

Research Article

A Mean Value Related to Primitive Roots and Golomb's Conjectures

Weiqiong Wang^{1,2} and Wenpeng Zhang¹

¹ Department of Mathematics, Northwest University, Xi'an, Shaanxi 710127, China

² School of Science, Chang'an University, Xi'an, Shaanxi 710064, China

Correspondence should be addressed to Weiqiong Wang; wqwang18@126.com

Received 12 November 2013; Accepted 3 January 2014; Published 20 February 2014

Academic Editor: Josip E. Pečarić

Copyright © 2014 W. Wang and W. Zhang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The main purpose of this paper is using the properties of Gauss sums and the estimate for character sums to study a mean value problem related to the primitive roots mod p and the different forms of Golomb's conjectures and propose an interesting asymptotic formula for it.

1. Introduction

Let $q > 1$ be an integer. For any integer a with $(a, q) = 1$, from the Euler-Fermat theorem we know that $a^{\phi(q)} \equiv 1 \pmod{q}$, where $\phi(q)$ denotes Euler function. Let k be the smallest positive integer such that $a^k \equiv 1 \pmod{q}$. 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 moduli have primitive roots. In fact primitive roots exist only for the following moduli:

$$q = 1, 2, 4, p^\alpha, 2p^\alpha, \quad (1)$$

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

Many researchers focused on the properties of primitive roots and some related problems and have obtained many interesting results; see [1–7]. For example, Moreno and Sotero [4] proved that Golomb's conjecture is true for all $q < 2^{60}$. That is, there exist two primitive elements α and β in finite fields \mathbb{F}_q such that $\alpha + \beta = 1$, if $q < 2^{60}$. Cohen and Mullen [2] established a generalization of Golomb's conjecture by proving the existence of $q_0 > 0$ such that, whenever $q > q_0$,

there exist primitive $\alpha, \beta \in \mathbb{F}_q$ with $\gamma\alpha + \delta\beta = \varepsilon$, where γ, δ , and ε are arbitrary nonzero members of \mathbb{F}_q . What is more, they also gave an asymptotic formula for the number of solutions. But we think the error term is too big and can be improved. In order to verify our viewpoint, we take the mean value properties of the error term into account. By using the properties of Gauss sums and the estimate for character sums, we obtained a stronger asymptotic formula.

Let $p > 3$ be an odd prime number. For any integer c with $(c, p) = 1$, let $N(c, p)$ denote the number of all solutions of the congruence equation $x - y \equiv c \pmod{p}$, where x and y are the primitive roots mod p . We define $E(c, p) = 0$, if $c \equiv 0 \pmod{p}$, and

$$E(c, p) = N(c, p) - \frac{(p-2) \cdot \phi^2(p-1)}{(p-1)^2}, \quad \text{if } (c, p) = 1. \quad (2)$$

In this paper, we give an interesting asymptotic formula for the mean value of $E(c, p)$. This problem is interesting, because it cannot only reveal the profound properties of Golomb's conjecture and provide the distribution law of the error term $E(c, p)$, but it is also a generalization of the related contents.

Theorem 1. Let $p > 3$ be a prime. Then for any three integers a, b , and c with $(abc, p) = (a^2 - 4b, p) = 1$, one has the asymptotic formula

$$\begin{aligned} \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} E(x^2 + axy + by^2 + c, p) \\ = -p \cdot \phi(p-1) + \phi^2(p-1) \\ + \theta \cdot \frac{p^{3/2} \cdot \phi^2(p-1)}{(p-1)^2} \cdot 4^{\omega(p-1)}, \end{aligned} \tag{3}$$

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

We may immediately deduce the following corollary from this theorem.

