Research Article

Nelson Carella*

# The least primitive roots mod *p*

https://doi.org/10.1515/jmc-2024-0017
received April 10, 2024; accepted December 12, 2024

**Abstract:** Let $p > 1$ be a large prime number, and let $\varepsilon > 0$ be a small number. The established unconditional upper bounds of the least primitive root $u \neq \pm 1, v^2$ in the prime finite field $\mathbb{F}_p$ have exponential magnitudes $u \ll p^{1/4+\varepsilon}$. This note contributes a new result to the literature. It proves that the upper bound of the least primitive root has polynomial magnitude $u \leq (\log p)^{1+\varepsilon}$ unconditionally.

**Keywords:** primitive root, least primitive root, finite field, cryptographic algorithm, complexity theory

**MSC 2020:** 11A07, 11N05, 11N32

## 1 Introduction

The established unconditional upper bounds of the least primitive root $u \neq \pm 1, v^2$ in the prime finite field $\mathbb{F}_p$ seem to have exponential magnitudes $u \ll p^{1/4+\varepsilon}$, see [1, Theorem 3], and the established conditional upper bounds seem to have polynomial magnitudes $u \ll (\log p)^{6+\varepsilon}$ (see [2, Theorem 1.3]). Moreover, there is a partial result of the form $u < 475(\log p)^{8/5}$ for infinitely many primes (see [3, Theorem 3]). Finally, there is a conjectured upper bound of the form $u \ll (\log p)(\log \log p)^2$ – the heuristic appears in [4, Section 4]. This note proposes a new result on the theory of primitive roots in finite fields, and it proves the conjectured upper bound for all large primes unconditionally. This result sharpens both the established unconditional results and the established conditional results.

**Theorem 1.1.** *Let $p \geq p_0$ be a large prime number, and let $\varepsilon > 0$ be a small real number. Then, there exists a primitive root $u \neq \pm 1, v^2$ in the prime finite field $\mathbb{F}_p$ such that*

$$u \ll (\log p)^{1+\varepsilon}.$$

In practice, this result holds for prime numbers $p$ that are significantly smaller than the explicit lower bound $p \geq p_0 > 2^{2145} \approx 10^{645}$ estimated in Section 5. In fact, the numerical data in [5, Table 1] show that the least primitive roots modulo $p$ have very small magnitudes $O((\log p)(\log \log p)^2)$ for all primes, as conjectured, even the least prime primitive roots have the same upper bound.

Given the prime factorization of the totient $p - 1$, an application of Theorem 1.1 leads to a deterministic primitive root search algorithm of polynomial time complexity $O((\log p)^c)$, where $c > 1$ is constant. In contrast, the established deterministic primitive root search algorithm seems to have exponential time complexity $O(p^{1/4+\varepsilon})$ (see [6, Theorem]). Similar primitive root search algorithms are studied by Grossman [7] and a survey of the literature and the most recent primitive root search algorithm appear by the study by Shparlinski [8]. Another application of Theorem 1.1 leads to a deterministic primality test algorithm of polynomial time complexity $O((\log p)^{4+\varepsilon})$, and the technical details appear in previous studies [9], [10], and [11, p. 1]. In contrast, the established deterministic primality test algorithms have higher time complexities: the AKS

* **Corresponding author: Nelson Carella,** Department of Mathematics, Fordham University and CUNY, Bronx, NY 10458, New York, United States of America, e-mail: pobox5050@gmail.com

algorithm has a running time complexity of $O((\log p)^{15/2})$ arithmetic operations (see [12, Theorem 5.3]) and the Gaussian period algorithm has a running time complexity of $O((\log p)^{6})$ arithmetic operations (see [13, Theorem 1]. Furthermore, this result can be used to construct other related deterministic cryptographic algorithms of polynomial time complexities, such as the squareroot mod $p$ and signature schemes as in the study by Brier et al. [14], etc.

This innovation is made possible by a new representation of the characteristic function for primitive roots, described in Lemma 3.2. It is much simpler than the standard characteristic function for primitive roots in finite fields, described in Lemma 3.1. In addition, it significantly simplifies some of the standard analytic methods utilized in the theory of primitive roots; consult the relevant literature such as [15], [16], [17], [5], et al. to compare the differences. The foundation of the main result is covered in Sections 3–8. Last but not least, the proof of Theorem 1.1 appears in Section 9.

# 2 Notation

The set $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ denotes the set of nonnegative integers, the set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ denotes the set of integers, and the set $\mathbb{P} = \{2, 3, 5, \ldots\}$ denotes the set of prime numbers. The letters $p, q, r \in \mathbb{P}$ usually denote arbitrary prime numbers, and the letters $a, b, c, k, m, n \in \mathbb{N}$ usually denote arbitrary integers.

