Remarks on the distribution of the primitive roots of a prime

Shane Chern

Abstract. Let $\mathbb{F}_p$ be a finite field of size $p$ where $p$ is an odd prime. Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of positive degree $k$ that is not a $d$-th power in $\mathbb{F}_p[x]$ for all $d \mid p - 1$. Furthermore, we require that $f(x)$ and $x$ are coprime. The main purpose of this paper is to give an estimate of the number of pairs $(\xi, \xi^\alpha f(\xi))$ such that both $\xi$ and $\xi^\alpha f(\xi)$ are primitive roots of $p$ where $\alpha$ is a given integer. This answers a question of Han and Zhang.

Keywords. Primitive root, character sum, Weil bound.

2010MSC. Primary 11A07; Secondary 11L40.

1. Introduction

Let $a$ and $q$ be relatively prime integers, with $q \geq 1$. We know from the Euler-Fermat theorem that $a^{\phi(q)} \equiv 1 \pmod{q}$, where $\phi(q)$ is the Euler totient function. We say an integer $f$ is the exponent of $a$ modulo $q$ if $f$ is smallest positive integer such that $a^f \equiv 1 \pmod{q}$. If $f = \phi(q)$, then $a$ is called a primitive root of $q$. If $q$ has a primitive root $a$, then the group of the reduced residue classes mod $q$ is the cyclic group generated by the residue class $\bar{a}$. It is well-known that primitive roots exist only for the following moduli:

$$q = 1, 2, 4, p^\alpha, \text{ and } 2p^\alpha,$$

where $p$ is an odd prime and $\alpha \geq 1$. The reader may refer to Chapter 10 of T. M. Apostol’s book [1] for detailed contents.

There has been a long history studying the distribution of the primitive roots of a prime. In a recent paper, D. Han and W. Zhang [3] considered the number of pairs $(\xi, m\xi^k + n\xi)$ such that both $\xi$ and $m\xi^k + n\xi$ are primitive roots of an odd prime $p$ where $m$, $n$ and $k$ are given integers with $k \neq 1$ and $(mn, p) = 1$. The reader may also find some descriptions of other interesting problems on primitive roots such as the Golomb’s conjecture in [3] and references therein. After presenting their main results, Han and Zhang proposed the following

Question 1.1. Let $\mathbb{F}_p$ be a finite field of size $p$ and $f(x)$ be an irreducible polynomial in $\mathbb{F}_p[x]$. Whether there exists a primitive element $\xi \in \mathbb{F}_p$ such that $f(\xi)$ is also a primitive element in $\mathbb{F}_p$?

In this paper, we let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of positive degree $k$ that is not a $d$-th power in $\mathbb{F}_p[x]$ for all $d \mid p - 1$. Furthermore, we require that $f(x)$ and $x$ are coprime. Let $\alpha$ be a given integer, we denote by $N(\alpha, f; p)$ the number of pairs $(\xi, \xi^\alpha f(\xi))$ such that both $\xi$ and $\xi^\alpha f(\xi)$ are primitive roots of $p$. Our result is
Theorem 1.1. It holds that
\[ N(\alpha, f; p) = (p - 1 - R(f)) \left( \frac{\phi(p - 1)}{p - 1} \right)^2 + \theta k 4^{\omega(p-1)} \sqrt{p} \left( \frac{\phi(p - 1)}{p - 1} \right)^2, \]  
(1.1)
where \(|\theta| < 1\), \(\omega(n)\) denotes the number of distinct prime divisors of \(n\), and \(R(f)\) denotes the number of distinct zeros of \(f(x)\) in \(\mathbb{F}_p\).

Now if we take \(\alpha = 0\) and \(f(x) = x + 1\), then we get the famous result on consecutive primitive roots obtained by J. Johnsen [4] and M. Szalay [5]. If we take \(\alpha = 1\) and \(f(x) = m x^{k-1} + n\) if \(k > 1\), \(\alpha = k\) and \(f(x) = n x^{1-k} + m\) if \(k < 1\), then we get Han and Zhang’s result immediately.

