \frac{P(x) \cdot x}{\log x} \left(\frac{e^{-\gamma \cdot \alpha}}{\Gamma(\alpha)} + o(1) \right),$$

where P is the Euler product

$$P(x) = \prod_{p \leq x} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^k}.$$

2.2 A Particular Arithmetic Function

We will now define the *characteristic function* f, which is an arithmetic function.

Definition 2.2. For prime powers p^k for which 2 is a primitive root modulo p^k, we define $f(p^k)$ as

- 1, if $p = 2$ and $k \leq 2$, or $p > 2$ and 2 is a primitive root modulo p^k, and
- 0 otherwise.

Furthermore, f is multiplicative, and thus the evaluation of f at prime powers characterizes $f(n)$ for all $n \in \mathbb{N}$.

Note that we f is not completely multiplicative. However, it is also important to consider the nontrivial cases of complete multiplicative nature of the function f. Before this, we define *Wieferich primes.*

Definition 2.3. A *Wieferich prime* is any prime p that satisfies

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

We will denote $\mathcal{W}$ by the set of Wieferich primes, and $\mathcal{P}$ as the set of primes under which 2 is a primitive root.

A useful fact about Wieferich primes is that they are precisely the set of primes p under which 2 is a primitive root modulo p but is *not* a primitive root modulo p^2, which we state without proof (one can apply Lemma 1.5). We will utilize this fact extensively in Section 3.

Proposition 2.4. *We have $f(p^2) = f(p)^2$ if and only if p is a non-Wieferich prime.*

Proof. This condition is equivalent to $f(p^2) = f(p)$. Note that the property of being a non-Wieferich prime is achieved when 2 is a primitive root modulo p^2 or 2 is not a primitive root modulo p. By Definition 2.2, the result is clear. □

We end this section by noting the relevance of the characteristic function: if we use the notation for $N_2(x)$ as in Theorem 1.2, then

$$\sum_{p \text{ prime},\ p \leq x} f(n) = N_2(x).$$

In our new function $N(x)$,

$$\sum_{n \leq x} f(n) = N(x).$$

3 A Computational Fact

First, we define *Artin's constant.*

Definition 3.1. *Artin's constant C* is given by the infinite product

$$C = \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right).$$

Moreover, under the assumption of GRH, C is also the density of primes in $\mathcal{P}$.

We will require the following lemma.

Lemma 3.2. *Assume that GRH holds. For some constant γ', the following identity holds:*

$$\prod_{p \leq x, p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)^{-1} = e^C \log(x)^{\gamma'} + O\left(\frac{\log \log x}{\log x}\right).$$

Proof (Sketch). First, take the natural logarithm of both sides and expand all series of the form $\log(1 + a)$. The result follows from Theorem 1.2 and the Stieltjes integral representation. □

4 The Main Theorem

Now, onto the final result:

Theorem 4.1. *Assume that GRH holds. Let γ denote the Euler-Mascheroni constant. Let $N(x)$ denote the number of positive integers $n \leq x$ for which 2 is a primitive root modulo n. Then, if we let C denote Artin's constant (as before), then*

$$N(x) = \left(\frac{e^{\gamma' - \gamma \cdot C}}{\Gamma(C)} + o(1)\right) \frac{x}{(\log(x))^{1-C}} \prod_{p \in \mathcal{W}} \left(1 - \frac{1}{p^2}\right)$$

as x approaches ∞.

Proof. First, we can plug in the characteristic function f into Wirsing's formula (Theorem 2.1) with $\alpha = C$ (by Theorem 1.2), which produces

$$\sum_{n \leq x} f(n) = \left(\frac{e^{-\gamma \cdot C}}{\Gamma(C)} + o(1) \right) \frac{x}{\log x} \cdot P(x),$$

where $P(x)$ is the Euler product defined in Wirsing's formula. Via the definition of f, we can write

$$P(x) = \prod_{p \in \mathcal{W}} \left(1 - \frac{1}{p^2}\right) \prod_{p \leq x,\ p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)^{-1} + O(1/x).$$

Hence

$$N(x) = \left(\frac{e^{-\gamma \cdot C}}{\Gamma(C)} + o(1) \right) \frac{x}{\log x} \left[\prod_{p \in \mathcal{W}} \left(1 - \frac{1}{p^2}\right) \prod_{p \leq x,\ p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)^{-1} + O(1/x) \right].$$

Now, by substituting Lemma 3.2, we can effectively remove the "product of $1 - 1/p^2$" term, as follows: we have

$$N(x) = \left(\frac{e^{\gamma' - \gamma \cdot C}}{\Gamma(C)} + o(1) \right) \frac{x}{(\log(x))^{1-C}} \prod_{p \in \mathcal{W}} \left(1 - \frac{1}{p^2}\right),$$

and all error terms vanish. This is the desired result. □