- The symbol $\log x = \ln x$ denotes the natural logarithm.
- Let $f, g : [x_0, \infty] \longrightarrow \mathbb{R}$ be a pair of functions and assume $g(x) > 0$. The big O notation is defined by
$$f(x) = O(g(x)) \Leftrightarrow |f(x)| \leq cg(x), \tag{1}$$
for some constant $c > 0$ as $x \to \infty$.
- The symbol $\ll$ is defined by
$$f(x) \ll g(x) \Leftrightarrow |f(x)| \leq cg(x), \tag{2}$$
for some constant $c > 0$ as $x \to \infty$.

# 3 Representations of the characteristic function

The *multiplicative order* of an element in a finite field is defined by $\operatorname{ord}_p u = \min\{k : u^k \equiv 1 \bmod p\}$. An element $u \neq \pm 1, v^2$ is called a *primitive root* if $\operatorname{ord}_p u = p - 1$. The *characteristic function* $\Psi : G \longrightarrow \{0, 1\}$ of primitive elements is one of the standard analytic tools employed to investigate the various properties of primitive roots in cyclic groups $G$. Many equivalent representations of the characteristic function $\Psi$ of primitive elements are possible. Two of these representations are investigated here.

## 3.1 Divisor-dependent characteristic function

The *divisor-dependent* characteristic function was developed about a century ago (see [18, Theorem 496], [16, Lemma 2.3], [19, p. 258]), et al. This characteristic function detects the multiplicative order of an element by means of the divisors of the totient $p - 1$. The precise description is stated in the following.

**Lemma 3.1.** *Let $p \geq 2$ be a prime, and let $\chi$ be a multiplicative character of multiplicative order* $\operatorname{ord}\chi = d$, *where* $d | p - 1$. *If $u \in \mathbb{F}_p$ is a nonzero element, then*
$$\Psi(u) = \frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}\chi = d} \chi(u) = \begin{cases} 1, & \textit{if } \operatorname{ord}_p(u) = p - 1, \\ 0, & \textit{if } \operatorname{ord}_p(u) \neq p - 1, \end{cases}$$
*where $\mu : \mathbb{N} \longrightarrow \{-1, 0, 1\}$ is the Mobius function.*

There are a few variant proofs of this result, and these proofs are widely available in the literature. Almost every result in the theory of primitive roots in finite fields is based on this characteristic function, but sometimes written in different forms. This techniques was developed by Landau [18], Vinogradov, [20], Erdos [21]. An extension of this characteristic function to the finite ring $\mathbb{Z}/n\mathbb{Z}$ is presented in [22, Lemma 4]. The main obstacle in this technique is the prime decomposition of the totients $p-1$.

### 3.2 Divisor-free characteristic function

A new *divisors-free* representation of the characteristic function of primitive element is developed here. It is completely independent of the prime decomposition of the totients $p-1$. It detects the multiplicative order $\operatorname{ord}_p(u) \geq 1$ of the element $u \in \mathbb{F}_p$ by means of the solutions of the equation $\tau^n - u = 0$ in $\mathbb{F}_p$, where $u$ and $\tau$ are constants, and $n \in \mathscr{R} = \{n < p : \gcd(n, p-1) = 1\}$ is a variable. This is the original source of this result, and it is the product of many years of research in number theory and finite fields.

**Lemma 3.2.** *Let $p \geq 2$ be a prime, and let $\tau$ be a primitive root mod $p$ and let $\psi \neq 1$ be a nonprincipal additive character of order* $\operatorname{ord}\psi = p$. *If $u \in \mathbb{F}_p$ is a nonzero element, then*

$$\Psi(u) = \sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0 \leq s \leq p-1} \psi((\tau^n - u)s) = \begin{cases} 1, & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0, & \text{if } \operatorname{ord}_p(u) \neq p-1. \end{cases}$$

**Proof.** Set the additive character $\psi(s) = e^{i2\pi as/p}$, where $a \in \mathbb{F}_p^\times$. As the index $n \in \mathscr{R} = \{n < p : \gcd(n, p-1) = 1\}$ ranges over the integers relatively prime to $\varphi(p) = p-1$, the element $\tau^n \in \mathbb{F}_p^\times$ ranges over the primitive roots modulo $p$. Accordingly, the equation $a = \tau^n - u = 0$ has a unique solution $n \in \mathscr{R}$ if and only if the fixed element $u \in \mathbb{F}_p$ is a primitive root. This implies that the inner sum in

$$\sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0 \leq s < p} e^{i2\pi \frac{(\tau^n - u)s}{p}} = \begin{cases} 1, & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0, & \text{if } \operatorname{ord}_p(u) \neq p-1. \end{cases} \tag{3}$$

collapses to $\sum_{0 \leq s < p} e^{i2\pi as/p} = \sum_{0 \leq s < p} 1 = p$. Otherwise, if the element $u \in \mathbb{F}_p$ is not a primitive root, then the equation $a = \tau^n - u = 0$ has no solution $n \in \mathscr{R}$, and the inner sum in (3) collapses to $\sum_{0 \leq s < p} e^{i2\pi as/p} = 0$, this follows from the geometric series formula $\sum_{0 \leq n \leq N-1} w^n = (w^N - 1)/(w-1)$, where $w = e^{i2\pi a/p} \neq 1$ and $N = p$. □

## 4 Results on exponential sums

The exponential sums of interest in this analysis are presented in this section.

