AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 5(4): 3899–3905.
DOI:10.3934/math.2020252
Received: 10 March 2020
Accepted: 20 April 2020
Published: 26 April 2020

Research article

The primitive roots and a problem related to the Golomb conjecture

Wenpeng Zhang[1] **and Tingting Wang**[2,*]

[1] School of Mathematics, Northwest University, Xi'an, Shaanxi, P. R. China
[2] College of Science, Northwest A&F University, Yangling, Shaanxi, P. R. China

* **Correspondence:** Email: ttwang@nwafu.edu.cn.

Abstract: In this paper, we use elementary methods, properties of Gauss sums and estimates for character sums to study a problem related to primitive roots, and prove the following result. Let p be a large enough odd prime. Then for any two distinct integers $a, b \in \{1, 2, \cdots, p-1\}$, there exist three primitive roots α, β and γ modulo p such that the congruence equations $\alpha + \gamma \equiv a \bmod p$ and $\beta + \gamma \equiv b \bmod p$ hold.

Keywords: primitive roots; the Golomb conjecture; character sums; Gauss sums; asymptotic formula
Mathematics Subject Classification: 11A07, 11D85

1. Introduction

Let p be an odd prime, $\mathbf{A}(p)$ denotes the set of all primitive roots g modulo p with $1 \le g \le p-1$. The Golomb conjecture (see [1]) in a reduced residue system modulo p is whether there exist two primitive roots α and $\beta \in \mathbf{A}(p)$ such that the congruence

$$\alpha + \beta \equiv 1 \bmod p \text{ holds ?} \tag{1.1}$$

This conjecture has been basically solved in the finite field $\mathbb{F}_q$. Interested readers can refer to the references [2–13]. In fact, people have proved versions of the above result. Here, we simply describe one of them as follows: Let p be an odd prime large enough. Then for any integers a, b and c with abc coprime to p (i.e., $(abc, p) = 1$), there are at least two primitive roots α and β mod p such that the congruence $a\alpha + b\beta \equiv c \bmod p$ holds. See Qi Sun [3].

In this paper, we continue to work on this problem, because we find that the Golomb conjecture can be further strengthened. To make our problem more general, we will describe it in a finite field. Let $\mathbb{F}_q$ be a finite field of q elements with characteristic p. Our problem in $\mathbb{F}_q$ can be summarized as follows:

For any two non-zero elements $a \neq b \in \mathbb{F}_q$, do there exist three primitive elements α, β and $\gamma \in \mathbb{F}_q$ such that the equations $\alpha + \gamma = a$ and $\beta + \gamma = b$ hold?

Obviously, if this problem is correct, then the Golomb conjecture must be true. The converse is not necessarily true. So, our problem can be seen as a further generalization and extension of the Golomb conjecture.

In this paper, we use elementary methods, properties of Gauss sums and estimates for character sums to give an affirmative answer to the above problem. To better describe our results, we use the counting function $N(\alpha,\beta;p)$, which denotes the number of all primitive roots u, v and $w \in \mathbf{A}(p)$ such that the equations $u+w \equiv \alpha \bmod p$ and $v+w \equiv \beta \bmod p$ hold. Then we have the following result:

Theorem. Let p be an odd prime. Then for any integers $1 \le \alpha \ne \beta \le p-1$, we have the asymptotic formula

$$N(\alpha,\beta;p) = \frac{\phi^3(p-1)}{p^2} + O\left(\frac{\phi^3(p-1)}{p^2\cdot\sqrt{p}}\cdot 8^{\omega(p-1)}\right),$$

where as usual, $\phi(n)$ denotes the Euler function, and $\omega(n)$ denotes the number of all distinct prime divisors of n.

Obviously, our conclusion can also be generalized to the finite field $\mathbb{F}_q$. From our theorem we may immediately deduce the following:

Corollary. Let p be an odd prime large enough. Then for any integers $1 \le a \ne b \le p-1$, there exist three primitive roots α, β and $\gamma \bmod p$ such that the congruence equations

$$\alpha+\gamma \equiv a \bmod p \quad \text{and} \quad \beta+\gamma \equiv b \bmod p \ \text{ hold.}$$

Obviously one can ask: Can the Golomb conjecture be extended further? Specifically, for three pairwise distinct nonzero elements α, β and $\gamma \in \mathbb{F}_q$, do there exist four primitive elements a, b, c and $d \in \mathbb{F}_q$ such that the equations

$$a+d=\alpha, \ \ b+d=\beta \ \text{ and } \ c+d=\gamma \ \text{ are satisfied ?}$$

We leave this as an open problem.

