Ministry of Higher Education and Scientific Research
Salahaddin University-Erbil
College of Science - Department of Mathematics

زانکۆی سەلاحەدین - هەولێر
Salahaddin University-Erbil

Final Year Research Project

On Artin Conjecture

Submitted by
Ahmed Jawhar Hamad

Supervisor
Dr. Andam Ali Mustafa

A Project submitted in partial fulfillment of the requirements for the Degree of B.Sc. in Mathematics

Abstract

The Artin conjecture is a famous open problem in algebraic number theory that was proposed by Emil Artin in 1927. The Artin conjecture has been partially resolved in some special cases, but remains open in general. Its resolution would have far-reaching consequences in number theory and related areas of mathematics, and is considered one of the most important open problems in the field. In this study, we only review at this conjecture and some of its partial results.

Keywords: Artin conjecture, Primitive Root, Algebraic Number Theory, Analytic Number Theory.

1. Introduction

There are many fascinating conjectures in number theory, but Artin's primitive root conjecture is probably the most famous one. This dissertation is related to the generalization of this conjecture. The aim of this chapter is to present the background behind the problems that we are looking at, lay out our objectives, and provide an overview of the contribution that this dissertation makes.

The Artin conjecture has important implications in many areas of mathematics. While some special cases of the conjecture have been proved, the full conjecture remains open. In fact, it is considered to be one of the most important open problems in algebraic number theory. Many mathematicians continue to work on this problem, using a wide range of techniques from algebraic geometry, representation theory, and analytic number theory.

In a conversation with H. Hasse in 1927, E. Artin postulated a conjectural density about how many primes p there are for which a given integer a is a primitive root modulo p (see (Frei et al., 2008)). In reality, the conjecture was sparked by the following straightforward fact: If we pick a prime number p that is not 2 nor 5, then the decimal expansion of its reciprocal $1/p$ will have a periodic pattern as follows:

$$1/3 = 0.\overline{3} \qquad 1/11 = 0.\overline{09} \qquad 1/17 = 0.\overline{0588235294117647}$$

$$1/7 = 0.\overline{142857} \qquad 1/13 = 0.\overline{076923} \qquad 1/19 = 0.\overline{052631578947368421}$$

When we look at the above instances, a number of questions may come to mind, such as the following: Why does the period length of $1/7$ equal 6, while the period length of $1/11$ is only 2? Gauss explored this problem and even the generic probability of the period lengths of $1/p$.

Thus, in articles 315-317 of his Disquisitiones Aritheoremeticae (1801), he demonstrated that the period length corresponds to the order of 10 in the cyclic group $\mathbb{F}_p^*$ of $p-1$ elements, which is the smallest positive integer k such that $10^k \equiv 1 (\mathrm{mod}\, p)$. This integer k denotes $ord_p(10)$ and is the order of the subgroup generated by 10 in $\mathbb{F}_p^*$.

We can deduct that $ord_p(10)|(p-1)$. If $ord_p(10) = p-1$, then 10 is a primitive root $mod\ p$. As seen by the preceding examples, 10 is a primitive root of modulo 7, 17, and 19, but not modulo 3, 11, or 13. Gauss was particularly curious to know how frequent 10 would be a primitive root modulo p, given that p can vary over primes [4].

The conjecture of Artin provides what is thought to be a necessary and sufficient condition for figuring out when there are an infinite number of primes p for which a given integer a is a primitive root modulo p. It is important to keep in mind that Gauss had already conjectured that there existed an unlimited prime p with the primitive root 10 in the exceptional case where $a = 10$.

Gauss's table has a few more examples like this, and he must have wondered if there are an infinite number of such primes, that is, primes whose decimal period is $p - 1$. $Li(x)$ is an abbreviation for the logarithmic integral, which is defined as $\int_2^x dt/\log t$. By using the method of partial integration, one may determine that the expression $Li(x) \sim x/\log x$ holds. The prime number theorem defined as

$$\pi(x) := \#\{p \leq x\} \sim Li(x), x \to \infty,$$

argues that the probability that a number n is prime is equal to $1/\log n$. (Thus, we may anticipate that $\sum_{2\leq n\leq x} 1/\log n$ primes $\leq x$ which is asymptotically identical to $Li(x)$.)

This conjecture is widely credited to Gauss, but there is no documented evidence for it to the author's knowledge. As a result, Emil Artin formulated the conjecture in 1927 as follows:

Conjecture 1.1 For a given $a \in \mathbb{Q}\backslash\{-1,0,1\}$, define

$$\pi_a = \{p: ord_p(a) = p - 1\} \text{ and } \pi(a,x) = \#\{p \in \pi_a : p \leq x\}.$$

• **Qualitative form:** If a is not a square of a rational number, the set π_a is infinite.

