Congruences for Brewer sums

Šaban Alaca

Centre for Research in Algebra and Number Theory, School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6

Received 27 October 2004
Communicated by Peter Shiue
Available online 10 August 2005

Abstract
We prove congruences modulo 4 and modulo 8 for certain polynomial character sums, and use these congruences to give conditions for the nonvanishing of Brewer sums.

© 2005 Elsevier Inc. All rights reserved.

MSC: 11L10; 11T24; 12Y05; 12E10; 12D05; 13P05

Keywords: Brewer sums; Character sums; Jacobsthal sums; Gauss sums; Dickson polynomials; Special polynomials; Factorization of polynomials; Finite fields

1. Introduction

For each natural number $n$ and each nonzero complex number $a$, the Dickson polynomial $V_n(x, a)$ of the first kind of degree $n$ is defined by

$$V_n(x, a) = \sum_{j=0}^{[n/2]} \frac{n}{n-j} \binom{n-j}{j} (-1)^j a^j x^{n-2j},$$

$E-mail$ address: salaca@math.carleton.ca.
or inductively, by

\[ V_1(x, a) = x, \quad V_2(x, a) = x^2 - 2a, \]

\[ V_{n+1}(x, a) = xV_n(x, a) - aV_{n-1}(x, a), \quad n \geq 2. \]

The Dickson polynomial \( V_n(x, a) \in \mathbb{C}[x] \) can also be defined to be the unique polynomial with the property that

\[ V_n(y + (a/y)^{-1}, a) = y^n + (a/y)^n, \quad n \geq 1, \]

or equivalently by the explicit expression

\[ V_n(x, a) = \left( x + \frac{\sqrt{x^2 - 4a}}{2} \right)^n + \left( x - \frac{\sqrt{x^2 - 4a}}{2} \right)^n, \quad n \geq 1. \]

When \( a = 1 \), we set \( V_n(x) = V_n(x, 1) \). For more information on Dickson polynomials, see Berndt et al.’s book [1, p. 440], Lidl et al.’s book [7], or Lidl and Niederreiter’s book [8, p. 355].

For an odd prime \( p \) and an integer \( a \) not divisible by \( p \), the generalized Brewer sum \( \Lambda_n(a) \) is defined for a natural number \( n \) by

\[ \Lambda_n(a) = \sum_{x=0}^{p-1} \left( \frac{V_n(x, a)}{p} \right), \]

where \( \left( \frac{\ast}{p} \right) \) is the Legendre symbol (mod \( p \)). For \( a = 1 \), we set \( \Lambda_n = \Lambda_n(1) \), which is called the ordinary Brewer sum.

Brewer sums \( \Lambda_n \) were first studied by Brewer [3] in 1961. In his paper Brewer evaluated \( \Lambda_3, \Lambda_4 \) and \( \Lambda_5 \). In 1966 Brewer [4] introduced the sum \( \Lambda_n(a) \) and evaluated it for \( n = 5 \). In 1997 Leprévost and Morain [6] used the evaluation of \( \Lambda_5(a) \) in order to count the number of points on a certain elliptic curve with complex multiplication by \( \mathbb{Z}[\sqrt{-5}] \).

For detailed properties of Brewer sums, see [1, Chapter 13]. This chapter is devoted to Brewer sums, and at the end of Chapter 13 an excellent survey on the historical development of the subject is given.

An important question is to determine a necessary and sufficient condition for \( \Lambda_n(a) = 0 \) (or \( \Lambda_n(a) \neq 0 \)). In this paper we focus our attention on the vanishing or nonvanishing of \( \Lambda_n(a) \) when \( n \) is an odd prime.

It is known that \( V_n(x, a) \) is a permutation polynomial over \( \mathbb{F}_p \) if and only if \((n, p^2 - 1) = 1\), and so \( \Lambda_n(a) = 0 \), see [8, 7.16 Theorem]. For \((n, p^2 - 1) > 1\), the question of determining when \( \Lambda_n(a) = 0 \) remains open.
If \( p \equiv 3(\text{mod } 4) \), then it is known that \( \Lambda_n(a) = 0 \), see [1, Theorem 13.2.2]. Thus, the question remains open when \( p \equiv 1(\text{mod } 4) \).

For odd primes \( n \) and \( p \) with \( (n, p^2 - 1) > 1 \) and \( p \equiv 1(\text{mod } 4) \), either \( p \equiv 1(\text{mod } n) \) or \( p \equiv -1(\text{mod } n) \). For these two cases, we develop some properties of certain polynomial character sums. Then, we make use of the factorization properties of Dickson polynomials over finite fields, see [2,9], and prove congruences \( (\text{mod } 4) \) and \( (\text{mod } 8) \) for \( \Lambda_n(a) \), see Theorems 3.3 and 3.4. From these theorems we deduce our main result:

**Theorem 1.1.** Let \( n \) and \( p \) be odd primes with \( (n, p^2 - 1) > 1 \) and \( p \equiv 1(\text{mod } 4) \).

(i) Let \( p \equiv 1(\text{mod } n) \). If \( a \in \mathbb{F}_p \) is a quadratic residue and \( n \equiv 3(\text{mod } 4) \), or if \( a \in \mathbb{F}_p \) is a quadratic nonresidue, then \( \Lambda_n(a) \neq 0 \).

