DOI: 10.1515/auom-2017-0033
An. Şt. Univ. Ovidius Constanţa **Vol. 25(3),2017, 37–44**

On some special Legendre sums of the form $\sum_{x=1}^{p-1}\left(\frac{f(x)}{p}\right)g(x)$

Dorin Andrica and Vlad Crişan

Abstract

We prove that sums of the form $S=\sum_{x=0}^{p-1}\left(\frac{g(x)}{p}\right)f(x)$ with $f(X)$, $g(X)\in\mathbb{Z}[X]$ can be explicitly computed whenever f and g are subject to some certain conditions which are defined in the paper.

1 Introduction

Problem 11728 published in The American Mathematical Monthly, October 2013 asks to prove the identity

$$\sum_{k=1}^{p}\lfloor\frac{k^2+k}{p}\rfloor=\frac{2p^2+3p+7}{6}.$$

where $\lfloor x\rfloor$ is the floor of x and p is a prime of the form $8n-1$. In The American Mathematical Monthly, October 2015, O.P.Lossers gives a direct proof to this identity. It has been noted on several forums and also in [3] that the problem is equivalent to proving the identity

Key Words: Legendre sums, Elementary Number Theory, computable.
2010 Mathematics Subject Classification: Primary 11A07, 11A15; Secondary 11C08, 11C20.
Received: 11.01.2017
Accepted: 31.01.2017

$$\sum_{j=1}^{p-1}\left(\frac{4j+1}{p}\right)j=0,$$

where $(\frac{a}{p})$ is the Legendre symbol (see [1] for definition and basic properties). The work is then further generalized in [3], showing how one can explicitly compute sums of the form

$$S=\sum_{x=1}^{p-1}\left(\frac{ax+b}{p}\right)x.$$

In this article we generalise this to showing that sums of the form $S=\sum_{x=0}^{p-1}\left(\frac{g(x)}{p}\right)f(x)$ with $f(X),g(X)\in\mathbb{Z}[X]$ can be explicitly computed whenever f and g are subject to some certain conditions, which are explicitly stated in Definition 1, Definition 2 and Definition 3 in the next section. The main result of this paper is Theorem 1.

2 Main results

Definition 1. *Let p be a prime number, $n\geq 0$ a non-negative integer and let $f_n(X)=a_{2n+1}X^{2n+1}+a_{2n}X^{2n}+\ldots+a_1X+a_0\in\mathbb{Z}[X]$ be a polynomial of degree $2n+1$. We say that f_n is* **good for** *p if there exists a sequence of integers $0=n_0<n_1<\ldots<n_k=2n+1$ (here $k\geq 1$) and polynomials $f_{n_0},f_{n_1},\ldots,f_{n_k}\in\mathbb{Z}[X]$ with $\deg(f_k)=n_k$ such that $f_{n_j}(p-X)+f_{n_j}(X)=f_{n_{j-1}}(X)$ for all $1\leq j\leq k$.*

Notice that in particular all linear polynomials are good for p. We will prove that for each $n\geq 0$, there exist infinitely many polynomials of degree $2n+1$ which are good for p. Before we do this, we prove the following result, which shows that if a polynomial good for p of degree $2n+1$ exists, it satisfies a very rigid property.

Lemma 1. *If $f_n(X)$ is a good polynomial for p of degree $2n+1$, then $f_n(X)+f_n(p-X)$ is a constant polynomial. In particular, k is always equal to 1 in the above definition.*

Proof. We shall prove the result by induction on $n\geq 0$. When $n=0$, things are clear, since $f_0(X)$ is then a linear polynomial, hence $f_0(X)+f_0(p-X)$ must be a a constant polynomial.

Assume now that the result holds for all polynomials of degree at most $2n-1$ ($n\geq 1$) and consider a polynomial $f_n(X)$ of degree $2n+1$ which is good for p.

