Shuguang, Li. (2024). Contrib Pure Appl Math,2(1):107. https://doi.org/10.33790/cpam1100107

Gexin Publications

Contributions to Pure and Applied Mathematics

# A Survey of Primitive $\lambda$-roots

Shuguang Li*

Department of Mathematics, College of Natural and Health Sciences, University of Hawaii at Hilo, 200 West Kawili Street,Hilo, HI 96720-4091, USA.

Article Details

Article Type: Mini Review

Received date: 30th November, 2023

Accepted date: 31st January, 2024

Published date: 02nd February, 2024

***Corresponding Author**: Shuguang Li, Department of Mathematics, College of Natural and Health Sciences, University of Hawaii at Hilo, 200 West Kawili Street,Hilo, HI 96720-4091, USA.

**Citation**: Li, S. (2024). A Survey of Primitive $\lambda$-roots. Contrib Pure Appl Math, 2(1): 107. doi: https://doi.org/10.33790/cpam1100107.



**Abstract:** A survey about the distribution of primitive roots and primitive $\lambda$-roots is presented in the article with more focus on the distribution of primitive $\lambda$-roots and explanation of the source of oscillation in the distribution of primitive $\lambda$-roots.

**Keywords:** primitive roots, primitive $\lambda$-roots, distribution of primitive $\lambda$-roots.

Let $\mathbb{Z}$ be the set of integers, and let $n > 1$ be an integer. Then the set of all integers that have the same remainder modulo $n$ is called a residue class mod$n$. If a residue class contains an integer that is relatively prime to $n$, then it is called a reduced residue class. The set of all reduced residue classes mod $n$ forms an Abelian group with a multiplication induced from the multiplication of integers, which is denoted by $(\mathbb{Z}/n\mathbb{Z})^*$. If the group is cyclic, then its generator or all integers in the generator are called primitive roots $\bmod n$. It is well-known that $(\mathbb{Z}/n\mathbb{Z})^*$ is a cyclic group if $n = 2, 4, p^r$ or $2p^r$, where $p$ is an odd prime and $r \geq 1$. However, research on primitive roots for prime moduli becomes the focus of the research on primitive roots. One of the major questions is about the distribution of the primitive roots for prime moduli. This question can be investigated in two perspectives. If we fix prime modulus $p$, then one can easily see that the proportion of primitive roots for $p$ in the group of $(\mathbb{Z}/p\mathbb{Z})^*$ is $\phi(p-1)/(p-1)$, where $\phi$ is Euler $\phi$-function. Elliott proved that $\phi(p-1)/(p-1)$ has a limiting distribution function [2], in the sense that $\lim_{x\to\infty} \frac{1}{\pi(x)} \#\{p \leq x : \phi(p-1)/(p-1) \leq u\}$, where $\pi(x)$ is the number of primes up to $x$, exists for all real numbers $u$. This indicates that the values of $\phi(p-1)/(p-1)$ are asymptotically evenly distributed in the interval $[2, x]$ as $x$ goes to infinity. If we fix integer $a$ and count the number $P_a(x)$ of prime moduli $p$ up to $x$ for which $a$ is a primitive root, we are led to the famous Artin's conjecture.

## 1. Distribution of Primitive Roots and Artin's Conjecture

In 1927, Artin conjectured that for any integer $a$, which is not $-1$ and not a square, $\lim_{x\to\infty} P_a(x) = \infty$. He formulated his conjecture as an asymptotic formula:

$$P_a(x) \sim \frac{A(a)x}{\ln x}$$

as $x \to \infty$, where $A(a) > 0$ is a constant depending on $a$. $A(a)$ was revised by Heilbronn in [20] due to the work of D.H. Lehmer.

Although Artin's conjecture has not been proved unconditionally, there are many results [3, 5, 6] in favor of the conjecture. The reader may refer to Murty [15] for a survey of Artin's conjecture. The closest result in favor of Artin's conjecture comes from Hooley [6]. He proved the conjecture under the assumption of the extended Riemann Hypothesis for Dedekind zeta function over certain Kummerian fields. Hooley also gave the constants $A(a)$ in his article. Let $a = a_1 a_2^2$, where $a_1$ is squarefree. Let $h$ be the largest integer such that $a$ is an $h$-th power. Here $h$ is an odd integer since $a$ cannot be a square. Then

$$A(a) = \begin{cases} A, & \text{if } a_1 \not\equiv 1 \bmod 4 \text{ and } h = 1 \\ A\left(1 - \prod_{q \mid a_1} \frac{1}{1+q-q^2}\right), & \text{if } a_1 \equiv 1 \bmod 4 \text{ and } h = 1 \end{cases}$$

where constant $A = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right)$. If $h > 1$, $A$ needs to be modified with an extra factor depending on $h$ and $a$. One may refer to [6] for more detail.

