International Journal of Mathematics and
Computer Science, **10**(2015), no. 2, 185–194

# Least Prime Primitive Roots

**Nelson A. Carella**

Department of Mathematics and Computer Science
York college, City University of New York
Jamaica, NY 11451, USA

email: ncarella@york.cuny.edu

(Received April 5, 2015, Revised Aug. 11, 2015, Accepted Aug. 25, 2015)

**Abstract**

This note presents an upper bound for the least prime primitive roots $g^*(p)$ modulo $p$, a large prime. The current literature has several estimates of the least prime primitive root $g^*(p)$ modulo a prime $p \geq 2$ such as $g^*(p) \ll p^c, c > 2.8$. The estimate provided within seems to sharpen this estimate to the smaller estimate $g^*(p) \ll p^{5/\log\log p}$ uniformly for all large primes $p \geq 2$.

## 1 Introduction

This note provides the details for the analysis of some estimates for the least primitive root $g(p)$, and the least prime primitive root $g^*(p)$ in the cyclic group $\mathbb{Z}/(p-1)\mathbb{Z}, p \geq 2$ prime. The current literature has several estimates for the least prime primitive root $g^*(p)$ modulo a prime $p \geq 2$ such as $g^*(p) \ll p^c, c > 2.8$. The actual constant $c > 2.8$ depends on various conditions such as the factorization of $p-1$, et cetera. These results are based on sieve methods and the least primes in arithmetic progressions, see [16], [15], [10]. Moreover, there are a few other conditional estimates such as $g(p) \leq g^*(p) \ll (\log p)^6$, see [24], and the conjectured upper bound $g^*(p) \ll (\log p)(\log\log p)^2$, see [2]. On the other direction, there is the Turan lower bound $g^*(p) \geq g(p) = \Omega(\log p \log\log p)$, refer to [3], [22, p. 24], and [18] for discussions. The result stated in Theorem 1 improves the current estimate to the smaller estimate $g^*(p) \ll p^{5/\log\log p}$ uniformly for all large primes $p \geqslant 2$.

**Theorem 1.1.** Let $p \geq 3$ be a large prime. Then the following hold.

**Key words and phrases:** Prime number, Primitive root, Least primitive root, Prime primitive root, Cyclic group.
**AMS (MOS) Subject Classifications**: Primary 11A07, Secondary 11Y16, 11M26.
**ISSN** 1814-0432, 2015, http://ijmcs.future-in-tech.net

1. Almost every prime $p \geq 3$ has a prime primitive root $g^*(p) \ll (\log p)^c, c > 1$ constant.

2. Every prime $p \geq 3$ has a prime primitive root $g^*(p) \ll p^{5/\log\log p}$.

Case (1) explains the frequent occurrence of very small primitive roots for almost every prime; and case (2) explains the rare occurrence of large prime primitive roots modulo $p \geq 2$ on a subset of density zero in the set of primes. The term *for almost every prime* refers to the set of all primes, but a subset of primes of zero density. The subset of exceptional primes are of the form $p - 1 = \prod_{q \leq \log p} q^v$, where $q \geq 2$ is prime, and $v \geq 1$. The proof appears in Section five.

## 2 Basic Concepts

Let $G$ be a finite group of order $q = \#G$. The order $\text{ord}(u)$ of an element $u \in G$ is the smallest integer $d \mid q$ such that $u^d = 1$. An element $u \in G$ is called a *primitive element* if it has order $\text{ord}(u) = q$. A cyclic group $G$ is a group generated by a primitive element $\tau \in G$. Given a primitive root $\tau \in G$, every element $0 \neq u \in G$ in a cyclic group has a representation as $u = \tau^v, 0 \leq v < q$. The integer $v = \log u = \log_\tau u$ is called the *discrete logarithm* of $u$ with respect to $\tau$.

