Functiones et Approximatio
57.1 (2017), 39–46
doi: 10.7169/facm/1612

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 ξ and $\xi^\alpha f(\xi)$ are primitive roots of p where α is a given integer. This answers a question of Han and Zhang.

Keywords: primitive root, character sum, Weil bound.

1. Introduction

Let a and q be relatively prime integers, with $q \geqslant 1$. We know from the Euler–Fermat theorem that $a^{\phi(q)} \equiv 1 \bmod q$, 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 $a^f \equiv 1 \bmod q$. 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 $\hat{a}$. 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 $\alpha \geqslant 1$. 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 ξ 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

2010 Mathematics Subject Classification: primary: 11A07; secondary: 11L40

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 $d \mid p-1$ with $d > 1$. Furthermore, we require that x does not divide $f(x)$. Let α be a given integer, we denote by $N(\alpha, f; p)$ the number of pairs $(\xi, \xi^\alpha f(\xi))$ such that both ξ and $\xi^\alpha f(\xi)$ are primitive roots of p. Our result is

Theorem 1.1. *It holds that*

$$N(\alpha, f; p) = (p-1-R(f)) \left(\frac{\phi(p-1)}{p-1}\right)^2 + \theta k 4^{\omega(p-1)} \sqrt{p} \left(\frac{\phi(p-1)}{p-1}\right)^2, \quad (1.1)$$

where $|\theta| < 1$, $\omega(n)$ *denotes the number of distinct prime divisors of* n, $R(f)$ *denotes the number of distinct zeros of* $f(x)$ *in* $\mathbb{F}_p$, *and* $k = \deg f$.

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

$$\begin{cases} \alpha = 1 \text{ and } f(x) = mx^{k-1} + n & \text{if } k > 1, \\ \alpha = k \text{ and } f(x) = nx^{1-k} + m & \text{if } k < 1, \end{cases}$$

where $(mn, p) = 1$, then we have $\deg f = |k-1|$ and $\xi^\alpha f(\xi) = m\xi^k + n\xi$. It follows from Theorem 1.1 that the asymptotic formula for the number of pairs $(\xi, m\xi^k + n\xi) \in \mathbb{F}_p^2$ such that both ξ and $m\xi^k + n\xi$ are primitive roots of p is

$$(p-1-R(f)) \left(\frac{\phi(p-1)}{p-1}\right)^2 + \theta |k-1| 4^{\omega(p-1)} \sqrt{p} \left(\frac{\phi(p-1)}{p-1}\right)^2.$$

We should mention that there is a minor mistake in Han and Zhang's result. (However, this does not affect the existence of such pairs; see our Corollary 1.2.) 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 $\phi^2(p-1)/(p-1)$.

From Theorem 1.1 we also immediately deduce the existence of pairs $(\xi, \xi^\alpha f(\xi))$ such that both ξ and $\xi^\alpha f(\xi)$ are primitive roots of p. Again, we write $k = \deg f$ where $f(x) \in \mathbb{F}_p[x]$ is a polynomial that is not a d-th power in $\mathbb{F}_p[x]$ for all $d \mid p-1$.

Corollary 1.2. *Let* p *be an odd prime large enough, then for any given integers* $k > 0$ *and* α, *there exists a primitive root* ξ *of* p *such that* $\xi^\alpha f(\xi)$ *is also a primitive root of* p. *Moreover, as* p *goes to infinity, the number of such* ξ *also goes to infinity.*

2. Preliminary lemmas

We first introduce the indicator function of primitive roots.