Another achievement in favor of Artin's conjecture is the unconditional result obtained by Stephens [19], who proved that if $N > \exp\left(4(\ln x \ln\ln x)^{\frac{1}{2}}\right)$, then

$$\frac{1}{N}\sum_{a\leq N} P_a(x) = A\cdot \mathrm{li}(x) + O\left(x/(\ln x)^D\right) \tag{1}$$

where $D > 1$ is an arbitrary constant. Note that constant $A$ is the asymptotic average of the constants $A(a)$ in Hooley's result. One can substitute Hooley's formula for $P_a(x)$ in (1) to get the similar estimate as in (1) except with a weaker error term. So the unconditional result in (1) is a kind of verification of Hooley's achievement.

It should be pointed out that Stephens established a connection between the two counting functions $P_a(x)$ and $\phi(p-1)$ for primitive roots. Indeed, in his proof, Stephens found out that

$$\frac{1}{N}\sum_{a\leq N} P_a(x) = \sum_{p\leq x}\frac{\phi(p-1)}{p-1} + O\left(x/(\ln x)^D\right). \tag{2}$$

where $D > 1$ is an arbitrary constant. From this identity, we can see that the asymptotic even distribution of values of $\phi(p-1)/(p-1)$ for $p \in [2, x]$ induces the smooth function $A\cdot \mathrm{li}(x)$ for the average of $P_a(x)$, which is a pattern followed by individual $P_a(x)$ with a constant factor depending on $a$. The unconditional result achieved in (1) is possible thanks to a characteristic function by a sum of Dirichlet characters for a primitive root $a \bmod p$. This creates a chance for interchange of an order of sums of a triple sum in $\sum_{a\leq N} P_a(x)$. The properties of sums of Dirichlet characters make it possible to yield the sum of $\phi(p-1)/(p-1)$ in (2) and to cut the error terms down significantly. These techniques still work when we consider the distribution of primitive $\lambda$-roots below. The multiplicative property of function $\phi(n)$ makes it possible to turn the identity in (2) to (1).

## 2. Distribution of Primitive $\lambda$-roots and Artin's Conjecture for Composite Moduli

When $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic, there is no primitive root mod$n$. However, the group always has residue classes that have the maximal order. Carmichael [1] called each such residue class or any integer in it as a primitive $\lambda$-root modulo $n$. Here $\lambda$ refers to Carmichael function $\lambda(n)$, which is the maximal order of elements in $(\mathbb{Z}/n\mathbb{Z})^*$. It is well-known that if $n = p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ where $p_1, p_2, \cdots, p_k$ are distinct primes, then $\lambda(n) = \mathrm{lcm}\,(\lambda(p_1^{r_1}), \lambda(p_2^{r_2}), \cdots, \lambda(p_k^{r_k}))$, $\lambda(p^r) = \frac{1}{2}\phi(p^r)$ if $p = 2$ and $r \geq 3$, and $\lambda(p^r) = \phi(p^r)$ in all other cases. When $n = 2, 4, p^r$ or $2p^r$, where $p$ is an odd prime, a primitive $\lambda$-root mod$n$ is a primitive root mod$n$. So primitive $\lambda$-root is a generalization of the primitive root.