### 2.1 Simple Characters Sums

Let $d|q$. A character $\chi$ modulo $q \geq 2$, is a complex-valued periodic function $\chi : \mathbb{N} \longrightarrow \mathbb{C}$, and it has order $\text{ord}(\chi) = d \geq 1$ if and only if $\chi(n)^d = 1$ for all integers $n \in \mathbb{N}, \gcd(n, q) = 1$. For $q \neq 2^r, r \geq 2$, a multiplicative character $\chi \neq 1$ of order $\text{ord}(\chi) = d$, has a representation as

$$\chi(u) = e^{i2\pi k \log(u)/d}, \tag{1}$$

where $v = \log u$ is the discrete logarithm of $u \neq 0$ with respect to some primitive root, and for some integer $k \in \mathbb{Z}$, see [14, p. 187], [19, p. 118], and [12, p. 271]. The principal character $\chi_0 = 1 \bmod q$ has order $d = 1$, and it is defined by the relation

$$\chi_0(n) = \begin{cases} 1 & \text{if } \gcd(n, q) = 1, \\ 0 & \text{if } \gcd(n, q) \neq 1. \end{cases} \tag{2}$$

And the nonprincipal character $\chi \neq 1 \bmod q$ of order $\text{ord}(\chi) = d > 1$ is defined by the relation

$$\chi(n) = \begin{cases} \omega^{\log n} & \text{if } \gcd(n, q) = 1, \\ 0 & \text{if } \gcd(n, q) \neq 1. \end{cases} \tag{3}$$

where $\omega \in \mathbb{C}$ is a $d$th root of unity.

The Mobius function and Euler totient function occur in various formulae. For an integer $n = p_1^{v_1} p_2^{v_2} \cdots p_t^{v_t}$, with $p_k \geq 2$ prime, and $v_i \geq 1$, the Mobius function is defined by

$$\mu(n) = \begin{cases} (-1)^t & \text{if } n = p_1 p_2 \cdots p_t,\ v_k = 1 \text{ all } k \geq 1, \\ 0 & \text{if } n \neq p_1 p_2 \cdots p_t,\ v_k \geq 2 \text{ for some } k \geq 1. \end{cases} \tag{4}$$

The Euler totient function counts the number of relatively prime integers $\varphi(n) = \#\{k : \gcd(k, n) = 1\}$. This is compactly expressed by the analytic formula

$$\varphi(n) = n \prod_{d|n} (1 - 1/p) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{5}$$

**Lemma 2.1.** For a fixed integer $u \neq 0$, and an integer $q \in \mathbb{N}$, let $\chi \neq 1$ be nonprincipal character mod $q$, then

1. $$\sum_{\mathrm{ord}(\chi)=\varphi(q)} \chi(u) = \begin{cases} \varphi(q) & \text{if } u \equiv 1 \bmod q, \\ -1 & \text{if } u \not\equiv 1 \bmod q. \end{cases}$$

2. $$\sum_{1 \leq a < \varphi(q)} \chi(au) = \begin{cases} \varphi(q) & \text{if } u \equiv 1 \bmod q, \\ -1 & \text{if } u \not\equiv 1 \bmod q. \end{cases}$$

## 2.2 Representation of the Characteristic Function

The characteristic function $\Psi : G \longrightarrow \{0, 1\}$ of primitive element is one of the standard tools employed to investigate the various properties of primitive roots in cyclic groups $G$. Many equivalent representations of characteristic function $\Psi$ of primitive elements are possible. The best known representation of the characteristic function of primitive elements in finite rings is stated below.

**Lemma 2.2.** Let $G$ be a finite group of order $q = \#G$, and let $0 \neq u \in G$ be an invertible element of the group. Assume that $v = \log u$, and $e = \gcd(d, v)$. Then

$$\Psi(u) = \frac{\varphi(q)}{q} \sum_{d|q} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\chi)=d} \chi(u) = \begin{cases} 1 & \text{if } \mathrm{ord}(u) = q, \\ 0 & \text{if } \mathrm{ord}(u) \neq q. \end{cases} \tag{6}$$

Finer details on the characteristic function are given in [9, p. 863], [14, p. 258], [17, p. 18], [26], et alii. The characteristic function for multiple primitive roots is used in [6, p. 146] to study consecutive primitive roots. In [13] it is used to study the gap between primitive roots with respect to the Hamming metric. In [23] it is used to study Fermat quotients as primitive roots. And in [26] it is used to prove the existence of primitive roots in certain small subsets $A \subset \mathbb{F}_{p^n}, n \geq 1$. Many other applications are available in the literature. An introduction to character sums as in Lemmas 2.1 and 2.2 appears in [14, Chapter 6].

