Simultaneous Primitive Root Values Of Polynomials Over Finite Fields

N. A. Carella

Abstract: Let $z \neq \pm 1, w^2$ be a fixed integer, and let $f(t) \neq g(t)^2$ be a fixed polynomial over the integers. It is shown that the subset of primes $p \geq 2$ such that $z$ and $f(z)$ is a pair of simultaneous primitive roots modulo $p$ has nonzero density in the set of primes. The same analysis generalizes to admissible $k$-tuple of polynomials $z, f_1(z), f_2(z), \ldots, f_k(z)$, such that $f_i(z) \neq g_i(z)^2$, and $k \ll \log p$ is a small integer.

Contents

| Section | Title |
|---------|-------|
| 1 | Introduction |
| 2 | Representation of the Characteristic Function |
| 3 | Evaluation Of The Main Term $M(x)$ |
| 4 | Evaluation Of The Main Term $M(f, p)$ |
| 5 | Estimate For The Error Terms $E_i(x)$ |
| 6 | Estimate For The Error Terms $E_i(f, p)$ |
| 7 | Proof Of Theorem 1.1 |
| 8 | Proof Of Theorem 1.2 |
| 9 | Some Numerical Examples |
| 10 | Problems |
| 10.1 | Primitive Root Algorithm Problems |
| 10.2 | Prime Primitive Roots Problems |
| 10.3 | Density and Distribution Problems |
| 10.4 | Average Order Problems |
| 10.5 | Value Set Problems |

April 6, 2022

AMS MSC2020: Primary 11A07, 11N13, Secondary 11N05, 11N37.

Keywords: Distribution of primes; Primitive root; Simultaneous primitive roots.
1 Introduction

The investigation of the density of the subset of primes $p$ such that an admissible integers $k$-tuple $z_1, z_2, \ldots, z_k$ are simultaneous primitive roots modulo $p$ has a well established conditional proof, see [3]. The investigation of the density of the subset of primes $p$ such that an admissible polynomials $k$-tuple $z, f_1(z), f_2(z), \ldots, f_{k-1}(z)$ are simultaneous primitive roots modulo $p$, which is a topic of current interest, is simply a variation of the result proved by Mathews.

Definition 1.1. A subset of polynomials $\{z, f_1(z), f_2(z), \ldots, f_{k-1}(z)\}$, such that $f_i(z) \neq g_i(z)^2$, is an admissible $k$-tuple if there exists a prime $p \geq 2$ that supports one or more $k$-tuple of simultaneous primitive roots modulo $p$. Specifically,

$$\text{ord}_p z = \text{ord}_p f_1(z) = \text{ord}_p f_2(z) = \cdots = \text{ord}_p f_{k-1}(z) = p - 1.$$  

The simplest case consists of a fixed pair of simultaneous primitive root values of polynomials $z \neq \pm 1, w^2$, and $f(z) \neq g(z)^2$. A related and conditional result for a fixed prime, and admissible quadratic polynomials is presented in [1, Theorem 3]. In addition, some numerical data for small primes that support a pair of simultaneous primitive roots is compiled, opus citatum. Here, unconditional proofs are given for pair of simultaneous primitive root values of admissible polynomials of any degree.

Define the primes counting function

$$\pi_f(x, z) = \# \{p \leq x : \text{ord}_p z = p - 1 \text{ and } \text{ord}_p(f(z)) = p - 1\}. \quad (1)$$

Theorem 1.1. Let $z \neq 1, w^2$ be a fixed integer, and let $f(t) \neq g(t)^2$ be a fixed polynomial over the integers. Then, the number of primes for which $z$ and $f(z)$ is a pair of simultaneous primitive roots has the asymptotic formula

$$\pi_f(x, z) = \delta_f(z) \text{li}(x) + O \left( \frac{x}{\log^b x} \right), \quad (2)$$

where $x \geq 1$ is a large number, $\delta_f(z) > 0$ is the density constant, and $b > 1$ is constant.

Define the primes counting function

$$N(f, p) = \# \{z < p : \text{ord}_p z = p - 1 \text{ and } \text{ord}_p(f(z)) = p - 1\}. \quad (3)$$

Theorem 1.2. Let $p \geq 2$ be a fixed large prime, and let $f(t) \neq g(t)^2$ be a fixed polynomial over the integers. Then, the number of integers $z < p$ for which $z$ and $f(z)$ is a pair of simultaneous primitive roots modulo $p$ has the asymptotic formula

$$N_f(p) = c(f, p) \left( \frac{\varphi(p-1)}{p-1} \right)^2 p + O \left( p^{1-2\varepsilon} \right), \quad (4)$$

where $c(f, p) > 0$ is the density constant, and $\varepsilon > 0$ is a small number.

The preliminary notation, definitions, background results are discussed in Section 2 to Section 6. The proof of Theorem 1.1 appears in Section 7, and the proof of Theorem 1.2 appears in Section 8.
2 Representation of the Characteristic Function

The result in Lemma 2.1 provides a divisor-free of the representation of the characteristic function of primitive elements in finite fields $\mathbb{F}_p$.