2. Several lemmas

To complete the proof of our main result, we need following three simple lemmas. For the sake of simplicity, we do not repeat some elementary number theory and analytic number theory results, which can be found in references [14] and [15]. First, we have the following:

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

$$\frac{\phi(p-1)}{p-1}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{r=1}^{k}{}' e\left(\frac{r\cdot \mathrm{ind}(a)}{k}\right) = \begin{cases} 1 & \text{if } a \text{ is a primitive root mod } p;\\ 0 & \text{if } a \text{ is not a primitive root mod } p,\end{cases}$$

where $e(y)=e^{2\pi iy}$, $\sum_{r=1}^{k}{}'$ denotes the summation over all integers $1 \le r \le k$ such that r is coprime to k, $\mu(n)$ is the Möbius function, and $\mathrm{ind}(a)$ denotes the index of a relative to some fixed primitive root $g \bmod p$.

Proof. See Proposition 2.2 in [16].

Lemma 2. Let p be a prime. Then for any integer h with $(h, p) = 1$, we have the identity

$$\sum_{a\in\mathbf{A}(p)} e\left(\frac{ha}{p}\right) = \frac{\phi(p-1)}{p-1}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{r=1}^{k}{}'\overline{\chi}_{r,k}(h)\cdot\tau\left(\chi_{r,k}\right),$$

where χ denotes a Dirichlet character modulo p, and $\tau(\chi) = \sum_{a=1}^{p-1}\chi(a)e\left(\frac{a}{p}\right)$ denotes the classical Gauss sums corresponding to χ.

Proof. For integers $1 \le r \le k \le p-1$ with $k \mid p-1$ and $(r, k) = 1$, we write $e\left(\frac{r\cdot\mathrm{ind}(a)}{k}\right) = \chi_{r,k}(a)$, and $\chi_{r,k}(a) = 0$, if $p \mid a$. It is clear that $\chi_{r,k}(a)$ is a Dirichlet character modulo p. Note that by the properties of the classical Gauss sums we have

$$\sum_{a=1}^{p-1}\chi(a)e\left(\frac{ha}{p}\right) = \overline{\chi}(h)\sum_{a=1}^{p-1}\chi(a)e\left(\frac{a}{p}\right) = \overline{\chi}(h)\cdot\tau(\chi).$$

Applying the above with $\chi := \chi_{r,k}$ and using Lemma 1, we immediately deduce the identity

$$\begin{aligned}\sum_{a\in\mathbf{A}(p)} e\left(\frac{ha}{p}\right) &= \frac{\phi(p-1)}{p-1}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{r=1}^{k}{}'\sum_{a=1}^{p-1}\chi_{r,k}(a)\,e\left(\frac{ha}{p}\right)\\ &= \frac{\phi(p-1)}{p-1}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{r=1}^{k}{}'\overline{\chi}_{r,k}(h)\cdot\tau\left(\chi_{r,k}\right).\end{aligned}$$

This proves Lemma 2.

Lemma 3. Let p be an odd prime, χ_1, ..., χ_r be Dirichlet characters modulo p, at least one of which is non-principal character. Let $f(x)$ be an integral coefficient polynomial of degree d. Then for pairwise distinct integers $a_1, ..., a_r$, we have the estimate

$$\sum_{a=1}^{p-1}\chi_1(a+a_1)\chi_2(a+a_2)\cdots\chi_r(a+a_r)\,e\left(\frac{f(a)}{p}\right) \le (r+d)\cdot p^{\frac{1}{2}}.$$

Proof. This is Lemma 17 in [17]. Some related work can also be found in [18].

Lemma 4. Let p be a prime. Then for any integer d with $(d, p) = 1$, we have the estimate

$$\sum_{u=1}^{p-1} e\left(\frac{-ud}{p}\right)\sum_{a\in\mathbf{A}(p)} e\left(\frac{ua}{p}\right)\sum_{c\in\mathbf{A}(p)} e\left(\frac{uc}{p}\right) = O\left(\frac{\phi^2(p-1)}{\sqrt{p}}\cdot 4^{\omega(p-1)}\right).$$

