Journal of Integer Sequences, Vol. 21 (2018),
Article 18.4.7

On Certain Sums with Quadratic Expressions Involving the Legendre Symbol

Ram Krishna Pandey
Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee 247667
Haridwar
India
ramkpfma@iitr.ac.in

Anshumaan Parashar
Department of Mechanical and Industrial Engineering
Indian Institute of Technology Roorkee
Roorkee 247667
Haridwar
India
apairs.anshumaan@gmail.com

Abstract

In this paper, we find some identities for sums with quadratic and higher-order expressions involving the Legendre symbol. Some of these identities generalize identities recently obtained by Karaivanov and Vassilev.

1 Introduction

Let a be an integer and p be an odd prime. The well-known Legendre symbol, denoted by $(\frac{a}{p})$, is defined by

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

Introduced by Legendre [10], the Legendre symbol is a convenient formalism for discussing quadratic residues. Using the Legendre symbol, we can easily state the classical "quadratic reciprocity law", which was first formulated by Euler and Legendre. Besides this formulation, Legendre also partially proved the law.

The first complete proof of the law was given by Gauss [3]. Gauss was extremely proud of his proof, and he called it the *Theorema Aureum* (the golden theorem). In his whole lifetime, Gauss provided a total of eight proofs, out of which only six are published. There are over a hundred proofs of the law now in existence.

An efficient algorithm to compute the Legendre symbol has been discussed by Bach and Shallit [2, Thm. 5.9.3, p. 113]. There are several generalizations of the Legendre symbol now in the literature. The Jacobi symbol is one of them. Almost all the generalizations of the quadratic reciprocity law may be found in the textbook by Lemmermeyer [11].

Since the Legendre symbol is a multiplicative character on $\mathbb{Z}/p\mathbb{Z}$, this symbol is extensively used in counting the number of solutions of an equation with coefficients in a finite field by introducing the notion of Jacobi sums, as can be seen, for example, in the textbook by Ireland and Rosen [6] .

In this paper, we consider certain sums involving Legendre symbol with linear, quadratic, and higher-order expressions. Sums involving linear expressions in the Legendre symbol can be easily evaluated, and may be found in textbooks such as [5, 6], mostly as an exercise. The sum involving a quadratic expression was evaluated by Hua [5, Thm. 8.2, p. 174] in a particular case. We evaluate two sums in Section 2.

Finding estimates of sums involving the Legendre symbol has been a main topic of research in the twentieth century. Some of the work on estimates of sums may be found in the work of several authors [4, 7, 9, 12, 13, 14, 15]. In a recent work, Wright [15, Thm. 9.1, p. 213, Thm. 9.2, p. 214] estimated both the *complete Weil sum* and *incomplete Weil sum*.

Evaluating the sums of higher-order expressions involving the Legendre symbol is quite challenging. We find certain sums of higher-order expressions in Section 3. To the best of our knowledge, these sums are new and have not appeared before. Some of our identities generalize the identities recently obtained by Karaivanov and Vassilev [8]. The identities obtained by Karaivanov and Vassilev [8] are basically the main motivation of the paper. Sums considered in Theorem 4 and Theorem 9 are also motivated by an exercise [6, Exercise 28, p. 107].

The definitions and properties are used in this paper related to the Legendre symbol may be found in any introductory number theory textbook.

2 Preliminary results

Theorem 1. *Let a, b, and c be integers, and let p be an odd prime. Then*

$$\sum_{\ell=0}^{p-1}\left(\frac{a\ell^2+b\ell+c}{p}\right)=\begin{cases}-(\frac{a}{p}), & \text{if } p\nmid(b^2-4ac);\\ (\frac{a}{p})(p-1), & \text{if } p\mid(b^2-4ac).\end{cases}$$

