Research Article

The Legendre's Symbol Modulo p and Its Some Elementary Results

Jianghua Li and Yuan Zhang

College of Sciences, Xi'an University of Technology, Xi'an, Shaanxi, China

Correspondence should be addressed to Jianghua Li; jianghuali@xaut.edu.cn

Received 20 April 2021; Accepted 6 May 2021; Published 17 May 2021

Academic Editor: Tingting Wang

Copyright © 2021 Jianghua Li and Yuan 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 article is using the elementary methods and the properties of the character sums to study the calculating problem of the number of the solutions for one kind congruence equation modulo p (an odd prime) and give some interesting identities and asymptotic formulas for it.

1. Introduction

Let $p \geq 3$ be a prime. For any integer n , the Legendre's symbol (n/p) modulo p is defined as follows:

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & \text{if } (n, p) = 1 \text{ and } n \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } (n, p) = 1 \text{ and } n \text{ is a quadratic nonresidue modulo } p, \\ 0, & \text{if } p \mid n. \end{cases} \quad (1)$$

This arithmetical function occupies a very important position in the elementary number theory and analytic number theory, and many classical number theory problems are closely related to it, for example, the least quadratic nonresidue problem, the class number formula of the quadratic field, and the prime number structure. In particular, if p is a prime with $p \equiv 1 \pmod{4}$, then we have the identity (see Theorems 4–11 in [1])

$$p = \left(\sum_{a=1}^{p-1/2} \left(\frac{a+\bar{a}}{p} \right) \right)^2 + \left(\sum_{a=1}^{p-1/2} \left(\frac{a+r \cdot \bar{a}}{p} \right) \right)^2 \quad (2)$$

$$\equiv \alpha^2(p) + \beta^2(p),$$

where r is any quadratic nonresidue modulo p , and $a \cdot \bar{a} \equiv 1 \pmod{p}$.

In addition to its wide range of applications, the Legendre's symbol has a number of interesting and important

properties of its own. The quadratic reciprocity law is one of them. That is, for any two odd primes p and q with $p \neq q$, we have the identity (see Theorem 9.8 in [2])

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}. \quad (3)$$

Some other papers related to character sums can be referred to [3–9]. There is no need to give detailed examples of their contents here, the interested readers may refer to them.

In this paper, we will consider the following elementary number theory problem related to k -th residue modulo p , in particular, the quadratic residue modulo p .

For any integer n with $(n, p) = 1$, let $i, j = \pm 1$, and $N(n, i, j; p)$ denote the number of the solutions of the congruence equation $n \equiv a + b \pmod{p}$ ($1 \leq a, b \leq p-1$) such that $(a/p) = i$ and $(b/p) = j$.

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

$$N(n, i, j; p) = \frac{p-2}{4} - \frac{i+j}{4} \cdot \left(\frac{n}{p}\right) - \frac{i \cdot j}{4} \cdot \left(\frac{-1}{p}\right). \quad (4)$$

For any fixed positive integer $k \geq 3$ and any prime p with $p \equiv 1 \pmod{k}$, if we let $M(n, k; p)$ denote the number of the solutions of the congruence equation $n \equiv a + b \pmod{p}$ with

$1 \leq a, b \leq p-1$, both a and b are the k -th residues modulo p . Then, we also have the following.

Theorem 2. Let p be a prime with $p \equiv 1 \pmod{3}$. Then, for any integer n with $(n, p) = 1$, we have the identity

$$M(n, 3; p) = \frac{p-4}{9} - \frac{2(\lambda(n)\tau^2(\lambda) + \bar{\lambda}(n)\tau^2(\bar{\lambda})) - \bar{\lambda}(n)\tau^3(\lambda) - \lambda(n)\tau^3(\bar{\lambda})}{9p}, \quad (5)$$

if n is a cubic residue modulo p , then we have

$$M(n, 3; p) = \frac{p+d-4}{9} - \frac{2(\tau^2(\lambda) + \tau^2(\bar{\lambda}))}{9p}, \quad (6)$$

where λ is any third-order character modulo p , $\tau(\lambda) = \sum_{a=1}^{p-1} \lambda(a)e(a/p)$ denotes the classical Gauss sums, $4p = d^2 + 27 \cdot b^2$, and d is uniquely determined by $d \equiv 1 \pmod{3}$.