Since $f_n(X)$ is good for p, by definition it must be that $h(X) = f_n(X)+f_n(p-X)$ is either a constant polynomial, or $h(X)$ is a polynomial which is also good for p. If the former holds, we are done. Otherwise, we deduce that $h(X)$ must be a polynomial of odd degree, as otherwise $\deg(h(X)+h(p-X)) = \deg(h(X))$ whenever $h(X)$ is a polynomial of even degree, contradicting the fact that $h(X)$ is good for p. As $\deg(h) < \deg(f)$, it follows that $\deg(h(X)) \leq 2n-1$. But now by the induction hypothesis one has that $h(X)+h(p-X)$ is a constant polynomial. As $h(X)+h(p-x) = 2(f(X)+f(p-X))$, we obtain the desired result. □

We now prove that for each $n \geq 0$, there exist infinitely many polynomials of degree $2n+1$ which are good for p, and also give an explicit description of the degrees of freedom we have in choosing such polynomials.

Lemma 2. *For each $n \geq 0$, there exist infinitely many polynomials of degree $2n+1$ which are good for p. Moreover, certain $n+2$ out of the $2n+2$ coefficients a_0, a_1, …, a_{2n+1} can be chosen up to some divisibility conditions as free variables.*

Proof. By Lemma 1, it suffices to prove the result when $f_n(X) = a_0 + a_1X + \ldots + a_{2n+1}X^{2n+1} \in \mathbb{Z}[X]$ satisfies $f_n(X) + f_n(p-X) = c$, for some $c \in \mathbb{Z}$. It can be easily seen by identifying the coefficients of X^k for $k = 1, 2, \ldots, 2n+1$, that the problem reduces to studying the linear system

$$A\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{2n+1}\end{pmatrix} = \begin{pmatrix} c \\ 0 \\ 0 \\ \vdots \\ 0\end{pmatrix},$$

where the matrix $A \in \mathcal{M}_{2n+2}(\mathbb{Z})$ has its rows and columns indexed from 0 to $2n+1$ (to ease the other notations) and is given by

$$A_{jk} = \begin{cases} (-1)^j\binom{k}{j}p^{k-j} & \text{if } k > j; \\ 1+(-1)^j & \text{if } j = k; \\ 0 & \text{if } j > k, \end{cases} \tag{*}$$

for all $0 \leq j, k \leq 2n+1$.

We first note that the system is compatible, since none of the operations which are required for bringing A in row-reduced form involves the first row, hence the extended matrix obtained by adjoining $\begin{pmatrix} c \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ to A leaves the rank of A unchanged. Therefore, the system is compatible and a good polynomial exists for every $n \geq 0$.

We now claim that the rank of A is equal to $n+1$. It is easy to see that this is a lower bound for the rank, since A is upper triangular and it has $n+1$ non-zero entries on the main diagonal. To prove that equality is attained, we will use induction on n:

The result is clear for $n = 0$. Assume now that the result holds for $n-1$ ($n \geq 1$) and let B denote the matrix which is obtained in this case by the above procedure. To prove the induction step, we consider the $(2n+2) \times (2n+2)$ matrix A as above. Notice that by deleting the last two rows and the last two columns of A, we obtain the matrix B. Moreover, we have $\frac{A_{2n-1,2n}}{A_{2n,2n}} = \frac{A_{2n-1,2n+1}}{A_{2n,2n+1}} = -np$ (recall that the rows and columns are labeled from 0 to $2n+1$), so by performing the operation $R_{2n} \to R_{2n} \cdot np + R_{2n-1}$, we obtain the last two rows in the matrix A equal to 0. Hence $\operatorname{rank}(A) \leq \operatorname{rank}(B)+1 = n+1$ and since $\operatorname{rank}(A) \geq n+1$ by the above observation, we obtain $\operatorname{rank}(A) = n+1$, as we wanted. Since up to some divisibility conditions, the integer c from (*) can be chosen itself to be a free variable, we obtain a total of $n+2$ degrees of freedom in choosing the coefficients a_0, a_1, …, a_{2n+1}, as we claimed. □