Let us explore the distribution of primitive $\lambda$-roots. As in the case concerning the distribution of primitive roots, we come to two counting functions for primitive $\lambda$-roots mod$n$: $N_a(x)$ and $R(n)$, where $N_a(x)$ is the number of moduli $n$ up to $x$, for which $a$ is a primitive $\lambda$-root and $R(n)$ is the number of primitive $\lambda$-roots mod$n$. Although the two functions count different parts of primitive $\lambda$-roots modulo $n$, they are connected through the average of $N_a(x)$ in a similar way as the average of $P_a(x)$ in (2) in Stephens' work [19], including a characteristic function for each pair of primitive $\lambda$-root and its modulus by a sum of Dirichlet characters for the modulus. It is proved [11] that, for $x > e^3$ and $y \geq \exp\left((\ln x)^{3/4}\right)$, we have

$$\frac{1}{y}\sum_{a\leq y} N_a(x) = \sum_{n\leq x}\frac{R(n)}{n} + O\left(x\cdot\exp\left(-\frac{5}{16}(\ln x)^{1/2}\right)\right). \tag{3}$$

So the magnitude of $\sum_{n\leq x} R(n)/n$ is the average order of $N_a(x)$. Unfortunately this sum oscillates as $x$ goes to infinity [9] in the sense that there exists a positive constant $c$ such that $\sum_{n\leq x} R(n)/n \geq cx$ on a unbounded set of real numbers $x$; and $\sum_{n\leq x} R(n)/n = o(x)$ on another unbounded set of real numbers $x$. Asymptotically this oscillation indicates that most individual $N_a(x)$ would oscillates between $o(x)$ and $cx$ for some positive constant $c$, as $x$ goes to infinity. To be more precise, let us introduce the exceptional cases first. Let $\mathcal{E}$ be the set of integers $a$ such that $|a| \leq 1$, or $|a|$ is a non-trivial power, or $|a|$ is the product of 2 and a square. Then it is proved in [10] that, for an absolute constant $c > 0$,

$$N_a(x) \leq \begin{cases} 8, & \text{if } a = -1 \text{ or } a = b^2 \text{ for some integer } b \\ c\,x(\ln x)^{-1/4}, & \text{if } |a| = 2b^2 \text{ for some integer } b \\ c\,x(\ln x)^{-1/\phi(2q)}, & \text{if } |a| \text{ is a } q\text{-th power for some prime } q \end{cases}$$

If $a \notin \mathcal{E}$, it was conjectured that

$$\varliminf_{x\to\infty} N_a(x)/x = 0, \text{ and } \varlimsup_{x\to\infty} N_a(x)/x > 0.$$

This was considered as Artin't conjecture for composite moduli. The first part of the conjecture was proved in [10] free of any hypothesis, while the second part was proved in [13] under assumption of GRH. A conjecture about the value of the lim sup was also given in [13]. Let

$$F_q = \varliminf_{t\to\infty}\sum_{j=0}^{\infty}\frac{\exp\left(tq^{-j-1}\right)-1}{\exp\left(t\phi(q^j)^{-1}\right)}.$$

for each prime $q$, and let $\alpha = \Pi_q(1 - F_q)$. It is conjectured that if integer $a \notin \mathcal{E}$, then

$$\overline{\lim_{x\to\infty}} N_a(x)/x = \alpha\phi(|a|)/|a|,$$

and this limit is attained on an unbounded set of positive real numbers independent of $a \notin \mathcal{E}$.

Therefore, Artin's conjecture for composite moduli is not in analogy to Artin's conjecture. Because, in Artin's conjecture, $P_a(x)$ is proportional to $\pi(x)$, the number of prime moduli up $x$, while in Artin's conjecture for composite moduli we don't have that $N_a(x)$ is proportional to $[x]$, the number of moduli up to $x$. We do not even have a formula for $N_a(x)$. However, the reason behind the oscillations of $N_a(x)$ and its average $\sum_{n\le x} \frac{R(n)}{n}$ are also interesting. The authors [12] used a probability model in explaining of the oscillation in $N_a(x)$. In the following we will try a heuristic approach to reveal the mechanism that results in the oscillations. We would like to look at the first moment of $R(n)/n$, namely $\sum_{n\le x} R(n)/n$. This is not a proof, but rather an outline of the mechanism.

## 3. Oscillation in $\sum_{n\le x} R(n)/n$

First let us look at a formula for $R(n)$. In the following, we will use $p, q$ and $l$ to denote primes. We use notation $p^r \| n$ to mean that $p^r$ is a divisor of $n$, but $p^{r+1}$ isn't. In [14, 8], it was proved that

$$R(n) = \phi(n) \cdot \prod_{q|\lambda(n)} \left(1 - \frac{1}{q^{\Delta_q(n)}}\right), \tag{4}$$

where $\Delta_q(n) := \#\{\text{prime } p: \ p^e \| n \text{ and } q^k | \lambda(p^e)\}$ for prime $q$ with $q^k \| \lambda(n)$, except the case $2^3 \| n$ and $2 \| \lambda(n)$, for which $\Delta_2(n) := 1 + \#\{\text{prime } p: \ p | n\}$.