**Lemma 4.1.** *Let $p \geq 2$ be a large prime, and let $x \leq p$. If $\tau$ is a primitive root modulo $p$ and $a \in [1, p-1]$, then*

$$\sum_{\substack{1 \leq n \leq x \\ \gcd(n,p-1)=1}} e^{i2\pi a\tau^n/p} \ll p^{1/2+\delta}, \tag{4}$$

*where $\delta > 0$ is a small real number.*

**Proof.** The complete proof appears in [23, Lemma 4.1]. □

**Lemma 4.2.** *Let $p \geq 2$ be a large prime, and let $x \leq p$. If $\tau$ is a primitive root modulo $p$ and $a \in [1, p-1]$, then*

$$\sum_{\substack{1 \leq n \leq x \\ \gcd(n,p-1)=1}} e^{i2\pi a\tau^n/p} = \sum_{\substack{1 \leq n \leq x \\ \gcd(n,p-1)=1}} e^{i2\pi\tau^n/p} + O(p^{1/2+\delta}), \tag{5}$$

*where $\delta > 0$ is a small real number and the implied constant is independent of $a \neq 0$.*

**Proof.** The complete proof appears in [23, Lemma 4.3]. □

## 5 Lower bound of the totient function

The totient function is defined by $\varphi(n) = \#\{m : \gcd(m, n) = 1\} = n\prod_{r\mid n}(1 - 1/r)$, where $r \geq 2$ varies over the prime divisors of $n$ (see [24, Theorem 2.4]). This subsection provides a detailed proof of the lower bound of this function.

**Lemma 5.1.** *If $p$ is a large prime, then*

$$\frac{\varphi(p-1)}{p} \gg \frac{1}{\log\log p}.$$

**Proof.** For any prime $p$, the ratio $\varphi(p-1)/p$ can be rewritten as a product over the prime

$$\frac{\varphi(p-1)}{p} = \frac{p-1}{p} \cdot \frac{\varphi(p-1)}{p-1} = \frac{p-1}{p} \prod_{r\mid p-1}\left(1 - \frac{1}{r}\right), \tag{6}$$

where $r \geq 2$ ranges over the prime divisor of $p - 1$. This step follows from the identity $\varphi(n)/n = \prod_{r\mid n}(1 - 1/r)$, where $r \geq 2$ ranges over the prime divisors of $n$. Since the number $p - 1$ has fewer than $2\log p$ prime divisors (see [25, Theorem 2.10]), let $x = 2\log p$. Then, an application of the lower bound of the product given in [26, Theorem 6.12] yields

$$\begin{aligned} \frac{\varphi(p-1)}{p} &\geq \frac{p-1}{p} \prod_{r \leq 2\log p}\left(1 - \frac{1}{r}\right) \\ &> \frac{p-1}{p} \cdot \frac{e^{-\gamma}}{\log(2\log p)}\left(1 - \frac{0.2}{(\log(2\log p))^2}\right) \\ &\gg \frac{1}{\log\log p} > 0, \end{aligned} \tag{7}$$

where $\gamma > 0$ is the Euler constant. □

An alternative result for the lower bound of the ratio $\varphi(n)/n$ appears in [25, Theorem 2.9].

**Remark 5.1.** The explicit lower bound $p \geq p_0 > 2^{2145} \approx 10^{645}$ is derived from the explicit parameter $x = 2\log p_0 > 2{,}973$ for the totient product given in [26, Theorem 6.12] and the extreme value of the prime divisor counting function $\omega(p-1) \leq 2\log p$. However, on average, the order of $\omega(p-1)$ is significantly smaller, i.e., $x = (\log\log p)^3/2$ (see [27, Theorem 3.1] for more details). Thus, on average, the explicit lower bound is expected to be significantly smaller than $p_0 > 10^{645}$.

## 6 Fibers and multiplicities result

The multiplicities of certain values occurring in the estimate of the error term $E(z)$ are computed in this section.