Corollary 2. Let $p > 3$ be a prime number. Then for any three integers a, b , and c with $(abc, p) = (a^2 - 4b, p) = 1$, one has

$$\begin{aligned} \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} E(x^2 + axy + by^2 + c, p) \\ \sim \phi^2(p-1) - p \cdot \phi(p-1), \quad \text{as } p \rightarrow \infty. \end{aligned} \tag{4}$$

2. Several Lemmas

In this section, we provide several lemmas that will be necessary for the proof of our theorem. Throughout this paper, we used many properties of Dirichlet characters and Gauss sums, which can be found in [8]. Firstly, we have the following lemma.

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

$$\frac{\phi(p-1)}{p-1} \sum_{h|p-1} \frac{\mu(h)}{\phi(h)} \sum_{\substack{h \\ (h,k)=1}}^h e\left(\frac{k \operatorname{ind} c}{h}\right) \tag{5}$$

$$= \begin{cases} 1, & \text{if } c \text{ is a primitive root of } p, \\ 0, & \text{otherwise,} \end{cases}$$

where $\operatorname{ind} c$ 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 [9]. □

Lemma 4. Let p be an odd prime; a, b , and c are three integers with $(abc, p) = (a^2 - 4b, p) = 1$. Then for any nonprincipal character $\chi \pmod p$, one has the identity

$$\begin{aligned} \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} \chi(r^2 + ars + bs^2 + c) \\ = \chi(c) \cdot \left(\frac{a^2 - 4b}{p}\right) \cdot p, \end{aligned} \tag{6}$$

where $(*/p)$ denotes the Legendre symbol.

Proof. Since any nonprincipal character $\chi \pmod p$ is a primitive character mod p , so from the properties of Gauss sums we conclude that

$$\begin{aligned} \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} \chi(r^2 + ars + bs^2 + c) \\ = \frac{1}{\tau(\bar{\chi})} \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} \sum_{t=1}^{p-1} \bar{\chi}(t) e\left(\frac{t(r^2 + ars + bs^2 + c)}{p}\right) \\ = \frac{1}{\tau(\bar{\chi})} \sum_{t=1}^{p-1} \bar{\chi}(t) e\left(\frac{ct}{p}\right) \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} e\left(\frac{tr^2 + tars + tbs^2}{p}\right) \\ = \frac{1}{\tau(\bar{\chi})} \sum_{t=1}^{p-1} \bar{\chi}(t) e\left(\frac{ct}{p}\right) \\ \times \left(\sum_{r=0}^{p-1} e\left(\frac{tr^2}{p}\right) + \sum_{r=0}^{p-1} \sum_{s=1}^{p-1} e\left(\frac{t(r^2 + ars + bs^2)}{p}\right) \right) \\ = \frac{1}{\tau(\bar{\chi})} \sum_{t=1}^{p-1} \bar{\chi}(t) e\left(\frac{ct}{p}\right) \\ \times \left(\sum_{r=0}^{p-1} e\left(\frac{tr^2}{p}\right) + \sum_{r=0}^{p-1} \sum_{s=1}^{p-1} e\left(\frac{ts^2(r^2 + ar + b)}{p}\right) \right) \\ = \frac{1}{\tau(\bar{\chi})} \sum_{t=1}^{p-1} \bar{\chi}(t) e\left(\frac{ct}{p}\right) \\ \times \left(\sum_{r=0}^{p-1} e\left(\frac{tr^2}{p}\right) - p + \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} e\left(\frac{ts^2(r^2 + ar + b)}{p}\right) \right), \end{aligned} \tag{7}$$

where $\tau(\chi) = \sum_{a=1}^{p-1} \chi(a)e(a/p)$ is the classical Gauss sums.