## 3 Basic *L*-Functions Estimates

For a character $\chi$ modulo $q \geq 2$, and a complex number $s \in \mathbb{C}, \mathcal{R}e(s) > 1$, an $L$-function is defined by the infinite sum $L(s,\chi) = \sum_{n\geq 1} \chi(n)n^{-s}$. Simple elementary estimates associated with the characteristic function of primitive roots are calculated here.

### 3.1 An *L*-Function for Prime Primitive Roots

The analysis of the least prime primitive root mod $p$ is based on the Dirichlet series

$$L(s,\Psi\Lambda) = \sum_{n\geq 1} \frac{\Psi(n)\Lambda(n)}{n^s}, \tag{7}$$

where $\Psi(n)\Lambda(n)/n^s$ is the weighted characteristic function of prime power primitive roots mod $p$. This is constructed using the characteristic function of primitive roots, which is defined by

$$\Psi(n) = \begin{cases} 1 & \text{if } n \text{ is a primitive root,} \\ 0 & \text{if } n \text{ is not a primitive root,} \end{cases} \tag{8}$$

where $p \geq 2$ is a prime, see Lemma 3 for the exact formula, and the von-Mangoldt function

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, k \geq 1, \\ 0 & \text{if } n \neq p^k, k \geq 1. \end{cases} \tag{9}$$

The function $L(s,\Psi\Lambda)$ is zerofree, and analytic on the complex half plane $\{s \in \mathbb{C} : \mathcal{R}\mathrm{e}(s) = \sigma > 1\}$. Furthermore, it has a pole at $s = 1$. This technique has a lot of flexibility and does not require delicate information on the zerofree regions $\{s \in \mathbb{C} : 0 < \mathcal{R}\mathrm{e}(s) = \sigma < 1\}$ of the associated $L$-functions. Moreover, the analysis is much simpler than the sieve methods used in the current literature – lex parsimoniae.

**Lemma 3.1.** Let $p \geq 2$ be a prime number, and let $s \in \mathbb{C}$ be a complex number, $\mathcal{R}e(s) = \sigma > 1$. Then, there is a nonnegative constant $\kappa_2 > 0$, depending on $p$, such that

$$L(s, \Psi\Lambda) = \sum_{n\geq 1} \frac{\Psi(n)\Lambda(n)}{n^s} = \kappa_2. \tag{10}$$

**Proof:** Fix a prime $p \geq 2$, and let $r_1, r_2, \ldots, r_{\varphi(p-1)}$ be the primitive roots mod $p$. Since $\Psi(n)\Lambda(n) \leq \log n$ for all integers $n \geq 2$, the series

$$L(s, \Psi\Lambda) = \sum_{n\geq 1} \frac{\Psi(n)\Lambda(n)}{n^s} \tag{11}$$

$$= \frac{\Lambda(r_1)}{r_1^s} + \frac{\Lambda(r_2)}{r_2^s} + \cdots + \frac{\Lambda\left(r_{\varphi(p-1)}\right)}{r_{\varphi(p-1)}^s} + \frac{\Lambda(p+r_1)}{(p+r_1)^s} + \frac{\Lambda(p+r_2)}{(p+r_2)^s} + \cdots$$

converges to a constant $\kappa_2 = \kappa_2(p) > 0$ whenever $\mathcal{R}e(s) = \sigma > 1$ is a real number. ■