Theorem 3. Let p be a prime with $p \equiv 1 \pmod{4}$. If integer n is a quadratic residue modulo p , then have the identity

$$M(n, 4; p) = \begin{cases} 1/16 \cdot (p - 2\alpha(p) - 7), & \text{if } p \equiv 1 \pmod{8}, \\ 1/16 \cdot (p + 6\alpha(p) - 11), & \text{if } p \equiv 5 \pmod{8}, \end{cases} \quad (7)$$

where $\alpha(p)$ is defined as the same as in (2).

It is clear that from Theorem 1, we can deduce the following several corollaries.

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

$$N(n, 1, 1; p) = \begin{cases} p - 5/4, & \text{if } p \equiv 1 \pmod{4} \text{ and } \left(\frac{n}{p}\right) = 1, \\ p - 1/4, & \text{if } p \equiv 1 \pmod{4} \text{ and } \left(\frac{n}{p}\right) = -1, \\ p - 3/4, & \text{if } p \equiv 3 \pmod{4} \text{ and } \left(\frac{n}{p}\right) = 1, \\ p + 1/4, & \text{if } p \equiv 3 \pmod{4} \text{ and } \left(\frac{n}{p}\right) = -1. \end{cases} \quad (8)$$

Corollary 2. Let $p \equiv 3 \pmod{4}$ be an odd prime. Then, for any integer n with $(n, p) = 1$, we have the identity

$$N(n, -1, -1; p) = \begin{cases} \frac{p-1}{4}, & \text{if } p \equiv 1 \pmod{4} \text{ and } \left(\frac{n}{p}\right) = 1, \\ \frac{p-5}{4}, & \text{if } p \equiv 1 \pmod{4} \text{ and } \left(\frac{n}{p}\right) = -1, \\ \frac{p+1}{4}, & \text{if } p \equiv 3 \pmod{4} \text{ and } \left(\frac{n}{p}\right) = 1, \\ \frac{p-3}{4}, & \text{if } p \equiv 3 \pmod{4} \text{ and } \left(\frac{n}{p}\right) = -1. \end{cases} \quad (9)$$

Corollary 3. Let $p \equiv 3 \pmod{4}$ be an odd prime. Then, for any integer n with $(n, p) = 1$, we have the identity

$$N(n, 1, -1; p) = N(n, -1, 1; p) = \begin{cases} \frac{p-1}{4}, & \text{if } p \equiv 1 \pmod{4}, \\ \frac{p-3}{4}, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \quad (10)$$

Note that the estimate $|\tau^2(\lambda) + \tau^2(\bar{\lambda})| \leq 2p$ and $|\alpha(p)| \leq \sqrt{p}$, from Theorem 2 and Theorem 3; we can also deduce the following corollaries.

Corollary 4. Let p be an odd prime with $p \equiv 1 \pmod{3}$. Then, for any integer n with $(n, p) = 1$, we have the asymptotic formula

$$M(n, 3; p) = \frac{1}{9} \cdot p + O(\sqrt{p}). \quad (11)$$

Corollary 5. Let p be a prime with $p \equiv 1 \pmod{3}$. Then, for any cubic residue n modulo p , we have the identity

$$M(n, 3; p) = \left\lfloor \frac{p+d}{9} \right\rfloor \text{ or } \left\lceil \frac{p+d}{9} \right\rceil - 1. \quad (12)$$

Corollary 6. Let p be a prime with $p \equiv 1 \pmod{4}$. Then, for any quadratic residue $n \pmod{p}$, we have the asymptotic formula

$$M(n, 4; p) = \frac{1}{16} \cdot p + O(\sqrt{p}). \quad (13)$$

Some notes: it is very interesting that the right hand side of the identity in Corollary 3 does not depend on constant n . Of course, the research content and methods in this paper can be further promoted.

2. Several Lemmas

In this section, we will give several necessary lemmas. Of course, the proofs of the theorems and these lemmas need the knowledge of elementary and analytic number theory, in particular, the properties of the quadratic residues modulo p and the classical Gauss sums. All these can be found in references [1, 2, 10], and we do not repeat them. First, we have the following.