Proof. Let S be the required sum to be calculated. Let $p\mid a$. Then

$$S=\sum_{\ell=0}^{p-1}\left(\frac{b\ell+c}{p}\right).$$

Clearly, the numbers $b\ell+c$, where ℓ varies from 0 to $p-1$, form a complete residue system modulo p, if $b\not\equiv 0 \pmod{p}$. Hence, $S=0=-(\frac{a}{p})$. Next let $p\nmid a$. Then

$$S=\left(\frac{a}{p}\right)\left(\frac{4}{p}\right)\sum_{\ell=0}^{p-1}\left(\frac{4a^2\ell^2+4ab\ell+4ac}{p}\right)=\left(\frac{a}{p}\right)\sum_{\ell=0}^{p-1}\left(\frac{(2a\ell+b)^2+(4ac-b^2)}{p}\right).$$

Since $p\nmid 2a$, the set of integers $2a\ell+b$, where ℓ varies from 0 to $p-1$, forms a complete set of residues modulo p. Thus

$$S=\left(\frac{a}{p}\right)\sum_{\ell=0}^{p-1}\left(\frac{\ell^2+(4ac-b^2)}{p}\right).$$

Now let $p\mid(4ac-b^2)$. Then

$$S=\left(\frac{a}{p}\right)\sum_{\ell=0}^{p-1}\left(\frac{\ell^2+(4ac-b^2)}{p}\right)=\left(\frac{a}{p}\right)\sum_{\ell=0}^{p-1}\left(\frac{\ell^2}{p}\right)=\left(\frac{a}{p}\right)\left(0+\sum_{\ell=1}^{p-1}1\right)=\left(\frac{a}{p}\right)(p-1).$$

It remains to consider the case $p\nmid(4ac-b^2)$. Taking the summation modulo p and putting $k=(4ac-b^2)$, we get

$$S\equiv\left(\frac{a}{p}\right)\sum_{\ell=0}^{p-1}\left(\frac{\ell^2+k}{p}\right)\equiv\left(\frac{a}{p}\right)\sum_{\ell=0}^{p-1}(\ell^2+k)^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\sum_{\ell=1}^{p}(\ell^2+k)^{\frac{p-1}{2}} \pmod{p}.$$

Putting $x=\frac{p-1}{2}$ and using the binomial theorem, we can write

$$S\equiv\left(\frac{a}{p}\right)\sum_{\ell=1}^{p}\sum_{r=0}^{x}\binom{x}{r}k^{x-r}\ell^{2r} \pmod{p}.$$

Rearranging the sum, we get

$$S \equiv \left(\frac{a}{p}\right) \sum_{r=0}^{x} \left(\binom{x}{r} k^{x-r} \sum_{\ell=1}^{p} \ell^{2r} \right) \pmod{p}.$$

To calculate the sum $\sum_{\ell=1}^{p} \ell^{2r}$ modulo p, we use the following sum, which is a simple exercise in [1, Exercise 7, Chapter 10],

$$\sum_{\ell=1}^{p} \ell^n \equiv \begin{cases} -1, & \text{if } (p-1) \mid n; \\ 0, & \text{if } (p-1) \nmid n, \end{cases}$$

where $n \geq 1$.

Since $2r \leq p-1$, $\sum_{\ell=1}^{p} \ell^{2r} = -1$, only if $2r = p-1$, i.e., $r = \frac{p-1}{2}$ and 0 otherwise. Therefore, in our main summation, all terms are zero except for $r = x$. Thus,

$$S \equiv -\left(\frac{a}{p}\right) \pmod{p}.$$

Now, since each term in the summation S, is either -1 or 0 or 1, the value of S lies between $-p$ and p. If $(\frac{a}{p}) = -1$, then S is either 1 or $-p+1$. We have

$$S = \left(\frac{a}{p}\right) \sum_{\ell=0}^{p-1} \left(\frac{\ell^2 + k}{p}\right).$$