**Example 3.2.** Take the prime $p = 13$, and its $\varphi(p-1) = 4$ primitive roots $r_1 = 2, r_2 = 6, r_3 = 7, r_4 = 11 \bmod p$. The numerical value of the series evaluated at $s = 2$ is

$$L(s, \Psi\Lambda) = \sum_{n\geqslant 1} \frac{\Psi(n)\Lambda(n)}{n^s}$$

$$= \frac{\log 2}{2^2} + \frac{\log 7}{7^2} + \frac{\log 11}{11^2} + \frac{\log 19}{19^2} + \frac{\log 37}{(2\cdot 13+11)^2} + \frac{\log 41}{(3\cdot 13+2)^2} + \cdots \tag{12}$$

$=0.243611\ldots$

**Lemma 3.3.** Let $x \geqslant 2$ be a large number. Let $p \geq 2$ be a prime, and let $\chi$ be the characters modulo $d$, where $d|(p-1)$. If $s \in \mathbb{C}$ is a complex number, $\mathcal{R}e(s) = \sigma > 1$, then

$$\sum_{n>x} \frac{\Lambda(n)}{n^s} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\chi)=d} \chi(n) = O\left(\frac{2^{\omega(p-1)}}{x^{\sigma-1}}\right). \tag{13}$$

**Proof:** For $\mathcal{R}e(s) = \sigma > 1$, the series $\sum_{n>x} \Lambda(n)n^{-s}$ is absolutely convergent. Rearranging the absolutely convergent series and taking absolute value yield

$$\left|\sum_{n>x} \frac{\Lambda(n)}{n^s} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\chi)=d} \chi(n)\right| = \left|\sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\chi)=d,} \sum_{n>x} \frac{\chi(n)\Lambda(n)}{n^s}\right|$$

$$\leq \sum_{d|p-1} \mu^2(d) \left| \sum_{n>x} \frac{\chi(n)\Lambda(n)}{n^s} \right| \tag{14}$$

The infinite sum is estimated, using Abel summation formula, (discussed in [19, p. 12] and [25], as

$$\sum_{n>x} \frac{\chi(n)\Lambda(n)}{n^s} = \int_x^\infty \frac{1}{t^s} d\psi_\chi(t), \tag{15}$$

where

$$|\psi_\chi(x)| = \left| \sum_{n\leq x} \chi(n)\Lambda(n) \right| \ll x. \tag{16}$$

Estimate the integral to complete the calculation. ■

## 4 Prime Divisors Counting Function

For $n \in \mathbb{N}$, the prime counting function is defined by $\omega(n) = \#\{p|n\}$. Somewhat similar proofs of the various properties of the arithmetic function $\omega(n)$ are given in [11, p. 473], [19, p. 55], [7, p. 34], [25, p. 83], and other references.

**Lemma 4.1.** Let $n \geq 1$ be a large integer. Then,

1. Almost every integer $n \geq 1$ satisfies the inequality

$$\omega(n) \leq \log\log n + B_1 + (\gamma - 1)/\log n + O\left(e^{-c\sqrt{\log n}}\right). \tag{17}$$

2. Every integer $n \geqslant 1$ satisfies the inequality

$$\omega(n) \leq \log n/\log\log n + O\left(\log n e^{-c\sqrt{\log n}}\right). \tag{18}$$

**Lemma 4.2.** Let $n \geq 1$ be a large integer. Then,

1. Almost every integer $n \geq 1$ satisfies the number of squarefree divisors inequality

$$2^{\omega(n)} \leq 2^{\log\log n + B_1 + (\gamma-1)/\log n + o(1)}. \tag{19}$$

2. For every integer $n \geq 1$, the number of squarefree divisors satisfies the inequality

$$2^{\omega(n)} \leq 2^{\log n/\log\log n + o(\log n/\log\log n)}. \tag{20}$$

The Euler constant is defined by the asymptotic formula

$$\gamma = \lim_{x\to\infty} \left( \sum_{n\leq x} 1/n - \log x \right) \tag{21}$$

the Mertens constant is defined by the asymptotic formula

$$B_1 = \lim_{x\to\infty} \left( \sum_{p\leq x} 1/p - \text{loglog}x \right), \tag{22}$$

and $c > 0$ is an absolute constant.