**Lemma 6.1.** *Let $p$ be an odd prime, let $z = (\log p)^{1+\varepsilon}$, and let $\tau \in \mathbb{F}_p$ be a primitive root in the finite field $\mathbb{F}_p$. Define the maps*

$$\alpha(n, u) \equiv (\tau^n - u) \bmod p \quad \text{and} \quad \beta(a, b) \equiv ab \bmod p. \tag{8}$$

*Then, the fibers $\alpha^{-1}(m)$ and $\beta^{-1}(m)$ of an element $0 \neq m \in \mathbb{F}_p$ have the cardinalities*

$$\#\alpha^{-1}(m) \leq z - 1 \quad \text{and} \quad \#\beta^{-1}(m) = z, \tag{9}$$

*respectively.*

**Proof.** Let $\mathscr{R} = \{n < p : \gcd(n, p-1) = 1\}$. Given a fixed $u \in [2, z]$, the map

$$\alpha : \mathscr{R} \times [2, z] \longrightarrow \mathbb{F}_p, \quad \text{defined by} \quad \alpha(n, u) \equiv (\tau^n - u) \bmod p, \tag{10}$$

is one-to-one. This follows from the fact that the map $n \longrightarrow \tau^n \bmod p$ is a permutation of the nonezero elements of the finite field $\mathbb{F}_p$, and the restriction map $n \longrightarrow (\tau^n - u) \bmod p$ is a shifted permutation, and it maps the subset

$$\mathscr{R} \subset \mathbb{F}_p \quad \text{to} \quad \mathscr{R} - u \subset \mathbb{F}_p, \tag{11}$$

see [19, Chapter 7] for extensive details on the theory of permutation functions of finite fields. Thus, as $(n, u) \in \mathscr{R} \times [2, z]$ varies, a value $m = \alpha(n, u) \in \mathbb{F}_p$ is repeated at most $z - 1$ times. Moreover, the premises no primitive root $u \le z = (\log p)^{1+\varepsilon}$ implies that $m = \alpha(n, u) \ne 0$. This verifies that the cardinality of the fiber is

$$\#\alpha^{-1}(m) = \#\{(n, u) \in \mathscr{R} \times [2, z] : m \equiv (\tau^n - u) \bmod p\} \le z - 1. \tag{12}$$

Similarly, given a fixed $a \in [1, z]$, the map

$$\beta : [1, z] \times [1, p-1] \longrightarrow \mathbb{F}_p, \quad \text{defined by} \quad \beta(a, b) \equiv ab \bmod p, \tag{13}$$

is one-to-one. Here, the map $b \longrightarrow ab \bmod p$ permutes the nonzero elements of the finite field $\mathbb{F}_p$. Thus, as $(a, b) \in [1, z] \times [1, p-1]$ varies, each value $m = \beta(a, b) \in \mathbb{F}_p^\times$ is repeated exactly $z$ times. This verifies that the cardinality of the fiber is

$$\#\beta^{-1}(m) = \#\{(a, b) \in [1, z] \times [1, p-1] : m \equiv ab \bmod p\} = z. \tag{14}$$

□

## 7 Evaluation of the main term

An asymptotic formula for the main term $M(z)$ is computed in this section.

**Lemma 7.1.** *Let $\varepsilon > 0$ be a small real number. If $p \ge 2$ is a large prime and $u \le z = (\log p)^{1+\varepsilon}$, then*

$$\sum_{2 \le u \le z} \frac{1}{p} \sum_{\substack{1 \le n \le p-1 \\ \gcd(n, p-1) = 1}} 1 = \frac{\varphi(p-1)}{p} \cdot (\log p)^{1+\varepsilon} + O(1).$$

**Proof.** The number of relatively prime integers $n < p$ coincides with the values of the totient function. Thus, a routine rearrangement gives

$$\begin{aligned}\sum_{2 \le u \le z} \frac{1}{p} \sum_{\substack{1 \le n \le p-1 \\ \gcd(n, p-1) = 1}} 1 &= \frac{\varphi(p-1)}{p} \sum_{2 \le u \le z} 1 \\ &= \frac{\varphi(p-1)}{p} ((\log p)^{1+\varepsilon} - 1) \\ &= \frac{\varphi(p-1)}{p} \cdot (\log p)^{1+\varepsilon} + O(1),\end{aligned} \tag{15}$$

where $\varphi(p-1)/p < 1$. □

## 8 Estimate of the error term

A nontrivial upper bound of the error term is computed in this section. To achieve this objective, the error term is partitioned as $E(z) = E_0(z) + E_1(z)$. The upper bound of the first term $E_0(z)$ for $n < p/z$ is derived using geometric summation/sine approximation techniques, and the upper bound of the second term $E_1(z)$ for $p/z \le n \le p$ is derived using exponential sums techniques.