(ii) Let \( p \equiv -1(\text{mod } n) \). If \( a \in \mathbb{F}_p \) is a quadratic residue, \( p \equiv 5(\text{mod } 8) \) and \( n \equiv 3(\text{mod } 4) \), or if \( a \in \mathbb{F}_p \) is a quadratic nonresidue and \( n \equiv 3(\text{mod } 4) \), then \( \Lambda_n(a) \neq 0 \).

2. **Explicit factorization of Dickson polynomials over \( \mathbb{F}_p \)**

In order to prove Theorem 1.1, we make use of the factorization of Dickson polynomials over \( \mathbb{F}_p \).

Let \( p \) be an odd prime, let \( n \) be an odd prime with \( p \nmid n \), let \( a \) be an integer not divisible by \( p \), and let \( \sqrt{a} \) represent a fixed square root of \( a \) in the algebraic closure \( \overline{\mathbb{F}}_p \) of \( \mathbb{F}_p \). It is known that the factorization of \( V_n(x, a) \) over \( \overline{\mathbb{F}}_p[x] \) is given by

\[
V_n(x, a) = \prod_{l=1}^{2n} \left( x - \sqrt{a} \left( \rho^l + \rho^{-l} \right) \right),
\]

where \( \sqrt{a} \) represents a fixed square root of \( a \) in \( \overline{\mathbb{F}}_p \). See [2, Theorem 1], [5, Corollary 7], [7, p. 45] or [9, Theorem 1].

The following two Theorems give the explicit factorization of \( V_n(x, a) \) over \( \mathbb{F}_p[x] \), which follow from the factorization in (2.1).

**Theorem 2.1.** Let \( n \) and \( p \) be odd primes such that \( p \equiv 1(\text{mod } 4) \) and \( p \equiv 1(\text{mod } n) \). Let \( g \) be a primitive root \( (\text{mod } p) \), and let \( h = g^{\frac{p-1}{4n}} \).

(i) If \( a \in \mathbb{F}_p \) is a quadratic residue, then the factorization of \( V_n(x, a) \) into irreducibles in \( \mathbb{F}_p[x] \) is

\[
V_n(x, a) = \prod_{l=1}^{2n} \left( x - \sqrt{a} \left( h^l + h^{-l} \right) \right),
\]

where \( \sqrt{a} \) represents a fixed square root of \( a \) in \( \mathbb{F}_p \).
(ii) If \(a \in \mathbb{F}_p\) is a quadratic nonresidue, then the factorization of \(V_n(x, a)\) into irreducibles in \(\mathbb{F}_p[x]\) is
\[
V_n(x, a) = x \prod_{l=1}^{n-2} \left( x^2 - a \left( h^l + h^{-l} \right)^2 \right). \tag{2.3}
\]

**Proof.** We note that \(h = g^{p-1 \over 4n}\) is a primitive \(4n\)th root of unity in \(\mathbb{F}_p\) and \(h^n + h^{-n} = 0\).

(i) Since \(a \in \mathbb{F}_p\) is a quadratic residue, the factorization of \(V_n(x, a)\) given in (2.2) follows from the factorization in (2.1).

(ii) Since \(a \in \mathbb{F}_p\) is a quadratic nonresidue, then \(\sqrt{a} (h^l + h^{-l}) \notin \mathbb{F}_p\), where \(\sqrt{a}\) represents a fixed square root of \(a\) in \(\mathbb{F}_p\). It follows from
\[
h^{2n-l} + h^{-(2n-l)} = -h^{-l} - h^l
\]
that
\[
\left( x - \sqrt{a} \left( h^l + h^{-l} \right) \right) \left( x - \sqrt{a} \left( h^{2n-l} + h^{-(2n-l)} \right) \right)
\]
\[
= \left( x - \sqrt{a} \left( h^l + h^{-l} \right) \right) \left( x + \sqrt{a} \left( h^l + h^{-l} \right) \right)
\]
\[
= x^2 - a \left( h^l + h^{-l} \right)^2,
\]
which is irreducible in \(\mathbb{F}_p[x]\). Thus, the factorization of \(V_n(x, a)\) given in (2.3) follows from the factorization in (2.1). \(\square\)

**Theorem 2.2.** Let \(n\) and \(p\) be odd primes such that \(p \equiv 1 \pmod{4}\) and \(p \equiv -1 \pmod{n}\), so that \(p^2 - 1 \in \mathbb{N}\). Let \(\gamma\) be a generator of the cyclic group \(\mathbb{F}_p^*\) of order \(p^2 - 1\). Set
\[
\theta = \gamma^{(p^2-1)/4n} \in \mathbb{F}_p^2.
\]

(i) If \(a \in \mathbb{F}_p\) is a quadratic residue, then the factorization of \(V_n(x, a)\) into irreducibles in \(\mathbb{F}_p[x]\) is
\[
V_n(x, a) = x \prod_{l=1}^{n-2} \left( x^2 - a \left( \theta^l + \theta^{-l} \right)^2 \right). \tag{2.4}
\]

(ii) If \(a \in \mathbb{F}_p\) is a quadratic nonresidue, then the factorization of \(V_n(x, a)\) into irreducibles in \(\mathbb{F}_p[x]\) is
\[
V_n(x, a) = x \prod_{l=1}^{2n-1} \left( x - \sqrt{a} \left( \theta^l + \theta^{-l} \right)^2 \right), \tag{2.5}
\]
where \(\sqrt{a} \left( \theta^l + \theta^{-l} \right)^2\) represents a fixed square root of \(a \left( \theta^l + \theta^{-l} \right)^2\) in \(\mathbb{F}_p\).
Proof. We note that $\theta = \gamma^{(p^2-1)/4n}$ is a primitive $4n$th root of unity in $\mathbb{F}_{p^2}$ and $\theta^n + \theta^{-n} = 0$.

