Hindawi
Journal of Mathematics
Volume 2021, Article ID 7639259, 4 pages
https://doi.org/10.1155/2021/7639259

Research Article

A Note on the Primitive Roots and the Golomb Conjecture

Yiwei Hou[1] **and Hongyan Wang**[2]

[1] *School of Big Data Science, Hebei Science and Technology Finance Key Laboratory, Hebei Finance University, Baoding, Hebei, China*
[2] *School of Big Data Science, Hebei Finance University, Baoding, Hebei, China*

Correspondence should be addressed to Yiwei Hou; hyiwei1983@126.com

Received 14 July 2021; Accepted 24 July 2021; Published 31 July 2021

Academic Editor: Wenpeng Zhang

In this paper, we use the elementary methods and the estimates for character sums to prove the following conclusion. Let p be a prime large enough. Then, for any positive integer n with $p^{(1/2)+\varepsilon} \leq n < p$, there must exist two primitive roots α and β modulo p with $1 < \alpha, \beta \leq n-1$ such that the equation $n = \alpha + \beta$ holds, where $0 < \varepsilon < (1/2)$ is a fixed positive number. In other words, n can be expressed as the exact sum of two primitive roots modulo p.

1. Introduction

Let p be a prime and $\mathbb{F}_q$ be a finite field of $q\ (= p^h, h \geq 1)$ elements with characteristic p. The Golomb conjecture (see [1]) can be summarized as follows: for any nonzero element $c \in \mathbb{F}_q$, there exist two primitive elements α and $\beta \in \mathbb{F}_q$ such that the equation $\alpha + \beta = c$ holds.

If we assume that $\mathbf{A}(p)$ denotes the set of all primitive roots g modulo p with $1 \leq g \leq p-1$, then the Golomb conjecture in a reduced residue system modulo p can be described as that, for any integer $1 \leq n \leq p-1$, there exist two primitive roots α and $\beta \in \mathbf{A}(p)$ such that the congruence $\alpha + \beta \equiv n \bmod p$ holds.

This conjecture is not only basically solved but also carried on various generalizations. Interested readers can refer to the references [2–11]. For example, let p be an odd prime large enough. Then, for any integers a, b, and c with $(abc, p) = 1$, there are at least two primitive roots α and $\beta \bmod p$ such that the congruence $a\alpha + b\beta \equiv c \bmod p$ holds (see Sun [2]).

It is clear that if integer $1 < n < p$ and the primitive roots $1 < \alpha, \beta \leq p-1$ satisfy the congruence $\alpha + \beta \equiv n \bmod p$, then $\alpha + \beta = n$ or $\alpha + \beta = n + p$.

A natural question is whether for a fixed $1 < n < p$, there are two primitive roots $1 < \alpha, \beta \leq n-1$ of p such that

$$\alpha + \beta = n?. \tag{1}$$

Of course, for some positive integers n, equation (1) has no solutions. For example, $n = 1$, $n = 2$ and 3. So, we think that the problem in (1) is meaningful, and it is also closely related to the minimum primitive root modulo p.

On the other hand, we also want to know how large n is (relative to p), so that equation (1) must have a solution.

For the sake of convenience, for any odd prime p and integer $1 < n \leq p-1$, let $S(n; p)$ denote the number of all solutions of the equation $\alpha + \beta = n$, where α and β are two primitive roots modulo p with $1 < \alpha, \beta \leq n-1$.

In this paper, we shall use the elementary methods and the estimates for character sums to study the asymptotic properties of $S(n; p)$ and prove the following.

Theorem 1. *Let p be an odd prime. Then, for any integer $1 < n \leq p-1$, we have the asymptotic formula:*

$$S(n; p) = \frac{\phi^2(p-1)}{p^2} \cdot n + O\left(\frac{\phi^2(p-1)}{p^{(3/2)}} \cdot 4^{\omega(p-1)} \cdot \ln p\right), \tag{2}$$

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

It is clear that, for any positive number $0 < \varepsilon < (1/2)$, if prime p is large enough, then our theorem is nontrivial for all integers $p^{(1/2)+\varepsilon} \leq n \leq p-1$. That is, the main term is much big than the error term in our theorem. So, from our theorem, we may immediately deduce the following:

Corollary 1. *Let p be an odd prime large enough, $0 < \varepsilon < (1/2)$ be a fixed positive number. Then, for any positive integer n with $p^{(1/2)+\varepsilon} \leq n \leq p-1$, there must exist two primitive roots α and β modulo p such that*

$$\alpha + \beta = n. \tag{3}$$

Note: first, the conclusion in our theorem can also be generalized. That is, let p be an odd prime and k be a fixed positive integer. For any integers $1 < n_1 < n_2 < n_3 < \cdots < n_k < p$, if $S(n_1, n_2, \ldots, n_k; p)$ denotes the number of all solutions of the equations $n_1 = \alpha + \beta_1$, $n_2 = \alpha + \beta_2, \ldots$, $n_k = \alpha + \beta_k$, where α and all β_i $(i = 1, 2, \ldots, k)$ are the primitive roots modulo p, then we have the following asymptotic formula:

$$S(n_1, n_2, \ldots, n_k; p) = \frac{\phi^{k+1}(p-1)}{p^{k+1}} \cdot n_1 + O\left(\frac{\phi^{k+1}(p-1)}{p^{k+(1/2)}} \cdot 2^{(k+1)\omega(p-1)} \cdot \ln p\right). \tag{4}$$

If $0 < \varepsilon < (1/2)$ and $p^{(1/2)+\varepsilon} < n_1 < p$, then this asymptotic formula is nontrivial.

Second, the lower bound $p^{(1/2)+\varepsilon}$ of n in our corollary is very rough. How to improve the constant $(1/2)$ is an interesting open problem.

Conjecture 1. *Let $0 < \delta < 1$ be a fixed positive number and p be a prime large enough. Then, for any positive integer $p^{\delta} < n < p$, there must exist two primitive roots α and β modulo p such that the equation $\alpha + \beta = n$ holds.*

2. Several Lemmas

In order to complete the proof of the main result, we need several 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 [12–14]. 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*

$$\frac{\phi(p-1)}{p-1} \sum_{k \mid p-1} \frac{\mu(k)}{\phi(k)} \sum_{r=1}^{k}{}' e\left(\frac{r \cdot \operatorname{ind}(a)}{k}\right) = \begin{cases} 1, & \text{if } a \text{ is a primitive root mod } p, \\ 0, & \text{if } a \text{ is not a primitive root mod } p, \end{cases} \tag{5}$$

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

Proof. See Proposition 2.2 in [13]. □

Lemma 2. *Let p be an odd prime and $\chi_1, \ldots, \chi_r$ be Dirichlet characters modulo p, at least one of which is nonprincipal character. Let $f(x)$ be an integral coefficient polynomial of degree d. Then, for pairwise distinct integers $a_1, \ldots, a_r$, we have the estimate*

$$\sum_{a=1}^{p-1} \chi_1(a + a_1)\chi_2(a + a_2) \ldots \chi_r(a + a_r) e\left(\frac{f(a)}{p}\right) \leq (r + d) \cdot p^{(1/2)}. \tag{6}$$

Proof. In fact, this result is Lemma 17 in [15]. Some related works can also be found in [16–19]. □

Lemma 3. *Let p be an odd prime. Then, for any integer $1 < n < p$ and any two Dirichlet characters χ_1 and χ_2 (at least one of which is nonprincipal character) modulo p, we have the estimate*

$$\sum_{a=1}^{n-1} \chi_1(a)\chi_2(n-a) \ll p^{(1/2)} \cdot \ln p. \tag{7}$$

Proof. It is clear that, for any integer m, we have the trigonometric identity

$$\sum_{r=0}^{p-1} e\left(\frac{mr}{p}\right) = \begin{cases} p, & \text{if } p \mid m, \\ 0, & \text{if } p \nmid m, \end{cases} \tag{8}$$

and the estimate

$$\left|\sum_{b=1}^{n-1} e\left(\frac{-rb}{p}\right)\right| \ll \frac{1}{|\sin(\pi r/p)|} \ll \frac{p}{r}. \tag{9}$$