Lemma 1. Let p be an odd prime with $p \equiv 1 \pmod{3}$. Then, for any three-order character $\lambda \pmod{p}$, we have the identity

$$\tau^3(\lambda) + \tau^3(\bar{\lambda}) = dp, \quad (14)$$

where $4p = d^2 + 27 \cdot b^2$, and d is uniquely determined by $d \equiv 1 \pmod{3}$,

Proof. See the study by Zhang and Hu [4] or Berndt and Evans [5]. $\square$

Lemma 2. Let p be an odd prime with $p \equiv 1 \pmod{3}$. Then, we have

$$\begin{aligned} & \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) (-1 + \bar{\lambda}(m)\tau(\lambda) + \lambda(m)\tau(\bar{\lambda}))^2 \\ &= -(2p+1) - 2(\lambda(n)\tau^2(\lambda) + \bar{\lambda}(n)\tau^2(\bar{\lambda})) \\ &+ \bar{\lambda}(n)\tau^3(\lambda) + \lambda(n)\tau^3(\bar{\lambda}). \end{aligned} \quad (15)$$

If n is a cubic residue modulo p , then we have

$$\begin{aligned} & \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) (-1 + \bar{\lambda}(m)\tau(\lambda) + \lambda(m)\tau(\bar{\lambda}))^2 \\ &= dp - 2p - 1 - 2(\tau^2(\lambda) + \tau^2(\bar{\lambda})), \end{aligned} \quad (16)$$

where d is defined as the same as in Lemma 1.

Proof. For any integer $1 \leq a \leq p-1$, note that $\bar{\lambda} = \lambda^2$ and $\tau(\lambda) \cdot \tau(\bar{\lambda}) = p$; from the properties of the three-order

character $\lambda \pmod{p}$ and the classical Gauss sums $\tau(\lambda)$ modulo p , we have

$$\begin{aligned} & \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) (-1 + \bar{\lambda}(m)\tau(\lambda) + \lambda(m)\tau(\bar{\lambda}))^2 \\ &= -1 - 2 \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) (\bar{\lambda}(m)\tau(\lambda) + \lambda(m)\tau(\bar{\lambda})) \\ &+ \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) (2p + \lambda(m)\tau^2(\lambda) + \bar{\lambda}(m)\tau^2(\bar{\lambda})) \\ &= -(2p+1) - 2(\lambda(n)\tau^2(\lambda) + \bar{\lambda}(n)\tau^2(\bar{\lambda})) \\ &+ \bar{\lambda}(n)\tau^3(\lambda) + \lambda(n)\tau^3(\bar{\lambda}). \end{aligned} \quad (17)$$

If n is a cubic residue modulo p , then we have $\lambda(-1) = 1$ and $\lambda(n) = \bar{\lambda}(n) = 1$; from (17) and Lemma 1, we have

$$\begin{aligned} & \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) (-1 + \bar{\lambda}(m)\tau(\lambda) + \lambda(m)\tau(\bar{\lambda}))^2 \\ &= -(2p+1) - 2(\tau^2(\lambda) + \tau^2(\bar{\lambda})) + \tau^3(\lambda) + \tau^3(\bar{\lambda}) \\ &= dp - 2p - 1 - 2(\tau^2(\lambda) + \tau^2(\bar{\lambda})). \end{aligned} \quad (18)$$

Now, Lemma 2 follows from (18). $\square$

Lemma 3. Let p be an odd prime with $p \equiv 1 \pmod{4}$. Then, for any four-order character ψ modulo p , we have the identity

$$\tau^2(\psi) + \tau^2(\bar{\psi}) = 2\sqrt{p} \cdot \alpha(p), \quad (19)$$

where $\alpha(p)$ is defined as in (2).

Proof. See Lemma 2.2 in the study by Chen and Zhang [7]. $\square$

3. Proofs of the Theorems

Applying three simple lemmas in Section 2, we can easily complete the proofs of our theorems. First, we prove Theorem 1. Note that the trigonometric identity

$$\sum_{m=0}^{p-1} e\left(\frac{nm}{p}\right) = \begin{cases} p, & \text{if } (n, p) = p, \\ 0, & \text{if } (n, p) = 1, \end{cases} \quad (20)$$