**Lemma 8.1.** *Let $\varepsilon > 0$ be a small real number. Suppose $p \ge 2$ is a large prime and $u \le z = (\log p)^{1+\varepsilon}$ . If there is no primitive root $u \le z = (\log p)^{1+\varepsilon}$ , then*

$$\sum_{2\le u\le z} \frac{1}{p} \sum_{\substack{1\le n\le p-1\\ \gcd(n,p-1)=1}} \sum_{1\le s\le p-1} \psi((\tau^n - u)s) \ll (\log p)(\log\log p),$$

*where $\psi(s) = e^{i2\pi ks/p}$, with $0 < k < p$, is an additive character.*

**Proof.** The product of a point $(a, b) \in [1, z] \times [1, p/z)$ satisfies $ab < p$. This leads to the partition $[1, p/z) \cup [p/z, p)$ of the index $n$, which is suitable for the sine approximation $ab/p \ll \sin(\pi ab/p) \ll ab/p$ for $|ab/p| < 1$ on the first subinterval $[1, p/z)$ (21). Thus, consider the partition of the triple finite sum

$$\begin{aligned} E(z) &= \sum_{2\le u\le z} \frac{1}{p} \sum_{\substack{1\le n\le p-1\\ \gcd(n,p-1)=1}} \sum_{1\le s\le p-1} e^{i2\pi\frac{(\tau^n-u)s}{p}} \\ &= \sum_{2\le u\le z} \frac{1}{p} \sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}} \sum_{1\le s\le p-1} e^{i2\pi\frac{(\tau^n-u)s}{p}} + \sum_{2\le u\le z} \frac{1}{p} \sum_{\substack{p/z\le n\le p-1\\ \gcd(n,p-1)=1}} \sum_{1\le s\le p-1} e^{i2\pi\frac{(\tau^n-u)s}{p}} \\ &= E_0(z) + E_1(z). \end{aligned} \tag{16}$$

The first suberror term $E_0(z)$ is estimated in Lemma 8.2, and the second suberror term $E_1(z)$ is estimated in Lemma 8.3. Summing these estimates yields

$$E(z) = E_0(z) + E_1(z) \ll (\log z)(\log p) + \frac{z}{p^{1/2-\delta}} \ll (\log z)(\log p), \tag{17}$$

where $\delta > 0$ is a small real number. This completes the estimate of the error term. □

**Lemma 8.2.** *Let $p \ge 2$ be large primes. If $\tau$ is a primitive root modulo $p$ and there is no primitive root $u \le z = (\log p)^{1+\varepsilon}$ , then*

$$E_0(z) = \sum_{2\le u\le z} \frac{1}{p} \sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}} \sum_{1\le s\le p-1} e^{i2\pi\frac{(\tau^n-u)s}{p}} = O((\log z)(\log p)). \tag{18}$$

**Proof.** To apply the geometric summation/sine approximation techniques, the subsum $E_0(z)$ is partitioned as follows:

$$\begin{aligned} E_0(z) &= \sum_{2\le u\le z} \frac{1}{p} \sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}} \sum_{1\le s\le p-1} e^{i2\pi\frac{(\tau^n-u)s}{p}} \\ &= \sum_{2\le u\le z} \frac{1}{p} \sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}} \left( \sum_{1\le s\le p/2} e^{i2\pi\frac{(\tau^n-u)s}{p}} + \sum_{p/2<s\le p-1} e^{i2\pi\frac{(\tau^n-u)s}{p}} \right) \\ &= E_{0,0}(z) + E_{0,1}(z). \end{aligned} \tag{19}$$

Now, a geometric series summation of the inner finite sum in the first term yields

$$\begin{aligned} E_{0,0}(z) &= \sum_{2\le u\le z}\frac{1}{p}\sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}}\ \sum_{1\le s\le p/2} e^{i2\pi\frac{(\tau^n-u)s}{p}} \\ &= \frac{1}{p}\sum_{2\le u\le z}\ \sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}} \frac{e^{i2\pi(\frac{\tau^n-u}{p})(\frac{p}{2}+1)}-e^{i2\pi\frac{(\tau^n-u)}{p}}}{1-e^{i2\pi\frac{(\tau^n-u)}{p}}} \\ &\le \frac{1}{p}\sum_{2\le u\le z}\ \sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}} \frac{2}{|\sin\pi(\tau^n-u)/p|}, \end{aligned} \tag{20}$$

where the last line in (20) follows from the hypothesis that $u$ is not a primitive root. Specifically, $0\ne\tau^n-u\in\mathbb{F}_p$ for any $n\ge1$ such that $\gcd(n,p-1)=1$ and any $u\le z=(\log p)^{1+\varepsilon}$. Similar estimations using geometric series summation/sine approximation appear in [28, Chapter 23]. Utilizing Lemma 6.1, the first term has the upper bound

$$\begin{aligned} E_{0,0}(z) &= \frac{1}{p}\sum_{2\le u\le z}\ \sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}} \frac{2}{|\sin\pi(\tau^n-u)/p|} \\ &\ll \frac{2}{p}\sum_{1\le a\le z}\ \sum_{1\le b<p/z}\frac{1}{|\sin\pi ab/p|} \\ &\ll \frac{2}{p}\sum_{1\le a\le z}\ \sum_{1\le b<p}\frac{p}{\pi ab} \\ &\ll \sum_{1\le a\le z}\frac{1}{a}\sum_{1\le b<p}\frac{1}{b} \\ &\ll (\log z)(\log p), \end{aligned} \tag{21}$$