(i) We have

$$\theta^{p+1} = \left(\gamma^{\frac{p^2-1}{4n}}\right)^{p+1} = \gamma^{\frac{(p^2-1)(p+1)}{4n}} = \gamma^{\frac{p^2-1}{2} \cdot \frac{p+1}{2n}} = (-1)^{\frac{p+1}{2n}} = -1,$$

which implies that $\theta^p = -\theta^{-1}$. Hence for $(l, 2n) = 1$ we have

$$(\theta^l + \theta^{-l})^p = (\theta^p)^l + (\theta^p)^{-l} = -\theta^{-l} - \theta^l.$$

Thus $\theta^l + \theta^{-l} \notin \mathbb{F}_p$. On the other hand, we have

$$\left((\theta^l + \theta^{-l})^2\right)^p = \left((\theta^l + \theta^{-l})^p\right)^2 = (-\theta^l + \theta^{-l})^2 = (\theta^l + \theta^{-l})^2.$$

Thus $(\theta^l + \theta^{-l})^2 \in \mathbb{F}_p$ is a quadratic nonresidue. Since $a$ is a quadratic residue in $\mathbb{F}_p$, we see that $a(\theta^l + \theta^{-l})^2$ is a quadratic nonresidue in $\mathbb{F}_p$. We also note that

$$\theta^{2n} = \left(\gamma^{\frac{p^2-1}{4n}}\right)^{2n} = \gamma^{\frac{p^2-1}{2}} = -1$$

and

$$\theta^{2n-l} + \theta^{-(2n-l)} = \theta^{2n} \theta^{-l} + \theta^{-2n} \theta^l = -\theta^{-l} - \theta^l.$$

Hence we have

$$(x - \sqrt{a}(\theta^l + \theta^{-l}))(x - \sqrt{a}(\theta^{2n-l} + \theta^{-(2n-l)}))$$

$$= (x - \sqrt{a}(\theta^l + \theta^{-l}))(x + \sqrt{a}(\theta^l + \theta^{-l}))$$

$$= x^2 - a(\theta^l + \theta^{-l})^2,$$

which is irreducible in $\mathbb{F}_p[x]$. Thus, the factorization of $V_n(x, a)$ given in (2.4) follows from the factorization in (2.1).

(ii) If $a \in \mathbb{F}_p$ is a quadratic nonresidue, then $a(\theta^l + \theta^{-l})^2 \in \mathbb{F}_p$ is a quadratic residue, and the factorization of $V_n(x, a)$ given in (2.5) follows from the factorization in (2.1). □
3. Congruences for certain character sums

In this section we prove some congruences modulo 4 and modulo 8 for certain character sums. These congruences are used together with the factorization of Dickson polynomials given in Section 2 to prove our main result (Theorem 1.1) in the next section.

**Theorem 3.1.** Let $p$ be a prime with $p \equiv 1 \pmod{4}$. Let $k$ be a nonnegative integer. Let $a_0, a_1, \ldots, a_k$ be integers which are incongruent modulo $p$. Then

$$
\sum_{x=0}^{p-1} \left( \frac{(x+a_0)(x+a_1)\cdots(x+a_k)}{p} \right) \equiv \begin{cases} 
0 \pmod{4} & \text{if } k \equiv 0 \pmod{4}, \\
3 \pmod{4} & \text{if } k \equiv 1 \pmod{4}, \\
2 \pmod{4} & \text{if } k \equiv 2 \pmod{4}, \\
1 \pmod{4} & \text{if } k \equiv 3 \pmod{4}.
\end{cases}
$$

**Proof.** We note that as $a_0, a_1, \ldots, a_k$ are incongruent modulo $p$ we have $k \leq p-1$. Set

$$S(a_0, a_1, \ldots, a_k) := \sum_{x=0}^{p-1} \left( \frac{(x+a_0)(x+a_1)\cdots(x+a_k)}{p} \right).$$

Since

$$S(a_0) = \sum_{x=0}^{p-1} \left( \frac{x+a_0}{p} \right) = 0 \equiv 0 \pmod{4}$$

the result is true for $k = 0$.

It follows from [1, Theorem 2.1.2] that (as $a_0 \not\equiv a_1 \pmod{p}$)

$$S(a_0, a_1) = \sum_{x=0}^{p-1} \left( \frac{(x+a_0)(x+a_1)}{p} \right) = -1 \equiv 3 \pmod{4}.$$

Thus the result is true for $k = 1$.