On the other hand, for any integer t with $(t, p) = 1$, we have

$$\begin{aligned} \sum_{r=0}^{p-1} e\left(\frac{tr^2}{p}\right) &= 1 + \sum_{r=1}^{p-1} \left(1 + \left(\frac{r}{p}\right)\right) e\left(\frac{tr}{p}\right) \\ &= \sum_{r=0}^{p-1} e\left(\frac{r}{p}\right) + \sum_{r=1}^{p-1} \left(\frac{r}{p}\right) e\left(\frac{tr}{p}\right) \\ &= \left(\frac{t}{p}\right) \sum_{r=1}^{p-1} \left(\frac{r}{p}\right) e\left(\frac{r}{p}\right) \\ &= \left(\frac{t}{p}\right) \sum_{r=0}^{p-1} e\left(\frac{r^2}{p}\right) \equiv \left(\frac{t}{p}\right) \cdot G(p). \end{aligned} \tag{8}$$

For any integer n with $(n, p) = 1$, from [10] (Section 7.8, Theorem 8.2) we also have

$$\sum_{r=0}^{p-1} \left(\frac{r^2 + n}{p}\right) = -1. \tag{9}$$

Therefore,

$$\begin{aligned} & \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} e\left(\frac{ts^2(r^2 + ar + b)}{p}\right) \\ &= \sum_{r=0}^{p-1} \left(\frac{t(r^2 + ar + b)}{p}\right) \cdot G(p) + p \cdot \sum_{\substack{r=0 \\ r^2+ar+b \equiv 0 \pmod p}}^{p-1} 1 \\ &= \left(\frac{t}{p}\right) \cdot G(p) \cdot \sum_{r=0}^{p-1} \left(\frac{(2r+a)^2 + 4b - a^2}{p}\right) \\ & \quad + p \cdot \sum_{\substack{r=0 \\ (2r+a)^2+4b-a^2 \equiv 0 \pmod p}}^{p-1} 1 \\ &= -\left(\frac{t}{p}\right) \cdot G(p) + \left(1 + \left(\frac{a^2 - 4b}{p}\right)\right) \cdot p. \end{aligned} \tag{10}$$

Then from (7), (8), (9), and (10) we deduce the identity

$$\begin{aligned} & \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} \chi(r^2 + ars + bs^2 + c) \\ &= \frac{1}{\tau(\bar{\chi})} \sum_{t=1}^{p-1} \bar{\chi}(t) e\left(\frac{ct}{p}\right) \left(\left(\frac{t}{p}\right) \cdot G(p) - p - \left(\frac{t}{p}\right) \cdot G(p)\right. \\ & \quad \left. + \left(1 + \left(\frac{a^2 - 4b}{p}\right)\right) \cdot p\right) \\ &= \left(\frac{a^2 - 4b}{p}\right) \cdot p \cdot \frac{1}{\tau(\bar{\chi})} \sum_{t=1}^{p-1} \bar{\chi}(t) e\left(\frac{ct}{p}\right) \\ &= \chi(c) \cdot \left(\frac{a^2 - 4b}{p}\right) \cdot p. \end{aligned} \tag{11}$$

This proves Lemma 4. \square

Lemma 5. Let p be an odd prime and let c be an integer with $(c, p) = 1$. Then one has the identity

$$\begin{aligned} E(c, p) &= \frac{\phi^2(p-1)}{p(p-1)^2} \\ & \quad \times \sum_{\substack{h|p-1 \\ h>1}} \sum_{\substack{u|p-1 \\ u>1}} \frac{\mu(h)}{\phi(h)} \frac{\mu(u)}{\phi(u)} \\ & \quad \times \sum_{s=1}^h \sum_{v=1}^u \chi_{s,h} \chi_{v,u}(-c) \bar{\chi}_{v,u}(-1) \end{aligned}$$

$$\begin{aligned} & \times \tau(\bar{\chi}_{s,h} \bar{\chi}_{v,u}) \cdot \tau(\chi_{s,h}) \cdot \tau(\chi_{v,u}) \\ & \quad - \frac{2 \cdot \phi^2(p-1)}{(p-1)^2} \sum_{\substack{h|p-1 \\ h>1}} \frac{\mu(h)}{\phi(h)} \sum_{\substack{s=1 \\ (h,s)=1}}^h \chi_{s,h}(-c), \end{aligned} \tag{12}$$

where $e((k \text{ ind } y)/h) = \chi_{k,h}(y)$ is the Dirichlet character mod p .