## 5 The Least Prime Primitive Roots

It is expected that there are estimates for the least prime primitive roots $g(p)^* \geq g(p)$, which are quite similar to the estimates for the least primitive roots $g(p)$. This is a very small quantity and nowhere near the currently proved results. In fact, the numerical tables confirm that the least prime primitive roots are very small, and nearly the same magnitude as the least primitive roots, but have more complex patterns, see [21].

**Proof of Theorem 1.1:** Fix a large prime $p \geq 2$, and consider summing the weighted characteristic function $\Psi(n)\Lambda(n)/n^s$ over a small range of prime powers $q^k \leq x, k \geq 1$, see Lemma 2.2. Then, the nonexistence equation

$$0 = \sum_{n\leq x} \frac{\Psi(n)\Lambda(n)}{n^s} = \sum_{n\leq x} \frac{\Lambda(n)}{n^s} \left( \frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\text{ord}(\chi)=d} \chi(n) \right), \tag{23}$$

where $s \in \mathbb{C}$ is a complex number, $\mathcal{R}e(s) = \sigma \geq 1$, holds if and only if there are no prime power primitive roots in the interval $[1, x]$.

Applying Lemma 4.1, and Lemma 4.2 with $q = p - 1$, and $s = 2$, yield

$$\begin{aligned} 0 &= \sum_{n\leq x} \frac{\Lambda(n)}{n^s} \left( \frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\text{ord}(\chi)=d} \chi(n) \right) && (24) \\ &= \sum_{n\geq 1} \frac{\Psi(n)\Lambda(n)}{n^s} - \sum_{n>x} \frac{\Psi(n)\Lambda(n)}{n^s} && (25) \\ &= \kappa_2 + O\left( \frac{2^{\omega(p-1)}}{x} \right), && (26) \end{aligned}$$

where $\kappa_2 = \kappa_2(p) > 0$ is a constant, which depends on the fixed prime $p \geq 2$.

**Case (i):** Restriction to the average integers $p-1$, with $2^{\omega(p-1)} \ll \log p$. Refer to Lemmas 4.1 and 4.2.

Let $x = (\log p)^{1+\varepsilon}, \varepsilon > 0$, and suppose that the short interval $[2, (\log p)^{1+\varepsilon}]$ does not contain prime primitive roots. Then, replacing these information in (24) yield

$$\begin{aligned} 0 &= \sum_{n\leq x} \frac{\Lambda(n)}{n^2}\left(\frac{\varphi(p-1)}{p-1}\sum_{d|p-1}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(n)\right) && (27)\\ &= \kappa_2 + O\left(\frac{2^{\omega(p-1)}}{x}\right) && (28)\\ &= \kappa_2 + O\left(\frac{1}{(\log p)^{\varepsilon}}\right) > 0. && (29)\end{aligned}$$

Since $\kappa_2 > 0$ is a constant, this is a contradiction for all sufficiently large prime $p \geq 3$.

**Case (ii):** No restrictions on the integers $p-1$, with $2^{\omega(p-1)} \ll p^{4/\log\log p}$. Refer to Lemmas 4.1 and 4.2.

Let $x = p^{5/\log\log p}$, and suppose that the short interval $[2, p^{5/\log\log p}]$ does not contain prime primitive roots. Then, replacing these information in (24) yield

$$\begin{aligned} 0 &= \sum_{n\leq x} \frac{\Lambda(n)}{n^2}\left(\frac{\varphi(p-1)}{p-1}\sum_{d|p-1}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(n)\right) && (30)\\ &= \kappa_2 + O\left(\frac{2^{\omega(p-1)}}{x}\right) && (31)\\ &= \kappa_2 + O\left(\frac{1}{p^{1/\log\log p}}\right) > 0. && (32)\end{aligned}$$

Since $\kappa_2 > 0$ is a constant, this is a contradiction for all sufficiently large prime $p \geq 3$. ■

## References

[1] Christopher Ambrose, On the least primitive root expressible as a sum of two squares, Mathematisches Institut, Universitat Gottingen, PhD Thesis, 2014.

