ON CERTAIN SUMS INVOLVING THE LEGENDRE SYMBOL

Borislav Karaivanov
Sigma Space Inc., Lanham, Maryland
borislav.karaivanov@sigmaspace.com

Tzvetalin S. Vassilev
Department of Computer Science and Mathematics, Nipissing University, North Bay, Ontario, Canada
tzvetalv@nipissingu.ca

Received: 8/10/15, Accepted: 2/13/16, Published: 2/29/16

Abstract

We prove several identities on parametric sums involving the Legendre symbol.

1. Introduction

Our work is motivated by several recent problems published in the American Mathematical Monthly that dealt with sums involving the Legendre symbol, most notably Problem 11728 from October 2013 [1]. Here we consider more general expressions. We begin by recalling the well-known definition from any introductory number theory textbook.

Definition 1. For an odd prime number p and an integer a, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } a \equiv 0 \pmod{p} \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p} \\ -1, & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Below we list several important properties of the Legendre symbol that are used throughout the text. In all of them p denotes a prime.

Property 1 (Periodicity).

$$\text{If } a \equiv b \pmod{p}, \text{ then } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Property 2 (Multiplicity).

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

While it is clear from the definition that 1 is always a quadratic residue modulo any prime p, that is not the case with 2 and $p-1$ (usually -1 is used instead).

Property 3.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

Additionally, when $p \neq 3$

$$\left(\frac{3}{p}\right) = (-1)^{\lfloor \frac{p+1}{6} \rfloor} = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 11 \pmod{12} \\ -1, & \text{if } p \equiv 5 \text{ or } 7 \pmod{12}. \end{cases}$$

When $p \neq 5$

$$\left(\frac{5}{p}\right) = (-1)^{\lfloor \frac{p+2}{5} \rfloor} = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 4 \pmod 5 \\ -1, & \text{if } p \equiv 2 \text{ or } 3 \pmod 5. \end{cases}$$

Property 4. For $1 \leq j \leq (p-1)$,

$$\left(\frac{p-j}{p}\right) = \begin{cases} \left(\frac{j}{p}\right), & \text{if } p \equiv 1 \pmod 4 \\ -\left(\frac{j}{p}\right), & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. By Property 1 and Property 2, we have

$$\left(\frac{p-j}{p}\right) = \left(\frac{-j}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{j}{p}\right).$$

Now, the result follows from Property 3. □

In his original work [3], Legendre gave the explicit formula

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

Another fundamental result, due to Gauss [2], is the law of quadratic reciprocity.

Property 5 (Law of Quadratic Reciprocity). For any two odd primes p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

2. Preliminaries

Lemma 1. *For any a and b such that $p \nmid a$,*

$$\sum_{l=0}^{p-1} \left(\frac{al+b}{p}\right) = 0. \tag{1}$$

Proof. First, notice that the numbers $(al+b)$ for $l = 0, \ldots, p-1$ form a complete set of residues modulo p. Indeed, if $l_1 \neq l_2$ are such that $al_1 + b \equiv al_2 + b \pmod{p}$, then $a(l_1 - l_2) \equiv 0 \pmod{p}$ which contradicts the fact that $p \nmid a$. Hence, for the given sum we find

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

The last sum vanishes, since exactly half of the numbers $1, \ldots, p-1$ are quadratic residues modulo p while the other half are quadratic non-residues. Indeed, the congruence $j^2 \equiv (p-j)^2 \pmod{p}$ implies that the squares of the numbers in the set $\{1, \ldots, (p-1)/2\}$ are the same, up to ordering and modulo p, as the squares of the numbers in the set $\{(p+1)/2, \ldots, p-1\}$. On the other hand, $x^2 \not\equiv y^2 \pmod{p}$ for any x and y in the first set. Thus, there are exactly $(p-1)/2$ quadratic residues modulo p, and exactly $(p-1)/2$ quadratic non-residues modulo p among the numbers $1, \ldots, p-1$ as claimed. □