where $ab<p$ and $|\sin\pi ab/p|\ne0$ since $p\nmid ab$. Similarly, the second term has the upper bound

$$\begin{aligned} E_{0,1}(z) &= \sum_{2\le u\le z}\frac{1}{p}\sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}}\ \sum_{p/2<s\le p-1} e^{i2\pi\frac{(\tau^n-u)s}{p}} \\ &= \frac{1}{p}\sum_{2\le u\le z}\ \sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}} \frac{e^{i2\pi\frac{(\tau^n-u)}{p}}-e^{i2\pi(\frac{\tau^n-u}{p})(\frac{p}{2}+1)}}{1-e^{i2\pi\frac{(\tau^n-u)}{p}}} \\ &\le \frac{1}{p}\sum_{2\le u\le z}\ \sum_{\substack{1\le n<p/z\\ \gcd(n,p-1)=1}} \frac{2}{|\sin\pi(\tau^n-u)/p|} \\ &\ll (\log z)(\log p). \end{aligned} \tag{22}$$

This is computed in the way as done in (20) to (21), mutatis mutandis. Summing (21) and (22) yields

$$E_0(z)=E_{0,0}(z)+E_{0,1}(z)\ll(\log z)(\log p). \tag{23}$$

□

**Lemma 8.3.** *Let $p\ge2$ be a large prime. If $\tau$ is a primitive root modulo $p$ and there is no primitive root $u\le z=(\log p)^{1+\varepsilon}$, then*

$$E_1(z)=\sum_{2\le u\le z}\frac{1}{p}\sum_{\substack{p/z\le n\le p-1\\ \gcd(n,p-1)=1}}\ \sum_{1\le s\le p-1} e^{i2\pi\frac{(\tau^n-u)s}{p}}=O\left(\frac{z}{p^{1/2-\delta}}\right), \tag{24}$$

*where $\delta>0$ is a small real number.*

**Proof.** The hypothesis that there is no primitive root such that $\tau^n - u \neq 0$ in the finite field $\mathbb{F}_p$ for any $u \leq z$ and $\gcd(n, p-1) = 1$, implies that $E_1(z)$ has a nontrivial upper bound. To determine an upper bound, rearrange the triple finite sum $E_1(z)$ and apply Lemma 4.2 to the new inner sum on the second line in the following:

$$\begin{aligned} E_1(z) &= \sum_{2\leq u\leq z} \frac{1}{p} \sum_{\substack{p/z\leq n\leq p-1\\ \gcd(n,p-1)=1}} \sum_{1\leq s\leq p-1} e^{i2\pi\frac{(\tau^n-u)s}{p}} \\ &= \frac{1}{p} \sum_{2\leq u\leq z} \sum_{1\leq s\leq p-1} e^{\frac{-i2\pi us}{p}} \sum_{\substack{p/z\leq n\leq p-1\\ \gcd(n,p-1)=1}} e^{i2\pi s\frac{\tau^n}{p}} \\ &= \frac{1}{p} \sum_{2\leq u\leq z} \sum_{1\leq s\leq p-1} e^{\frac{-i2\pi us}{p}} \left( \sum_{\substack{p/z\leq n\leq p-1\\ \gcd(n,p-1)=1}} e^{i2\pi\frac{\tau^n}{p}} + O(p^{1/2+\delta}) \right), \end{aligned} \tag{25}$$

where $\delta > 0$ is a small real number. The application of Lemma 4.2 to the inner exponential sum on the second line of (25) removes the dependence on the variable $s \neq 0$ in exchange for a simpler exponential sum and an error term, which are both independent of the variable $s$. Now, use the exact evaluation $\sum_{1\leq s\leq p-1} e^{\frac{-i2\pi us}{p}} = -1$, take absolute value, and apply the triangle inequality:

$$\begin{aligned} |E_1(z)| &\leq \frac{1}{p} \sum_{2\leq u\leq z} \left| \sum_{1\leq s\leq p-1} e^{\frac{-i2\pi us}{p}} \right| \left| \sum_{\substack{p/z\leq n\leq p-1\\ \gcd(n,p-1)=1}} e^{i2\pi\frac{\tau^n}{p}} + O(p^{1/2+\delta}) \right| \\ &\ll \frac{1}{p} \sum_{2\leq u\leq z} |-1| \left( \left| \sum_{\substack{p/z\leq n\leq p-1\\ \gcd(n,p-1)=1}} e^{i2\pi\frac{\tau^n}{p}} \right| + |p^{1/2+\delta}| \right) \\ &\ll \frac{1}{p} \sum_{2\leq u\leq z} |-1||p^{1/2+\delta}| \\ &\ll \frac{z}{p^{1/2-\delta}}, \end{aligned} \tag{26}$$

where the exponential sum estimate

$$\sum_{\substack{p/z\leq n\leq p-1\\ \gcd(n,p-1)=1}} e^{i2\pi\frac{\tau^n}{p}} \ll p^{1/2+\delta} \tag{27}$$

follows from Lemma 4.1. □

# 9 Least primitive roots in finite fields

The determination of an upper bound for the smallest primitive root in the finite field $\mathbb{F}_p$ is based on a new characteristic function for primitive roots in finite field $\mathbb{F}_p$ introduced in Section 3. The proof is broken up into several lemmas proved in Sections 3–8.