[2] Eric Bach, Comments on search procedures for primitive roots, Math. Comp., **66,** no. 220, (1997), 1719-1727.

[3] D. A. Burgess, The average of the least primitive root modulo $p > 2$, Acta Arith., **18,** (1971), 263-271.

[4] D. A. Burgess, P. D. T. A. Elliott, The average of the least primitive root, Mathematika, **15,** (1968), 39-50.

[5] D. A. Burgess, On character sums and primitive roots, Proc. London Math. Soc., **3,** no. 12, (1962), 179-192.

[6] C. I. Cobeli, S. M. Gonek, A. Zaharescu, On the distribution of small powers of a primitive root, J. Number Theory, **88,** no. 1, (2001), 49-58.

[7] Alina Carmen Cojocaru, M. Ram Murty, An introduction to sieve methods and their applications, London Mathematical Society Student Texts, **66,** Cambridge University Press, Cambridge, 2006.

[8] P. D. T. A. Elliott, Leo Murata, On the average of the least primitive root modulo $p$, J. London Math. Soc., **(2) 56,** no. 3, (1997), 435-454.

[9] Paul Erdos, Harold N. Shapiro, On The Least Primitive Root Of a Prime, 1957, euclidproject.org.

[10] Junsoo Ha, On the least prime primitive root, J. Number Theory, **133,** no. 11, (2013), 3645-3669.

[11] G. H. Hardy, E. M. Wright, An introduction to the theory of numbers, Sixth edition, Revised by D. R. Heath-Brown, J. H. Silverman with a foreword by Andrew Wiles, Oxford University Press, 2008.

[12] Henryk Iwaniec, Emmanuel Kowalski, Analytic number theory, American Mathematical Society Colloquium Publications, **53,** American Mathematical Society, Providence, RI, 2004.

[13] Sergei V. Konyagin, Igor E. Shparlinski, On the consecutive powers of a primitive root: gaps and exponential sums, Mathematika, **58,** (2012), no. 1, 11-20.

[14] Rudolf Lidl, Harald Niederreiter, Finite fields, with a foreword by P. M. Cohn, Second edition, Encyclopedia of Mathematics and its Applications, **20,** Cambridge University Press, Cambridge, 1997.

[15] Martin, Greg. Uniform bounds for the least almost-prime primitive root, Mathematika, **45,** (1998), no. 1, 191-207.

[16] Greg Martin, The least prime primitive root and the shifted sieve, Acta Arith., **80,** no. 3, (1997), 277-288.

[17] Pieter Moree, Artin's primitive root conjecture, a survey, arXiv:math/0412262.

[18] Leo Murata, On the magnitude of the least prime primitive root, J. Number Theory **37,** no. 1, (1991), 47-66.

[19] Hugh L. Montgomery, Robert C. Vaughan, Multiplicative number theory I. Classical theory, Cambridge University Press, Cambridge, 2007.

[20] W. Narkiewicz, The development of prime number theory, from Euclid to Hardy and Littlewood, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[21] A. Paszkiewicz, A. Schinzel, On the least prime primitive root modulo a prime, Math. Comp. **71,** no. 239, (2002), 1307-1321.

[22] Paulo Ribenboim, The new book of prime number records, Springer-Verlag, Berlin, New York, 1996.

[23] Igor E. Shparlinski, Fermat quotients: Exponential sums, value set and primitive roots, arXiv:1104.3909.

[24] Vicor Shoup, Searching for primitive roots in finite fields, Math. Comp., **58,** no. 197, (1992), 369-380.

[25] G. Tenenbaum, Introduction to analytic and probabilistic number theory, Cambridge Studies in Advanced Mathematics, **46,** Cambridge University Press, Cambridge, 1995.

[26] Arne Winterhof, Character sums, primitive elements, and powers in finite fields, J. Number Theory, **91,** no. 1, (2001), 153-163.