**Lemma 2.1.** Let $p \geq 2$ be a prime, and let $\tau$ be a primitive root mod $p$. If $u \in \mathbb{F}_p$ is a nonzero element, then

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

**Proof.** A complete proof appears in Lemma 2.1 in [2].

3 Evaluation Of The Main Term $M(x)$

The precise evaluation of the main term $M(x)$ occurring in the proof of Theorem 1.1 is recorded here. The symbol $li(x)$ denotes the logarithm integral.

**Lemma 3.1.** ([6, Lemma 4]) Let $x \geq 1$ be a large number, and let $k \geq 1$ be a fixed constant. Then,

$$
\sum_{p \leq x} \left( \frac{\varphi(p-1)}{p-1} \right)^k = a_k li(x) + O \left( \frac{x}{\log^b x} \right),
$$

where $p$ varies over the primes, and $a_k > 0$, and $b > 1$ are constants.

**Lemma 3.2.** If $x \geq 1$ is a large number, then,

$$
\sum_{p \leq x} \left( \frac{1}{p} \sum_{\gcd(k,p-1)=1} 1 \right) \left( \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 \right) = a_2 li(x) + O \left( \frac{x}{\log^b x} \right),
$$

where $a_2 > 0$, and $b > 1$ are constants.

**Proof.** Evaluate the inner sums and apply Lemma 3.1 to obtain

$$
M(x) = \sum_{p \leq x} \left( \frac{1}{p} \sum_{\gcd(k,p-1)=1} 1 \right) \left( \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 \right) = a_2 li(x) + O \left( \frac{x}{\log^b x} \right),
$$

as claimed.

The constant for $k = 1$, which is the average density of primitive roots modulo $p$, is given by $a_1 = \prod_{p \geq 2} \left( 1 - 1/p(p-1) \right) = 0.37395581361920228805 \ldots$, see [5]. The numerical value for $a_2$, which is for the average density of a pair of simultaneous primitive roots, is not available in the literature.
4 Evaluation Of The Main Term $M(f, p)$

The precise evaluation of the main term $M(f, p)$ occurring in the proof of Theorem 1.2 is recorded here.

Lemma 4.1. If $x \geq 1$ is a large number, then,

$$
\sum_{z \leq p} \left( \frac{1}{p} \sum_{\gcd(k, p-1)=1} 1 \right) \left( \frac{1}{p} \sum_{\gcd(n, p-1)=1} 1 \right) = \left( \frac{\varphi(p-1)}{p-1} \right)^2 p + O(1).
$$

Proof. Rearrange the triple sum as

$$
M(f, p) = \sum_{z \leq p} \left( \frac{1}{p} \sum_{\gcd(k, p-1)=1} 1 \right) \left( \frac{1}{p} \sum_{\gcd(n, p-1)=1} 1 \right)
= \sum_{z \leq p} \left( \frac{\varphi(p-1)}{p-1} \right)^2 \left( 1 - \frac{1}{p} \right)^2
= \left( \frac{\varphi(p-1)}{p-1} \right)^2 p + O(1),
$$

as claimed.

5 Estimate For The Error Terms $E_i(x)$

The upper bounds for the error terms $E_0(x)$, $E_1(x)$, and $E_2(x)$ in the proof of Theorem 1.1 are recorded here.

Lemma 5.1. If $x$ is a large number, then

$$
E_0(x) = \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{0 \leq b < p \atop \gcd(n, p-1)=1} e^{\frac{i \tau a (e^n - u)}{p}} \cdot \frac{1}{p} \sum_{0 \leq b < p \atop \gcd(m, p-1)=1} e^{\frac{i \tau b (e^m - v)}{p}} = 0.
$$

Proof. By hypothesis, $\text{ord}_p u \neq p - 1$, so the first finite sum

$$
\sum_{0 \leq a < p \atop \gcd(n, p-1)=1} e^{\frac{i \tau a (e^n - u)}{p}} = 0
$$

is a geometric series, which vanishes.

Lemma 5.2. If $x$ is a large number, then

$$
E_1(x) = \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{0 \leq b < p \atop \gcd(m, p-1)=1} e^{\frac{i \tau b (e^m - v)}{p}} \cdot \frac{1}{p} \sum_{0 \leq b < p \atop \gcd(m, p-1)=1} e^{\frac{i \tau b (e^m - v)}{p}} = 0.
$$
Proof. By hypothesis, \(\text{ord}_p v \neq p - 1\), so the second finite sum

\[
\sum_{\substack{0 \leq b < p \\text{gcd}(m, p-1) = 1}} e^{\frac{2\pi i (e^{vm} - v)}{p}} = 0
\]  

is a geometric series, which vanishes. ■

**Lemma 5.3.** If \(x\) is a large number, then

\[
E_2(x) = \sum_{x \leq p \leq 2x} \frac{1}{p} e^{\frac{2\pi i (x^n - u)}{p}} \sum_{0 < a < p \\text{gcd}(n, p-1) = 1} e^{\frac{2\pi i a}{p}} \sum_{0 < b < p \\text{gcd}(m, p-1) = 1} e^{\frac{2\pi i b}{p}} \ll x^{1-2\varepsilon}.
\]