Proof. From the trigonometric identity, the properties of classical Gauss sums, and Lemma 3 we have

$$\begin{aligned} & N(c, p) \\ &= \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \frac{\phi^2(p-1)}{(p-1)^2} \\ & \quad \times \sum_{h|p-1} \sum_{u|p-1} \frac{\mu(h)}{\phi(h)} \frac{\mu(u)}{\phi(u)} \sum_{\substack{s=1 \\ (h,s)=1}}^h \sum_{\substack{v=1 \\ (v,u)=1}}^u \chi_{s,h}(x) \chi_{v,u}(y) \\ & \quad \times \frac{1}{p} \sum_{r=1}^p e\left(\frac{r(x-y-c)}{p}\right) \\ &= \frac{\phi^2(p-1)}{p} + \frac{\phi^2(p-1)}{p(p-1)^2} \\ & \quad \times \sum_{h|p-1} \sum_{u|p-1} \frac{\mu(h)}{\phi(h)} \frac{\mu(u)}{\phi(u)} \sum_{\substack{s=1 \\ (h,s)=1}}^h \sum_{\substack{v=1 \\ (v,u)=1}}^u \sum_{r=1}^{p-1} e\left(\frac{-rc}{p}\right) \\ & \quad \times \left(\sum_{x=1}^{p-1} \chi_{s,h}(x) e\left(\frac{rx}{p}\right)\right) \cdot \left(\sum_{y=1}^{p-1} \chi_{v,u}(y) e\left(\frac{-ry}{p}\right)\right) \\ &= \frac{\phi^2(p-1)}{p} + \frac{\phi^2(p-1)}{p(p-1)^2} \\ & \quad \times \sum_{h|p-1} \sum_{u|p-1} \frac{\mu(h)}{\phi(h)} \frac{\mu(u)}{\phi(u)} \sum_{\substack{s=1 \\ (h,s)=1}}^h \sum_{\substack{v=1 \\ (v,u)=1}}^u \chi_{s,h} \chi_{v,u}(-c) \\ & \quad \times \bar{\chi}_{v,u}(-1) \tau(\bar{\chi}_{s,h} \bar{\chi}_{v,u}) \cdot \tau(\chi_{s,h}) \cdot \tau(\chi_{v,u}) \\ &= \frac{(p-2) \cdot \phi^2(p-1)}{(p-1)^2} - \frac{2 \cdot \phi^2(p-1)}{(p-1)^2} \\ & \quad \times \sum_{\substack{h|p-1 \\ h>1}} \frac{\mu(h)}{\phi(h)} \sum_{\substack{s=1 \\ (h,s)=1}}^h \chi_{s,h}(-c) \\ & \quad + \frac{\phi^2(p-1)}{p(p-1)^2} \sum_{\substack{h|p-1 \\ h>1}} \sum_{\substack{u|p-1 \\ u>1}} \frac{\mu(h)}{\phi(h)} \frac{\mu(u)}{\phi(u)} \end{aligned}$$

$$\begin{aligned} & \times \sum_{\substack{s=1 \\ (h,s)=1}}^h \sum_{\substack{v=1 \\ (v,u)=1}}^u \chi_{s,h} \chi_{v,u}(-c) \\ & \times \bar{\chi}_{v,u}(-1) \tau(\bar{\chi}_{s,h} \bar{\chi}_{v,u}) \cdot \tau(\chi_{s,h}) \cdot \tau(\chi_{v,u}), \end{aligned} \tag{13}$$

where we used the properties $|\tau(\chi)| = \sqrt{p}$, if χ is not a principal character mod p .