For $k = 2$, we have

$$\sum_{x=0}^{p-1} \left( \frac{x+a_0}{p} \right) \left( \frac{x+a_1}{p} \right) \left( \frac{x+a_2}{p} \right) \equiv 0 \pmod{4}. $$
Thus
\[
\sum_{x=0}^{p-1} \frac{(x + a_0)(x + a_1)(x + a_2)}{p} - \sum_{x=0}^{p-1} \frac{(x + a_1)(x + a_2)}{p}
\]
\[
- \sum_{x=0}^{p-1} \frac{(x + a_0)(x + a_2)}{p} + \sum_{x=0}^{p-1} \frac{x + a_2}{p} \equiv 0 \pmod{4}.
\]

Hence
\[
S(a_0, a_1, a_2) - \left( S(a_1, a_2) - \frac{(a_1 - a_0)}{p} \left( \frac{a_2 - a_0}{p} \right) \right)
\]
\[
- \left( S(a_0, a_2) - \frac{(a_0 - a_1)}{p} \left( \frac{a_2 - a_1}{p} \right) \right)
\]
\[
+ S(a_2) - \frac{(a_2 - a_0)}{p} - \frac{(a_2 - a_1)}{p} \equiv 0 \pmod{4}.
\]

Set
\[
A = \left( \frac{a_0 - a_1}{p} \right) = \pm 1, \quad B = \left( \frac{a_1 - a_2}{p} \right) = \pm 1, \quad C = \left( \frac{a_2 - a_0}{p} \right) = \pm 1.
\]

As \( p \equiv 1 \pmod{4} \), we have
\[
A = \left( \frac{a_1 - a_0}{p} \right), \quad B = \left( \frac{a_2 - a_1}{p} \right), \quad C = \left( \frac{a_0 - a_2}{p} \right).
\]

Hence
\[
S(a_0, a_1, a_2) + 1 + AC + 1 + AB + 0 - C - B \equiv 0 \pmod{4}.
\]

Thus
\[
S(a_0, a_1, a_2) \equiv -2 + (B + C) - A(B + C)
\]
\[
\equiv -2 + (B + C)(1 - A)
\]
\[
\equiv 2 \pmod{4}.
\]

Thus the result is true for \( k = 2 \) as well.
For $k \geq 3$, we have
\[
\sum_{x=0}^{p-1} \left( \left( \frac{x + a_0}{p} \right) - 1 \right) \left( \left( \frac{x + a_1}{p} \right) - 1 \right) \times \left( \frac{x + a_2}{p} \right) \cdots \left( \frac{x + a_k}{p} \right) \equiv 0 \pmod{4}.
\]

Expanding the product, we obtain
\[
S(a_0, a_1, \ldots, a_k) - S(a_1, \ldots, a_k) - \left( \frac{(a_1 - a_0)(a_2 - a_0) \cdots (a_k - a_0)}{p} \right)
- \left( S(a_0, a_2, \ldots, a_k) - \left( \frac{(a_0 - a_1)(a_2 - a_1) \cdots (a_k - a_1)}{p} \right) \right)
+ S(a_2, \ldots, a_k) - \left( \frac{(a_2 - a_0)(a_3 - a_0) \cdots (a_k - a_0)}{p} \right)
- \left( \frac{(a_2 - a_1) \cdots (a_k - a_1)}{p} \right) \equiv 0 \pmod{4}.
\]

Set
\[
A_i = \left( \frac{a_i - a_0}{p} \right), \quad B_i = \left( \frac{a_i - a_1}{p} \right), \quad i = 0, 1, \ldots, k.
\]

Then
\[
S(a_0, a_1, \ldots, a_k) - S(a_1, \ldots, a_k) - S(a_0, a_2, \ldots, a_k) + S(a_2, \ldots, a_k)
+ A_1 \cdots A_k + B_0 B_2 \cdots B_k - A_2 \cdots A_k - B_2 \cdots B_k \equiv 0 \pmod{4}.
\]

Hence, as $A_1 = B_0$ (since $p \equiv 1 \pmod{4}$), we have
\[
S(a_0, a_1, \ldots, a_k) - S(a_1, \ldots, a_k) - S(a_0, a_2, \ldots, a_k) + S(a_2, \ldots, a_k)
+ (A_1 - 1)(A_2 \cdots A_k + B_2 \cdots B_k) \equiv 0 \pmod{4}.
\]

Thus
\[
S(a_0, a_1, \ldots, a_k) \equiv S(a_1, \ldots, a_k) + S(a_0, a_2, \ldots, a_k)
- S(a_2, \ldots, a_k) \pmod{4}.
\]

(3.1)
For $k = 3$, from (3.1) we have

$$S(a_0, a_1, a_2, a_3) \equiv S(a_1, a_2, a_3) + S(a_0, a_2, a_3) - S(a_2, a_3) \pmod{4}$$

$$\equiv 2 + 2 - 3 \equiv 1 \pmod{4},$$

so the result is true for $k = 3$.