From (8), (9), and Lemma 2, we have

$$\begin{aligned}\sum_{a=1}^{n-1}\chi_1(a)\chi_2(n-a) &= \frac{1}{p}\sum_{a=1}^{p-1}\sum_{b=1}^{n-1}\chi_1(a)\chi_2(n-a)\sum_{r=0}^{p-1} e\left(\frac{r(a-b)}{p}\right)\\ &= \frac{1}{p}\sum_{r=1}^{p-1}\left(\sum_{a=1}^{p-1}\chi_1(a)\chi_2(n-a)e\left(\frac{ra}{p}\right)\right)\left(\sum_{b=1}^{n-1} e\left(\frac{-rb}{p}\right)\right) + \frac{n-1}{p}\sum_{a=1}^{p-1}\chi_1(a)\chi_2(n-a)\\ &\ll \frac{\sqrt{p}}{p}\cdot\sum_{r=1}^{p-1}\frac{p}{r} + \frac{n-1}{p}\cdot\sqrt{p} \ll p^{(1/2)}\cdot\ \ln p.\end{aligned} \tag{10}$$

This proves Lemma 3. □

3. Proof of the Theorem

Now, we shall complete the proof of our main result. For any integer $1 < n \le p-1$, from the definition of $S(n,p)$ and Lemma 1, we have

$$S(n,p) = \frac{\phi^2(p-1)}{(p-1)^2}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}{\sum_{r=1}^{k}}'\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}{\sum_{s=1}^{h}}'\times\sum_{a=1}^{n-1} e\left(\frac{r\cdot \mathrm{ind}(a)}{k}\right)\cdot e\left(\frac{s\cdot \mathrm{ind}(n-a)}{h}\right). \tag{11}$$

It is clear that $\chi_{t,k}(a) = e(t\cdot \mathrm{ind}(a)/k)$ is a Dirichlet character modulo p. So, from the Polya and Vinogradov's classical work (see [12]; Theorem 8.21 and Theorem 13.15), we have the estimate

$$\sum_{a=1}^{n-1}\chi(a) \ll p^{(1/2)}\ln p, \tag{12}$$

where χ is any nonprincipal character modulo p.

Now, from (11), (12), and Lemma 3, we have

$$\begin{aligned} S(n;p) &= \frac{\phi^2(p-1)}{(p-1)^2}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}{\sum_{r=1}^{k}}'\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}{\sum_{s=1}^{h}}'\sum_{a=1}^{n-1}\chi_{r,k}(a)\chi_{s,h}(n-a)\\ &= \frac{\phi^2(p-1)}{(p-1)^2}\sum_{a=1}^{n-1}1 + \frac{\phi^2(p-1)}{(p-1)^2}\sum_{\substack{k|p-1\\ k>1}}\frac{\mu(k)}{\phi(k)}{\sum_{r=1}^{k}}'\sum_{a=1}^{n-1}\chi_{r,k}(a)\\ &\quad + \frac{\phi^2(p-1)}{(p-1)^2}\sum_{\substack{k|p-1\\ k>1}}\frac{\mu(k)}{\phi(k)}{\sum_{r=1}^{k}}'\sum_{\substack{h|p-1\\ h>1}}\frac{\mu(h)}{\phi(h)}{\sum_{s=1}^{h}}'\sum_{a=1}^{n-1}\chi_{r,k}(a)\chi_{s,h}(n-a)\\ &\quad + \frac{\phi^2(p-1)}{(p-1)^2}\sum_{\substack{h|p-1\\ h>1}}\frac{\mu(h)}{\phi(h)}{\sum_{s=1}^{h}}'\sum_{a=1}^{n-1}\chi_{s,h}(n-a)\\ &= \frac{\phi^2(p-1)}{(p-1)^2}\cdot(n-1) + O\left(\frac{\phi^2(p-1)}{p^{(3/2)}}.\sum_{k|(p-1)}|\mu(k)|\right)\\ &\quad + O\left(\frac{\phi^2(p-1)}{p^{(3/2)}}.\sum_{k|(p-1)}|\mu(k)|.\sum_{h|(p-1)}|\mu(h)|.\ \ln p\right)\\ &= \frac{\phi^2(p-1)}{p^2}\cdot n + O\left(\frac{\phi^2(p-1)}{p^{(3/2)}}\cdot 4^{\omega(p-1)}\cdot\ \ln p\right),\end{aligned} \tag{13}$$

where we have used the identity

$$\sum_{k|m} |\mu(k)| = \prod_{p^{\alpha} m} (1 + |\mu(p)|) = 2^{\omega(m)}, \tag{14}$$

and $\omega(m)$ denotes the number of all distinct prime divisors of m.