• **Quantitative form:** Let k be the largest integer for which $a = a_0^k$ with $a_0 \in \mathbb{Q}$. As x approaches infinity, we have

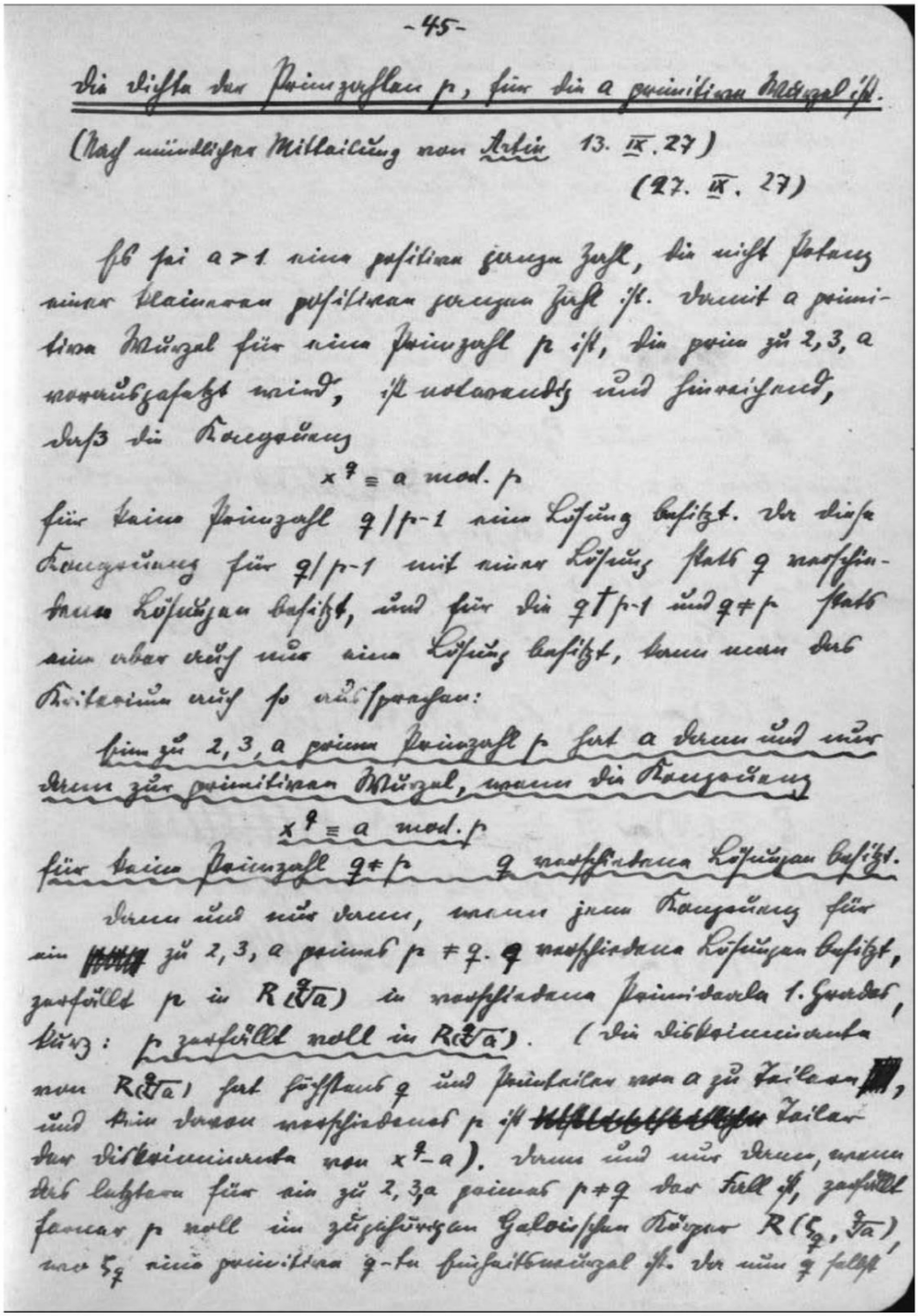
$$\pi(a,x) = \prod_{\ell \nmid k} \left(1 - \frac{1}{\ell(\ell-1)}\right) \prod_{\ell | k} \left(1 - \frac{1}{(\ell-1)}\right) \frac{x}{\log x} + O\left(\frac{x}{\log x}\right) \qquad (1.1)$$

Here, $\prod_\ell f(\ell)$ is a Euler product with $f(\ell) = 1 + O(\ell^{-2})$ (to guarantee convergence) and ℓ sweeps over the primes.

