Bull. Math. Soc. Sci. Math. Roumanie
Tome 58(106) No. 1, 2015, 59–66

On the existence of some special primitive roots mod p *

by
Di Han[1] and Wenpeng Zhang[2]

Abstract

The main purpose of this paper is using the properties of Gauss sums and the estimate for character sums to study the properties of the primitive roots of p (an odd prime), and prove that for any integers $k \neq 1$ and $(mn, p) = 1$, there exists a primitive root ξ of p such that $m\xi^k + n\xi$ is also a primitive root of p, provide p large enough. Let $N(k, m, n; p)$ denotes the number of all primitive roots ξ of p such that $m\xi^k + n\xi$ is also a primitive root of p. Then we can also give an interesting asymptotic formula for $N(k, m, n; p)$.

Key Words: Primitive root of p, Gauss sums, character sums, Asymptotic formula.
2010 Mathematics Subject Classification: Primary 11M20, Secondary 11L40.

1 Introduction

Let $q > 1$ be a integer. For any integer a with $(a, q) = 1$, from the Euler-Fermat theorem we know that $a^{\phi(q)} \equiv 1 \bmod q$, where $\phi(q)$ denotes Euler function. Let k is the smallest positive integer such that $a^k \equiv 1 \bmod q$. If $k = \phi(q)$, then a is called a primitive root of q. If q has a primitive root, then each reduced residue system mod q can be expressed as a geometric progression. This gives a powerful tool that can be used in problems involving reduced residue systems. Unfortunately, not all modulo have primitive roots. In fact primitive roots exist only for the following modulo:

$$q = 1,\ 2,\ 4,\ p^\alpha,\ 2p^\alpha,$$

where p is an odd prime and $\alpha \geq 1$.

About the properties of primitive roots and related problems, many people had studied it, and obtained many interesting results, see [3]-[8] and [11]. For example, Juping Wang [6] proved that Golomb's conjecture is true for almost all $q = p^n$. That is, there exist two primitive elements α and β in finite fields $\mathbf{F}_q$ such that $\alpha + \beta = 1$. S. D. Cohen and G. L. Mullen [4] established a generalization of Golobm's conjecture by proving the existence of $q_0 > 0$ such that, whenever $q > q_0$, there exist $\alpha, \beta \in \mathbf{F}_q$ with $\gamma\alpha + \delta\beta = \varepsilon$, where γ, δ and ε are arbitrary non-zero members of $\mathbf{F}_q$. In this paper, we will study the existence of some special primitive

*This work is supported by the N. S. F. (11371291, 61202437) of P. R. China.

roots of p, such as ξ and $\xi+\overline{\xi}$ both are primitive root of p. Furthermore, for any integers $k \neq 1$ and $(mn,p)=1$), whether there exists a primitive root ξ of p such that $m\xi^k+n\xi$ is also a primitive root of p ? Let $N(k,m,n;p)$ denotes the number of all primitive roots ξ of p such that $m\xi^k+n\xi$ is also a primitive root of p. How about the asymptotic properties of $N(k,m,n;p)$?

These problems are very interesting and important, because they contained Golobm's conjecture. In fact, if the problems are true in finite field $\mathbf{F}_p$, then we can take $k=0$, $m=1$ and $n=-1$, this time, both ξ and $1-\xi=\eta$ are primitive elements in $\mathbf{F}_p$, and $\xi+\eta=1$. That is, Golobm's conjecture is true.

In this paper, we shall study these problems, and prove the following conclusion:

Theorem. Let p be an odd prime, then for any integers $k \neq 1$ and $(mn,p)=1$, we have the asymptotic formula

$$N(k,m,n;p)=\frac{\phi^2(p-1)}{p-1}+\theta\cdot|k-1|\cdot\frac{\phi^2(p-1)}{(p-1)^2}\cdot 4^{\omega(p-1)}\cdot\sqrt{p},$$

where $|\theta|\leq 1$, $\omega(n)$ denotes the number of all distinct prime divisors of n.