Lemma 2.1 (L. Carlitz [2, Lemma 2]). *We have*

$$\frac{\phi(p-1)}{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{\chi \bmod p\\ \mathrm{ord}\chi=d}}\chi(n)=\begin{cases}1 & \text{if } n \text{ is a primitive root of } p,\\ 0 & \text{otherwise.}\end{cases} \tag{2.1}$$

Here μ is the Möbius function, and $\mathrm{ord}\chi$ *denotes the order of a Dirichlet character* $\chi \bmod p$*, that is, the smallest positive integer f such that $\chi^f=\chi_0$, the principal character modulo p.*

Remark 2.1. We should mention that Carlitz proved more than Lemma 2.1. In fact, for an arbitrary finite field $\mathbb{F}_q$, where $q=p^\alpha$, Carlitz obtained the indicator function of numbers belonging to an exponent e, where $e \mid q-1$. Let $q-1=ee'$. It follows that

$$\frac{\phi(e)}{q-1}\sum_{d|q-1}\frac{\mu(d')}{\phi(d')}\sum_{\substack{\chi \bmod q\\ \mathrm{ord}\chi=d}}\chi(n)=\begin{cases}1 & \text{if } n \text{ belongs to the exponent } e,\\ 0 & \text{otherwise,}\end{cases}$$

where $d'=d/\gcd(d,e')$. To get Lemma 2.1, we only need to take $q=p$ and $e=p-1$.

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

Lemma 2.2 (A. Weil [7]). *Let χ be a non-principal Dirichlet character modulo p of 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*

$$\left|\sum_{n=1}^{p-1}\chi(f(n))\right|\leqslant (k-1)\sqrt{p}. \tag{2.2}$$

We also need the less-known extension of Weil bound obtained by D. Wan.

Lemma 2.3 (D. Wan [6, Corollary 2.3]). *Let χ_1, χ_2, …, χ_m be non-principal Dirichlet characters modulo p of orders d_1, d_2, …, d_m, respectively. Suppose $f_1(x)$, $f_2(x)$, …, $f_m(x)\in\mathbb{F}_p[x]$ are pairwise coprime polynomials of positive degrees k_1, k_2, …, k_m. Suppose also that $f_i(x)$ is not a d_i-th power in $\mathbb{F}_p[x]$ for all $i=1,2,\dots,m$. Then we have*

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

From Lemmas 2.2 and 2.3, we have

Lemma 2.4. *Let χ_1 be a Dirichlet character modulo p, and χ_2 be a non-principal Dirichlet character modulo p of 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 x does not divide $f(x)$. Furthermore, let α be a given integer. Then we have*

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

Proof. Note that

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

Now if χ_1^α is the principal character, then it follows that

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

and we get the bound from Lemma 2.2. If χ_1^α is not the principal character, then the bound is obtained through a direct application of Lemma 2.3. ■

3. Proofs

Proof of Theorem 1.1. It follows by Lemma 2.1 that

$$\begin{aligned}
&N(\alpha, f; p) \\
&= \sum_{n=1}^{p-1} \left(\frac{\phi(p-1)}{p-1}\right)^2 \sum_{d_1|p-1} \sum_{d_2|p-1} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{\chi_1 \bmod p \\ \mathrm{ord}\chi_1 = d_1}} \sum_{\substack{\chi_2 \bmod p \\ \mathrm{ord}\chi_2 = d_2}} \chi_1(n)\chi_2(n^\alpha f(n)) \\
&= (p-1-R(f)) \left(\frac{\phi(p-1)}{p-1}\right)^2 \\
&\quad + \left(\frac{\phi(p-1)}{p-1}\right)^2 \sum_{\substack{d_1|p-1 \\ d_1>1}} \frac{\mu(d_1)}{\phi(d_1)} \sum_{\substack{\chi_1 \bmod p \\ \mathrm{ord}\chi_1 = d_1}} \sum_{n-1}^{p-1} \chi_1(n) \\
&\quad + \left(\frac{\phi(p-1)}{p-1}\right)^2 \sum_{\substack{d_2|p-1 \\ d_2>1}} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{\chi_2 \bmod p \\ \mathrm{ord}\chi_2 = d_2}} \sum_{n-1}^{p-1} \chi_2(n^\alpha f(n)) \\
&\quad + \left(\frac{\phi(p-1)}{p-1}\right)^2 \sum_{\substack{d_1|p-1 \\ d_1>1}} \sum_{\substack{d_2|p-1 \\ d_2>1}} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{\chi_1 \bmod p \\ \mathrm{ord}\chi_1 = d_1}} \sum_{\substack{\chi_2 \bmod p \\ \mathrm{ord}\chi_2 = d_2}} \sum_{n=1}^{p-1} \chi_1(n)\chi_2(n^\alpha f(n)).
\end{aligned}$$