Remark 1.1. We should mention that there is a minor mistake in Han and Zhang’s result. In fact, they forgot to consider the zeros of \(f(x)\) in \(\mathbb{F}_p\). For example, if we choose \(f(x) = x^{-1} + x = x^{-1}(x^2 + 1)\), then there are \(1 + (-1|p)\) distinct zeros of \(x^2 + 1\) in \(\mathbb{F}_p\) where \((*|p)\) is the Legendre symbol. In this sense, the main term of \(N(-1, x^2 + 1; p)\) (or their \(N(-1, 1, 1, p)\)) should be
\[ (p - 2 - (-1|p)) \left( \frac{\phi(p - 1)}{p - 1} \right)^2 \]
while not \(\phi^2(p - 1)/(p - 1)\).

2. Preliminary lemmas
We first introduce the indicator function of primitive roots.

Lemma 2.1 (L. Carlitz [2, Lemma 2]). We have
\[ \frac{\phi(p - 1)}{p - 1} \sum_{d|p-1} \mu(d) \phi(d) \sum_{\chi \equiv d \mod p} \chi(n) = \begin{cases} 1 & \text{if } n \text{ is a primitive root of } p, \\ 0 & \text{otherwise}. \end{cases} \]  
(2.1)
Here \(\mu\) is the Möbius function, and \(\text{ord}_\chi\) denotes the order of a Dirichlet character \(\chi \mod p\), that is, the smallest positive integer \(f\) such that \(\chi^f = \chi_0\), the principal character modulo \(p\).

The following famous Weil bound for character sums plays an important role in our proof.

Lemma 2.2 (A. Weil [7]). Let \(\chi\) be a non-principal Dirichlet character modulo \(p\) with order \(d\). Suppose \(f(x) \in \mathbb{F}_p[x]\) is a polynomial of positive degree \(k\) that is not a \(d\)-th power in \(\mathbb{F}_p[x]\). Then we have
\[ \left| \sum_{n=1}^{p-1} \chi(f(n)) \right| \leq (k - 1)\sqrt{p}. \]
(2.2)

We also need the less-known extension of Weil bound obtained by D. Wan.
Lemma 2.3 (D. Wan [6, Corollary 2.3]). Let $\chi_1, \chi_2, \ldots, \chi_m$ be non-principal Dirichlet characters modulo $p$ with orders $d_1, d_2, \ldots, d_m$, respectively. Suppose $f_1(x), f_2(x), \ldots, f_m(x) \in \mathbb{F}_p[x]$ are pairwise prime polynomials of positive degrees $k_1, k_2, \ldots, k_m$. Suppose also that $f_i(x)$ is not a $d_i$-th power in $\mathbb{F}_p[x]$ for all $i = 1, 2, \ldots, m$. Then we have

$$\left| \sum_{n=1}^{p-1} \chi_1(f_1(n))\chi_2(f_2(n)) \cdots \chi_m(f_m(n)) \right| \leq \left( \sum_{i=1}^m k_i - 1 \right) \sqrt{p}. \quad (2.3)$$

From Lemmas 2.2 and 2.3, we have

Lemma 2.4. Let $\chi_1$ be a Dirichlet character modulo $p$, and $\chi_2$ be a non-principal Dirichlet character modulo $p$ with order $d$. Suppose $f(x) \in \mathbb{F}_p[x]$ is a polynomial of positive degree $k$ that is not a $d$-th power in $\mathbb{F}_p[x]$. We also require that $f(x)$ and $x$ are coprime. Furthermore, let $\alpha$ be a given integer. Then we have

$$\left| \sum_{n=1}^{p-1} \chi_1(\alpha^n)\chi_2(f(n)) \right| \leq \begin{cases} (k - 1)\sqrt{p} & \text{if } \chi_1^\alpha \text{ is the principal character}, \\ k\sqrt{p} & \text{otherwise}. \end{cases} \quad (2.4)$$

Proof. Note that

$$\sum_{n=1}^{p-1} \chi_1(\alpha^n)\chi_2(f(n)) = \sum_{n=1}^{p-1} \chi_1^n(n)\chi_2(f(n)).$$