The primary component in 1.1 should be written as $A(k)\frac{x}{\log x}$. If k is an even number, then $A(k) = 0$, and π_a is obviously finite, and then the statement 1.1 is obvious. Then, for π_a to be infinite, the fact that a is not a square is necessary (and, accorollaryding to Artin, is sufficient). For an odd number k, we know that $A(k)$ is a rational multiple of the Artin constant.

$$A(1) = A = \prod_{\ell} \left(1 - \frac{1}{\ell(\ell-1)}\right) \approx 0.3739558$$

Moreover, the quantitative form implies the qualitative form. A rapid convergence is not seen in the product that defines the Artin constant [3,7].



-45-

Die Ziffer der Primzahlen p, für die a primitive Wurzel ist.

(Nach mündlicher Mitteilung von Artin 13. IX. 27)

(27. IX. 27)

Ob bei $a > 1$ eine positive ganze Zahl, die nicht Potenz einer kleineren positiven ganzen Zahl ist. Damit a primitive Wurzel für eine Primzahl p ist, die prim zu $2, 3, a$ vorausgesetzt wird, ist notwendig und hinreichend, daß die Kongruenz

$$x^q \equiv a \mod p$$

für keine Primzahl $q \mid p-1$ eine Lösung besitzt. Ist diese Kongruenz für $q \mid p-1$ mit einer Lösung stets q verschiedene Lösungen besitzt, und für die $q \nmid p-1$ und $q \neq p$ stets eine aber nicht eine Lösung besitzt, kann man das Kriterium auch so aussprechen:

Dann zu $2, 3, a$ prim Primzahl p ist a dann und nur dann zur primitiven Wurzel, wenn die Kongruenz

$$x^q \equiv a \mod p$$

für keine Primzahl $q \neq p$ q verschiedene Lösungen besitzt.

Dann und nur dann, wenn jene Kongruenz für ein zu $2, 3, a$ primes $p \neq q$ q verschiedene Lösungen besitzt, zerfällt p in $R(\sqrt[q]{a})$ in verschiedene Primideale 1. Grades, kurz: p zerfällt voll in $R(\sqrt[q]{a})$. (Die Diskriminante von $R(\sqrt[q]{a})$ ist teilerfremd zu q und teilerfremd von a zu keinem, und ein jeder verschiedene p ist [illegible] Teiler der Diskriminante von $x^q - a$). Dann und nur dann, wenn das letztere für ein zu $2, 3a$ primes $p \neq q$ der Fall ist, zerfällt ferner p voll in gewissen Galoisschen Körper $R(\zeta_q, \sqrt[q]{a})$, wo ζ_q eine primitive q-te Einheitswurzel ist. Ist nun q selbst

Figure 1. Hasse's mathematical notebook entry from 1927 on Artin's primitive root conjecture.

In addition, enthusiastic readers of the dissertation are expected to have at least a fundamental knowledge of Algebraic Number Theory and Analytic Number Theory. To do this, In the next section we have some basic concepts in Algebraic Number Theory.

1.1 Some of Algebraic Number Theory's concept

We will begin by writing down some basic definitions and proving elementary properties about number fields.

Definition 1.1 (Ring) a ring is a set R equipped with two binary operations, usually denoted by addition (+) and multiplication (·), which satisfy certain axioms. Specifically, a ring is an algebraic structure that satisfies the following axioms:

1. R is an abelian group under addition, meaning that:
    - $(a + b) + c = a + (b + c)$ for all a, b, c in R (that is, + is associative)
    - $a + b = b + a$ for all a, b in R (that is, + is commutative).
    - There is an element 0 in R such that $a + 0 = a$ for all a in R (that is, 0 is the additive identity).
    - For each a in R there exists $-a$ in R such that $a + (-a) = 0$ (that is, $-a$ is the additive inverse of a).
2. R is a monoid under multiplication, meaning that:
    - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in R (that is, · is associative).
    - There is an element 1 in R such that $a \cdot 1 = a$ and $1 \cdot a = a$ for all a in R (that is, 1 is the multiplicative identity).[b]
3. Multiplication is distributive with respect to addition, meaning that:
    - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all a, b, c in R (left distributivity).
    - $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all a, b, c in R (right distributivity).

Examples of rings include the integers, the rational numbers, and the real numbers, as well as other algebraic structures such as polynomial rings and matrix rings. The study of rings is an important part of algebraic geometry, algebraic number theory, and other branches of abstract algebra [6].