Since $\ell^2 \equiv (-\ell)^2 \equiv (p-\ell)^2 \pmod{p}$,

$$S = \left(\frac{a}{p}\right) \left(\left(\frac{k}{p}\right) + 2 \sum_{\ell=1}^{\frac{p-1}{2}} \left(\frac{\ell^2 + k}{p}\right) \right).$$

The above identity proves that if $p \nmid k$, then S is odd. But $-p+1$ is even. Therefore, $S \neq -p+1$, consequently, $S = 1$. A similar argument would show that $S = -1$, when $(\frac{a}{p}) = 1$. Hence, in both the cases

$$S = -\left(\frac{a}{p}\right).$$

This completes the proof of the theorem. □

We obtain Lemma 1 of Karaivanov and Vassilev [8] and a theorem of Hua [5, Thm. 8.2, p. 174] as special cases of the above theorem as follows:

Corollary 2. *For integers b and c with $p \nmid b$,*

$$\sum_{\ell=0}^{p-1} \left(\frac{b\ell + c}{p}\right) = 0.$$

Proof. Setting $a \equiv 0 \pmod{p}$ in Theorem 1, we get the result. □

Corollary 3. *Let $p > 2$ and $b^2 - 4c \not\equiv 0 \pmod{p}$. Then*

$$\sum_{\ell=1}^{p} \left(\frac{\ell^2 + b\ell + c}{p} \right) = -1.$$

Proof. Setting $a = 1$ in Theorem 1, we get the corollary. □

3 Main results

Theorem 4. *Let p be an odd prime and c be an integer. Then*

$$\sum_{\ell=0}^{p-1} \left(\frac{\ell^n + c}{p} \right) \equiv \begin{cases} -\sum_{k=1}^{\lfloor \frac{\gcd(p-1,n)}{2} \rfloor} \binom{\frac{p-1}{2}}{k\frac{p-1}{\gcd(p-1,n)}} c^{\left(\frac{p-1}{2} - k\frac{p-1}{\gcd(p-1,n)}\right)}, & \text{if } p \nmid c; \\ -1, & \text{if } p \mid c \text{ and } n \equiv 0 \pmod{2}; \\ 0, & \text{if } p \mid c \text{ and } n \equiv 1 \pmod{2}. \end{cases}$$

Proof. Let S be the required sum to be calculated. Then

$$S \equiv \sum_{\ell=0}^{p-1} (\ell^n + c)^{\frac{p-1}{2}} \pmod{p}.$$

If $p \mid c$, then

$$S = \sum_{\ell=0}^{p-1} \left(\frac{\ell^n}{p} \right) \mod p.$$

Hence,

$$S = \begin{cases} \sum_{\ell=0}^{p-1} \left(\frac{\ell^2}{p}\right) = p - 1, & \text{if } n \equiv 0 \pmod{2}; \\ \sum_{\ell=0}^{p-1} \left(\frac{\ell}{p}\right) = 0, & \text{if } n \equiv 1 \pmod{2}. \end{cases}$$

Now let $p \nmid c$. Then taking the summation limits from $\ell = 1$ to $\ell = p$ and using the binomial theorem, we can write

$$S \equiv \sum_{\ell=1}^{p} \sum_{r=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{r} c^{\left(\frac{p-1}{2} - r\right)} \ell^{nr} \pmod{p}.$$

Rearranging the sum, we get

$$S \equiv \sum_{r=0}^{\frac{p-1}{2}} \left(\binom{\frac{p-1}{2}}{r} c^{\left(\frac{p-1}{2} - r\right)} \sum_{\ell=1}^{p} \ell^{nr} \right) \pmod{p}.$$

The value of the sum $\sum_{\ell=1}^{p} \ell^{nr}$ modulo p is -1 if $(p-1) \mid nr$ and 0 otherwise, for $r \geq 1$. For $r = 0$, the value modulo p is clearly 0. Thus

$$S \equiv - \sum_{r\geq 1,\ (p-1)\mid nr}^{r \leq \frac{p-1}{2}} \binom{\frac{p-1}{2}}{r} c^{\left(\frac{p-1}{2}-r\right)} \pmod{p}.$$