Proof. To compute an upper bound, define the exponential sum

\[
T(u, p) = \sum_{0 < a < p \\text{gcd}(n, p-1) = 1} e^{\frac{2\pi i a}{p}} e^{\frac{2\pi i a(n^n - u)}{p}}.
\]

Now, apply Lemma 5.4 to each factor \(T(u, p)\) and \(T(v, p)\) to obtain the followings.

\[
E_2(x) = \sum_{x \leq p \leq 2x} \frac{1}{p} \cdot T(u, p) \cdot \frac{1}{p} \cdot T(v, p)
\]

\[
\ll \sum_{x \leq p \leq 2x} \left( \frac{1}{p} \cdot p^{1-\varepsilon} \right) \cdot \left( \frac{1}{p} \cdot p^{1-\varepsilon} \right).
\]

Take an upper bound, and apply the prime number theorem:

\[
E_2(x) \ll \frac{1}{x^{2\varepsilon}} \sum_{x \leq p \leq 2x} 1
\]

\[
\ll x^{1-2\varepsilon},
\]

as \(x \to \infty\). ■

**Lemma 5.4.** Given a small number \(\varepsilon > 0\). Let \(p\) be a large prime number, and let \(\tau\) be a primitive root modulo \(p\). Then,

\[
\sum_{0 < a < p \\text{gcd}(n, p-1) = 1} e^{\frac{2\pi i a(n^n - u)}{p}} \ll p^{1-\varepsilon}.
\]

Proof. A complete detailed proof is given in [2, Lemma 8.1]. ■

### 6 Estimate For The Error Terms \(E_i(f, p)\)

The upper bounds for the error terms \(E_0(f, p), E_1(f, p),\) and \(E_2(f, p)\) in the proof of Theorem 1.2 are recorded here.
Lemma 6.1. If \( x \) is a large number, then
\[
E_0(f, p) = \sum_{z \leq p} \frac{1}{p} \sum_{0 \leq a < p \atop \gcd(n, p-1) = 1} e^{\frac{i2\pi a(n-u)}{p}} \cdot \frac{1}{p} \sum_{0 \leq b < p \atop \gcd(m, p-1) = 1} e^{\frac{i2\pi b(m-v)}{p}} = 0.
\]

Proof. By hypothesis, \( \text{ord}_p u \neq p-1 \), so the first finite sum
\[
\sum_{0 \leq a < p \atop \gcd(n, p-1) = 1} e^{\frac{i2\pi a(n-u)}{p}} = 0
\]
is a geometric series, which vanishes. \( \blacksquare \)

Lemma 6.2. If \( x \) is a large number, then
\[
E_1(f, p) = \sum_{z \leq p} \frac{1}{p} \sum_{0 \leq b < p \atop \gcd(m, p-1) = 1} e^{\frac{i2\pi b(m-v)}{p}} \cdot \frac{1}{p} \sum_{0 \leq a < p \atop \gcd(n, p-1) = 1} e^{\frac{i2\pi a(n-u)}{p}} = 0.
\]

Proof. By hypothesis, \( \text{ord}_p v \neq p-1 \), so the second finite sum
\[
\sum_{0 \leq b < p \atop \gcd(m, p-1) = 1} e^{\frac{i2\pi b(m-v)}{p}} = 0
\]
is a geometric series, which vanishes. \( \blacksquare \)

Lemma 6.3. If \( x \) is a large number, then
\[
E_2(f, p) = \sum_{z \leq p} \frac{1}{p} \sum_{0 \leq a < p \atop \gcd(n, p-1) = 1} e^{\frac{i2\pi a(n-u)}{p}} \cdot \frac{1}{p} \sum_{0 \leq b < p \atop \gcd(m, p-1) = 1} e^{\frac{i2\pi b(m-v)}{p}} \ll p^{1-2\varepsilon}.
\]

Proof. To compute an upper bound, define the exponential sum
\[
T(u, p) = \sum_{0 \leq a < p \atop \gcd(n, p-1) = 1} e^{\frac{i2\pi a(n-u)}{p}}.
\]
(15)

Now, apply Lemma 5.4 to each factor \( T(u, p) \) and \( T(v, p) \) to obtain the followings.
\[
E_2(f, p) = \sum_{z \leq p} \left( \frac{1}{p} \cdot T(u, p) \right) \cdot \left( \frac{1}{p} \cdot T(v, p) \right) \ll \sum_{z \leq p} \left( \frac{1}{p} \cdot p^{1-\varepsilon} \right) \cdot \left( \frac{1}{p} \cdot p^{1-\varepsilon} \right).
\]