Remark 1. *In view of the above result, we have the following examples for good polynomials of degree n for* $n = 0, 1, 2$*:* $f_0 = v_1X + v_2$, $f_1(X) = -2v_1X^3 + 3pv_1X^2 + v_2X + v_3$ *and* $f_2(X) = -2v_1X^5 + 5pv_1X^4 + 2pv_2X^3 - (5p^3v_1 + 3pv_2)X^2 + v_3X + v_4$*, where* $v_1, v_2, \ldots$ *are arbitrary integers. The general form can be explicitly determined for every n from the above result, but it is not the purpose of this article to do that.*

We shall now consider sums of the form $S = \sum_{x=1}^{p-1}\left(\frac{g(x)}{p}\right)f(x)$ when $f(X) \in \mathbb{Z}[X]$ is a polynomial good for p and $g(X) \in \mathbb{Z}[X]$ satisfies some required properties. This will generalize the results discussed in [3] to higher order sums. We introduce the following definitions:

Definition 2. *We call a polynomial* $g(X) \in \mathbb{Z}[X]$ **nice for** p *if the sum* $\sum_{x=0}^{p-1}\left(\frac{g(x)}{p}\right)$ *can be explicitly computed.*

Notice that every constant polynomial is nice and every linear polynomial is also nice, since for $p \nmid a$ ($p \mid a$ reduces the problem to a constant polynomial) one has that $\{ax + b : x \in (\mathbb{Z}/p\mathbb{Z})^*\}$ is a complete set of residues modulo p, hence $\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right) = 0$. Moreover, using Euler's criterion and other elementary manipulations one can easily show that

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

In particular, this shows that every polynomial of degree at most 2 is nice for p. Furthermore, using the multiplicativity of the Legendre symbol, we deduce immediately that we can generate another family of polynomials which are nice for p, namely those of the form $g(X) = h(X)^2 \cdot s(X)$, where $h(X), s(X) \in \mathbb{Z}[X]$ and $\deg(s(X)) \leq 2$.

Things become significantly more involved when one has general sums of the form

$$S = \sum_{x=0}^{p-1}\left(\frac{g(x)}{p}\right),$$

for $g(X) \in \mathbb{Z}[X]$ a polynomial of degree at least 3. Explicit computation of such sums seems out of reach and one is content to find bounds for this kind of expressions. First good bounds were obtained by Weil in [6] and more recent improvements can be found in [2] and [5].

Definition 3. *A sum* $S = \sum_{x=1}^{p-1}\left(\frac{g(x)}{p}\right)f(x)$ *is called* **friendly** *if* $f(X) \in \mathbb{Z}[X]$ *is a polynomial which is good for* p *and* $g(X) \in \mathbb{Z}[X]$ *is a polynomial which is nice for* p *and one of the following situations holds:*

a) $g(X)$ *is linear and then also* $f(X)$ *is linear;*

b) $\deg(g(X))$ *is even and* $g(X) - g(p - X)$ *is the zero polynomial when reduced modulo* p*;*

c) $\deg(g(X))$ *is odd and then* $p \equiv 1 \pmod 4$ *and* $g(X) + g(p - X)$ *is the zero polynomial when reduced modulo* p.

Notice that friendly sums include in particular all sums of the form $S = \sum_{x=1}^{p-1}\left(\frac{g(x)}{p}\right)f(x)$ where both f and g are linear polynomials.