If $(p-1) \mid nr$, then $\frac{p-1}{\gcd(p-1,n)} \mid r$. Therefore, the possible values of r are $k\frac{p-1}{\gcd(p-1,n)}$, where k is an integer satisfying $1 \leq k \leq \lfloor \frac{\gcd(p-1,n)}{2} \rfloor$. So, we have

$$S \equiv - \sum_{k=1}^{\lfloor \frac{\gcd(p-1,n)}{2} \rfloor} \binom{\frac{p-1}{2}}{k\frac{p-1}{\gcd(p-1,n)}} c^{\left(\frac{p-1}{2} - k\frac{p-1}{\gcd(p-1,n)}\right)} \pmod{p}.$$

This completes the proof. □

Theorem 5. *Let* $\xi(a,b,c) = \sum_{\ell=0}^{p-1} (\frac{a\ell^2+b\ell+c}{p})\ell$. *Then*

$$2a\left(\frac{a}{p}\right)\xi(a,b,c) \equiv b \pmod{p}.$$

Proof. Clearly,

$$\begin{aligned} 2a\left(\frac{a}{p}\right)\xi(a,b,c) &= \sum_{\ell=0}^{p-1}\left(\frac{(2a\ell+b)^2+(4ac-b^2)}{p}\right)2a\ell \\ &= \sum_{\ell=0}^{p-1}\left(\frac{(2a\ell+b)^2+(4ac-b^2)}{p}\right)(2a\ell+b) - b\sum_{\ell=0}^{p-1}\left(\frac{(2a\ell+b)^2+(4ac-b^2)}{p}\right). \end{aligned}$$

Since the set of integers $2a\ell + b$ forms a complete set of residues,

$$2a\left(\frac{a}{p}\right)\xi(a,b,c) \equiv \sum_{\ell=0}^{p-1}\left(\frac{\ell^2+(4ac-b^2)}{p}\right)\ell - b\sum_{\ell=0}^{p-1}\left(\frac{l^2+(4ac-b^2)}{p}\right) \pmod{p}.$$

By Theorem 1,

$$\sum_{\ell=0}^{p-1}\left(\frac{\ell^2+(4ac-b^2)}{p}\right) \equiv -1 \pmod{p}.$$

This gives

$$2a\left(\frac{a}{p}\right)\xi(a,b,c) \equiv \sum_{\ell=0}^{p-1}\left(\frac{\ell^2+(4ac-b^2)}{p}\right)\ell + b \equiv \xi(1,0,4ac-b^2) + b \pmod{p}. \quad (1)$$

Note that

$$\xi(1,0,4ac-b^2) = \sum_{\ell=0}^{p-1} \frac{\ell^2+(4ac-b^2)}{p}\ell \equiv \sum_{\ell=1}^{p}(\ell^2+(4ac-b^2))^{\frac{p-1}{2}}\ell \pmod p.$$

Hence, using the binomial theorem, we get

$$\xi(1,0,4ac-b^2) \equiv \sum_{\ell=1}^{p}\sum_{r=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{r}(4ac-b^2)^{(\frac{p-1}{2}-r)}\ell^{2r+1} \pmod p.$$

Thus, rearranging the terms, we get

$$\xi(1,0,4ac-b^2) \equiv \sum_{r=0}^{\frac{p-1}{2}} \left(\binom{\frac{p-1}{2}}{r}(4ac-b^2)^{(\frac{p-1}{2}-r)} \sum_{\ell=1}^{p}\ell^{2r+1} \right) \pmod p.$$

The sum $\sum_{\ell=1}^{p}\ell^{2r+1}$, is equal to -1 modulo p if $(p-1) \mid (2r+1)$ and 0 otherwise. But $p-1$ is even and $2r+1$ is odd. Therefore, $(p-1) \nmid (2r+1)$ and the sum $\sum_{\ell=1}^{p}\ell^{2r+1}$, is equal to 0 modulo p for all values of r. Therefore,

$$\xi(1,0,4ac-b^2) \equiv 0 \pmod p.$$

Using this in (1), we get

$$2a\left(\frac{a}{p}\right)\xi(a,b,c) \equiv b \pmod p.$$

□

Corollary 6. *We have* $\xi(ka,kb,kc) = (\frac{k}{p})\xi(a,b,c)$ *for all integers* k.