$\tau^2(\chi_2) = (-1/p) \cdot p$, so from the definition of $N(n, i, j; p)$ and the properties of the Legendre's symbol, we have

$$\begin{aligned}
N(n, i, j; p) &= \frac{1}{p} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{4} \left(1 + i \left(\frac{a}{p}\right)\right) \left(1 + j \left(\frac{b}{p}\right)\right) \sum_{m=0}^{p-1} e\left(\frac{m(a+b-n)}{p}\right) \\
&= \frac{1}{4p} \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \left(1 + i \left(\frac{a}{p}\right)\right) \left(1 + j \left(\frac{b}{p}\right)\right) e\left(\frac{m(a+b)}{p}\right) + \frac{1}{4p} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \left(1 + i \left(\frac{a}{p}\right)\right) \left(1 + j \left(\frac{b}{p}\right)\right) \\
&= \frac{1}{4p} \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) \left(-1 + i \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e\left(\frac{ma}{p}\right)\right) \cdot \left(-1 + j \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) e\left(\frac{mb}{p}\right)\right) + \frac{1}{4p} \left(p-1 + i \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)\right) \\
&\quad \cdot \left(p-1 + j \sum_{b=1}^{p-1} \left(\frac{b}{p}\right)\right) \\
&= \frac{1}{4p} \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) \left(-1 + i \left(\frac{m}{p}\right) \tau(\chi_2)\right) \left(-1 + j \left(\frac{m}{p}\right) \tau(\chi_2)\right) + \frac{(p-1)^2}{4p} \\
&= \frac{1}{4p} \left(-1 - i \left(\frac{-n}{p}\right) \tau^2(\chi_2) - j \left(\frac{-n}{p}\right) \tau^2(\chi_2) - i \cdot j \cdot \tau^2(\chi_2)\right) + \frac{(p-1)^2}{4p} \\
&= \frac{p-2}{4} - \frac{i+j}{4} \cdot \left(\frac{n}{p}\right) - \frac{i \cdot j}{4} \cdot \left(\frac{-1}{p}\right),
\end{aligned} \tag{21}$$

where $\chi_2 = (*/p)$ is the Legendre's symbol modulo p . This proves Theorem 1.

Now, we prove Theorem 2. For any integer $1 \leq a \leq p-1$, from the properties of the third-order character λ modulo p , we have

$$1 + \lambda(a) + \bar{\lambda}(a) = \begin{cases} 3, & \text{if } a \text{ is a cubic residue modulo } p, \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

Applying formulas (20) and (22) and Lemma 2, the definition of $M(n, 3; p)$, and the properties of the classical Gauss sums, we have

$$\begin{aligned}
M(n, 3; p) &= \frac{1}{9p} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} (1 + \lambda(a) + \bar{\lambda}(a)) (1 + \lambda(b) + \bar{\lambda}(b)) \sum_{m=0}^{p-1} e\left(\frac{m(a+b-n)}{p}\right) \\
&= \frac{1}{9p} \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) \left(\sum_{a=1}^{p-1} (1 + \lambda(a) + \bar{\lambda}(a)) e\left(\frac{ma}{p}\right)\right)^2 + \frac{1}{9p} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} (1 + \lambda(a) + \bar{\lambda}(a)) (1 + \lambda(b) + \bar{\lambda}(b)) \\
&= \frac{(p-1)^2}{9p} + \frac{1}{9p} \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) (-1 + \bar{\lambda}(m) \tau(\lambda) + \lambda(m) \tau(\bar{\lambda}))^2 \\
&= \frac{p-4}{9} - \frac{2(\lambda(n) \tau^2(\lambda) + \bar{\lambda}(n) \tau^2(\bar{\lambda})) - \bar{\lambda}(n) \tau^3(\lambda) - \lambda(n) \tau^3(\bar{\lambda})}{9p}.
\end{aligned} \tag{23}$$

If n is a cubic residue modulo p , then we have $\lambda(n) = \bar{\lambda}(n) = 1$. From (23) and Lemma 1, we may immediately deduce

$$M(n, 3; p) = \frac{p+d-4}{9} - \frac{2}{9p} \cdot (\tau^2(\lambda) + \tau^2(\bar{\lambda})). \tag{24}$$

Now, Theorem 2 follows from (23) and (24).