Definition 1.2 (Field) a field is a set F equipped with two binary operations, usually denoted by addition (+) and multiplication (·), which satisfy certain axioms. Specifically, a field is an algebraic structure that satisfies the following axioms:

- Associativity of addition and multiplication: $a + (b + c) = (a + b) + c$, and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Commutativity of addition and multiplication: $a + b = b + a$, and $a \cdot b = b \cdot a$.
- Additive and multiplicative identity: there exist two different elements 0 and 1 in F such that $a + 0 = a$ and $a \cdot 1 = a$.
- Additive inverses: for every a in F, there exists an element in F, denoted $-a$, called the *additive inverse* of a, such that $a + (-a) = 0$.
- Multiplicative inverses: for every $a \neq 0$ in F, there exists an element in F, denoted by a^{-1} or $1/a$, called the *multiplicative inverse* of a, such that $a \cdot a^{-1} = 1$.
- Distributivity of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Examples of fields include the rational numbers, the real numbers, and the complex numbers. Other examples of fields include finite fields, which have a finite number of elements [6].

Definition 1.3 (Field extension) A field extension is an inclusion of fields $K \subseteq L$. We sometimes write this as L/K [6].

Definition 1.4 (Degree of field extension) Let $K \subseteq L$ be fields. Then L is a vector space over K, and the degree of the field extension is

$$[L: K] = \dim_K(L).$$

Definition 1.5 (Number field) A number field is a finite field extension over $\mathbb{Q}$ [6].

Definition 1.6 (Algebraic integer) *Let L be a number field. An algebraic integer is an $\alpha \in L$ such that there is some monic $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$. We write $\mathcal{O}_L$ for the set of algebraic integers in L* [6].

Definition 1.7 (Ideal) An ideal is a subset of a ring that satisfies certain algebraic conditions. Specifically, an ideal I of a ring R is a non-empty subset of R that satisfies the following properties:

- I is closed under addition: if a and b are in I, then $a + b$ is in I.
- I is closed under multiplication by elements of R: if a is in I and r is any element of R, then ra and ar are both in I.

The first property ensures that I is a subgroup of R under addition, while the second property ensures that I is closed under multiplication by elements of R.

Examples of ideals include the set of all multiples of a fixed integer in the ring of integers, the set of all polynomials with a given factor in a polynomial ring [6].

Definition 1.8 (Prime ideal) Let R be a ring. An ideal $\mathfrak{p} \subseteq R$ is prime if for all $x, y \in R$, $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Here, we take the convention that a prime ideal is non-zero. This is not standard, but it saves us from saying "non-zero" all the time [6].

1.1.1 Structure of prime ideals:

We can now move on to find all prime ideals. We know that every ideal factors as a product of prime ideals, but we don't know what the prime ideals are.

Lemma 1.1 Let $\mathfrak{p} \lhd \mathcal{O}_L$ be a prime ideal. Then there exists a unique $p \in \mathbb{Z}$, p prime, with $\mathfrak{p}|\langle p \rangle$. Moreover, $N(\mathfrak{p}) = p^f$ for some $1 \leq f \leq n$.

This is not really too exciting, as soon as we realize that $\mathfrak{p}|\langle p \rangle$ is the same as saying $\langle p \rangle \subseteq \mathfrak{p}$, and we already know $\mathfrak{p} \cap \mathbb{Z}$ is non-empty. So, all we have to do is to figure out how principal ideals $\langle p \rangle$ factor into prime ideals.

We write

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$$

for some distinct prime ideals $\mathfrak{p}_i$, with $N(\mathfrak{p}_i) = p^{f_i}$ for some positive integers e_i. Taking norms, we get

$$p^n = \prod p^{f_i e_i}.$$

So

$$n = \sum e_i f_i.$$

We start by giving some names to the possible scenarios.

Definition 1.9 (Ramification indices) Let $\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ be the factorization into prime ideals. Then $e_1, \cdots, e_m$ are the ramification indices.

Definition 1.10 (Ramified prime) We say p is ramified if some $e_i > 1$.

Definition 1.11 (Inert prime) We say p is inert if $m = 1$ and $e_m = 1$, i.e., $\langle p \rangle$ remains prime.

Definition 1.12 (Splitting prime) We say p splits completely if $e_1 = \cdots = e_m = 1 = f_1 = \cdots = f_m$. So $m = n$.

Note that this does not exhaust all possibilities. The importance of these terms, especially ramification, will become clear later [6].