Actually $\Delta_q(n)$ is the number of cyclic subgroups of order $q^k$ in the factorization of $(\mathbb{Z}/n\mathbb{Z})^*$ into a direct product of cyclic subgroups. Although it is not clearly labeled, exponent $k$ depends on both $q$ and modulus $n$ like $\Delta_q$. It should be pointed out that $R(n)$ is not a multiplicative function. One can easily find many counterexamples for this. It is proved [7] that $R(mn) \ge R(m)R(n)$ if $m, n > 1$ and $\gcd(m, n) = 1$ with the strict equality holding for infinitely many such pairs of $m$ and $n$.

Note that $R(n)/n = (R(n)/\phi(n))(\phi(n)/n)$. But $\phi(n)/n$ is a multiplicative function and has a limiting distribution function $w(t)$ [18] in the sense that $\lim_{x\to\infty} \frac{1}{x}\#\{n \le x : \phi(n)/n \le t\}$ exists for all $t \in (0, 1)$. $w(t)$ is continuous and strictly increasing in $(0, 1)$. So the values of $\phi(n)/n$ are asymptotically evenly distributed along the number line. To see the oscillation of $\sum_{n\le x} R(n)/n$, we just need to turn our attention to $\sum_{n\le x} R(n)/\phi(n)$. Let us denote $R(n)/\phi(n)$ by $r(n)$.

For the orders for $r(n)$, it is found [8] that $\overline{\lim}_{n\to\infty} r(n) = 1$ and $\underline{\lim}_{x\to\infty} r(n)\ln\ln n = e^{-\gamma}$, where $\gamma$ is Euler's constant. It is not easy to estimate and describe the lower order of $\sum_{n\le x} r(n)$. However, if we consider $\sum_{n\le x} |\ln r(n)|$, the situation will change dramatically. Although the orders of $\sum_{n\le x} |\ln r(n)|$ may not yield directly the orders for $\sum_{n\le x} r(n)$, we can definitely get something interesting about the distribution of values of $r(n)$. It can be seen from (4) that

$$\ln r(n) = \sum_{q|\lambda(n)} \ln\left(1 - \frac{1}{q^{\Delta_q(n)}}\right) = -\sum_{\substack{\text{prime } q:\\ \Delta_q(n)=1}} \frac{1}{q} + O(1).$$

We can drop the condition $q|\lambda(n)$ in the above sum because $\Delta_q(n) = 1$ implies that $q|\lambda(n)$. Here $O(1)$ is a quantity in the interval $(-c, 0)$ for some positive constant $c$. Thus

$$\sum_{n\le x} |\ln r(n)| = \sum_{q\le x} \frac{1}{q} \sum_{\substack{n\le x\\ \Delta_q(n)=1}} 1 + O(x). \tag{5}$$

It is critical to get an accurate estimate of the inner sum in (5). For each integer $n$ counted by the inner sum, we have $\Delta_q(n) = 1$, which implies that $q^k \| \lambda(n)$ for some positive integer $k$ and $q^k \| \lambda(p^r)$ for exactly one prime power $p^r \| n$. So we can write $n = p^r \cdot m$, where $\gcd(p, m) = 1$ and $q^k \nmid \lambda(m)$. Definitely $q^k \nmid p' - 1$ for each prime factor $p'$ of $m$. Let us introduce a few notations of the sieve method. Let $\mathcal{P}_{q^k}$ be the set of primes $p \equiv 1 \bmod q^k$ and $P_{q^k}(u) := \prod_{\substack{p\le u\\ p\in\mathcal{P}_{q^k}}} p$. In addition, let us use the notation $\ln_2 x$ to represent $\ln\ln x$ and similarly for other iterations of the natural logarithmic function. We can write the inner sum of (5) as

$$\sum_{\substack{n\le x\\ \Delta_q(n)=1}} 1 = \sum_{k\ge 1} \sum_{\substack{n\le x\\ q^k\|\lambda(n)\\ \Delta_q(n)=1}} 1.$$