Take an upper bound, and apply the prime number theorem:
\[
E_2(f, p) \ll \frac{1}{p^{2\varepsilon}} \sum_{z \leq p} 1 \ll p^{1-2\varepsilon},
\]
as \( p \to \infty \). \( \blacksquare \)
7 Proof Of Theorem 1.1

Given a fixed integer \( z \neq \pm 1, w^2 \), and a fixed polynomial \( f(t) \neq g(t)^2 \), define the primes counting functions

\[
\pi(x) = \#\{ p \leq x : p \text{ is prime} \},
\]

and

\[
\pi_f(x, z) = \# \{ p \leq x : \text{ord}_p z = p - 1 \text{ and ord}_p(f(z)) = p - 1 \}.
\]

The density of the subset of primes

\[
\mathcal{D} = \{ p \in \mathbb{P} : \text{ord}_p z = p - 1 \text{ and ord}_p(f(z)) = p - 1 \},
\]

is defined by the limit

\[
\delta_f(z) = \lim_{x \to \infty} \frac{\pi_f(x, z)}{\pi(x)} = c_f(z)a_2,
\]

where \( c_f(z) \geq 0 \) is a correction factor (rational number), and \( a_2 > 0 \) is defined in Lemma 3.1. The proof below shows that for any given fixed pair \( z \neq \pm 1, w^2 \) and \( f(t) \neq g(t)^2 \), the subset \( \mathcal{D} \) of primes has nonzero density in the set of primes \( \mathbb{P} = \{2, 3, 5, 7, \ldots \} \).

Proof. (Theorem 1.1). Let \( x \geq x_0 \) be a large number, and let \( p \geq x \) be a prime. The characteristic function of a pair of simultaneous primitive roots \( z \) and \( f(z) \) in \( \mathbb{F}_p \) has the exact formula

\[
\Psi(z)\Psi(f(z)),
\]

where \( \Psi(z) \) is characteristic function of primitive root in \( \mathbb{F}_p \). Now suppose that there are no primes \( p \geq x \) that support any pair of simultaneous primitive roots \( z \) and \( f(z) \). Summing of the exact formula (22) over the short interval \([x, 2x]\) returns the nonexistence equation

\[
0 = \sum_{x \leq p \leq 2x} \Psi(z)\Psi(f(z)).
\]

Replacing the characteristic function, Lemma 2.1, and expanding the nonexistence equation (23) yield

\[
0 = \sum_{x \leq p \leq 2x} \Psi(z)\Psi(f(z))
\]

\[
= \sum_{x \leq p \leq 2x} \left( \frac{1}{p} \sum_{\gcd(k, p-1) = 1} \sum_{0 \leq a \leq p-1} e^{i2\pi(\tau^k-z)a/p} \right)
\]

\[
\times \left( \frac{1}{p} \sum_{\gcd(n, p-1) = 1} \sum_{0 \leq b \leq p-1} e^{i2\pi(\tau^n-f(z))b/p} \right)
\]

\[
= M(x) + E_0(x) + E_1(x) + E_2(x).
\]
1. The main term $M(x)$ is determined by a finite sum over the trivial additive characters pair \( \psi_a(t) = e^{i2\pi at/p} = 1 \) at \( a = 0 \), and \( \psi_b(t) = e^{i2\pi bt/p} = 1 \) at \( b = 0 \). This is computed in Lemma 3.2.

2. The error term $E_0(x)$ is determined by a finite sum over the nontrivial additive characters pair \( \psi_a(t) = e^{i2\pi at/p} = 1 \) at \( a = 0 \), and \( \psi_b(t) = e^{i2\pi bt/p} \neq 1 \) at \( b \neq 0 \). This is estimated in Lemma 5.1.

3. The error term $E_1(x)$ is determined by a finite sum over the nontrivial additive characters pair \( \psi_a(t) = e^{i2\pi at/p} \neq 1 \) at \( a \neq 0 \), and \( \psi_b(t) = e^{i2\pi bt/p} = 1 \) at \( b = 0 \). This is computed in Lemma 5.2.

4. The error term $E_2(x)$ is determined by a finite sum over the nontrivial additive characters pair \( \psi_a(t) = e^{i2\pi at/p} \neq 1 \) at \( a \neq 0 \), and \( \psi_b(t) = e^{i2\pi bt/p} \neq 1 \) at \( b \neq 0 \). This is computed in Lemma 5.3.

Applying Lemma 3.2 to the main term, and Lemmas 5.1 to 5.3 to the error terms yield

\[
\sum_{x \leq p \leq 2x} \Psi(z)\Psi(f(z)) = M(x) + E_0(x) + E_1(x) + E_2(x)
\]

\[
= \delta_f(z) (\text{li}(2x) - \text{li}(x)) + O\left(\frac{x}{\log^b x}\right) + O\left(x^{1-\varepsilon}\right)
\]

\[
= \delta_f(z) (\text{li}(2x) - \text{li}(x)) + O\left(\frac{x}{\log^b x}\right),
\]

where \( \delta_f(z) \geq 0 \) is defined in (20).