Define the counting function

$$N_p(z) = \#\{u \leq z : \mathrm{ord}_p u = p-1\}. \tag{28}$$

**Proof of Theorem 1.1.** Let $p \geq p_0$ be a large prime number, and let $z = (\log p)^{1+\varepsilon}$, where $\varepsilon > 0$ is a small number. Suppose, by contradiction, that the least primitive root $u_0 > z$ and consider the sum of the characteristic function over the short interval $[2, z]$, i.e.,

$$N_p(z) = \sum_{2 \leq u \leq z} \Psi(u) = 0. \tag{29}$$

Replacing the characteristic function, Lemma 3.2, into the nonexistence equation (29) and expanding it yield

$$\begin{aligned} N_p(z) &= \sum_{2 \leq u \leq z} \Psi(u) \\ &= \sum_{2 \leq u \leq z} \left( \frac{1}{p} \sum_{\substack{1 \leq n \leq p-1 \\ \gcd(n,p-1)=1}} \sum_{0 \leq s \leq p-1} \psi((\tau^n - u)s) \right) \\ &= \sum_{2 \leq u \leq z} \frac{1}{p} \sum_{\substack{1 \leq n \leq p-1 \\ \gcd(n,p-1)=1}} 1 + \sum_{2 \leq u \leq z} \frac{1}{p} \sum_{\substack{1 \leq n \leq p-1 \\ \gcd(n,p-1)=1}} \sum_{1 \leq s \leq p-1} \psi((\tau^n - u)s) \\ &= M(z) \;+\; E(z). \end{aligned} \tag{30}$$

The main term $M(z)$, which is determined by a double finite sum over the trivial additive character $\psi(s) = 1$, is computed in Lemma 7.1, and the error term $E(z)$, which is determined by a triple finite sum over the nontrivial additive characters $\psi(s) = e^{i2\pi ks/p} \neq 1$, is computed in Lemma 8.1.

Substituting these evaluation and estimate yields

$$\begin{aligned} N_p(z) &= \sum_{2 \leq u \leq z} \Psi(u) \\ &= M(z) + E(z) \\ &= \frac{\varphi(p-1)}{p}((\log p)^{1+\varepsilon} + O(1)) + O((\log p)(\log\log p)). \end{aligned} \tag{31}$$

Applying Lemma 5.1 to the totient ratio $\varphi(p-1)/p$ show that the main term in (31) dominates the error term:

$$\begin{aligned} N_p(z) &\gg \frac{1}{\log\log p} \cdot (\log p)^{1+\varepsilon} + O((\log p)(\log\log p)) \\ &\gg \frac{(\log p)^{1+\varepsilon}}{(\log\log p)} \left( 1 + O\left( \frac{(\log\log p)^2}{(\log p)^{\varepsilon}} \right) \right) \\ &> 0, \end{aligned} \tag{32}$$

as $p \to \infty$. Clearly, this contradicts the hypothesis (29) for all sufficiently large prime numbers $p \geq p_0$. Therefore, there exists a small primitive root $u_0 \leq z = (\log p)^{1+\varepsilon}$, quod erat inveniendum. □

In synopsis, this result proves that the smallest primitive roots satisfy the conjectured upper bound $c(p)(\log p)(\log\log p)^2$, where $c(p) > 0$ is a constant. Furthermore, the mean value of the constant $c(p)$ over the set of primes seems to be bounded by the limit supremum:

$$\bar{c} = \lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x} c(p) \leq \limsup_{p \to \infty} \frac{\hat{g}(p)}{(\log p)(\log\log p)^2} = e^{\gamma} = 1.781072\ldots. \tag{33}$$

The limit supremum for prime primitive roots $\hat{g}$ is discussed in [4, Section 4]. Hence, on average, the smallest primitive root satisfies the mean explicit inequality

$$g(p) \leq \hat{g} < 2(\log p)(\log\log p)^2, \tag{34}$$

where $e^{\gamma} < 2$, and this follows from (33). The numerical data in the study by McGown et al. [5] shows that (34) is true for all primes up to $p = 6525032504501281$. For example, for the prime $p = 6525032504501281$, there is an abundance of primitive roots (both composite and prime) bounded by the mean explicit upper bound (34):

$$\begin{aligned} &417,431,467,473,479,499,521,527,556,571,581,602,617,691,695,769,801,817,821,823,829,834 \\ &\quad \le \; e^{\gamma}(\log p)(\log\log p)^2 \; = 838.1936 \qquad (35) \\ &\quad < \; 2(\log p)(\log\log p)^2 \; = 941.2234. \end{aligned}$$

The closest explicit result in this direction seems to be the claim that $g(p) < p^{5/8}$ for all prime $p > 10^{22}$, which is proved in [17, Corollary 1] using the standard characteristic function given in Lemma 3.1.