Proof. Note that $|\tau(\chi)| = \sqrt{p}$, if χ is any non-principal character modulo p, and $|\tau(\chi)| = 1$, if χ is the principal character modulo p. From the identity

$$\sum_{k|p-1}|\mu(k)| = \prod_{q^\alpha\|p-1}\left(\sum_{d|q^\alpha}|\mu(d)|\right) = \prod_{q^\alpha\|p-1}2 = 2^{\omega(p-1)}$$

and Lemma 2, we have

$$\begin{aligned}
&\sum_{u=1}^{p-1} e\left(\frac{-ud}{p}\right) \sum_{a\in\mathbf{A}(p)} e\left(\frac{ua}{p}\right) \sum_{c\in\mathbf{A}(p)} e\left(\frac{uc}{p}\right)\\
=\ & \frac{\phi^2(p-1)}{(p-1)^2} \sum_{u=1}^{p-1} e\left(\frac{-ud}{p}\right) \sum_{k|p-1} \sum_{h|p-1} \frac{\mu(k)\mu(h)}{\phi(k)\phi(h)} \sum_{r=1}^{k}{}' \overline{\chi}_{r,k}(u)\cdot\tau(\chi_{r,k})\\
&\times \sum_{s=1}^{h}{}' \overline{\chi}_{s,h}(u)\cdot\tau(\chi_{s,h})\\
=\ & \frac{\phi^2(p-1)}{(p-1)^2} \sum_{k|p-1} \sum_{h|p-1} \frac{\mu(k)\mu(h)}{\phi(k)\phi(h)} \sum_{r=1}^{k}{}' \sum_{s=1}^{h}{}' \tau(\chi_{r,k})\tau(\chi_{s,h})\\
&\times \sum_{u=1}^{p-1} \overline{\chi}_{r,k}(u)\overline{\chi}_{s,h}(u) e\left(\frac{-ud}{p}\right)\\
=\ & \frac{\phi^2(p-1)}{(p-1)^2} \sum_{k|p-1} \sum_{h|p-1} \frac{\mu(k)\mu(h)}{\phi(k)\phi(h)} \sum_{r=1}^{k}{}' \sum_{s=1}^{h}{}' \chi_{r,k}(-d)\chi_{s,h}(-d)\\
&\times\tau(\chi_{r,k})\tau(\chi_{s,h})\tau\left(\overline{\chi}_{r,k}\overline{\chi}_{s,h}\right)\\
=\ & O\left(\frac{\phi^2(p-1)}{(p-1)^2}\cdot p^{\frac{3}{2}}\cdot\left(\sum_{k|p-1}|\mu(k)|\right)^2\right) = O\left(\frac{\phi^2(p-1)}{\sqrt{p}}\cdot 4^{\omega(p-1)}\right).
\end{aligned}$$

This proves Lemma 4.

Lemma 5. Let p be a prime. Then for any integers $1 \le \alpha \ne \beta \le p-1$, we have the estimate

$$\begin{aligned}
&\sum_{u=1}^{p-1}\sum_{v=1}^{p-1} e\left(\frac{-u\alpha - v\beta}{p}\right) \sum_{a\in\mathbf{A}(p)} e\left(\frac{ua}{p}\right) \sum_{b\in\mathbf{A}(p)} e\left(\frac{vb}{p}\right) \sum_{c\in\mathbf{A}(p)} e\left(\frac{(u+v)c}{p}\right)\\
=\ & O\left(\frac{\phi^3(p-1)}{\sqrt{p}}\cdot 8^{\omega(p-1)}\right).
\end{aligned}$$

Proof. Note that $|\tau(\chi)| = 1$, if χ is the principal character modulo p. And if $(v,p) = 1$, u pass through a reduced residue system modulo p, then uv also pass through a reduced residue system modulo p. So from Lemma 2, Lemma 3 and the methods of proving Lemma 4 we have