Proof. Follows directly from the above theorem. □

Remark 7. As a consequence of the above theorem, we get that $\xi(a,b,c)$ is the unique solution of the congruence $2a(\frac{a}{p})x \equiv b \pmod p$.

Theorem 8. *Let*

$$S(a,b,c) = \sum_{\ell=0}^{p-1}\left(\frac{a\ell^2+b\ell+c}{p}\right)$$

and m *be a positive integer. Then*

$$\xi(a, b+2ma, m^2a+mb+c) = \xi(a,b,c) + p\sum_{r=0}^{m-1}\left(\frac{r^2a+rb+c}{p}\right) - mS(a,b,c).$$

Proof. The proof is by induction on m. We have

$$\begin{aligned}
\xi(a, b+2a, a+b+c) &= \sum_{\ell=0}^{p-1} \left(\frac{a\ell^2 + (b+2a)\ell + (a+b+c)}{p}\right) \ell \\
&= \sum_{\ell=0}^{p-1} \left(\frac{a(\ell+1)^2 + b(\ell+1) + c}{p}\right) (\ell+1) - S(a,b,c) \\
&= \sum_{\ell=1}^{p} \left(\frac{a\ell^2 + b\ell + c}{p}\right) \ell - S(a,b,c) \\
&= \sum_{\ell=0}^{p-1} \left(\frac{a\ell^2 + b\ell + c}{p}\right) \ell + p\left(\frac{c}{p}\right) - S(a,b,c) \\
&= \xi(a,b,c) + p\left(\frac{c}{p}\right) - S(a,b,c).
\end{aligned}$$

So the basis step, $m = 1$, is satisfied. Now let the identity hold for $m-1$; we prove it for m. Let $B = b + 2(m-1)a$ and $C = (m-1)^2 a + (m-1)b + c$. Then

$$\xi(a, b+2ma, m^2a+mb+c) = \xi(a, B+2a, a+B+C) = \xi(a,B,C) + p\left(\frac{C}{p}\right) - S(a,B,C).$$

Using the induction hypothesis on $\xi(a,B,C)$, we can write

$$\begin{aligned}
\xi(a, b+2ma, m^2a+mb+c) &= \xi(a,b,c) + p\sum_{r=0}^{m-2}\left(\frac{r^2a+rb+c}{p}\right) - (m-1)S(a,b,c) \\
&\quad + p\left(\frac{(m-1)^2a+(m-1)b+c}{p}\right) - S(a,B,C).
\end{aligned}$$

We have $4aC - B^2 = 4ac - b^2$. Hence, by Theorem 1, $S(a,b,c) = S(a,B,C)$. This implies that

$$\xi(a, b+2ma, m^2a+mb+c) = \xi(a,b,c) + p\sum_{r=0}^{m-1}\left(\frac{r^2a+rb+c}{p}\right) - mS(a,b,c).$$

This completes the proof of the theorem. □

Theorem 9. *Let p be an odd prime and c, $n \geq 1$, and $k \geq 1$ be integers. Then, modulo p, we have*

$$\sum_{\ell=0}^{p-1}\left(\frac{\ell^n + c}{p}\right)\ell^k \equiv \begin{cases} -\sum_{\substack{0\le r\le (p-1)/2 \\ (p-1)\mid(nr+k)}} \binom{\frac{p-1}{2}}{r} c^{\left(\frac{p-1}{2}-r\right)}, & \text{if } p \nmid c; \\ -1, & \text{if } p \mid c \text{ and } (p-1) \mid (n(\frac{p-1}{2})+k); \\ 0, & \text{if } p \mid c \text{ and } (p-1) \nmid (n(\frac{p-1}{2})+k). \end{cases}$$