Now if $\chi_1^\alpha$ is the principal character, then it follows that

$$\sum_{n=1}^{p-1} \chi_1(\alpha^n)\chi_2(f(n)) = \sum_{n=1}^{p-1} \chi_2(f(n)),$$

and we get the bound from Lemma 2.2. If $\chi_1^\alpha$ is not the principal character, then the bound is obtained through a direct application of Lemma 2.3. \qed

3. Proof of the main result

It follows by Lemma 2.1 that

$$N(\alpha, f; p) = \sum_{n=1}^{p-1} \left( \frac{\phi(p-1)}{p-1} \right)^2 \sum_{d_1 \mid p-1} \sum_{d_2 \mid p-1} \mu(d_1) \mu(d_2) \phi(d_1) \phi(d_2) \sum_{\chi_1 \mod p \atop \ord_{\chi_1} = d_1} \sum_{\chi_2 \mod p \atop \ord_{\chi_2} = d_2} \chi_1(n)\chi_2(n^\alpha f(n))$$

$$= (p - 1 - R(f)) \left( \frac{\phi(p-1)}{p-1} \right)^2$$

$$+ \left( \frac{\phi(p-1)}{p-1} \right)^2 \sum_{d_1 \mid p-1 \atop d_1 > 1} \frac{\mu(d_1)}{\phi(d_1)} \sum_{\chi_1 \mod p \atop \ord_{\chi_1} = d_1} \sum_{n=1}^{p-1} \chi_1(n)$$

$$+ \left( \frac{\phi(p-1)}{p-1} \right)^2 \sum_{d_2 \mid p-1 \atop d_2 > 1} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi_2 \mod p \atop \ord_{\chi_2} = d_2} \sum_{n=1}^{p-1} \chi_2(n^\alpha f(n))$$
+ \left( \frac{\phi(p-1)}{p-1} \right)^2 \sum_{d_1 \mid p-1 \atop d_1 > 1} \sum_{d_2 \mid p-1 \atop d_2 > 1} \frac{\mu(d_1) \mu(d_2)}{\phi(d_1) \phi(d_2)} \sum_{\chi_1 \mod p \atop \text{ord} \chi_1 = d_1} \sum_{\chi_2 \mod p \atop \text{ord} \chi_2 = d_2} \sum_{n=1}^{p-1} \chi_1(n) \chi_2(n^\alpha f(n)).

\textbf{Claim 3.1.} We have

$$\sum_{d_1 \mid p-1 \atop d_1 > 1} \frac{\mu(d_1)}{\phi(d_1)} \sum_{\chi_1 \mod p \atop \text{ord} \chi_1 = d_1} \sum_{n=1}^{p-1} \chi_1(n) = 0.$$  

\textit{Proof.} We deduce it directly from

$$\sum_{n=1}^{p-1} \chi(n) = 0$$

if $\chi$ is not the principal character modulo $p$. \hfill \Box

\textbf{Claim 3.2.} We have

$$\left| \sum_{d_2 \mid p-1 \atop d_2 > 1} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi_2 \mod p \atop \text{ord} \chi_2 = d_2} \sum_{n=1}^{p-1} \chi_2(n^\alpha f(n)) \right| \leq (2^{\omega(p-1)} - 1)k\sqrt{p}.$$  

\textit{Proof.} Note that

$$\sum_{n=1}^{p-1} \chi_2(n^\alpha f(n)) = \sum_{n=1}^{p-1} \chi_2(n^\alpha) \chi_2(f(n)).$$