Lemma 2. *Let p be a prime congruent to 7 modulo 8. Then*

$$\sum_{l=1}^{p-1} \left(\frac{4l+1}{p}\right) l = 0. \tag{2}$$

Proof. Let S denote the sum to be shown to vanish. Using Lemma 1, we find

$$\begin{aligned} 4S &= \sum_{l=0}^{p-1} \left(\frac{4l+1}{p}\right) 4l + \sum_{l=0}^{p-1} \left(\frac{4l+1}{p}\right) \\ &= \sum_{l=0}^{p-1} \left(\frac{4l+1}{p}\right) (4l+1) = \sum_{\substack{0<l<4p \\ l \equiv 1 (\mathrm{mod}\ 4)}} \left(\frac{l}{p}\right) l. \end{aligned} \tag{3}$$

In the last sum, we change summation index from l to $4p - l$, and use Property 3

to obtain

$$4S = \left(\frac{-1}{p}\right) \sum_{\substack{0<l<4p \\ l\equiv 3 (\mathrm{mod}\ 4)}} \left(\frac{l}{p}\right)(4p-l)$$
$$= -4p\sum_{l=0}^{p-1}\left(\frac{4l+3}{p}\right) + \sum_{\substack{0<l<4p \\ l\equiv 3 (\mathrm{mod}\ 4)}} \left(\frac{l}{p}\right) l = \sum_{\substack{0<l<4p \\ l\equiv 3 (\mathrm{mod}\ 4)}} \left(\frac{l}{p}\right) l, \tag{4}$$

where for the last equality we used Lemma 1 again. After adding (3) and (4) together, we find

$$\begin{aligned} 8S &= \sum_{\substack{0<l<4p \\ l\ odd}} \left(\frac{l}{p}\right) l = \sum_{0<l<4p} \left(\frac{l}{p}\right) l - \sum_{\substack{0<l<4p \\ l\ even}} \left(\frac{l}{p}\right) l \\ &= \sum_{0<l<2p} \left(\left(\frac{l}{p}\right) l + \left(\frac{l+2p}{p}\right)(l+2p)\right) - \sum_{0<l<2p} \left(\frac{2l}{p}\right) 2l \\ &= 2\left(1-\left(\frac{2}{p}\right)\right) \sum_{0<l<2p} \left(\frac{l}{p}\right) l + 2p \sum_{0<l<2p} \left(\frac{l}{p}\right) \\ &= 0 + 2p \sum_{0<l<p} \left(\left(\frac{l}{p}\right) + \left(\frac{l+p}{p}\right)\right) = 0, \end{aligned}$$

because, by Property 3, $\left(\frac{2}{p}\right) = 1$ and, by Lemma 1, the last sum vanishes. □

3. Main Results

Definition 2. For any prime p and integers a and b, let

$$S_p(a,b) = \sum_{l=1}^{p-1} \left(\frac{al+b}{p}\right) l. \tag{5}$$

Claim 1. *For any odd prime $p \neq 3$, $S_p(a,b)$ is divisible by p.*

Proof. Let $a \neq 0$ be a number co-prime with the odd prime $p \neq 3$. Adding a zero term for $l = 0$, we have

$$S_p(a,b) = \sum_{l=0}^{p-1} \left(\frac{al+b}{p}\right) l\ .$$

By Property 1, there is no loss of generality in assuming that a and b are reduced modulo p. Multiplying both sides of the last identity by a, we obtain

$$aS_p(a,b) = a\sum_{l=0}^{p-1}\left(\frac{al+b}{p}\right)l = \sum_{l=0}^{p-1}\left(\frac{al+b}{p}\right)al = \sum_{l=0}^{p-1}\left(\frac{al+b}{p}\right)(al+b)\ ,$$

where the last step follows from Lemma 1. As discussed in the proof of Lemma 1, the numbers $al+b$, $l=0,1,\ldots,p-1$, form a complete set of residues modulo p. After proper reordering, we denote these numbers by q_jp+j, $j=0,\ldots,p-1$. Then,

$$aS_p(a,b) = \sum_{j=0}^{p-1}\left(\frac{q_jp+j}{p}\right)(q_jp+j) = p\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)q_j + \sum_{j=0}^{p-1}\left(\frac{j}{p}\right)j.$$