Proof. Let η denote the required sum to be calculated. If $p \mid c$, then the sum reduces to

$$\eta \equiv \sum_{\ell=0}^{p-1} \ell^{n(\frac{p-1}{2})+k} \pmod{p}.$$

This is equal to 0 if $(p-1) \nmid (n(\frac{p-1}{2})+k)$, and -1 otherwise. Next let $p \nmid c$. Proceeding in the same way as in the proof of Theorem 4, we obtain

$$\eta \equiv \sum_{r=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{r} c^{(\frac{p-1}{2}-r)} \sum_{\ell=1}^{p} \ell^{nr+k} \pmod{p}.$$

The sum $\sum_{\ell=1}^{p} \ell^{nr+k}$ modulo p is equal to 0 when $(p-1) \nmid (nr+k)$, and -1 otherwise. Thus

$$\eta \equiv -\sum_{\substack{0 \le r \le (p-1)/2 \\ (p-1) \mid (nr+k)}} \binom{\frac{p-1}{2}}{r} c^{(\frac{p-1}{2}-r)} \pmod{p}.$$

□

Corollary 10. *If n is even and k is odd, then*

$$\eta \equiv 0 \pmod{p}.$$

Proof. Since the given conditions imply that $nr+k$ is odd, there does not exist r such that $(p-1) \mid (nr+k)$. Therefore, by Theorem 9, we have $\eta \equiv 0 \pmod{p}$. □

As another corollary, we obtain [8, Claim 1] in a special case, when $a = 1$.

Corollary 11. *For odd primes p, the quantity $S_p(1,b)$ is divisible by p.*

Proof. The proof follows from the above theorem by taking $n = 1 = k$ and $c = b$. □

4 Acknowledgments

We thank the anonymous referee for his remarks on the results.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1989.

[2] E. Bach and J. Shallit, *Algorithmic Number Theory*, Volume I: Efficient Algorithms, Cambridge, 1996.

[3] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801.

[4] E. A. Grechnikov, An estimate for the sum of Legendre symbols, *Math. Notes* **88** (2010), 819–826.

[5] L. K. Hua, *Introduction to Number Theory*, Springer-Verlag, 1982.

[6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1990.

[7] A. A. Karacuba, Sums of Legendre symbols of polynomials of second degree over prime numbers, *Izv. Math.* **12** (1978), 299–308.

[8] B. Karaivanov and T. S. Vassilev, On certain sums involving the Legendre symbol, *Integers* **16** (2016), A14.

[9] P. M. Korobov, An estimate of the sum of the Legendre symbols, *Dokl. Akad. Nauk SSSR* **196** (1971), 764–767.

[10] A. M. Legendre, *Essai sur la Théorie des Nombres*, Dupart, Paris, 1798.

[11] F. Lemmermeyer, *Reciprocity Laws: from Euler to Eisenstein*, Springer, 2000.

[12] D. A. Mit'kin, Sharpening an estimate for the sum of the Legendre symbols of polynomials of odd degree, *Chebyshevskiĭ Sb.* **6** (2005), 123–126.

[13] A. Weil, *Number Theory: An Approach Through History*, Birkhäuser Boston, 2001.

[14] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, 1948.

[15] S. Wright, *Quadratic Residues and Non-Residues: Selected Topics*, Springer-Verlag, 2016.

2010 *Mathematics Subject Classification*: Primary 11A07; Secondary 11A15.
Keywords: quadratic residue, quadratic nonresidue, Legendre symbol.

Received November 28 2017; revised versions received January 9 2018; April 8 2018. Published in *Journal of Integer Sequences*, May 9 2018.

Return to Journal of Integer Sequences home page.