Taking $k=0,-1$, note that $a^{-1}\equiv\overline{a} \bmod p$, from this theorem we may immediately deduce the following three conclusions:

Corollary 1. Let p be an odd prime large enough, then for any integers $k \neq 1$ and $(mn,p)=1$, there exists a primitive root ξ of p such that $m\xi^k+n\xi$ is also a primitive root of p.

Corollary 2. Let p be an odd prime large enough, then for any integers m and n with $(mn,p)=1$, there exists a primitive root ξ of p such that $m\xi+n\overline{\xi}$ is also a primitive root of p, where $\xi\cdot\overline{\xi}\equiv 1 \bmod p$.

Corollary 3. Let p be an odd prime large enough, then there exists a primitive root ξ of p such that $1+\xi$ is also a primitive root of p.

Let $f(x)$ is a irreducible polynomial in $\mathbf{F}_p$. Whether there exists a primitive element $\xi\in\mathbf{F}_p$ such that $f(\xi)$ is also a primitive element in $\mathbf{F}_p$? This is an interesting open problem.

2 Several Lemmas

In this section, we shall give several lemmas, which are necessary in the proof of our theorem. Through out this paper, we used many properties of Dirichlet characters and Gauss sums, these contents can be found in [1], here no longer repeat. First we have the following:

Lemma 1. *Let p be an odd prime, χ be any non-principal character* mod p*, k be any positive integer such that $(k,p-1)=1$ or $k \mid p-1$. Then for any integer m with $(m,p)=1$, we have the identity*

$$\sum_{a=1}^{p-1}\chi(a)\ e\left(\frac{ma^k}{p}\right)=\begin{cases}\overline{\chi}^r(m)\cdot\tau\left(\chi^r\right), & \text{if } (k,p-1)=1,\\ 0, & \text{if } k\mid(p-1) \text{ and } \chi^{\frac{p-1}{k}}\neq\chi_0,\\ \overline{\chi_1}(m)\cdot\displaystyle\sum_{i=0}^{k-1}\overline{\chi_k}^i(m)\tau\left(\chi_1\chi_k^i\right), & \text{if } k\mid(p-1) \text{ and } \chi^{\frac{p-1}{k}}=\chi_0.\end{cases}$$

where $e(y)=e^{2\pi iy}$, $r\cdot k\equiv 1 \bmod (p-1)$, χ_0 denotes the principal character mod p*, χ_k denotes any k-order character* mod p*, and $\chi_1^k=\chi$.*

Proof: If $(k, p-1) = 1$, then there exists one integer r with $(r, p-1) = 1$ such that $r \cdot k \equiv 1 \bmod (p-1)$. This time, for any integer a with $(a, p) = 1$, we have $a^{rk} \equiv a \bmod p$. If a pass through a reduced residue system mod p, then a^r also pass through a reduced residue system mod p. Therefore, we have

$$\sum_{a=1}^{p-1} \chi(a)\ e\left(\frac{ma^k}{p}\right) = \sum_{a=1}^{p-1} \chi(a^r)\ e\left(\frac{ma^{rk}}{p}\right)$$
$$= \sum_{a=1}^{p-1} \chi^r(a)\ e\left(\frac{ma}{p}\right) = \overline{\chi}^r(m) \cdot \tau\left(\chi^r\right). \tag{2.1}$$