Since the density \( \delta_f(z) > 0 \) for a pair \( z \neq \pm 1, w^2 \), and \( f(z) \neq g(z)^2 \), see [3, Theorem 13.1], and the difference of logarithm integrals

\[
\text{li}(2x) - \text{li}(x) \gg \frac{x}{\log x} > 0
\]

for large \( x \gg 1 \), the expression

\[
\sum_{x \leq p \leq 2x} \Psi(z)\Psi(f(z)) = \delta_f(z) (\text{li}(2x) - \text{li}(x)) + O\left(\frac{x}{\log^b x}\right)
\]

\[
\gg \frac{x}{\log x} > 0,
\]

is false for all sufficiently large numbers \( x \gg 1 \), and contradicts the hypothesis (23). Therefore, the short interval \( [x, 2x] \) contains primes \( p \geq x \) such that \( z \neq \pm 1, w^2 \), and \( f(z) \neq g(z)^2 \) are simultaneous primitive roots modulo \( p \).
8 Proof of Theorem 1.2

As the main requirement for a primitive root value over the integers, $z \neq \pm 1, w^2$, the main requirement for a primitive root valued polynomial is $f(t) \neq g(t)^2$, see Example 9.3 for numerical evidence.

For a fixed prime $p \geq 2$, and a fixed polynomial $f(t) \neq g(t)^2$, the counting function for the pair of simultaneous primitive roots $z > 1$ and $f(z) > 1$ is defined by

$$S_p = \{z < p : \text{ord}_p z = p - 1 \text{ and ord}_p(f(z)) = p - 1\}, \quad (28)$$

and the average density over the set of primes $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ is defined by the limit

$$c(f, p) = \lim_{p \to \infty} \frac{S_p}{p}. \quad (29)$$

Proof. (Theorem 1.2). Let $p \geq 2$ be a prime, and let $z < p$. The characteristic function of a pair of simultaneous primitive roots $z$ and $f(z)$ in $\mathbb{F}_p$ has the exact formula

$$\Psi(z)\Psi(f(z)), \quad (30)$$

where $\Psi(z)$ is characteristic function of primitive root in $\mathbb{F}_p$. Now suppose that a large fixed prime $p \geq 2$ does not support any pair of simultaneous primitive roots $z$ and $f(z)$ modulo $p$. Summing of the exact formula (30) over the elements $z < p$ returns the nonexistence equation

$$0 = \sum_{z<p} \Psi(z)\Psi(f(z)). \quad (31)$$

Replacing the characteristic function, Lemma 2.1, and expanding the nonexistence equation (31) yield

$$0 = \sum_{z<p} \Psi(z)\Psi(f(z))$$

$$= \sum_{z<p} \left( \frac{1}{p} \sum_{\gcd(k, p-1)=1} \sum_{0 \leq a \leq p-1} e^{i2\pi(\tau^k z)a/p} \right)$$

$$\times \left( \frac{1}{p} \sum_{\gcd(n, p-1)=1} \sum_{0 \leq b \leq p-1} e^{i2\pi(\tau^n f(z))b/p} \right)$$

$$= M(f, p) + E_0(f, p) + E_1(f, p) + E_2(f, p).$$

1. The main term $M(f, p)$ is determined by a finite sum over the trivial additive characters pair $\psi_a(t) = e^{i2\pi at/p} = 1$ at $a = 0$, and $\psi_b(t) = e^{i2\pi bt/p} = 1$ at $b = 0$. This is computed in Lemma 4.1.

2. The error term $E_0(f, p)$ is determined by a finite sum over the nontrivial additive characters pair $\psi_a(t) = e^{i2\pi at/p} = 1$ at $a = 0$, and $\psi_b(t) = e^{i2\pi bt/p} \neq 1$ at $b \neq 0$. This is estimated in Lemma 6.1.
3. The error term $E_1(f, p)$ is determined by a finite sum over the nontrivial additive characters pair $\psi_a(t) = e^{i2\pi at/p} \neq 1$ at $a \neq 0$, and $\psi_b(t) = e^{i2\pi bt/p} = 1$ at $b = 0$. This is computed in Lemma 6.2.

4. The error term $E_2(f, p)$ is determined by a finite sum over the nontrivial additive characters pair $\psi_a(t) = e^{i2\pi at/p} \neq 1$ at $a \neq 0$, and $\psi_b(t) = e^{i2\pi bt/p} \neq 1$ at $b \neq 0$. This is computed in Lemma 6.3.

Applying Lemma 4.1 to the main term, and Lemmas 6.1 to 6.3 to the error terms yield

$$\sum_{z<p} \Psi(z)\Psi(f(z)) = M(f, p) + E_0(f, p) + E_1(f, p) + E_2(f, p)$$

$$= c(f, p) \left( \frac{\varphi(p-1)}{p-1} \right)^2 p + O(p^{1-2\varepsilon}),$$

where $c(f, z) \geq 0$ is defined in (29).