$$\begin{aligned}
&\sum_{u=1}^{p-1}\sum_{v=1}^{p-1} e\left(\frac{-u\alpha - v\beta}{p}\right) \sum_{a\in\mathbf{A}(p)} e\left(\frac{ua}{p}\right) \sum_{b\in\mathbf{A}(p)} e\left(\frac{vb}{p}\right) \sum_{c\in\mathbf{A}(p)} e\left(\frac{(u+v)c}{p}\right)\\
=\ & \frac{\phi^3(p-1)}{(p-1)^3} \sum_{u=1}^{p-1} e\left(\frac{-u\alpha}{p}\right) \sum_{v=1}^{p-1} e\left(\frac{-v\beta}{p}\right)\\
&\times \sum_{k|p-1} \frac{\mu(k)}{\phi(k)} \sum_{r=1}^{k}{}' \sum_{h|p-1} \frac{\mu(h)}{\phi(h)} \sum_{s=1}^{h}{}' \sum_{j|p-1} \frac{\mu(j)}{\phi(j)} \sum_{t=1}^{j}{}' \overline{\chi}_{r,k}(u)\cdot\tau(\chi_{r,k})\\
&\times\overline{\chi}_{s,h}(v)\cdot\tau(\chi_{s,h})\overline{\chi}_{t,j}(u+v)\cdot\tau\left(\chi_{t,j}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{\phi^3(p-1)}{(p-1)^3}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{r=1}^{k}{}^{'}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{s=1}^{h}{}^{'}\sum_{j|p-1}\frac{\mu(j)}{\phi(j)}\sum_{t=1}^{j}{}^{'}\\
&\quad\times\tau\left(\chi_{r,k}\right)\tau\left(\chi_{s,h}\right)\tau\left(\chi_{t,j}\right)\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}\overline{\chi}_{r,k}(u)\overline{\chi}_{s,h}(v)\overline{\chi}_{t,j}(u+v)e\left(\frac{-u\alpha-v\beta}{p}\right)\\
&= \frac{\phi^3(p-1)}{(p-1)^3}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{r=1}^{k}{}^{'}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{s=1}^{h}{}^{'}\sum_{j|p-1}\frac{\mu(j)}{\phi(j)}\sum_{t=1}^{j}{}^{'}\\
&\quad\times\tau\left(\chi_{r,k}\right)\tau\left(\chi_{s,h}\right)\tau\left(\chi_{t,j}\right)\sum_{u=1}^{p-1}\overline{\chi}_{r,k}(u)\overline{\chi}_{t,j}(u+1)\\
&\quad\times\sum_{v=1}^{p-1}\overline{\chi}_{s,h}(v)\overline{\chi}_{r,k}(v)\overline{\chi}_{t,j}(v)e\left(\frac{-v(u\alpha+\beta)}{p}\right)\\
&= \frac{\phi^3(p-1)}{(p-1)^3}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{r=1}^{k}{}^{'}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{s=1}^{h}{}^{'}\sum_{j|p-1}\frac{\mu(j)}{\phi(j)}\sum_{t=1}^{j}{}^{'}\\
&\quad\times\tau\left(\chi_{r,k}\right)\tau\left(\chi_{s,h}\right)\tau\left(\chi_{t,j}\right)\tau\left(\overline{\chi}_{r,k}\overline{\chi}_{s,h}\overline{\chi}_{t,j}\right)\sum_{u=1}^{p-1}\overline{\chi}_{r,k}(u)\overline{\chi}_{t,j}(u+1)\\
&\quad\times\chi_{s,h}\chi_{r,k}\chi_{t,j}\left(-u\alpha-\beta\right)\\
&= O\left(\frac{\phi^3(p-1)}{p^3}\cdot p^{\frac{5}{2}}\cdot\left(\sum_{k|p-1}|\mu(k)|\right)^3\right)=O\left(\frac{\phi^3(p-1)}{\sqrt{p}}\cdot 8^{\omega(p-1)}\right).
\end{aligned}
$$

This proves Lemma 5.

3. Proof of the theorem

In this section, we shall complete the proof of our main result. For any integers $1\le\alpha\ne\beta\le p-1$, note that the trigonometric identity

$$\sum_{r=0}^{p-1}e\left(\frac{nr}{p}\right)=\begin{cases}p, & \text{if } p\mid n;\\ 0, & \text{if } p\nmid n\end{cases}$$

and

$$\sum_{a\in\mathbf{A}(p)}1=\phi(p-1).$$

Thus, from Lemma 4 and Lemma 5 we have

$$
\begin{aligned}
N(\alpha,\beta;p)&=\frac{1}{p^2}\sum_{a\in\mathbf{A}(p)}\sum_{b\in\mathbf{A}(p)}\sum_{c\in\mathbf{A}(p)}\sum_{u=0}^{p-1}e\left(\frac{u(a+c-\alpha)}{p}\right)\sum_{v=0}^{p-1}e\left(\frac{v(b+c-\beta)}{p}\right)\\
&=\frac{1}{p^2}\sum_{u=1}^{p-1}e\left(\frac{-u\alpha}{p}\right)\sum_{v=1}^{p-1}e\left(\frac{-v\beta}{p}\right)\sum_{a\in\mathbf{A}(p)}e\left(\frac{ua}{p}\right)\sum_{b\in\mathbf{A}(p)}e\left(\frac{vb}{p}\right)
\end{aligned}
$$