Thus,

$$aS_p(a,b) \equiv \sum_{j=0}^{p-1}\left(\frac{j}{p}\right)j \pmod p.$$

In the case $p=4n+1$, using Property 4, we obtain

$$\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)j = \sum_{j=0}^{(p-1)/2}\left[\left(\frac{j}{p}\right)j + \left(\frac{p-j}{p}\right)(p-j)\right] = 2p\sum_{j=0}^{(p-1)/2}\left(\frac{j}{p}\right) \equiv 0 \pmod p.$$

In the case $p=4n+3$, using Property 4 again, we can pair the terms in the sum in the following fashion

$$\begin{aligned}\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)j &= \sum_{\left(\frac{j}{p}\right)=1}\left[\left(\frac{j}{p}\right)j + \left(\frac{p-j}{p}\right)(p-j)\right]\\ &= \sum_{\left(\frac{j}{p}\right)=1}(2j-p) = 2\sum_{\left(\frac{j}{p}\right)=1} j - \frac{p(p-1)}{2} \equiv 2\sum_{\left(\frac{j}{p}\right)=1} j \pmod p.\end{aligned}$$

As discussed in the proof of Lemma 1, the indices j for which $\left(\frac{j}{p}\right)=1$ are exactly $1^2, 2^2, \ldots, ((p-1)/2)^2 \pmod p$, up to ordering. Therefore,

$$2\sum_{\left(\frac{j}{p}\right)=1} j \equiv 2\sum_{j=0}^{(p-1)/2} j^2 \pmod p \equiv \frac{(p-1)p(p+1)}{12} \pmod p \equiv 0 \pmod p.$$

The last step is justified by the fact that p is co-prime with 12 when $p \neq 3$. □

Claim 2. *If p is prime and $p \nmid a$, then*

$$S_p(a,b) = -\left(\frac{-1}{p}\right)S_p(a,a-b). \tag{6}$$

Proof. Changing summation index in $S_p(a,b)$ from l to $p-1-l$, we obtain

$$\begin{aligned}
S_p(a,b) &= \sum_{l=0}^{p-2}\left(\frac{a(p-1-l)+b}{p}\right)(p-1-l)\\
&= (p-1)\sum_{l=0}^{p-2}\left(\frac{-al-(a-b)}{p}\right) - \sum_{l=0}^{p-2}\left(\frac{-al-(a-b)}{p}\right)l\\
&= (p-1)\sum_{l=0}^{p-1}\left(\frac{-al-(a-b)}{p}\right) - (p-1)\left(\frac{-ap+b}{p}\right)\\
&- \left(\frac{-1}{p}\right)\sum_{l=1}^{p-1}\left(\frac{al+(a-b)}{p}\right)l + (p-1)\left(\frac{-ap+b}{p}\right)\\
&= -\left(\frac{-1}{p}\right)S_p(a,a-b).
\end{aligned}$$

□

Claim 3. *For any integers a, b, and c,*

$$S_p(ca,cb) = \left(\frac{c}{p}\right)S_p(a,b). \tag{7}$$

Proof. The claim follows directly from Definition 2 and Property 2. □

The last claim indicates that it suffices to study the values of $S_p(a,b)$ only for co-prime pairs (a,b).
To reduce even further the set of uncharted pairs, we introduce the following result.

Claim 4. *For any integers a and b, the following formula holds*

$$S_p(a,a+b) = S_p(a,b) + \left(\frac{b}{p}\right)p. \tag{8}$$

Proof. By changing the summation index from l to $l-1$, we obtain

$$\begin{aligned}
S_p(a,a+b) &= \sum_{l=1}^{p-1}\left(\frac{al+a+b}{p}\right)l = \sum_{l=2}^{p}\left(\frac{al+b}{p}\right)(l-1)\\
&= \sum_{l=2}^{p}\left(\frac{al+b}{p}\right)l - \sum_{l=2}^{p}\left(\frac{al+b}{p}\right)\\
&= \sum_{l=1}^{p-1}\left(\frac{al+b}{p}\right)l - \left(\frac{a+b}{p}\right) + \left(\frac{b}{p}\right)p - \sum_{l=1}^{p}\left(\frac{al+b}{p}\right) + \left(\frac{a+b}{p}\right)\\
&= S_p(a,b) + \left(\frac{b}{p}\right)p\,,
\end{aligned}$$

where for the last equality we used Lemma 1. □

Corollary 1. *For any integers a, b, and $m \geq 1$ the following formula is valid*

$$S_p(a, ma + b) = S_p(a, b) + p \sum_{j=0}^{m-1} \left(\frac{ja + b}{p} \right). \tag{9}$$