From formula (13) and the definition of $E(c, p)$ we may immediately deduce Lemma 5. \square

3. Proof of Theorem 1

In this section, we shall complete the proof of our theorem. First from Lemma 5 and the definition of $E(c, p)$ we have

$$\begin{aligned} & \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} E(x^2 + axy + by^2 + c, p) \\ & = -\frac{2 \cdot \phi^2(p-1)}{(p-1)^2} \sum_{\substack{h|p-1 \\ h>1}} \frac{\mu(h)}{\phi(h)} \sum_{\substack{s=1 \\ (h,s)=1}}^h \chi_{s,h}(-1) \\ & \times \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \chi_{s,h}(x^2 + axy + by^2 + c) \\ & + \frac{\phi^2(p-1)}{p(p-1)^2} \sum_{\substack{h|p-1 \\ h>1}} \sum_{\substack{u|p-1 \\ u>1}} \frac{\mu(h)}{\phi(h)} \frac{\mu(u)}{\phi(u)} \\ & \times \sum_{\substack{s=1 \\ (h,s)=1}}^h \sum_{\substack{v=1 \\ (v,u)=1}}^u \chi_{s,h}(-1) \\ & \times \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \chi_{s,h} \chi_{v,u}(x^2 + axy + by^2 + c) \tau(\bar{\chi}_{s,h} \bar{\chi}_{v,u}) \\ & \cdot \tau(\chi_{s,h}) \cdot \tau(\chi_{v,u}) \\ & \equiv E_1 + E_2, \end{aligned} \tag{14}$$

where E_1 and E_2 denote the corresponding formula, respectively, in the summation.

Now we will estimate E_1 and E_2 in (14), respectively. It is clear that if $h > 1$ and $(s, h) = 1$, then $\chi_{s,h}$ must be a nonprincipal character mod p . So for any integer c with $(c, p) = 1$, from Lemma 4 we have the identity

$$\sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \chi_{s,h}(x^2 + axy + by^2 + c) = \chi_{s,h}(c) \cdot \left(\frac{a^2 - 4b}{p}\right) \cdot p. \tag{15}$$

Therefore, we have

$$\begin{aligned} |E_1| & \leq \frac{2 \cdot \phi^2(p-1)}{(p-1)^2} \sum_{\substack{h|p-1 \\ h>1}} |\mu(h)| \cdot p \\ & = \frac{2p \cdot \phi^2(p-1)}{(p-1)^2} \cdot (2^{\omega(p-1)} - 1). \end{aligned} \tag{16}$$

To estimate E_2 in (14), we write $E_2 = E_{21} + E_{22}$, where E_{21} includes all the characters such that $\chi_{s,h} \chi_{v,u} = \chi_0$, and χ_0 is the principal character mod p ; E_{22} includes all the characters such that $\chi_{s,h} \chi_{v,u} \neq \chi_0$. Now note that if $\chi_{s,h} \chi_{v,u}$ is the principal character mod p , then $h = u$ and $\tau(\bar{\chi}_{s,h} \bar{\chi}_{v,u}) = -1$, $\chi_{s,h}(-1) \tau(\chi_{s,h}) \cdot \tau(\chi_{v,u}) = \tau(\chi_{s,h}) \cdot \tau(\chi_{s,h}) = p$. This time, from identity (9) we have

$$\begin{aligned} & \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \chi_{s,h} \chi_{v,u}(x^2 + axy + by^2 + c) \\ & = p^2 - \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} 1_{x^2+axy+by^2+c \equiv 0 \pmod p} \\ & = p^2 - \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} 1_{(2x+ay)^2 \equiv y^2(a^2-4b)-4c \pmod p} \\ & = p^2 - \sum_{s=0}^{p-1} \left(1 + \left(\frac{s^2(a^2-4b)-4c}{p} \right) \right) \\ & = p^2 - p + \left(\frac{a^2-4b}{p} \right). \end{aligned} \tag{17}$$