Similarly, using the methods of proving Theorem 2, we can also deduce Theorem 3. In fact, let ψ be a four-order character modulo p , then $\psi^2 = \chi_2 = (*/p)$. From the properties of the four-order character, we have

$$1 + \psi(a) + \psi^2(a) + \bar{\psi}(a) = \begin{cases} 4, & \text{if } a \text{ is a quartic residue modulo } p, \\ 0, & \text{otherwise.} \end{cases} \quad (25)$$

Note that $\chi_2(-1) = 1$; from (25) and the methods of proving Theorem 2, we have

$$\begin{aligned} M(n, 4; p) &= \frac{1}{16p} \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) \left(\sum_{a=1}^{p-1} (1 + \psi(a) + \chi_2(a) + \bar{\psi}(a)) e\left(\frac{ma}{p}\right) \right)^2 \\ &\quad + \frac{1}{16p} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} (1 + \psi(a) + \chi_2(a) + \bar{\psi}(a)) (1 + \psi(b) + \chi_2(b) + \bar{\psi}(b)) \\ &= \frac{1}{16p} \sum_{m=1}^{p-1} e\left(\frac{-nm}{p}\right) \left(-1 + \bar{\psi}(m)\tau(\psi) + \chi_2(m)\sqrt{p} + \psi(m)\tau(\bar{\psi}) \right)^2 + \frac{(p-1)^2}{16p} \\ &= \frac{p-3}{16} - \frac{1}{8} \left(\frac{n}{p} \right) - \frac{1}{8p} (1 + \psi(-n) + \bar{\psi}(-n))\tau(\psi)\tau(\bar{\psi}) + \frac{1}{8\sqrt{p}} (\bar{\psi}(-n)\tau^2(\psi) + \psi(-n)\tau^2(\bar{\psi})) \\ &\quad + \frac{\chi_2(n)}{16\sqrt{p}} (\tau^2(\psi) + \tau^2(\bar{\psi})). \end{aligned} \quad (26)$$

If $p = 8k + 5$, n is a quadratic residue modulo p , then we have $\psi(-1) = \psi(n) = 1$ and $\tau(\psi)\tau(\bar{\psi}) = p$. Thus, from (26) and Lemma 3, we have

$$\begin{aligned} M(n, 4; p) &= \frac{p-3}{16} - \frac{1}{8} - \frac{3}{8} + \frac{2 \cdot \alpha(p)}{8} + \frac{2\alpha(p)}{16} \\ &= \frac{1}{16} \cdot (p + 6\alpha(p) - 11). \end{aligned} \quad (27)$$

If $p = 8k + 1$, n is a quadratic residue modulo p , then we have $\psi(-1) = -1$, $\psi(n) = 1$, and $\tau(\psi)\tau(\bar{\psi}) = -p$. Thus, from (26) and Lemma 3, we have

$$\begin{aligned} M(n, 4; p) &= \frac{p-3}{16} - \frac{1}{8} - \frac{1}{8} - \frac{2 \cdot \alpha(p)}{8} + \frac{2\alpha(p)}{16} \\ &= \frac{1}{16} \cdot (p - 2\alpha(p) - 7). \end{aligned} \quad (28)$$

Now, Theorem 3 follows from (27) and (28). This completes the proofs of all our results.

Data Availability

The data used to support the findings of this study are included within the article.

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 (11771351) of P. R. China.

References

- [1] W. P. Zhang and H. L. Li, *Elementary Number Theory*, Shaanxi Normal University Press, Xi'an, China, 2013.
- [2] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, NY, USA, 1976.
- [3] L. Chen and J. Y. Hu, "A linear recurrence formula involving cubic Gauss sums and kloosterman sums," *Acta Mathematica Sinica (Chinese Series)*, vol. 61, pp. 67–72, 2018.
- [4] W. P. Zhang and J. Y. Hu, "The number of solutions of the diagonal cubic congruence equation mod p ," *Mathematical Reports*, vol. 20, pp. 70–76, 2018.
- [5] B. C. Berndt and R. J. Evans, "The determination of Gauss sums," *Bulletin of the American Mathematical Society*, vol. 5, no. 2, pp. 107–130, 1981.
- [6] S. Chowla, J. Cowles, and M. Cowles, "On the number of zeros of diagonal cubic forms," *Journal of Number Theory*, vol. 9, no. 4, pp. 502–506, 1977.
- [7] Z. Y. Chen and W. P. Zhang, "On the fourth-order linear recurrence formula related to classical Gauss sums," *Open Mathematics*, vol. 15, pp. 1251–1255, 2017.

- [8] L. Chen, “On classical Gauss sums and some of their properties,” *Symmetry*, vol. 10, no. 11, p. 625, 2018.
- [9] Y. Y. Liu and W. P. Zhang, “The linear recurrence formula of the hybrid power mean involving the cubic Gauss sums and two-term exponential sums,” *Journal of Shaanxi Normal University (Natural Science Edition)*, vol. 45, pp. 14–17, 2017.
- [10] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, NY, USA, 1982.