If $k > 1$ and $k \mid (p-1)$ with $\chi^{\frac{p-1}{k}} \neq \chi_0$, then there must exist an integer n with $(n, p) = 1$ such that $\chi^{\frac{p-1}{k}}(n) \neq 1$. For this n, we have

$$\sum_{a=1}^{p-1} \chi(a)\ e\left(\frac{ma^k}{p}\right) = \sum_{a=1}^{p-1} \chi\left(a \cdot n^{\frac{p-1}{k}}\right)\ e\left(\frac{m\left(a \cdot n^{\frac{p-1}{k}}\right)^k}{p}\right)$$
$$= \chi\left(n^{\frac{p-1}{k}}\right) \sum_{a=1}^{p-1} \chi(a)\ e\left(\frac{ma^k n^{p-1}}{p}\right) = \chi^{\frac{p-1}{k}}(n) \sum_{a=1}^{p-1} \chi(a)\ e\left(\frac{ma^k}{p}\right)$$

or

$$\left(1 - \chi^{\frac{p-1}{k}}(n)\right) \sum_{a=1}^{p-1} \chi(a)\ e\left(\frac{ma^k}{p}\right) = 0.$$

Since $\chi^{\frac{p-1}{k}}(n) \neq 1$, so from the above identity we have

$$\sum_{a=1}^{p-1} \chi(a)\ e\left(\frac{ma^k}{p}\right) = 0. \tag{2.2}$$

If $\chi^{\frac{p-1}{k}} = \chi_0$, then χ must be a k-th character mod p, so there exists one character χ_1 mod p such that $\chi = \chi_1^k$. Let χ_k be a k-order character mod p (i.e., $\chi_k^k = \chi_0$), then for any integer a with $(a, p) = 1$, note that

$$1 + \chi_k(a) + \chi_k^2(a) + \cdots \chi_k^{k-1}(a) = \begin{cases} k, & \text{if } a \text{ is a } k\text{-th residue mod } p, \\ 0, & \text{otherwise.} \end{cases}$$

From the properties of Gauss sums we have

$$\sum_{a=1}^{p-1} \chi(a) e\left(\frac{ma^k}{p}\right) = \sum_{a=1}^{p-1} \chi_1^k(a) e\left(\frac{ma^k}{p}\right) = \sum_{a=1}^{p-1} \chi_1\left(a^k\right) e\left(\frac{ma^k}{p}\right)$$
$$= \sum_{a=1}^{p-1} \chi_1(a)\left(1 + \chi_k(a) + \chi_k^2(a) + \cdots \chi_k^{k-1}(a)\right) e\left(\frac{ma}{p}\right)$$
$$= \overline{\chi_1}(m) \cdot \sum_{i=0}^{k-1} \overline{\chi_k}^i(m) \tau\left(\chi_1 \chi_k^i\right). \tag{2.3}$$

Now Lemma 1 follows from (2.1), (2.2) and (2.3). ∎

Lemma 2. *Let p be an odd prime, χ_1 and χ_2 are any two non-principal character* mod p. *Then for any fixed integers $k \neq 1$ and $(mn, p) = 1$, we have the estimate*

$$\sum_{a=1}^{p-1} \chi_1(a)\chi_2\left(ma^k + na\right) \leq |k-1| \cdot \sqrt{p}.$$

Proof: First from the properties of Gauss sums we have

$$\begin{aligned} & \sum_{a=1}^{p-1} \chi_1(a)\chi_2\left(ma^k + na\right) \\ = & \frac{1}{\tau\left(\overline{\chi_2}\right)} \sum_{a=1}^{p-1} \chi_1(a) \sum_{b=1}^{p-1} \overline{\chi}_2(b) e\left(\frac{b\left(ma^k + na\right)}{p}\right) \\ = & \frac{1}{\tau\left(\overline{\chi_2}\right)} \sum_{b=1}^{p-1} \overline{\chi}_2(b) \sum_{a=1}^{p-1} \chi_1(a)\chi_2(a) e\left(\frac{bma^{k-1} + nb}{p}\right) \\ = & \frac{1}{\tau\left(\overline{\chi_2}\right)} \sum_{b=1}^{p-1} \overline{\chi}_2(b) e\left(\frac{nb}{p}\right) \sum_{a=1}^{p-1} \chi_1\chi_2(a) e\left(\frac{bma^{k-1}}{p}\right). \end{aligned} \tag{2.4}$$