Claim 3.1. *We have*

$$\sum_{\substack{d_1|p-1\\d_1>1}}\frac{\mu(d_1)}{\phi(d_1)}\sum_{\substack{\chi_1 \bmod p\\ \mathrm{ord}\chi_1=d_1}}\sum_{n-1}^{p-1}\chi_1(n)=0.$$

Proof. We deduce it directly from

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

if χ is not the principal character modulo p. ∎

Claim 3.2. *We have*

$$\left|\sum_{\substack{d_2|p-1\\d_2>1}}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\substack{\chi_2 \bmod p\\ \mathrm{ord}\chi_2=d_2}}\sum_{n-1}^{p-1}\chi_2(n^\alpha f(n))\right|\leqslant(2^{\omega(p-1)}-1)k\sqrt{p}.$$

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

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

Note also that

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

We therefore have

$$\begin{aligned}\left|\sum_{\substack{d_2|p-1\\d_2>1}}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\substack{\chi_2 \bmod p\\ \mathrm{ord}\chi_2=d_2}}\sum_{n-1}^{p-1}\chi_2(n^\alpha f(n))\right| &\leqslant \sum_{\substack{d_2|p-1\\d_2>1}}\left|\frac{\mu(d_2)}{\phi(d_2)}\right|\sum_{\substack{\chi_2 \bmod p\\ \mathrm{ord}\chi_2=d_2}}\left|\sum_{n-1}^{p-1}\chi_2(n^\alpha f(n))\right|\\ &\leqslant \sum_{\substack{d_2|p-1\\d_2>1}}\left|\frac{\mu(d_2)}{\phi(d_2)}\right|\phi(d_2)k\sqrt{p}\\ &=(2^{\omega(p-1)}-1)k\sqrt{p}.\end{aligned}$$

∎

Claim 3.3. *We have*

$$\left|\sum_{\substack{d_1|p-1\\ d_1>1}}\sum_{\substack{d_2|p-1\\ d_2>1}}\frac{\mu(d_1)}{\phi(d_1)}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\substack{\chi_1 \bmod p\\ \mathrm{ord}\chi_1=d_1}}\sum_{\substack{\chi_2 \bmod p\\ \mathrm{ord}\chi_2=d_2}}\sum_{n=1}^{p-1}\chi_1(n)\chi_2(n^\alpha f(n))\right| \leqslant (2^{\omega(p-1)}-1)^2 k\sqrt{p}.$$

Proof. Note that

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

Again by Lemma 2.4, we get

$$\left|\sum_{n=1}^{p-1}\chi_1(n)\chi_2(n^\alpha f(n))\right| \leqslant k\sqrt{p}.$$