Proof. Apply Claim 4 inductively m times. □

Thus, for any fixed a, we only need to know the values of $S_p(a, b)$ for the set $b \in \{0, \ldots, a-1\}$. By Claim 3, this set can be further reduced to those b's that are co-prime with a, assuming the sums $S_p(a, b)$ for smaller values of a are already known.

It is evident from the above formula, as it is from Definition 2, that the sum $S_p(a, ma + b)$ is periodic in m with period of p. An interesting special case of Claim 4 is $a = b$. On one hand, we have $S_p(a, a) = S_p(a, 0)$. On the other hand, from Claim 2 we have $S_p(a, a) = -\left(\frac{-1}{p} \right) S_p(a, 0)$. Thus, $S_p(a, a) = S_p(1, 1) = 0$ whenever $\left(\frac{-1}{p} \right) = 1$, which according to Property 3 is precisely when $p = 4n + 1$. In the case when $p = 4n + 3$, $S_p(a, a) = S_p(a, 0)$ is not necessarily zero as suggested by the proof of Claim 1. These considerations are sufficient to compute $S_p(1, m)$ for any m. We only need to know $S_p(1, 0)$ or some $S_p(1, j)$ for that matter. Also note that formula (9) can be applied "backwards", i.e.

$$S_p(a, -a + b) = S_p(a, b) - \left(\frac{-a + b}{p} \right) p, \tag{10}$$

and therefore

$$S_p(a, -ma + b) = S_p(a, b) - p \sum_{j=1}^{m} \left(\frac{-ja + b}{p} \right). \tag{11}$$

When $a > 1$, due to the periodicity, we need more initial values in order to compute the values of $S_p(a, b)$ for all b. In Claims 5 and 6 below, we provide the values of $S_p(a, b)$ for some other co-prime pairs (a, b).

Claim 5. *For any prime p congruent to 1 modulo 4,*

$$S_p(2, 1) = 0\,. \tag{12}$$

Proof. From Claim 2, we have $S_p(2, 1) = -S_p(2, 1)$, because $\left(\frac{-1}{p} \right) = 1$. □

Claim 6. *For any prime p congruent to 7 modulo 8,*

$$S_p(2, 1) = 0 \tag{13}$$

and

$$S_p(4,1) = 0 = S_p(4,3)\ . \tag{14}$$

Proof. We establish (13) as follows:

$$\begin{aligned}
2S_p(2,1) &= 2\sum_{k=0}^{p-1}\left(\frac{2k+1}{p}\right)k = \sum_{k=0}^{p-1}\left(\frac{2k+1}{p}\right)(2k+1) - \sum_{k=0}^{p-1}\left(\frac{2k+1}{p}\right) \\
&= \sum_{\substack{0<l<2p \\ l\ odd}}\left(\frac{l}{p}\right)l = \sum_{0<l<2p}\left(\frac{l}{p}\right)l - \sum_{\substack{0<l<2p \\ l\ even}}\left(\frac{l}{p}\right)l \\
&= \sum_{0<l<p}\left(\left(\frac{l}{p}\right)l + \left(\frac{l+p}{p}\right)(l+p)\right) - \sum_{0<l<p}\left(\frac{2l}{p}\right)2l \\
&= 2\left(1-\left(\frac{2}{p}\right)\right)\sum_{0<l<p}\left(\frac{l}{p}\right)l + p\sum_{0<l<p}\left(\frac{l}{p}\right) = 0,
\end{aligned}$$

because $\left(\frac{2}{p}\right) = 1$.

In (14), $S_p(4,1) = 0$ by Lemma 2. The second equality follows from the first by Claim 2.