Now assume that the result is true for $0 \leq k \leq N$, where $N \geq 3$. Then $N + 1 \geq 4$. From (3.1), we have

$$S(a_0, a_1, \ldots, a_{N+1}) \equiv S(a_1, \ldots, a_{N+1}) + S(a_0, a_2, \ldots, a_{N+1})$$

$$- S(a_2, \ldots, a_{N+1}) \pmod{4}. \quad (3.2)$$

If $N + 1 \equiv 0 \pmod{4}$, then $N \equiv 3 \pmod{4}$ and $N - 1 \equiv 2 \pmod{4}$. By induction hypothesis, we have

$$S(a_1, \ldots, a_{N+1}) \equiv 1 \pmod{4}, \quad S(a_0, a_2, \ldots, a_{N+1}) \equiv 1 \pmod{4}$$

and

$$S(a_2, \ldots, a_{N+1}) \equiv 2 \pmod{4}.$$

Thus from (3.2), we obtain

$$S(a_0, a_1, \ldots, a_{N+1}) \equiv 1 + 1 - 2 \equiv 0 \pmod{4}.$$ 

If $N + 1 \equiv 1 \pmod{4}$, then $N \equiv 0 \pmod{4}$ and $N - 1 \equiv 3 \pmod{4}$. By induction hypothesis, we have

$$S(a_1, \ldots, a_{N+1}) \equiv 0 \pmod{4}, \quad S(a_0, a_2, \ldots, a_{N+1}) \equiv 0 \pmod{4}$$

and

$$S(a_2, \ldots, a_{N+1}) \equiv 1 \pmod{4}.$$

Thus from (3.2), we obtain

$$S(a_0, a_1, \ldots, a_{N+1}) \equiv 0 + 0 - 1 \equiv 3 \pmod{4}.$$ 

If $N + 1 \equiv 2 \pmod{4}$, then $N \equiv 1 \pmod{4}$ and $N - 1 \equiv 0 \pmod{4}$. By induction hypothesis, we have

$$S(a_1, \ldots, a_{N+1}) \equiv 3 \pmod{4}, \quad S(a_0, a_2, \ldots, a_{N+1}) \equiv 3 \pmod{4}.$$
and
\[ S(a_2, \ldots, a_{N+1}) \equiv 0 \pmod{4}. \]

Thus from (3.2), we obtain
\[ S(a_0, a_1, \ldots, a_{N+1}) \equiv 3 + 3 - 0 \equiv 2 \pmod{4}. \]

If \( N + 1 \equiv 3 \pmod{4} \), then \( N \equiv 2 \pmod{4} \) and \( N - 1 \equiv 1 \pmod{4} \). By induction hypothesis, we have
\[ S(a_1, \ldots, a_{N+1}) \equiv 2 \pmod{4}, \quad S(a_0, a_2, \ldots, a_{N+1}) \equiv 2 \pmod{4} \]
and
\[ S(a_2, \ldots, a_{N+1}) \equiv 3 \pmod{4}. \]

Thus from (3.2), we obtain
\[ S(a_0, a_1, \ldots, a_{N+1}) \equiv 2 + 2 - 3 \equiv 1 \pmod{4}, \]

which completes the proof of the inductive step. \( \square \)

**Theorem 3.2.** Let \( p \) be a prime with \( p \equiv 1 \pmod{4} \). Let \( a_1, \ldots, a_k \) be quadratic nonresidues \((\mod p)\). Then
\[
\sum_{x=1}^{p-1} \left( \frac{x^2 + a_1}{p} \right) \cdots \left( \frac{x^2 + a_k}{p} \right) \equiv \left\{ \begin{array}{ll}
p - 1 \pmod{8} & \text{if } 2 \mid k, \\
0 \pmod{8} & \text{if } 2 \nmid k.
\end{array} \right.
\]

**Proof.** Set
\[ S_p(a_1, \ldots, a_k) := \sum_{x=1}^{p-1} \left( \frac{x^2 + a_1}{p} \right) \cdots \left( \frac{x^2 + a_k}{p} \right). \]

For \( k = 1 \), by [1, Theorem 2.1.2], we have
\[ S_p(a_1) = \sum_{x=1}^{p-1} \left( \frac{x^2 + a_1}{p} \right) = -1 - \left( \frac{a_1}{p} \right) = -1 - (-1) = 0 \equiv 0 \pmod{8}, \]
proving that the result is true for \( k = 1 \).
For \( k = 2 \), we have

\[
S_p(a_1, a_2) = \sum_{x=1}^{p-1} \left( \frac{(x^2 + a_1)(x^2 + a_2)}{p} \right)
\]

\[
= \sum_{x=1}^{p-1} \left( \left( \frac{x^2 + a_1}{p} \right) - 1 \right) \left( \frac{x^2 + a_2}{p} \right) - \sum_{x=1}^{p-1} 1.
\]

\[
= 2 \sum_{x=1}^{p-1} \left( \left( \frac{x^2 + a_1}{p} \right) - 1 \right) \left( \frac{x^2 + a_2}{p} \right) - \sum_{x=1}^{p-1} 1.
\]

\[
\equiv 0 + S_p(a_1) + S_p(a_2) - (p - 1)(\mod 8)
\]

\[
\equiv 0 + 0 + 0 - (p - 1)(\mod 8)
\]

\[
\equiv p - 1(\mod 8).
\]

Hence the result is true for \( k = 2 \).