Now by Lemma 2.4, we have

$$\left| \sum_{n=1}^{p-1} \chi_2(n^\alpha f(n)) \right| \leq k\sqrt{p}.$$

Note also that

$$\sum_{d \mid p-1 \atop d > 1} |\mu(d)| = 2^{\omega(p-1)} - 1.$$

We therefore have

$$\left| \sum_{d_2 \mid p-1 \atop d_2 > 1} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi_2 \mod p \atop \text{ord} \chi_2 = d_2} \sum_{n=1}^{p-1} \chi_2(n^\alpha f(n)) \right| \leq \sum_{d_2 \mid p-1 \atop d_2 > 1} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi_2 \mod p \atop \text{ord} \chi_2 = d_2} \sum_{n=1}^{p-1} \chi_2(n^\alpha f(n)) \leq \sum_{d_2 \mid p-1 \atop d_2 > 1} \frac{\mu(d_2)}{\phi(d_2)} \phi(d_2) k\sqrt{p} = (2^{\omega(p-1)} - 1)k\sqrt{p}. \hfill \Box
Claim 3.3. We have

\[
\sum_{d_1 \mid p-1} \sum_{d_2 \mid p-1} \frac{\mu(d_1) \mu(d_2)}{\phi(d_1) \phi(d_2)} \sum_{\chi_1 \mod p \atop \text{ord}_{\chi_1} = d_1} \sum_{\chi_2 \mod p \atop \text{ord}_{\chi_2} = d_2} \sum_{n=1}^{p-1} \chi_1(n) \chi_2(n^\alpha f(n)) \leq (2^{\omega(p-1)} - 1)^2 k \sqrt{p}.
\]

Proof. Note that

\[
\sum_{n=1}^{p-1} \chi_1(n) \chi_2(n^\alpha f(n)) = \sum_{n=1}^{p-1} \chi_1(n^\alpha) \chi_2(f(n)).
\]

Again by Lemma 2.4, we get

\[
\sum_{n=1}^{p-1} \chi_1(n) \chi_2(n^\alpha f(n)) \leq k \sqrt{p}.
\]

We therefore have

\[
\sum_{d_1 \mid p-1} \sum_{d_2 \mid p-1} \frac{\mu(d_1) \mu(d_2)}{\phi(d_1) \phi(d_2)} \sum_{\chi_1 \mod p \atop \text{ord}_{\chi_1} = d_1} \sum_{\chi_2 \mod p \atop \text{ord}_{\chi_2} = d_2} \sum_{n=1}^{p-1} \chi_1(n) \chi_2(n^\alpha f(n)) \leq \sum_{d_1 \mid p-1} \sum_{d_2 \mid p-1} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi_1 \mod p \atop \text{ord}_{\chi_1} = d_1} \sum_{\chi_2 \mod p \atop \text{ord}_{\chi_2} = d_2} \sum_{n=1}^{p-1} \chi_1(n) \chi_2(n^\alpha f(n)) \leq \sum_{d_1 \mid p-1} \sum_{d_2 \mid p-1} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \phi(d_1) \phi(d_2) k \sqrt{p} = (2^{\omega(p-1)} - 1)^2 k \sqrt{p}.
\]

We conclude by combining Claims 3.1-3.3 that

\[
N(\alpha, f; p) - (p - 1 - R(f)) \left( \frac{\phi(p-1)}{p-1} \right)^2 \leq \left( (2^{\omega(p-1)} - 1) + (2^{\omega(p-1)} - 1)^2 \right) k \sqrt{p} \left( \frac{\phi(p-1)}{p-1} \right)^2 < k 4^{\omega(p-1)} \sqrt{p} \left( \frac{\phi(p-1)}{p-1} \right)^2.
\]

This completes our proof.

References
1. T. M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976. xii+338 pp.
2. L. Carlitz, Sets of primitive roots, *Compositio Math.* 13 (1956), 65–70.
3. D. Han and W. Zhang, On the existence of some special primitive roots mod p, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)* 58(106) (2015), no. 1, 59–66.
4. J. Johnsen, On the distribution of powers in finite fields, *J. Reine Angew. Math.* **251** (1971), 10–19.
5. M. Szalay, On the distribution of the primitive roots of a prime, *J. Number Theory* **7** (1975), 184–188.
6. D. Wan, Generators and irreducible polynomials over finite fields, *Math. Comp.* **66** (1997), no. 219, 1194–1212.
7. A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U. S. A.* **34** (1948), 204–207.

School of Mathematical Sciences, Zhejiang University, Hangzhou, 310027, China

E-mail address: shanechern@zju.edu.cn; chenxiaohang92@gmail.com