For large prime $p$, the determination of the specific constant $c(p) > 0$, which depends on $p$, and the mean value $\bar{c}$ of these constants seem to be difficult problems in analytic and algebraic number theory.

**Acknowledgement:** The author would also like to thank the anonymous referees for the excellent comments and suggestions to improve the quality of this manuscript.

**Funding information:** Author states no funding involved.

**Author contributions**: The author accepted responsibility for the entire content of this manuscript and approved its submission.

**Conflict of interest**: There is no conflict of interest of any form.

**Data availability statement**: Data sharing is not applicable to this article.

## References

[1] Burgess DA. On character sums and primitive roots. Proc London Math Soc. 1962;12(3):179–92.
[2] Shoup V. Searching for primitive roots in finite fields. Math Comp. 1992;58(197):369–80.
[3] Elliott PDTA. The distribution of primitive roots. Canadian J Math. 1969;21:822–41.
[4] Bach E. Comments on search procedures for primitive roots. Math Comp. 1997;66(220):1719–27.
[5] McGown K, Sorenson J. Computation of the least primitive root. 2022. Arxiv.org/abs/2206.14193.
[6] Shparlinski IE. On finding primitive roots in finite fields. Theoret Comput Sci. 1996;157:273–5.
[7] Grossman O. Finding primitive roots pseudo-deterministically. Preprint. 2015. eccc.weizmann.ac.il/report/2015/207.
[8] Shparlinski IE. On constructing primitive roots in finite fields with advice. IEEE Trans Inform Theory. 2018;64(11):7132–6.
[9] Miller GL. Riemannas hypothesis and tests for primality. J Comput System Sci. 1976;13(3):300–17.
[10] Bach E. Explicit bounds for primality testing and related problems. Math Comp. 1990;55(191):355–80.
[11] Bach E, Huelsbergen L. Statistical evidence for small generating sets. Math Comp. 1993;61:69–82.
[12] Agrawal M, Kayal N, Saxena N. PRIMES is in P. Ann Math. 2004;160(2):781–93.
[13] Lenstra H, Pomerance C. Primality testing with Gaussian periods. J Eur Math Soc. 2019;21(4):1229–69.
[14] Brier E, Ferradi H, Joye M, Naccache D. New number-theoretic cryptographic primitives. J Math Cryptol. 2020;14(1):224–35.
[15] Erdos P, Shapiro H. On the least primitive root of a prime number. Pacific J Math. 1957:7(1):861–5.
[16] Winterhof A. Character sums, primitive elements, and powers in finite fields. J Number Theory. 2001;91(1):153–63.
[17] McGown K, Trudgian T. Explicit upper bounds on the least primitive root. Proc Amer Math Soc. 2020;148(3):1049–61.
[18] Landau E. Vorlesungen uuuuber Zahlentheorie: Vol.: 2. Aus der analytischen und geometrischen Zahlentheorie. New York: Chelsea Publishing Co.; 1969, [1927].
[19] Lidl R, Niederreiter H. Finite fields. Second edition. Encyclopedia of Mathematics and its Applications. vol. 20. Cambridge: Cambridge University Press; 1997.
[20] Vinogradov IM. On the least primitive root. Doklady Akad Nauk SSSR. 1930;1:7–11.
[21] Erdos P. On the least primitive root of a prime number. Bull Amer Math Soc. 1945;51(11):131–2.
[22] Martin G. Uniform bounds for the least almost-prime primitive root. Mathematika. 1998;45:19–207.
[23] Carella N. Upper bound of the least quadratic nonresidues. 2021. doi: Arxiv.org/abs/2106.00544.
[24] Apostol Tom M. Introduction to analytic number theory. Undergraduate Texts in Mathematics. New York-Heidelberg: Springer-Verlag; 1976.
[25] Montgomery HL, Vaughan RC. Multiplicative number theory. I. Classical theory. Cambridge: Cambridge University Press; 2007.
[26] Dusart P. Estimates of some functions over primes, without R.H. Math Comp. 2016;85(298):875–88.
[27] Erdos P, Pomerance C. The normal number of prime factors of $\varphi(n)$. Rocky Mtn J Math. 1985;15:343–52.
[28] Davenport H. Multiplicative number theory. Graduate Texts in Mathematics. Vol. 74. New York: Springer-Verlag; 2000.