□

The following procedure summarizes our findings:

Theorem 1. *Let p be an odd prime, and let a be an integer, relatively prime to p. For any integer b, relatively prime to a, the value of $S_p(a,b)$ can be computed in the following way:*

1. *Let k be the smallest (positive) integer such that $ka \equiv b \pmod{p}$. Then, by Property 1,*

$$S_p(a,b) = S_p(a,ka)\ . \tag{15}$$

2. *Using Claim 3, reduce $S_p(a,ka)$ by*

$$S_p(a,ka) = \left(\frac{a}{p}\right)S_p(1,k). \tag{16}$$

3. *Further reduce $S_p(1,k)$ according to*

$$S_p(1,k) = S_p(1,0) + p\sum_{j=0}^{k-1}\left(\frac{j}{p}\right) \tag{17}$$

which is a particular case of (9), the Corollary of Claim 4.

Or, summarizing 1–3 in a single formula,

$$S_p(a,b) = \left(\frac{a}{p}\right)\left(S_p(1,0) + p\sum_{j=0}^{k-1}\left(\frac{j}{p}\right)\right). \tag{18}$$

Below, we illustrate the use of Theorem 1.

Example. Compute $S_{53}(7,13)$.

Following the steps outlined above, we solve the linear congruence $7k \equiv 13 \pmod{53}$. The smallest positive integer solution is $k = 17$ and

$$S_{53}(7,13) = \left(\frac{7}{53}\right) S_{53}(1,17) = S_{53}(1,17), \text{ for } \left(\frac{7}{53}\right) = 1.$$

Thus, we need to find $S_{53}(1,17)$. Since 53 is of the form $4n+1$, the sum $S_{53}(1,0)$ vanishes. Therefore

$$S_{53}(1,17) = 53\sum_{j=0}^{16}\left(\frac{j}{53}\right).$$

Among the integers from 1 to 16, quadratic residues modulo 53 are 1, 4, 6, 7, 9, 10, 11, 13, 15, 16. Hence, the last sum above has one zero term, 10 positive terms and 6 negative terms. Thus, $S_{53}(1,17) = 53 \cdot 4 = 212$. □

In Table 1 we show the relatively prime pairs (a,b) with $1 \le a \le 16$ and $|b| \le 25$ for which the value of $S_p(a,b)$ is either $0, \pm p,$ or $\pm 2p$ for every prime p of the specified form.

p	$8n+1$	$8n+3$	$8n+5$	$8n+7$
$S_p(1,-2)$	$-2p$		0	
$S_p(1,0)$	0		0	
$S_p(1,2)$	p		p	
$S_p(1,3)$	$2p$		0	
$S_p(2,-1)$	$-p$		$-p$	p
$S_p(2,1)$	0		0	0
$S_p(2,3)$	p		p	p
$S_p(4,1)$				0
$S_p(6,1)$			0	0

Table 1: Relatively prime pairs (a,b) whose value of $S_p(a,b) = 0, \pm p, \pm 2p$.

Note that for $p = 8n+3$ the values of $S_p(a,b)$ do not follow any simple pattern.

Acknowledgements. The presented proof of Lemma 2 is a slightly modified version of a proof by Dr. Henryk Iwaniec, contributed by personal communication [4]. Our many thanks go to him. We thank Dr. Ognian Trifonov for his expert suggestions and enthusiastic encouragement without which this paper would not have materialized. He also suggested `Integers` as a publication venue. Dr. Tzvetalin S. Vassilev acknowledges the financial support of his research provided by the Natural Sciences and Engineering Research Council of Canada (NSERC) through Discovery Grant.

References

[1] Gerald A. Edgar, Doug Hensley and Douglas B. West, editors. Problems and Solutions. *Amer. Math. Monthly*, **120(8)** (2013), 754.

[2] Johann Carl Friedrich Gauß. *Disquisitiones Arithmeticæ* §4, arts 107-150, Leipzig, 1801.

[3] Adrien-Marie Legendre. *Essai sur la Theorie des Nombres*, p. 186, Paris, 1798.

[4] Henryk Iwaniec. Personal Communication. 2014.