For \( k = 3 \), we have

\[
S_p(a_1, a_2, a_3) = \sum_{x=1}^{p-1} \left( \frac{(x^2 + a_1)(x^2 + a_2)(x^2 + a_3)}{p} \right)
\]

\[
= \sum_{x=1}^{p-1} \left( \left( \frac{x^2 + a_1}{p} \right) - 1 \right) \left( \frac{x^2 + a_2}{p} \right) \left( \frac{x^2 + a_3}{p} \right) - \sum_{x=1}^{p-1} 1.
\]

\[
\equiv 0 + S_p(a_1, a_2) + S_p(a_1, a_3) + S_p(a_2, a_3)
\]
\[-S_p(a_1) - S_p(a_2) - S_p(a_3) + (p - 1) \pmod{8} \equiv 0 + (p - 1) + (p - 1) + (p - 1) - 0 - 0 - 0 + (p - 1) \pmod{8} \equiv 0 (\pmod{8}).\]

Hence the result is true for \( k = 3 \) as well.

Now assume that the result is true for \( k = 1, 2, \ldots, N \quad (N \geq 3) \). Then \( N + 1 \geq 4 \) and

\[
S_p(a_1, \ldots, a_{N+1}) = \sum_{x=1}^{p-1} \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N+1})}{p} \right)
\]
\[-S_p(a_1, \ldots, a_{N-2}, a_N) - S_p(a_1, \ldots, a_{N-2}, a_{N+1}) + S_p(a_1, \ldots, a_{N-2})(\text{mod } 8)\]
\[
\equiv \begin{cases} 
-3(p - 1)(\text{mod } 8) & \text{if } 2 \mid N + 1, \\
4(p - 1)(\text{mod } 8) & \text{if } 2 \nmid N + 1,
\end{cases}
\equiv \begin{cases} 
p - 1(\text{mod } 8) & \text{if } 2 \mid N + 1, \\
0(\text{mod } 8) & \text{if } 2 \nmid N + 1,
\end{cases}
\]

which completes the proof of the inductive step. □

**Theorem 3.3.** Let \( p \) be a prime with \( p \equiv 1(\text{mod } 4) \). Let \( a_1, \ldots, a_k \) be quadratic nonresidues \((\text{mod } p)\). Then

\[
\sum_{x=1}^{p-1} \left( \frac{x(x^2 + a_1) \cdots (x^2 + a_k)}{p} \right) \equiv \begin{cases} 
0(\text{mod } 8) & \text{if } 2 \mid k, \\
(p - 1)(\text{mod } 8) & \text{if } 2 \nmid k.
\end{cases}
\]

**Proof.** Set

\[
T_p(a_1, \ldots, a_k) := \sum_{x=1}^{p-1} \left( \frac{x(x^2 + a_1) \cdots (x^2 + a_k)}{p} \right).
\]

For \( k = 1 \), we have

\[
T_p(a_1) = \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_1}{p} \right).
\]

This sum is a Jacobsthal sum, and by [1, Theorem 6.2.9] we have

\[
T_p(a_1) \equiv \pm 2B(\text{mod } 8),
\]

where the integers \(|A|\) and \(|B|\) are given uniquely by

\[
p = A^2 + B^2, \quad A \equiv 1(\text{mod } 2), \quad B \equiv 0(\text{mod } 2). \quad \quad (3.3)
\]

From (3.3) we have

\[
\pm 2B \equiv B^2 \equiv p - A^2 \equiv p - 1(\text{mod } 8)
\]
so that

\[ T_p(a_1) \equiv p - 1 \pmod{8}. \]

For \( k = 2 \), we have

\[
T_p(a_1, a_2) = \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_1}{p} \right) \left( \frac{x^2 + a_2}{p} \right)
\]

\[
= \sum_{x=1}^{p-1} \left( \left( \frac{x}{p} \right) - 1 \right) \left( \left( \frac{x^2 + a_1}{p} \right) - 1 \right) \left( \left( \frac{x^2 + a_2}{p} \right) - 1 \right)
\]

\[
+ \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_1}{p} \right) + \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_2}{p} \right)
\]

\[
+ \sum_{x=1}^{p-1} \left( \frac{x^2 + a_1}{p} \right) - \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) - \sum_{x=1}^{p-1} \left( \frac{x^2 + a_1}{p} \right)
\]

\[
- \sum_{x=1}^{p-1} \left( \frac{x^2 + a_2}{p} \right) + \sum_{x=1}^{p-1} 1.
\]

\[ \equiv 0 + T_p(a_1) + T_p(a_2) + S_p(a_1, a_2) \]

\[ -0 - S_p(a_1) - S_p(a_2) + (p - 1) \pmod{8} \]

\[ \equiv 0 + (p - 1) + (p - 1) + (p - 1) - 0 + 0 + 0 + (p - 1) \pmod{8} \]

\[ \equiv 0 \pmod{8}. \]

Thus the result is true for \( k = 2 \).