Since there are pairs $z \neq \pm 1, w^2$, and $f(z) \neq g(z)^2$ of simultaneous primitive roots, see [3, Theorem 13.1], the density $c(f, z) > 0$. Moreover, the term

$$\left( \frac{\varphi(p-1)}{p-1} \right)^2 \gg \frac{1}{(\log \log p)^2} > 0$$

for large $p \gg 1$. Consequently, the expression

$$\sum_{z<p} \Psi(z)\Psi(f(z)) = c(f, p) \left( \frac{\varphi(p-1)}{p-1} \right)^2 p + O(p^{1-2\varepsilon}),$$

$$\gg \frac{p}{(\log \log p)^2} > 0,$$

is false for all sufficiently large primes $p \gg 1$, and contradicts the hypothesis (31). Therefore, the finite field $\mathbb{F}_p$ contains a small subset $\mathcal{S}_p$ of elements $z \in \mathbb{F}_p$ such that $z > 1$, and $f(z) > 1$ are simultaneous primitive roots for all sufficiently large primes $p \geq 2$. ■

9 Some Numerical Examples

A few small cases were computed to determine the accuracy of Theorem 1.2, and to establish some notation. This simple experiment shows that irreducible polynomials seem to generate simpler spectra (distribution patterns) than the reducible polynomials, compare Figure 2 and Figure 4.
**Example 9.1.** The preliminary statistics for the finite field $\mathbb{F}_{97}$ and the polynomial $f(t) = t^2 + 1$ are listed here.

1. $\varphi(p - 1) = 32$, the total number of primitive roots, listed in Table 1.

2. \[ \left( \frac{\varphi(p - 1)}{p - 1} \right)^2 p = \frac{24832}{2401} \approx 10.34, \] an estimate of the asymptotic (main term) for total number of pairs of simultaneous primitive roots $z, f(z)$, the actual number is 4, see Table 1.

Table 1 lists all the primitive roots $z$ modulo $p = 97$ and the corresponding simultaneous pairs, if a pair $z$ and $f(z)$ exists, and Figure 1 displays the spectrum of simultaneous pairs of primitive roots.

| $z$ | $f(z) = z^2 + 1$ | $z$ | $f(z) = z^2 + 1$ | $z$ | $f(z) = z^2 + 1$ | $z$ | $f(z) = z^2 + 1$ |
|-----|-----------------|-----|-----------------|-----|-----------------|-----|-----------------|
| 5   | 26              | 29  | 0              | 60  | 0              | 90  | 0              |
| 7   | 0               | 37  | 0              | 68  | 0              | 92  | 26             |
| 10  | 0               | 38  | 87             | 71  | 0              | 13  | 39             |
| 13  | 0               | 39  | 0              | 74  | 0              | 14  | 40             |
| 14  | 0               | 41  | 0              | 76  | 0              | 15  | 41             |
| 15  | 0               | 41  | 0              | 80  | 0              | 17  | 56             |
| 17  | 0               | 56  | 0              | 82  | 0              | 21  | 57             |
| 21  | 0               | 57  | 0              | 83  | 0              | 23  | 58             |
| 23  | 0               | 58  | 87             | 87  | 0              | 26  | 59             |

Figure 1: The spectrum of the pair $(z, f(z))$ of simultaneous primitive roots in $\mathbb{F}_{97}$
Example 9.2. The preliminary statistics for the finite field \( \mathbb{F}_{101} \) and the polynomial \( f(t) = t^2 + 1 \) are listed here.

1. \( \varphi(p - 1) = 40 \), the total number of primitive roots, listed in Table 2.

2. \( \left( \frac{\varphi(p - 1)}{p - 1} \right)^2 p = \frac{404}{25} \approx 16.16 \), an estimate of the asymptotic (main term) for the total number of pairs of simultaneous primitive roots \( z, f(z) \), the actual number is 12, see Table 2.

Table 2 lists all the primitive roots \( z \) modulo \( p = 101 \) and the corresponding simultaneous pairs, if a pair \( z \) and \( f(z) \) exists, and Figure 2 displays the spectrum of simultaneous pairs of primitive roots.

| \( z \) | \( f(z) = z^2 + 1 \) | \( z \) | \( f(z) = z^2 + 1 \) | \( z \) | \( f(z) = z^2 + 1 \) |
|---|---|---|---|---|---|
| 2 | 0 | 28 | 0 | 51 | 0 | 74 | 0 |
| 3 | 0 | 29 | 34 | 53 | 83 | 75 | 0 |
| 7 | 50 | 34 | 46 | 55 | 0 | 83 | 0 |
| 8 | 0 | 35 | 0 | 59 | 48 | 86 | 0 |
| 11 | 0 | 38 | 0 | 61 | 86 | 89 | 0 |
| 12 | 0 | 40 | 86 | 63 | 0 | 90 | 0 |
| 15 | 0 | 42 | 48 | 66 | 0 | 93 | 0 |
| 18 | 0 | 46 | 0 | 67 | 46 | 94 | 50 |
| 26 | 0 | 48 | 83 | 72 | 34 | 98 | 0 |
| 27 | 0 | 50 | 0 | 73 | 0 | 99 | 0 |

Figure 2: The spectrum of the pair \( (z, f(z)) \) of simultaneous primitive roots in \( \mathbb{F}_{101} \)
Example 9.3. The preliminary statistics for the finite field $\mathbb{F}_{127}$ and the polynomial $f(t) = (t + 2)(t + 1)^2$ are listed here.