Note that $\chi(a^{-k}) = \overline{\chi}^k(a)$, from (2.4) we know that if $k < 0$, then we have

$$\begin{aligned} & \sum_{a=1}^{p-1} \chi_1(a)\chi_2\left(ma^k + na\right) \\ = & \frac{1}{\tau\left(\overline{\chi_2}\right)} \sum_{b=1}^{p-1} \overline{\chi}_2(b) e\left(\frac{nb}{p}\right) \sum_{a=1}^{p-1} \overline{\chi}_1\overline{\chi}_2(a) e\left(\frac{bma^{|k-1|}}{p}\right). \end{aligned}$$

So without loss of generality we can assume that $k > 1$. If $(k-1, p-1) = 1$, then there exists an integer r with $(r, p-1) = 1$ such that $r(k-1) \equiv 1 \bmod (p-1)$. So from (2.4) and Lemma

1 we have

$$
\begin{aligned}
&\sum_{a=1}^{p-1}\chi_1(a)\chi_2\left(ma^k+na\right)\\
=\ &\frac{1}{\tau\left(\overline{\chi}_2\right)}\sum_{b=1}^{p-1}\overline{\chi}_2(b)e\left(\frac{nb}{p}\right)\sum_{a=1}^{p-1}\chi_1\chi_2(a^r)e\left(\frac{bma^{r(k-1)}}{p}\right)\\
=\ &\frac{1}{\tau\left(\overline{\chi}_2\right)}\sum_{b=1}^{p-1}\overline{\chi}_2(b)e\left(\frac{nb}{p}\right)\sum_{a=1}^{p-1}\chi_1^r\chi_2^r(a)e\left(\frac{bma}{p}\right)\\
=\ &\frac{\tau\left(\chi_1^r\chi_2^r\right)}{\tau\left(\overline{\chi}_2\right)}\overline{\chi}_1^r\overline{\chi}_2^r(m)\sum_{b=1}^{p-1}\overline{\chi}_2(b)\overline{\chi}_1^r\overline{\chi}_2^r(b)e\left(\frac{nb}{p}\right)\\
=\ &\overline{\chi}_1^r\overline{\chi}_2^r(m)\cdot\chi_1\chi_2^{r+1}(n)\cdot\frac{\tau\left(\chi_1^r\chi_2^r\right)\tau\left(\overline{\chi}_1^r\overline{\chi}_2^{r+1}\right)}{\tau\left(\overline{\chi}_2\right)}.
\end{aligned}\tag{2.5}
$$

Note that for any character χ mod p, from the properties of Gauss sums we have the estimate $|\tau(\chi)|\leq\sqrt{p}$. From (2.5) we may immediately deduce the estimate

$$
\left|\sum_{a=1}^{p-1}\chi_1(a)\chi_2\left(ma^k+na\right)\right|\leq\sqrt{p},\ \text{if}\ \ (k-1,p-1)=1.\tag{2.6}
$$

If $(k-1,p-1)=d>1$ and $\chi_1\chi_2$ is not a d-th character mod p, then from (2.4) and Lemma 1 we can deduce the identity

$$
\sum_{a=1}^{p-1}\chi_1(a)\chi_2\left(ma^k+na\right)=0.\tag{2.7}
$$

If $(k-1,p-1)=d>1$ and $\chi_1\chi_2$ is a d-th character mod p, let $\chi_1\chi_2=\chi_3^d$, χ_d be the d-order character mod p, then from (2.4) and Lemma 1 we have