$$\times \sum_{c\in\mathbf{A}(p)} e\left(\frac{(u+v)c}{p}\right) + \frac{1}{p^2}\sum_{u=1}^{p-1} e\left(\frac{-u\alpha}{p}\right)\sum_{a\in\mathbf{A}(p)} e\left(\frac{ua}{p}\right)\sum_{c\in\mathbf{A}(p)} e\left(\frac{uc}{p}\right)$$
$$+\frac{1}{p^2}\sum_{v=1}^{p-1} e\left(\frac{-v\beta}{p}\right)\sum_{b\in\mathbf{A}(p)} e\left(\frac{vb}{p}\right)\sum_{c\in\mathbf{A}(p)} e\left(\frac{vc}{p}\right) + \frac{\phi^3(p-1)}{p^2}$$
$$= \frac{\phi^3(p-1)}{p^2} + O\left(\frac{\phi^3(p-1)}{p^2\cdot\sqrt{p}}\cdot 8^{\omega(p-1)}\right) + O\left(\frac{\phi^2(p-1)}{p^2\cdot\sqrt{p}}\cdot 4^{\omega(p-1)}\right)$$
$$= \frac{\phi^3(p-1)}{p^2} + O\left(\frac{\phi^3(p-1)}{p^{\frac{5}{2}}}\cdot 8^{\omega(p-1)}\right).$$

This completes the proof of our theorem.

4. Conclusion

The main result of this paper is a theorem, which is closely related to the Golomb conjecture. It describes that when the prime p is large enough, for any integers $1 \le \alpha \ne \beta \le p-1$, there exist three primitive roots u, v and $w \in \mathbf{A}(p)$ such that the congruence equations $u + w \equiv \alpha \bmod p$ and $v + w \equiv \beta \bmod p$ hold. At the same time, we also give a sharp asymptotic formula for the counting function of all such solutions (u, v, w). Of course, our conclusion can also be generalized to the finite field $\mathbb{F}_q$. In order to further study the content related to the Golomb conjecture, we also proposed an open problem.

Acknowledgments

The authors would like to thank the referee for their very helpful and detailed comments. In particular, many English grammar and error correction, so that the text reads more smoothly.

This work is supported by the Y. S. T. N. S. P (2019KJXX-076), the N. S. B. R. P. (2019JM-207) of Shaanxi Province and the N. S. F. (11771351) of P. R. China.

Conflict of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. S. W. Golomb, *Algebraic constructions for costas arrays*, J. Comb. Theory Ser. A, **37** (1984), 13–21.
2. L. Qi, W. P. Zhang, *On the generalization of Golomb's conjecture*, Journal of Northwest University, Natural Science Edition, **45** (2015), 199–201.
3. Q. Sun, *On primitive roots in a finite field*, Journal of Sichuan University, Natural Science Edition, **25** (1988), 133–139.
4. T. Tian, W. Qi, *Primitive normal element and its inverse in finite fields*, Acta Math. Sin., **49** (2006), 657–668.

5. P. Wang, X. Cao, R. Feng, *On the existence of some specific elements in finite fields of characteristic 2*, Finite Fields Th. App., **18** (2012), 800–813.
6. J. P. Wang, *On Golomb's conjecture*, Sci. China Ser. A, **31** (1988), 152–161.
7. T. T. Wang, X. N. Wang, *On the Golomb's conjecture and Lehmer's numbers*, Open Math., **15** (2017), 1003–1009.
8. W. Q. Wang, W. P. Zhang, *A mean aalue related to primitive roots and Golomb's conjectures*, Abstr. Appl. Anal., **2014** (2014), 1–5.
9. W. P. Zhang, *On a problem related to Golomb's conjectures*, J. Syst. Sci. Complex., **16** (2003), 13–18.
10. S. D. Cohen, W. P. Zhang, *Sums of two exact powers*, Finite Fields Th. App., **8** (2002), 471–477.
11. S. D. Cohen, *Pairs of primitive roots*, Mathematica, **32** (1985), 276–285.
12. S. D. Cohen, T. Trudgian, *Lehmer numbers and primitive roots modulo a prime*, J. Number Theory, **203** (2019), 68–79.
13. R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, 1981.
14. W. P. Zhang, H. L. Li, *Elementary Number Theory*, Shaanxi Normal University Press, Xi'an, 2013.
15. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
16. W. Narkiewicz, *Classical Problems in Number Theory*, Polish Scientifc Publishers, Warszawa, 1987.
17. J. Bourgain, Z. M. Garaev, V. S. Konyagin, *On the hidden shifted power problem*, SIAM J. Comput., **41** (2012), 1524–1557.
18. K. Gong, C. H. Jia, *Shifted character sums with multiplicative coefficients*, J. Number Theory, **153** (2015), 364–371.

AIMS Press