1. $\varphi(p - 1) = 36$, the total number of primitive roots, listed in Table 3.

2. $\left( \frac{\varphi(p - 1)}{p - 1} \right)^2 p = \frac{508}{49} \approx 10.37$, an estimate of the asymptotic (main term) for the total number of pairs of simultaneous primitive roots $z, f(z)$, the actual number is 9, see Table 3.

Table 3 lists all the primitive roots $z$ modulo $p = 127$ and the corresponding simultaneous pairs, if a pair $z$ and $f(z) = (z + 2)(z + 1)^2$ exists, and Figure 3 displays the spectrum of simultaneous pairs of primitive roots.

| $z$ | $f(z) = (z + 2)(z + 1)^2$ | $z$ | $f(z)$ | $z$ | $f(z)$ |
|-----|--------------------------|-----|--------|-----|--------|
| 3   | 0                        | 46  | 114    | 83  | 0      | 109  | 0   |
| 6   | 0                        | 48  | 106    | 86  | 0      | 112  | 0   |
| 7   | 0                        | 53  | 106    | 86  | 0      | 112  | 0   |
| 12  | 0                        | 55  | 106    | 91  | 6      | 114  | 67  |
| 14  | 0                        | 56  | 106    | 92  | 0      | 116  | 116 |
| 23  | 0                        | 57  | 106    | 93  | 0      | 118  | 0   |
| 29  | 0                        | 58  | 106    | 96  | 0      |      |     |
| 39  | 0                        | 65  | 97     | 0   | 114    | 0    |     |
| 43  | 0                        | 67  | 101    | 96  | 0      |      |     |
| 45  | 0                        | 78  | 106    | 101 | 0      |      |     |

Figure 3: The spectrum of the pair $(z, f(z))$ of simultaneous primitive roots in $\mathbb{F}_{127}$.
Example 9.4. The preliminary statistics for the finite field $\mathbb{F}_{89}$ and the polynomial $f(t) = (t + 2)(t + 1)^2$ are listed here.

1. $\varphi(p - 1) = 40$, the total number of primitive roots, listed in Table 4.

2. $\left( \frac{\varphi(p - 1)}{p - 1} \right)^2 p = \frac{2225}{121} \approx 18.39$, an estimate of the asymptotic (main term) for the total number of pairs of simultaneous primitive roots $z, f(z)$, the actual number is 18, see Table 4.

Table 4 lists all the primitive roots $z$ modulo $p = 89$ and the corresponding simultaneous pairs, if a pair $z$ and $f(z) = (z + 2)(z + 1)^2$ exists, and Figure 4 displays the spectrum of simultaneous pairs of primitive roots.

| $z$ | $f(z) = (z + 2)(z + 1)^2$ | $z$ | $f(z)$ | $z$ | $f(z)$ |
|-----|---------------------------|-----|--------|-----|--------|
| 3   | 0                         | 27  | 41     | 46  | 33     | 63  | 41 |
| 6   | 0                         | 28  | 43     | 48  | 0      | 65  | 0  |
| 7   | 0                         | 29  | 43     | 51  | 0      | 66  | 0  |
| 13  | 3                         | 30  | 0      | 54  | 33     | 70  | 0  |
| 14  | 0                         | 31  | 61     | 56  | 29     | 74  | 33 |
| 15  | 0                         | 33  | 54     | 58  | 66     | 75  | 19 |
| 19  | 0                         | 35  | 70     | 59  | 0      | 76  | 0  |
| 23  | 0                         | 38  | 0      | 60  | 14     | 82  | 0  |
| 24  | 0                         | 41  | 24     | 61  | 3      | 83  | 0  |
| 26  | 31                        | 43  | 0      | 62  | 0      | 86  | 0  |

Figure 4: The spectrum of the pair $(z, f(z))$ of simultaneous primitive roots in $\mathbb{F}_{89}$
10 Problems

10.1 Primitive Root Algorithm Problems

Exercise 10.1. Develop a divisor-free primitive root test. The standard primitive root test is totally dependent on the divisors of $p - 1$.