This completes the proof of our theorem.

4. Conclusion

The main result in this paper is a theorem, which is closely related to Golomb's conjecture. It describes that when prime p is large enough, for any integer $p^{(1/2)+\varepsilon} \leq n \leq p - 1$, there must exist two primitive roots α and β modulo p such that the equation $n = \alpha + \beta$ holds, where $0 < \varepsilon < (1/2)$ be a fixed positive number. At the same time, we also give a sharp asymptotic formula for the counting function of all such solutions (α, β). In fact, our conclusion is much stronger than Golomb's conjecture in the reduced residue system $\{1, 2, 3, \ldots, p - 1\}$ modulo p. As a note of the corollary, we also proposed an open problem.

Data Availability

No data were used to support this study.

Conflicts of Interest

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

Authors' Contributions

All authors have equally contributed to this work. All authors read and approved the final manuscript.

Acknowledgments

This work was supported by the NSF of P. R. China (no. 11771351) and the Natural Science Foundation of Hebei Province (no. A2015410006).

References

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

[2] Q. Sun, "On primitive roots in a finite field," *Journal of Sichuan University, Natural Science Edition*, vol. 25, pp. 133–139, 1988.

[3] W. Zhang and T. Wang, "The primitive roots and a problem related to the golomb conjecture," *AIMS Mathematics*, vol. 5, no. 4, pp. 3899–3905, 2020.

[4] J. F. Zhang and X. X. Lv, "On the primitive roots and the generalized golomb's conjecture," *AIMS Mathematics*, vol. 5, pp. 5654–5663, 2020.

[5] T. Tian and W. Qi, "Primitive normal element and its inverse in finite fields," *Acta Mathematica Sinica*, vol. 49, pp. 657–668, 2006.

[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] J. P. Wang, "On golomb's conjecture," *Science in China (Series A)*, vol. 9, pp. 927–935, 1987.

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

[9] S. D. Cohen and T. Trudgian, "Lehmer numbers and primitive roots modulo a prime," *Journal of Number Theory*, vol. 203, pp. 68–79, 2019.

[10] T. T. Wang and X. N. Wang, "On the golomb's conjecture and lehmer's numbers," *Open Mathematics*, vol. 15, pp. 1003–1009, 2017.

[11] W. Q. Wang and W. P. Zhang, "A mean value related to primitive roots and golomb's conjectures," *Absract and Applied Analysis*, vol. 20145 pages, Article ID 908273, 2014.

[12] T. M. Apostol, *Introduction to Analytic Number Theory,*-Springer-Verlag, Berlin, Germany, 1976.

[13] W. Narkiewicz, *Classical Problems in Number Theory*, Polish Scientifc Publishers, Warszawa, Poland, 1986.

[14] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory,*Springer-Verlag, Berlin, Germany, 1982.

[15] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, "On the hidden shifted power problem," *SIAM Journal on Computing*, vol. 41, no. 6, pp. 1524–1557, 2012.

[16] K. Gong and C. Jia, "Shifted character sums with multiplicative coefficients," *Journal of Number Theory*, vol. 153, pp. 364–371, 2015.

[17] C. Mauduit and A. Sárközy, "On finite pseudorandom binary sequences I: measure of pseudorandomness, the legendre symbol," *Acta Arithmetica*, vol. 82, no. 4, pp. 365–377, 1997.

[18] W. P. Zhang and Y. Yi, "On Dirichlet characters of polynomials," *Bulletin of the London Mathematical Society*, vol. 34, pp. 469–473, 2002.

[19] W. Zhang and W. Yao, "A note on the dirichlet characters of polynomials," *Acta Arithmetica*, vol. 115, no. 3, pp. 225–229, 2004.