So how do we actually compute $\mathfrak{p}_i$ and e_i? In other words, how can we factor the ideal $\langle p \rangle$ into prime ideals?

Example 1.1 Consider $L = \mathbb{Q}(\sqrt{-11})$. We want to factor $\langle 5 \rangle$. We consider $\mathbb{Z}[\sqrt{-11}] \subseteq \mathcal{O}_L$. This has index 2, and $5 \nmid 2$. So, we can say

$$\langle 5 \rangle = \langle 5, \sqrt{-11} + 2 \rangle \langle 5, \sqrt{-11} - 2 \rangle.$$

In general, consider $L = \mathbb{Q}(\sqrt{d})$, $d \neq 0,1$ and square-free, and p an odd prime.

1.1.2 Cyclotomic fields:

A field F is cyclotomic field with the expression $F = \mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{\frac{2\pi i}{n}}$ and $n \in \mathbb{N}$. One might demonstrate that

$$f_{\zeta_n}(x) = \prod_{\substack{\alpha=1 \\ (\alpha,n)=1}} (x - \zeta_n^{\alpha}) = \Phi_n(x) \in \mathbb{Z}[x].$$

The $\Phi_n(x)$ polynomial is the nth cyclotomic polynomial. This leads us to conclude that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n(x) = \varphi(n)$. Moreover, the cyclotomic fields are normal. It is possible to demonstrate that p splits completely in F if and only if $p \equiv 1 (\mathrm{mod} n)$, if and only if $x^n - 1$ factors completely over $\mathbb{F}_p$ [1, 6].

1.2 Analytic Number Theory

Suppose that $\mathfrak{D}$ crosses the non-zero integral ideals of $\mathcal{O}_F$, where F is a number field. When $\Re(s) > 1$, we define $\zeta_F(s) = \sum_{\mathfrak{D}} N\mathfrak{D}^{-s}$, and use analytic continuation elsewhere. It is worth noting that if $F = Q$, then $\zeta_F(s) = \zeta(s)$, the standard Riemann zeta-function. In the case when $\Re(s) > 1$ we get a Euler product, denoted by $\zeta_F(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$, in which the product runs over all of the prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$ [1].

The Generalized Riemann Hypothesis (GRH) is a conjecture in mathematics that asserts that all non-trivial zeros of certain types of zeta functions lie on the critical line. The Riemann hypothesis itself is a special case of the GRH.

The zeta function is a mathematical function that was first studied by the mathematician Leonard Euler in the 18th century, and later extensively by Bernhard Riemann in the 19th century. The Riemann zeta function is defined as the sum of the reciprocal of the nth power of the positive integers, where n is a complex number.

The non-trivial zeros of the Riemann zeta function are all of the complex numbers s of the form s = 1/2 + it, where t is a real number and i is the imaginary unit. The Riemann hypothesis states that all of these zeros lie on the critical line s = 1/2. The GRH extends this conjecture to other zeta functions, such as Dirichlet L-functions and Hecke L-functions.

The importance of the GRH lies in its connections to other areas of mathematics, such as number theory and cryptography. If the GRH were proven to be true, it would have significant implications for these fields, as it would provide a powerful tool for understanding the distribution of prime numbers and for constructing secure cryptographic systems.

Despite extensive efforts by mathematicians over the past century, the GRH remains unproven. However, there have been many important partial results and related conjectures that have been proven, which have contributed to our understanding of this important problem [1].

2. Materials and Methods

At the very beginning, Artin's idea is that a is a primitive root $(\mathrm{mod}\, p)$ if and only if $a^{(p-1)/\ell} \not\equiv (\mathrm{mod}\, p)$ for all prime divisors ℓ of $(p-1)$. However, p splits completely in $F_\ell = \mathbb{Q}(\zeta_\ell, a^{1/\ell})$, where $\zeta_\ell = e^{2\pi i/\ell}$ if and only if $a^{(p-1)/\ell} \equiv (\mathrm{mod}\, p)$. As a result, he deduced that a is a primitive root $(\mathrm{mod}\, p)$ if and only if p does not split completely in any F_ℓ. Then he realized that the prime ideal theorem gives the density of primes which splits completely in F_ℓ, as

$$\frac{1}{[F_\ell : \mathbb{Q}]},$$

Hence, the probability that p does not split completely is

$$1 - \frac{1}{[F_\ell : \mathbb{Q}]}.$$

So, one would expect

$$A = \prod_{\ell} \left(l - \frac{1}{[F_\ell : \mathbb{Q}]} \right)$$

as the density of primes for which a is a primitive root.