We therefore have

$$\begin{aligned}
&\left|\sum_{\substack{d_1|p-1\\ d_1>1}}\sum_{\substack{d_2|p-1\\ d_2>1}}\frac{\mu(d_1)}{\phi(d_1)}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\substack{\chi_1 \bmod p\\ \mathrm{ord}\chi_1=d_1}}\sum_{\substack{\chi_2 \bmod p\\ \mathrm{ord}\chi_2=d_2}}\sum_{n=1}^{p-1}\chi_1(n)\chi_2(n^\alpha f(n))\right| \\
&\quad\leqslant \sum_{\substack{d_1|p-1\\ d_1>1}}\sum_{\substack{d_2|p-1\\ d_2>1}}\left|\frac{\mu(d_1)}{\phi(d_1)}\right|\left|\frac{\mu(d_2)}{\phi(d_2)}\right|\sum_{\substack{\chi_1 \bmod p\\ \mathrm{ord}\chi_1=d_1}}\sum_{\substack{\chi_2 \bmod p\\ \mathrm{ord}\chi_2=d_2}}\left|\sum_{n=1}^{p-1}\chi_1(n)\chi_2(n^\alpha f(n))\right| \\
&\quad\leqslant \sum_{\substack{d_1|p-1\\ d_1>1}}\sum_{\substack{d_2|p-1\\ d_2>1}}\left|\frac{\mu(d_1)}{\phi(d_1)}\right|\left|\frac{\mu(d_2)}{\phi(d_2)}\right|\phi(d_1)\phi(d_2)k\sqrt{p} \\
&\quad= (2^{\omega(p-1)}-1)^2 k\sqrt{p}.
\end{aligned}$$

■

We conclude by combining Claims 3.1–3.3 that

$$\begin{aligned}
&\left|N(\alpha, f; p) - (p-1-R(f))\left(\frac{\phi(p-1)}{p-1}\right)^2\right| \\
&\quad\leqslant \left((2^{\omega(p-1)}-1)+(2^{\omega(p-1)}-1)^2\right)k\sqrt{p}\left(\frac{\phi(p-1)}{p-1}\right)^2 \\
&\quad< k4^{\omega(p-1)}\sqrt{p}\left(\frac{\phi(p-1)}{p-1}\right)^2.
\end{aligned}$$

This completes our proof. ■

Proof of Corollary 1.2. We first estimate $4^{\omega(p-1)}$. In fact, we have the following

Proposition 3.4. *Let A and ϵ be given positive real numbers, then we have*

$$A^{\omega(n)} = o(n^{\epsilon})$$

as $n \to \infty$.

Proof. Let p_n denote the n-th prime, then we have

$$\log n \geqslant \log \prod_{i=1}^{\omega(n)} p_i \gg \omega(n) \log \omega(n).$$

This leads to $\omega(n) = o(\log n)$ as $n \to \infty$ and thus the desired estimate follows immediately. ■

Now taking $A = 4$ and $\epsilon = 1/2$, then

$$\theta k 4^{\omega(p-1)} \sqrt{p} \left(\frac{\phi(p-1)}{p-1} \right)^2 = o \left(\frac{\phi^2(p-1)}{p-1} \right).$$

On the other hand, we have $R(f) \leqslant k$. Thus

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

We therefore conclude

$$N(\alpha, f; p) = \frac{\phi^2(p-1)}{p-1} + o \left(\frac{\phi^2(p-1)}{p-1} \right).$$

At last, to show $N(\alpha, f; p) \to \infty$ as $p \to \infty$, we only need to estimate $\phi^2(n)/n$. Let $p_{\max}(n)$ be the largest prime factor of n and $\mathrm{ord}_{\max}(n)$ be the largest positive integer α such that $p^\alpha \mid n$ and $p^{\alpha+1} \nmid n$ for some prime factor p of n. As $n \to \infty$, either $p_{\max}(n)$ or $\mathrm{ord}_{\max}(n)$ goes to infinity. Finally, we note that $\phi^2(n)/n$ is multiplicative. Since

$$\frac{\phi^2(p^\alpha)}{p^\alpha} = p^{\alpha-2}(p-1)^2,$$

we conclude that $\phi^2(n)/n \to \infty$ as $n \to \infty$. This ends the proof of Corollary 1.2. ■

Acknowledgments. The author is grateful to the referee for some helpful comments that improve this paper.

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, 1195–1212.
[7] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207.

Address: Shane Chern: Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA.

E-mail: shanechern@psu.edu; chenxiaohang92@gmail.com

Received: 2 July 2016; **revised:** 28 December 2016