Note that $q^k \| \lambda(p^r)$ includes two cases: $q^k = p^{r-1}$ (except the case $8\|n$) and $q^k \| p - 1$. The total contribution from the first case to the sum is at most $O(x/q^2)$. Thus

$$\sum_{\substack{n\le x\\ \Delta_q(n)=1}} 1 = \sum_{k\ge 1} \sum_{\substack{p\le x\\ q^k\|p-1}} \sum_{r\ge 1} \sum_{\substack{m\le x/p^r\\ (m, P_{q^k}(x/p^r))=1}} 1 + O\left(\frac{x}{q^2}\right).$$

Analysis shows that some of the terms in the above sums are negligible, which can let us reduce the sums as

$$\sum_{\substack{n\le x\\ \Delta_q(n)=1}} 1=\sum_{k\ge 1}\sum_{\substack{p\le x^{\frac{1}{2}}\\ q^k\|p-1}}\sum_{\substack{m\le x/p\\ (m,P_{q^k}(x/p))=1}} 1+O\left(\frac{x\ln q}{q}\right). \tag{6}$$

By results of the sieve method [4] and results on primes in arithmetic progression [8, 16, 17], we have

$$\sum_{\substack{m\le x/p\\ (m,P_{q^k}(x/p))=1}} 1\ll \frac{x}{p}\prod_{\substack{l\le x/p\\ l\equiv 1 \bmod q^k}}\left(1-\frac{1}{l}\right)\ll \frac{x}{p}\exp\left(-\frac{\ln_2 x}{q^{k-1}(q-1)}\right).$$

Plug the estimate in (6), we have

$$\sum_{\substack{n\le x\\ \Delta_q(n)=1}} 1\ll x\sum_{k\ge 1}\frac{\ln_2 x}{q^k}\exp\left(-\frac{\ln_2 x}{q^k(1-1/q)}\right)+O\left(\frac{x\ln q}{q}\right).$$

Let $M$ be the least integer such that $q^M>\ln_2 x$. Then $M=\frac{\ln_3 x}{\ln q}-\left\{\frac{\ln_3 x}{\ln q}\right\}+1$, where $\{y\}$ represents the fractional part of number $y$. By straight calculation, it can be deduced that

$$\sum_{q^k>\ln_2 x}\frac{\ln_2 x}{q^k}\exp\left(-\frac{\ln_2 x}{q^k(1-1/q)}\right)\le \sum_{q^k>\ln_2 x}\frac{\ln_2 x}{q^k}\le \frac{2}{q^{1-\left\{\frac{\ln_3 x}{\ln q}\right\}}}.$$

On the other hand,

$$\sum_{q^k\le \ln_2 x}\frac{\ln_2 x}{q^k}\exp\left(-\frac{\ln_2 x}{q^k(1-1/q)}\right)\le \sum_{q^k\le \ln_2 x}\frac{\frac{\ln_2 x}{q^k}}{\frac{1}{2!}\left(\frac{\ln_2 x}{q^k(1-1/q)}\right)^2}\le \frac{2}{q^{\left\{\frac{\ln_3 x}{\ln q}\right\}}}.$$

For any real number $y$, let $\|y\|=\min_{n\in\mathbb{Z}}\{|y-n|\}$. Note that $\|u\|\le 1/2$. By (6), we have

$$\sum_{\substack{n\le x\\ \Delta_q(n)=1}} 1\ll \frac{x}{q^{\left\|\frac{\ln_3 x}{\ln q}\right\|}}+O\left(\frac{x\ln q}{q}\right)\ll \frac{x}{q^{\left\|\frac{\ln_3 x}{\ln q}\right\|}}.$$

By (5), we have

$$\sum_{n\le x}|\ln r(n)|\ll \sum_{q\le x}\frac{x}{q^{1+\left\|\frac{\ln_3 x}{\ln q}\right\|}}+O(x). \tag{7}$$