In other words, the following is the first thing we notice when we look at Artin's primitive root conjecture:

$$p \in \pi_a \Leftrightarrow a^{\frac{p-1}{\ell}} \not\equiv 1(\text{mod } p) \text{ for every prime } \ell \text{ dividing } p-1. \tag{2.1}$$

" $\Rightarrow$ " Obvious.

" $\Leftarrow$ " If $p \notin \pi_a$, then for any $h|(p-1), h>1$ we have $a^{\frac{p-1}{h}} \equiv 1(\text{mod } p)$. This means that $a^{\frac{p-1}{\ell_1}} \equiv 1(\text{mod } p)$ for any prime divisor ℓ_1 of h. This is an inconsistency.

Since Artin is responsible for several unsolved conjectures, it is more common to refer to the Artin primitive root conjecture than Artin's conjecture. In point of fact, there are even articles that have been written in which both of these conjectures are discussed, such as [5].

As a result, we have criteria for different ℓ corollaryresponding with a prime p. We will swap the roles of p and ℓ; that is, given a fixed ℓ, we will examine the set of primes p such that $p \equiv 1(\text{mod } \ell)$ and $a^{\frac{p-1}{\ell}} \not\equiv 1(\text{mod } p)$.

Now we fix a prime ℓ and attempt to determine the density of primes p satisfying the conditions $p \equiv 1(\text{mod } \ell)$ and $a^{\frac{p-1}{\ell}} \equiv 1 \text{mod } p$. As x approaches infinity, the prime number theorem for arithmetic progressions asserts

$$\pi(x;b,a) := \sum_{\substack{p \le x \\ p \equiv a(\text{mod} b)}} 1 \sim \frac{x}{\varphi(b)\log(x)} \tag{2.2}$$

It is argued that the residue classes $a(\text{mod } b)$ are called primitive where $(a,b)=1$. With several exceptions, given an integer b, a prime must be in a primitive residue class modulo b. Furthermore, due to the fact we have $\varphi(b)$ primitive residue classes modulo b, 2.2 tells us the primes asymptotically spread equally among the primitive residue classes modulo b. Dirichlet's theorem (1837) makes the weaker claim that every primitive residue class has an infinite number of primes.

From 2.2 $p \equiv 1(\text{mod } \ell)$ occurs for primes p with rate $1/\varphi(\ell) = 1/(\ell-1)$. We bring back Fermat's little theorem, which states that $a^{p-1} \equiv 1 \text{mod } p$ if $p \nmid a$. Thus, in the event that $p \nmid a$, we may deduce that $a^{\frac{p-1}{\ell}}$ is a solution to the equation $x^{\ell} \equiv 1(\text{mod } p)$. We assume that there will be ℓ solutions and we need that each solution has the value 1 modulo ℓ. Therefore, we predict being successful with a frequency of $\frac{1}{\ell}$, with the exception of the case when $\ell|k$. Then

$a^{\frac{p-1}{\ell}} = a^{k\frac{p-1}{\ell}} \equiv 1 \bmod p$, trivially. If we make the assumption that both occurrences are not reliant on one another, then the probability that both of these occurrences will take place is $\frac{1}{\ell(\ell-1)}$ if $p \nmid k$ and $\frac{1}{\ell-1}$ otherwise.

According to 2.1 the preceding occurrences should not happen for any ℓ, so that $p \in \pi_a$, which predicts a natural density of

$$\prod_{\ell \nmid k}\left(1-\frac{1}{\ell(\ell-1)}\right)\prod_{\ell \mid k}\left(1-\frac{1}{(\ell-1)}\right) = A(k).$$

for primes of this kind, we conclude that 1.1 holds [3,9].

Until approximately 1960, Lehmers performed some quantitative measures that did not always agree with Artin's heuristic, which was considered credible at the time. Later, Heilbronn presented a modified quantitative conjecture in 1968 after realizing that the case "p does not split completely in F_ℓ" is not always independent because of the fact that p and ℓ cover all primes.

However, Artin produced this modification even pretty earlier, in 1958, in a letter to the Lehmers in reply to a letter from the Lehmers about his quantitative work. Artin did not publish his revised guess, nor did the Lehmers mention Artin in their publication, despite providing the correction factor. Hasse included in the 1964 version of his book a correction factor that is wrong if $a \equiv 1(\bmod 4)$ is not a prime [5,2].