For \( k = 3 \), we have

\[
T_p(a_1, a_2, a_3) = \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_1}{p} \right) \left( \frac{x^2 + a_2}{p} \right) \left( \frac{x^2 + a_3}{p} \right)
\]

\[
= \sum_{x=1}^{p-1} \left( \left( \frac{x}{p} \right) - 1 \right) \left( \left( \frac{x^2 + a_1}{p} \right) - 1 \right) \left( \left( \frac{x^2 + a_2}{p} \right) - 1 \right) \left( \left( \frac{x^2 + a_3}{p} \right) - 1 \right)
\]

\[
+ \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_1}{p} \right) \left( \frac{x^2 + a_2}{p} \right) + \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_1}{p} \right) \left( \frac{x^2 + a_3}{p} \right)
\]
\[
\begin{align*}
+ \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_2 (x^2 + a_3)}{p} \right) \\
- \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_1}{p} \right) - \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_2}{p} \right) \\
- \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^2 + a_3}{p} \right) + \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \\
\equiv 0 + T_p(a_1, a_2) + T_p(a_1, a_3) + T_p(a_2, a_3) \\
- T_p(a_1) - T_p(a_2) - T_p(a_3) + 0 \pmod{8} \\
\equiv 0 + 0 + 0 - (p - 1) - (p - 1) - (p - 1) + 0 \pmod{8} \\
\equiv p - 1 \pmod{8}
\end{align*}
\]

Hence the result is true for \( k = 3 \) as well.

Assume now that the result is true for \( k = 1, 2, \ldots, N \ (N \geq 3) \). Then \( N + 1 \geq 4 \) and

\[
T_p(a_1, \ldots, a_{N+1}) = \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N+1})}{p} \right)
\]

\[
= \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N-2})}{p} \right) \\
\times \left( \left( \frac{x^2 + a_{N-1}}{p} \right) - 1 \right) \left( \left( \frac{x^2 + a_{N}}{p} \right) - 1 \right) \left( \left( \frac{x^2 + a_{N+1}}{p} \right) - 1 \right)
\]

\[
+ \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N-2}) (x^2 + a_{N-1}) (x^2 + a_N)}{p} \right)
\]

\[
+ \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N-2}) (x^2 + a_{N-1}) (x^2 + a_{N+1})}{p} \right)
\]

\[
+ \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N-2}) (x^2 + a_N) (x^2 + a_{N+1})}{p} \right)
\]

\[
- \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N-2}) (x^2 + a_{N-1})}{p} \right)
\]
\[ -\sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N-2})(x^2 + a_N)}{p} \right) \]

\[ -\sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N-2})(x^2 + a_{N+1})}{p} \right) \]

\[ +\sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x^2 + a_1) \cdots (x^2 + a_{N-2})}{p} \right) \]

\[ \equiv 0 + T_p(a_1, \ldots, a_{N-2}, a_{N-1}, a_N) + T_p(a_1, \ldots, a_{N-2}, a_{N-1}, a_{N+1}) \]

\[ +T_p(a_1, \ldots, a_{N-2}, a_N, a_{N+1}) - T_p(a_1, \ldots, a_{N-2}, a_{N-1}) \]

\[ -T_p(a_1, \ldots, a_{N-2}, a_N) - T_p(a_1, \ldots, a_{N-2}, a_{N+1}) \]

\[ +T_p(a_1, \ldots, a_{N-2})(\mod 8) \]

\[ \equiv \begin{cases} 
0 + (p - 1) + (p - 1) + (p - 1) & \text{if } 2 \mid N + 1, \\
-0 - 0 - 0 + (p - 1) & \equiv 0(\mod 8) \\
0 + 0 + 0 - (p - 1) - (p - 1) & \equiv p - 1(\mod 8) \\
-(p - 1) + 0 & \equiv p - 1(\mod 8) & \text{if } 2 \nmid N + 1, 
\end{cases} \]

which completes the proof of the inductive step. □

4. Proof of Theorem 1.1

We use Theorems 2.1, 2.2, 3.1 and 3.3 in order to prove the following two theorems from which our main result (Theorem 1.1) follows as a simple consequence.

**Theorem 4.1.** Let \( n \) and \( p \) be odd primes such that \( p \equiv 1(\mod 4) \) and \( p \equiv 1(\mod n) \).

(i) Let \( a \in \mathbb{F}_p \) be a quadratic residue. Then

\[ \Lambda_n(a) \equiv \begin{cases} 
0(\mod 4) & \text{if } n \equiv 1(\mod 4), \\
2(\mod 4) & \text{if } n \equiv 3(\mod 4). 
\end{cases} \]

(ii) Let \( a \in \mathbb{F}_p \) be a quadratic nonresidue. Then

\[ \Lambda_n(a) \equiv \begin{cases} 
0(\mod 8) & \text{if } n \equiv 1(\mod 4), \\
p - 1(\mod 8) & \text{if } n \equiv 3(\mod 4). 
\end{cases} \]

**Proof.** Let \( g \) be a primitive root \((\mod p)\), and let \( h = g^{\frac{p-1}{4n}} \).

(i) Assume that \( a \in \mathbb{F}_p \) is a quadratic residue. Let \( a_0 = 0 \), and let

\[ a_l = -\sqrt{a}(h^{l} + h^{-l}), \]

where \( 1 \leq l \leq 2n \) with \((l, 2n) = 1\) and \( k = \phi(2n) = n - 1\).
Then \( a_0, a_1, a_3, \ldots, a_{n-2}, a_{n+2}, \ldots, a_{2n-1} \) are incongruent modulo \( p \). By Theorems 2.1(i) and 3.1, we obtain

\[
\Lambda_n(a) = \sum_{x=0}^{p-1} \left( \frac{V_n(x,a)}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x(x + a_1)(x + a_3) \cdots (x + a_{2n-1})}{p} \right)
\]

\[
\equiv \begin{cases} 
0 \pmod{4} & \text{if } n - 1 \equiv 0 \pmod{4}, \\
2 \pmod{4} & \text{if } n - 1 \equiv 2 \pmod{4},
\end{cases}
\]

which completes the proof of (i).