$$
\begin{aligned}
&\sum_{a=1}^{p-1}\chi_1(a)\chi_2\left(ma^k+na\right)\\
=\ &\frac{1}{\tau\left(\overline{\chi}_2\right)}\sum_{b=1}^{p-1}\overline{\chi}_2(b)e\left(\frac{nb}{p}\right)\sum_{a=1}^{p-1}\chi_3^d(a)e\left(\frac{bma^{k-1}}{p}\right)\\
=\ &\frac{1}{\tau\left(\overline{\chi}_2\right)}\sum_{b=1}^{p-1}\overline{\chi}_2(b)e\left(\frac{nb}{p}\right)\sum_{a=1}^{p-1}\chi_3(a)\left(1+\chi_d(a)+\cdots+\chi_d^{d-1}(a)\right)e\left(\frac{bma^{\frac{k-1}{d}}}{p}\right)\\
=\ &\frac{1}{\tau\left(\overline{\chi}_2\right)}\sum_{b=1}^{p-1}\overline{\chi}_2(b)e\left(\frac{nb}{p}\right)\sum_{i=0}^{d-1}\sum_{a=1}^{p-1}\chi_3(a)\chi_d^i(a)e\left(\frac{bma^{\frac{k-1}{d}}}{p}\right).
\end{aligned}\tag{2.8}
$$

If $\left(\frac{k-1}{d}, p-1\right) = 1$, then from (2.8) and the methods of proving (2.5) and (2.6) we have the estimate

$$\left|\sum_{a=1}^{p-1} \chi_1(a)\chi_2\left(ma^k + na\right)\right| \le d \cdot \sqrt{p}. \tag{2.9}$$

If $\left(\frac{k-1}{d}, p-1\right) = d_1 > 1$, then using Lemma 1 and the methods of proving (2.5)-(2.9) repeatedly, we can get the estimate

$$\left|\sum_{a=1}^{p-1} \chi_1(a)\chi_2\left(ma^k + na\right)\right| \le d \cdot d_1 \cdots d_s \cdot \sqrt{p} \le (k-1) \cdot \sqrt{p}. \tag{2.10}$$

Now Lemma 2 follows from the estimate (2.6), (2.7), (2.9) and (2.10). □

Lemma 3. *Let p be an odd prime. Then for any integer c with $(c, p) = 1$, we have the identity*

$$\frac{\phi(p-1)}{p-1} \sum_{h|p-1} \frac{\mu(h)}{\phi(h)} \sum_{\substack{k=1\\(h,k)=1}}^{h} e\left(\frac{k \text{ ind } c}{h}\right) = \begin{cases} 1, & \text{if } c \text{ is a primitive root of } p,\\ 0, & \text{otherwise,}\end{cases}$$

where ind c denotes the index of c relative to some fixed primitive root of p, $\mu(n)$ is the Möbius function.

Proof: See Proposition 2.2 of reference [9]. □

3 Proof of the theorem

In this section, we shall complete the proof of our theorem. First we write $\chi_{s,h}(c) = e\left(\frac{s \text{ ind } c}{h}\right)$. It is clear that $\chi_{s,h}(c)$ is a Dirichlet character mod p. For any integer $k \neq 1$ and $(mn, p) = 1$, from Lemma 3 we have

$$\begin{aligned}
& N(k, m, n; p)\\
= & \sum_{c=1}^{p-1} \frac{\phi^2(p-1)}{(p-1)^2} \sum_{h|p-1}\sum_{u|p-1} \frac{\mu(h)}{\phi(h)}\frac{\mu(u)}{\phi(u)} \sum_{\substack{s=1\\(h,s)=1}}^{h} \sum_{\substack{v=1\\(v,u)=1}}^{u} \chi_{s,h}(c)\chi_{v,u}\left(mc^k + nc\right)\\
= & \frac{\phi^2(p-1)}{p-1} + \frac{\phi^2(p-1)}{(p-1)^2} \sum_{\substack{h|p-1\\h>1}} \frac{\mu(h)}{\phi(h)} \sum_{\substack{s=1\\(h,s)=1}}^{h} \sum_{c=1}^{p-1} \chi_{s,h}(c)\\
& + \frac{\phi^2(p-1)}{(p-1)^2} \sum_{\substack{u|p-1\\u>1}} \frac{\mu(u)}{\phi(u)} \sum_{\substack{v=1\\(v,u)=1}}^{u} \sum_{c=1}^{p-1} \chi_{v,u}\left(mc^k + nc\right)\\
& + \frac{\phi^2(p-1)}{(p-1)^2} \sum_{\substack{h|p-1\\h>1}}\sum_{\substack{u|p-1\\u>1}} \frac{\mu(h)}{\phi(h)}\frac{\mu(u)}{\phi(u)} \sum_{\substack{s=1\\(h,s)=1}}^{h} \sum_{\substack{v=1\\(v,u)=1}}^{u} A(s, h, v, u, k, m, n; p),
\end{aligned} \tag{3.1}$$