Bilharz demonstrated the function field equivalent to Artin's conjecture in 1937.. Artin's fundamental conjecture is a reasonable issue to ask if one assumes the generalized Riemann hypothesis for the number fields concerned. A positive response was given by Hooley in 1967. He demonstrated that if the Riemann Hypothesis exists for the number fields $\mathbb{Q}(\zeta_k, a^{1/k})$ with k square free, then we will get

$$\pi_a(x) = \rho(a).\frac{x}{\log x} + O_a\left(\frac{x\log\log x}{\log^2 x}\right),$$

and he specifically assessed the latter sum, say $\rho(a)$, as

$$\rho(a) = \begin{cases} A(h) & if\, d \not\equiv 1(mod\ 4), \\ \left(1-\mu(|d|)\prod_{\ell \mid d\ell \mid h}\frac{1}{\ell-2}\prod_{\ell \mid dp \nmid h}\frac{1}{\ell^2-\ell-2}\right)A(h) & other\ wise. \end{cases}$$

In a notable paper, Lenstra used Hooley's approach and, assuming GRH, established a number field analogue of the Artin Conjecture. Regarding Hooley's proof under GRH, various variations of the conjecture were investigated. The following are many typical extensions:

• Primes with a particular primitive root in aritheoremetic progressions;

• Near-primitive roots: $[F_p^*: \langle a \rangle] = m \in \mathbb{Z}_{>0}$;

• Two-variable Artin: $\langle a_1 \rangle \subset \langle a_2 \rangle \subset F_p^*$.

• Higher-rank Artin: $F_p^* = \langle a_1, a_2, \ldots, a_r \rangle$.

• Multiple primitive roots: $F_p^* = \langle a_1 \rangle = \langle a_2 \rangle = \ldots = \langle a_r \rangle$.

• Same order: $\langle a_1 \rangle = \langle a_2 \rangle = \ldots = \langle a_r \rangle \subset F_p^*$ [5,9].

3. Results and Discussion

Findings should be described without comments. Several people have generalized Hooley's work. In 1983, Rajiv Gupta and Ram Murty demonstrated, without any hypotheses, that three is a set of 13 numbers such that Artin conjecture is available for at least one of these 13 numbers.

Theorem 3.1 Assume that r, s, t are three different primes, and

$$S = \{rt^2, r^3s^2, r^2s, s^3t^2, s^2t, r$$
$$2t^3, rs^3, r^3st^2, st^3, r^2s^3t, r^3t, rs^2t^3, rst\},$$

then we have

$$\pi_a(x) := \pi_a \cap [1, x] \gg \frac{x}{\log^2 x}$$

For some $a \in S$ [4].

Subsequently, Gupta, Kumar Murty, and Ram Murty decreased the size of this set to seven. In 1986, however, Heath-Brown developed on earlier fundamental work by Gupta, Ram Murty, and Srinivasan that allowed Heath-Brown to prove the following improvement of the Theorem 3.1.

Theorem 3.2 Given $q, r, s \in \mathbb{Z}$ multiplicatively independent, such that none of $q, r, s, -3qr, -3qs, -3rs, qrs$ is a square, then there exists $a \in \{q, r, s\}$ with

$$\pi_a(x) := \pi_a \cap [1, x] \gg \frac{x}{\log^2 x},$$

Moreover, there exists $a \in \{2,3,5\}$ such that

$$\#\{p \leq x : p > 5, \langle a \bmod p \rangle = \mathbb{F}_p^*\rangle \gg \frac{\pi(x)}{\log x},$$

Specifically, the qualitative AC occurs for $r, s,$ and t[9].

As a consequence, there are only two primes, ℓ_1 and ℓ_2 for which π_{ℓ_1} and π_{ℓ_2} are finite, and no more than three square-free integers a_1, a_2 and a_3 for which π_{a_1}, π_{a_2} and π_{a_3} are finite. Given an integer $m \geq 1$, the prime counting function that counts the prime numbers p for which a is a near-primitive root modulo p of index m is:

$$\pi_\Gamma(x,m) := \#\{p \leq x : p \not\in Supp\Gamma, [\mathbb{F}_p^* : \Gamma_p] = m\}.$$

Hooley's approach has been expanded by numerous authors (such as Moree, Murata, Lenstra,Wagstaff, and others) who derive an asymptotic formula for $\pi_a(x,m)$. Specifically, Lenstra, Moree, and Stevenhagen provide in 2014 a full characterisation, assuming the GRH, of the pairings (a,m) for which there exists no $p|a$ with $ind_p(a) = m$. In a different route, L. Cangelmi and F. Pappalardi derived from GRH an asymptotic formula for $\pi_\Gamma(x,1)$, for which Γ_p includes a primitive root modulo p [7,8]. Later, in 2013, F. Pappalardi and A. Susa looked at $\pi_\Gamma(x,m)$ in a more general way and made the following suggestions [7,9]:

Theorem 3.3 Let $\Gamma \subset \mathbb{Q}^*$ has rank $r \geq 2$, let $m \in \mathbb{N}$. Assume GRH holds for the fields of the form $\mathbb{Q}(\zeta_k, \Gamma^{1/k})(k \in \mathbb{N})$. Then, for any $\forall \varepsilon > 0$ and for $m \leq x^{\frac{r-1}{(r+1)(4r+2)}-\varepsilon}$,

$$\pi_\Gamma(x,m) := \pi_\Gamma(m) \cap [1,x] = \left(\rho(\Gamma,m) + O\left(\frac{1}{\varphi(m^{r+1})\log^r(x)}\right)\right)\pi(x),$$

where

$$\rho(\Gamma,m) = \sum_{k\geq 1} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/mk}) : \mathbb{Q}]}.$$

In addition to this, they were successful in constructing an explicit formula for the density $\rho(\Gamma,m)$ in the case when Γ only contains positive rational numbers [8]. Specifically, they demonstrated:

Theorem 3.4 Let $\Gamma \subset \mathbb{Q}^+$ with $r = rank\Gamma \geq 2$, $m \in \mathbb{N}$, and $m_\ell := \ell^{v_\ell(m)}$.

$$\rho(\Gamma,m) = A_{\Gamma,m}\left(B_{\Gamma,m} - \frac{|\Gamma(m_2|}{(2,m)|\Gamma(2m_2)|}B_{\Gamma,2m}\right),$$

where

$$A_{\Gamma,m} = \frac{1}{\varphi(m)|\Gamma(m)|} \times \prod_{\ell>2 \ell\nmid m}\left(1 - \frac{1}{(\ell-1)|\Gamma(\ell)|}\right) \times \prod_{\ell>2 \ell|m}\left(1 - \frac{|\Gamma(m_\ell)|}{\ell|\Gamma(\ell m_\ell)|}\right),$$

and

$$B_{\Gamma,\alpha} = \sum_{\substack{\eta|\sigma_\Gamma \\ \eta^{\frac{\alpha_2}{2}}.\mathbb{Q}^{*\alpha_2}\in\Gamma(\alpha_2) \\ v_2(\partial(\eta))\leq\alpha}} \prod_{\substack{\ell|\partial(\eta) \\ \ell\nmid\alpha}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1}, \text{where} \alpha > 0.$$

Here, we could not list all the names and their works, but in order to have a general overview, we refer to [3].

4. Conclusions

In conclusion, the Artin conjecture is a significant problem in number theory that has captured the attention of mathematicians for almost a century. Although it has been proven for some cases, it remains unsolved in general, and its resolution would have important implications for other areas of mathematics.

Research on the Artin conjecture is ongoing, and mathematicians continue to make progress towards a solution. Advances in computational techniques, as well as new insights from related areas of mathematics, have helped to shed light on the problem and bring it closer to resolution.

While the Artin conjecture remains a challenging and complex problem, its study has led to important developments in number theory and has enriched our understanding of the behavior of algebraic functions. It is likely that the pursuit of this conjecture will continue to inspire and challenge mathematicians for many years to come.

References

[1] APOSTOL, T. M. (1998). Introduction to analytic number theory, Springer Science & Business Media.

[2] ARTIN, E. (1965). 'Collected papers. edited by S. Lang and T. John in 1982'.

[3] CANGELMI, L. AND PAPPALARDI, F. (1999). 'On the r-rank Artin conjecture, II', Journal of Number Theory 75(1), 120–132.

[4] GUPTA, R. AND MURTY, M. R. (1984). 'A remark on Artin's conjecture', Inventiones Mathematicae 78(1), 127–130.

[5] HOOLEY, C. (1967). 'On Artin's conjecture', Journal Für Die Reine Und Angewandte Mathematik 225, 209–220.

[6] LANG, S. (1984). Algebra, 2nd edition, Addison-Wesley, U.S.A.

[7] LENSTRA, H. W. (1977). 'On Artin's conjecture and Euclid's algorithm in global fields', Invent. Math. 42, 201–224.

[8] MOREE, P. (2012). ‘Artin’s primitive root conjecture–a survey’, Integers 12(6), 1305–1416.

[9] MURATA, L. (1991b). ‘A problem analogous to Artin’s conjecture for primitive roots and its applications’, Archiv der Mathematik 57, 555–565.

[10] PAPPALARDI, F. (1997). ‘The r-rank Artin conjecture’, Mathematics of Computation 66 (218), 853–868.