It can be seen easily [8] that

$$\sum_{\substack{n\le x\\ \Delta_q(n)=1}} 1\gg \sum_{q^k>\ln_2 x}\sum_{\substack{p\le x^{\frac{1}{2}}\\ q^k\|p-1}}\frac{x}{p}\gg \frac{x\ln_2 x}{q^M}=\frac{x}{q^{1-\left\{\frac{\ln_3 x}{\ln q}\right\}}}.$$

This estimate allows us to bound $\sum_{n\le x}|\ln r(n)|$ from below:

$$\sum_{n\le x}|\ln r(n)| \gg \sum_{q\le x}\frac{x}{q^{2-\left\{\frac{\ln_3 x}{\ln q}\right\}}}+O(x). \tag{8}$$

The two sums in (7) and (8) are interesting because they provide the source of oscillation in $\sum_{n\le x}|\ln r(n)|$. If there are enough primes $q$ such that $\|\ln_3 x/\ln q\|$ stay away from 0, even with $\|\ln_3 x/\ln q\| \gg 1/\ln q$, the sum in (7) will be bounded by a constant multiple of $x$. On the other hand, if there are enough primes $q$ such that $\{\ln_3 x/\ln q\}$ is close to 1, the sum in (8) will be unbounded. Although these ideas are not used directly in the actual proof, it is proved [8] that on an unbounded set of real numbers $x$, we have

$$\sum_{n\le x}|\ln r(n)| \gg x\ln_6 x,$$

and on another unbounded set of real numbers $x$, we have

$$\sum_{n\le x}|\ln r(n)| \ll x,$$

although the oscillation is really faint. The oscillations in individual functions $N_a(x)$ were found with more diligent analysis. Some of the ideas explained above are also involved.

**Competing Interests** The author declares that he has no competing interests in the artcle.

## References

[1] R.D. Carmichael (1914). The Theory of Numbers, Wiley, New York.
[2] P.D.T.A. Elliott (1980). Probabilistic number theory, volume II, Springer-Verlag, New York.
[3] R. Gupta & M. Ram Murty ((1984)). A remark on Artin's conjecture, Invent. *Math.* **78**,127 – 130.
[4] H. Halberstam & H. E. Richert (1974). Sieve methods, *Academic Press*, New York,
[5] D.R. Heath-Brown (1986). Artin's conjecture for primitive roots, *Quart. J. Math.* Oxford (2), **37**,27-38.
[6] C. Hooley (1967). On Artin's conjecture, *J. reine angew. Math.* **225**,209-20.
[7] B. Huang, Notes on the numbers of primitive $\lambda$-roots mod$n$ and its multiplicative properties, preprint.
[8] S. Li (1998). On the number of elements with maximal order in the multiplicative group modulo $n$, *Acta Arith.* **86**, 113-132.
[9] S. Li (2000). *Artin's conjecture on average for composite moduli*, *J. Number Theory* **84**, 93 - 118.
[10] S. Li (1999). *On extending Artin's conjecture to composite moduli*, Mathematika, **46**, 373 - 390.
[11] S. Li (2004). *An improvement of Artin's conjecture on average for composite moduli*, Mathematika **51** , 97-109.
[12] S. Li & C. Pomerance (2002). *Primitive roots: a survey*, Sūrikaisekikenkyūsho Kōkyūroku, no.1274, 77-87.
[13] S. Li & C. Pomerance (2003). *On generalizing Artin's conjecture on primitive roots to composite moduli*, *J. reine angew. Math.* **556**, 205-224.

[14] G. Martin (1997). The least prime primitive root and the shifted sieve, *Acta Arith.* **80**, 277-288.
[15] M.R. Murty (1988). *Artin's conjecture for primitive roots*, Math. Intelligencer **10** , no. 4, 59-67.
[16] K. K. Norton (1976). On the number of restricted prime factors of an integer I, Illinois J. Math. **20**, 681-705.
[17] C. Pomerance (1977). On the distribution of amicable numbers, *J. reine angew. Math.* **293/294**, 217-222.
[18] I. J. Schoenberg (1936). On asymptotic distributions of arithmetical functions, Trans. *Amer. Math. Soc.* **39**, 315-330.
[19] P.J. Stephens (1969). An average result for Artin's conjecture, Mathematika **16**, 178-188.
[20] A.E. Western & J.C.P. Miller (1968), Tables of Indices and Primitive roots, Royal Society Mathematical Tables, vol. 9, p. xxxviii, Cambridge, .