where

$$A(s,h,v,u,k,m,n;p)=\sum_{c=1}^{p-1}\chi_{s,h}(c)\chi_{v,u}\left(mc^k+nc\right).$$

Now we estimate each terms in (3.1) respectively. It is clear that for any integer $h>1$ and $(s,c)=1$, we have the identity

$$\sum_{c=1}^{p-1}\chi_{s,h}(c)=0. \tag{3.2}$$

For any non-principal character $\chi_{v,u}$ mod p, from the well known conclusion of Weil (see [2] and [10]) we can get the estimate

$$\left|\sum_{c=1}^{p-1}\chi_{v,u}\left(mc^k+nc\right)\right|\leq k\sqrt{p}. \tag{3.3}$$

Applying Lemma 2 we have

$$|A(s,h,v,u,k,m,n;p)|\leq|k-1|\cdot\sqrt{p}. \tag{3.4}$$

Note that

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

Combining (3.1)-(3.4) we may immediately get the asymptotic formula

$$N(k,m,n;p)=\frac{\phi^2(p-1)}{p-1}+\theta\cdot|k-1|\cdot\frac{\phi^2(p-1)}{(p-1)^2}\cdot 4^{\omega(p-1)}\cdot\sqrt{p},$$

where $|\theta|\leq 1$. This completes the proof of our theorem.

Acknowledgments. The authors would like to thank the referee for his very helpful and detailed comments which have significantly improved the presentation of this paper.

References

[1] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[2] D. A. Burgess, On Dirichlet characters of polynomials, Proc. London Math. Soc., 13(1963), 537-548.

[3] S. D. Cohen and Wenpeng Zhang, Sums of two exact powers, Finite fields and their applications, 8(2002), 471-477.

[4] S. D. Cohen and G. L. Mullen, Primitive elements in Costas arrays, Appl. Algebra Eng. Comm. Comput., 2(1991), 45-53; (Corrections) 2(1992), 297-299.

[5] S. Golomb, On the algebraic construction for Constas arrays, Journal of Combinatoial Theory (Ser. A.), 37(1984), 13-21.

[6] Wladyslaw Narkiewicz, Classical Problems in Number Theory, PWN-Polish Scientific Publishers, Warszawa, 1987, 79-80.

[7] Tian Tian and Wenfeng Qi, Primitive normal element and its inverse in finite fields, Acta Math. Sinica, 49(2006), 657-668.

[8] Juping Wang, On Golomb's conjecture, Science in China (Ser. A.), 9(1987), 927-935.

[9] Peipei Wang, Xiwang Cao and Rongquan Feng, On the existence of some specific elements in finite fields of characteristic 2, Finite fields and their applications, 18(2012), 800-813.

[10] A. Weil, On some exponential sums, Proc. Nat. Acad. Sci. U.S.A., 34 (1948), 204-207.

[11] Wenpeng Zhang, On a problem related to Golomb's conjecture, Journal of Systems Science and Complexity, 16(2003), 13-18.

Received: 27.12.2012

Accepted: 24.09.2013

School of Mathematics,
Northwest University,
Xi'an, Shaanxi, P. R. China
E-mail: [1]`handi515@163.com`
[2]`wpzhang@nwu.edu.cn`