The main result of this paper, which generalizes the work covered in [3], is the following:

Theorem 1. *If the sum* $S = \sum_{x=1}^{p-1}\left(\frac{g(x)}{p}\right)f(x)$ *is friendly, then* S *can be computed explicitly.*

Proof. The situation when S is of the form

$$S=\sum_{x=1}^{p-1}\left(\frac{ax+b}{p}\right)x$$

for $p\nmid a$ and $\gcd(a,b)=1$ was treated in [3], Theorem 1. This easily extends to the cases $\gcd(a,b)>1$ by the multiplicativity of the Legendre symbol and also to any expression of the form $S=\sum_{x=1}^{p-1}\left(\frac{ax+b}{p}\right)(cx+d)$ by writing

$$S=c\sum_{x=1}^{p-1}\left(\frac{ax+b}{p}\right)x+d\sum_{x=1}^{p-1}\left(\frac{ax+b}{p}\right)$$

and using the property that $\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)=0$, which we mentioned above.

When $\deg(g(X))$ is even and $g(X)\equiv g(p-X) \pmod p$, we proceed as follows:

$$\begin{aligned}S&=\sum_{x=1}^{p-1}\left(\frac{g(x)}{p}\right)f(x)\\&=\sum_{x=1}^{p-1}\left(\frac{g(p-x)}{p}\right)f(x-p)\\&=\sum_{x=1}^{p-1}\left(\frac{g(x)}{p}\right)(c-f(x)),\end{aligned}$$

where the last equality follows from the fact that $f(x)$ is good for p, hence by Lemma 1 there must be some constant $c\in\mathbb{Z}[X]$ such that $f(X)+f(p-X)=c$.

It follows that

$$2S=c\sum_{x=1}^{p-1}\left(\frac{g(x)}{p}\right),$$

and since $g(X)$ is a nice polynomial, the term in the right-hand side can be explicitly computed.

Finally, if $\deg(g(X))$ is odd, $p \equiv 1 \pmod 4$ and $g(X) \equiv -g(p-X) \pmod p$, we have

$$\begin{aligned} S &= \sum_{x=1}^{p-1} \left(\frac{g(x)}{p}\right) f(x) \\ &= \sum_{x=1}^{p-1} \left(\frac{g(p-x)}{p}\right) f(x-p) \\ &= \sum_{x=1}^{p-1} \left(\frac{-g(x)}{p}\right) (c - f(x)) \\ &= \sum_{x=1}^{p-1} \left(\frac{g(x)}{p}\right) (c - f(x)), \end{aligned}$$

where for the last equality we have used the fact that $\left(\frac{-1}{p}\right) = 1$, for $p \equiv 1 \pmod 4$. Hence, as above, we obtain that

$$2S = c \sum_{x=1}^{p-1} \left(\frac{g(x)}{p}\right),$$

which can be explicitly computed. □

References

[1] T. Andreescu, D. Andrica, *Number Theory. Structures, Examples, and Problems*, Birkhauser Verlag, Boston-Berlin-Basel, 2009.

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

[3] B. Karaivanov, *On certain sums involving the Legendre symbol*, INTEGERS nr. 16, 2016.

[4] N. M. Korobov, *Estimate of the sum of Legendre symbols*, Dokl. Akad. Nauk SSSR,196, No. 4, 764767 (1971).

[5] D.A. Mit'kin *Estimate of a sum of Legendre symbols of polynomials of even degree*, Mathematical notes of the Academy of Sciences of the USSR, July 1973, Volume 14, Issue 1, pp 597-602.

[6] A. Weil, *Sur les courbes algébriques et les variétés qui sen déduisent*, Actualités Sci. Ind. (Hermann et Cie., Paris, 1948), Vol. 1041.

Dorin ANDRICA,
Department of Mathematics,
"Babeş-Bolyai" University, Cluj Napoca,
Mihail Kogalniceanu Street 1, Cluj-Napoca, Romania.
Email: dandrica@math.ubbcluj.ro

Vlad CRIŞAN,
Department of Mathematics,
University of Göttingen,
Bunsenstraße 3-5, Göttingen, Germany.
Email: vlad.crisan@mathematik.uni-goettingen.de