So from (17) and Lemma 4 we have

$$\begin{aligned} E_{21} & = -\frac{\phi^2(p-1)}{p(p-1)^2} \\ & \times \sum_{\substack{h|p-1 \\ h>1}} \frac{|\mu(h)|}{\phi(h)} \left(p^2 - p + \left(\frac{a^2-4b}{p} \right) \right) \cdot p \\ & = -\frac{\phi^2(p-1)}{(p-1)^2} \left(p^2 - p + \left(\frac{a^2-4b}{p} \right) \right) \\ & \times \left(\frac{p-1}{\phi(p-1)} - 1 \right). \end{aligned} \tag{18}$$

Applying Lemma 4 and the estimate for Gauss sums we also have the estimate

$$\begin{aligned}
 |E_{22}| &= \frac{\phi^2(p-1)}{p(p-1)^2} \\
 &\quad \times \sum_{\substack{h|p-1 \\ h>1}} \sum_{\substack{u|p-1 \\ u>1}} |\mu(h)| \cdot |\mu(u)| \cdot p \cdot p^{3/2} \\
 &\leq \frac{p^{3/2} \cdot \phi^2(p-1)}{(p-1)^2} \cdot (2^{\omega(p-1)} - 1)^2 \quad (19) \\
 &= \frac{p^{3/2} \cdot \phi^2(p-1)}{(p-1)^2} \\
 &\quad \cdot (4^{\omega(p-1)} - 2 \cdot 2^{\omega(p-1)} + 1).
 \end{aligned}$$

Combining (14), (18), and (19) we may immediately deduce the asymptotic formula

$$\begin{aligned}
 &\sum_{x=0}^{p-1} \sum_{y=0}^{p-1} E(x^2 + axy + by^2 + c, p) \\
 &= -p \cdot \phi(p-1) + \phi^2(p-1) \quad (20) \\
 &\quad + \theta \cdot \frac{p^{3/2} \cdot \phi^2(p-1)}{(p-1)^2} \cdot 4^{\omega(p-1)},
 \end{aligned}$$

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

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to thank the referees for their very helpful and detailed comments, which have significantly improved the presentation of this paper. This work is supported by the N. S. F. (11371291, 61202437) of China.

References

[1] S. D. Cohen and W. Zhang, "Sums of two exact powers," *Finite Fields and their Applications*, vol. 8, no. 4, pp. 471–477, 2002.

[2] S. D. Cohen and G. L. Mullen, "Primitive elements in Costas arrays," *Applicable Algebra in Engineering, Communication and Computing*, vol. 2, pp. 45–53, 1991, erratum: vol. 2 pp. 297–299, 1992.

[3] S. W. Golomb, "Algebraic constructions for Costas arrays," *Journal of Combinatorial Theory A*, vol. 37, no. 1, pp. 13–21, 1984.

[4] O. Moreno and J. Sotero, "Computational approach to conjecture A of Golomb," *Congressus Numerantium*, vol. 70, pp. 7–16, 1990.

[5] W. Zhang, "On a problem related to Golomb's conjectures," *Journal of Systems Science and Complexity*, vol. 16, no. 1, pp. 13–18, 2003.

[6] P. Wang, X. Cao, and R. Feng, "On the existence of some specific elements in finite fields of characteristic 2," *Finite Fields and their Applications*, vol. 18, no. 4, pp. 800–813, 2012.

[7] T. Tian and W. F. Qi, "Primitive normal element and its inverse in finite fields," *Acta Mathematica Sinica*, vol. 49, no. 3, pp. 657–668, 2006.

[8] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, NY, USA, 1976.

[9] W. Narkiewicz, *Classical Problems in Number Theory*, vol. 62, Państwowe Wydawnictwo Naukowe (PWN), Warsaw, Poland, 1986.

[10] L. K. Hua, *Introduction to Number Theory*, Science Press, Beijing, China, 1979.