10.2 Prime Primitive Roots Problems

Exercise 10.2. Let $p \geq 2$ be a large prime. Estimate the number $U(p) \geq 1$ of prime primitive roots in the subset

$$U(p) = \{q < p : q \text{ is prime and } \text{ord}_p q = p - 1\}.$$ 

Prove or disprove that $U(p) \approx \pi(p)$, where $\pi(x) = \#\{p \leq x : p \text{ is prime}\}$ is the usual prime counting function.

10.3 Density and Distribution Problems

Exercise 10.3. Let $f(t) = x^2 + 1$. Compute the exact and numerical approximation for the density constant $c_f > 0$ appearing in Theorem 1.1, see [3], [4], etc., for some related theoretical background.

Exercise 10.4. Let $p$ be a large prime, and let $f(t) = x^2 + 1$. The distribution of simultaneous pairs of primitive roots $z$ and $f(z)$ seems to be symmetric around $(p - 1)/2$, see Examples 9.1 and 9.2. Determine or estimate the distribution of simultaneous pairs of primitive roots $z$ and $f(z)$ as $p \to \infty$.

10.4 Average Order Problems

Exercise 10.5. Let $p \geq 2$ be a large prime, let $x \leq p$, and let $T \subset \mathbb{F}_p$ be the subset of primitive roots modulo $p$. If $d(n) = \sum_{d|n} 1$ is the divisors function, compute or estimate the following restricted average orders.

a) $\sum_{n \in T} d(n)$, the complete finite sum over the subset of primitive roots.

b) $\sum_{n \leq x, n \in T} d(n)$, the incomplete finite sum over the subset of primitive roots.

The complete sum is expected to be simpler than the incomplete sum.

Exercise 10.6. Let $p \geq 2$ be a large prime, let $x \leq p$, and let $T \subset \mathbb{F}_p$ be the subset of primitive roots modulo $p$. If $\sigma(n) = \sum_{d|n} d$ is the sum of divisors function, compute or estimate the following restricted average orders.

a) $\sum_{n \in T} \sigma(n)$, the complete finite sum over the subset of primitive roots.
b) $\sum_{n \leq x, n \in \mathcal{T}} \sigma(n)$, the incomplete finite sum over the subset of primitive roots.

The complete sum is expected to be simpler than the incomplete sum.

**Exercise 10.7.** Let $p \geq 2$ be a large prime, let $x \leq p$, and let $\mathcal{T} \subset \mathbb{F}_p$ be the subset of primitive roots modulo $p$. If $\varphi(n) = n \sum_{d|n} \mu(d)/d$ is the totient function, compute or estimate the following restricted average orders.

a) $\sum_{n \in \mathcal{T}} \varphi(n)$, the complete finite sum over the subset of primitive roots.

b) $\sum_{n \leq x, n \in \mathcal{T}} \varphi(n)$, the incomplete finite sum over the subset of primitive roots.

The complete sum is expected to be simpler than the incomplete sum.

## 10.5 Value Set Problems

**Exercise 10.8.** Let $p \geq 2$ be a large prime, and let $\mathcal{T} \subset \mathbb{F}_p$ be the subset of primitive roots modulo $p$. Estimate the number of primitive roots

$$V_d(p) = \#V_d(p)$$

in the value set

$$V_d(p) = \{\tau : d(\tau) \text{ is a primitive root}\}.$$

**Exercise 10.9.** Let $p \geq 2$ be a large prime, and let $\mathcal{T} \subset \mathbb{F}_p$ be the subset of primitive roots modulo $p$. Estimate the number of primitive roots

$$V_\sigma(p) = \#V_\sigma(p)$$

in the value set

$$V_\sigma(p) = \{\tau : \sigma(\tau) \text{ is a primitive root}\}.$$

**Exercise 10.10.** Let $p \geq 2$ be a large prime, and let $\mathcal{T} \subset \mathbb{F}_p$ be the subset of primitive roots modulo $p$. Estimate the number of primitive roots

$$V_\varphi(p) = \#V_\varphi(p)$$

in the value set

$$V_\varphi(p) = \{\tau : \varphi(\tau) \text{ is a primitive root}\}.$$
References

[1] Andrew R. Booker, Stephen D. Cohen, Nicole Sutherland, Tim Trudgian. *Primitive values of quadratic polynomials in a finite field*. http://arxiv.org/abs/1803.01435.

[2] Carella, N. *Simultaneous Elements Of Prescribed Multiplicative Orders*. http://arxiv.org/abs/arxiv:2103.04822

[3] Matthews, K. R. *A generalisation of Artin’s conjecture for primitive roots*. Acta Arith. 29 (1976), no. 2, 113-146.

[4] Pappalardi, Francesco. *On the r-Rank Artin Conjecture*. Math. Comp. Volume 66, Number 218, April 1997, Pages 853-868.

[5] Stephens, P. J. *An average result for Artin conjecture*. Mathematika 16, (1969), 178-188. http://doi.org/10.1112/S0025579300008159.

[6] Vaughan, R. C. *Some applications of Montgomery’s sieve*. J. Number Theory 5 (1973), 64-79. MR0124305.