(ii) Assume that \( a \in \mathbb{F}_p \) is a quadratic nonresidue. Let

\[
a_l = -a \left( h^l + h^{-l} \right)^2,
\]

where \( 1 \leq l \leq n - 2 \) with \( l \) odd and \( k = \frac{n - 1}{2} \).

Then \( a_1, a_3, \ldots, a_{n-2} \) are quadratic nonresidues modulo \( p \). By Theorems 2.1(ii) and 3.3, we have

\[
\Lambda_n(a) = \sum_{x=0}^{p-1} \left( \frac{V_n(x,a)}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x(x^2 + a_1)(x^2 + a_3) \cdots (x^2 + a_{n-2})}{p} \right)
\]

\[
\equiv \begin{cases} 
0 \pmod{8} & \text{if } 2 \mid \frac{n - 1}{2}, \\
p - 1 \pmod{8} & \text{if } 2 \nmid \frac{n - 1}{2},
\end{cases}
\]

which completes the proof of (ii). \( \square \)

**Theorem 4.2.** Let \( n \) and \( p \) be odd primes such that \( p \equiv 1 \pmod{4} \) and \( p \equiv -1 \pmod{n} \).

(i) Let \( a \in \mathbb{F}_p \) be a quadratic residue. Then

\[
\Lambda_n(a) \equiv \begin{cases} 
0 \pmod{8} & \text{if } n \equiv 1 \pmod{4}, \\
p - 1 \pmod{8} & \text{if } n \equiv 3 \pmod{4}.
\end{cases}
\]

(ii) Let \( a \in \mathbb{F}_p \) be a quadratic nonresidue. Then

\[
\Lambda_n(a) \equiv \begin{cases} 
0 \pmod{4} & \text{if } n \equiv 1 \pmod{4}, \\
2 \pmod{4} & \text{if } n \equiv 3 \pmod{4}.
\end{cases}
\]
Proof. Let \( \gamma \) be a generator of the cyclic group \( \mathbb{F}_{p^2}^* \) of order \( p^2 - 1 \), and let 
\( \theta = \gamma^{(p^2 - 1)/4n} \in \mathbb{F}_{p^2}^* \).

(i) Let
\[
a_l = -a \left( \theta^l + \theta^{-l} \right)^2,
\]
where \( 1 \leq l \leq n - 2 \), with \( l \) odd and \( k = \frac{n - 1}{2} \).

As in the proof of Theorem 2.2, each \( a_l \in \mathbb{F}_p \) is a quadratic nonresidue. By Theorems 2.2(i) and 3.3, we have
\[
\Lambda_n(a) = \sum_{x=0}^{p-1} \left( \frac{V_n(x)}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x(x^2 + a_1)(x^2 + a_3) \cdots (x^2 + a_{n-2})}{p} \right)
\]
\[
\equiv \begin{cases} 
0 \pmod{8} & \text{if } 2 \mid \frac{n - 1}{2}, \\
p - 1 \pmod{8} & \text{if } 2 \nmid \frac{n - 1}{2}, 
\end{cases}
\]
\[
\equiv \begin{cases} 
0 \pmod{4} & \text{if } n \equiv 1 \pmod{4}, \\
p - 1 \pmod{4} & \text{if } n \equiv 3 \pmod{4}, 
\end{cases}
\]
which completes the proof of (i).

(ii) Let \( a_0 = 0 \), and let
\[
a_l = -\sqrt{a \left( \theta^l + \theta^{-l} \right)^2},
\]
where \( 1 \leq l \leq 2n \) with \( (l, 2n) = 1 \) and \( k = \phi(2n) = n - 1 \).

Then \( a_0, a_1, a_3, \ldots, a_{n-2}, a_{n+2}, \ldots, a_{2n-1} \) are incongruent modulo \( p \). By Theorems 2.2(ii) and 3.1, we have
\[
\Lambda_n(a) = \sum_{x=0}^{p-1} \left( \frac{V_n(x, a)}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x(x + a_1)(x + a_3) \cdots (x + a_{n-2})}{p} \right)
\]
\[
\equiv \begin{cases} 
0 \pmod{4} & \text{if } n \equiv 1 \pmod{4}, \\
2 \pmod{4} & \text{if } n \equiv 3 \pmod{4}, 
\end{cases}
\]
which completes the proof of (ii). \( \Box \)

Theorem 1.1 follows immediately from Theorems 4.1 and 4.2.
Acknowledgments

I would like to thank to Professor Kenneth S. Williams for helpful discussions during the preparation of this paper.

References