Closed Form Evaluations of Some Exponential Sums
N. A. Carella, March 2011.

Abstract: This note provides new closed form evaluations of a few classes of exponential sums associated with elliptic curves and hyperelliptic curves.

Keywords: Character sums, Exponential sums, Elliptic curves, Complex multiplication.
Mathematics Subject Classification: Primary 10G05, Secondary 14K22.

1 Introduction
This work deals with the closed forms evaluations of several exponential sums. Currently there is a handful classes of exponential sums that can be evaluated in closed forms. Extensive coverage of this subject is given in [BT], see also the research problem 14, p. 497. The exponential sum

\[ S(f) = \sum_{x=0}^{p-1} \left( \frac{f(x)}{p} \right) \]  \hspace{1cm} (1)

has been evaluated in closed forms for nine classes of cubic polynomials \( f_n(x) \in \mathbb{F}_p[x] \), and a few other polynomials, see [PD], [SK], [JM], et cetera. The nine classes of cubic polynomials are the followings:

1. \( f_1(x) = x^3 + ax \),
2. \( f_2(x) = x(x^2 + 4ax + 2a^2) \),
3. \( f_3(x) = x^3 + a \),
4. \( f_7(x) = x(x^2 + 21ax + 112a^2) \),
5. \( f_{11}(x) = x^3 - 2^5 \cdot 3 \cdot 11a^2 x + 2^4 \cdot 7 \cdot 11^2 a^3 \),
6. \( f_{19}(x) = x^3 - 2^3 \cdot 19a^2 x + 2 \cdot 19^2 a^3 \),
7. \( f_{43}(x) = x^3 - 2^4 \cdot 5 \cdot 43a^2 x + 2 \cdot 3 \cdot 7 \cdot 43^2 a^3 \),
8. \( f_{67}(x) = x^3 - 2^3 \cdot 5 \cdot 11 \cdot 67a^2 x + 2 \cdot 7 \cdot 31 \cdot 67^2 a^3 \),
9. \( f_{163}(x) = x^3 - 2^4 \cdot 5 \cdot 23 \cdot 29 \cdot 163a^2 x + 2 \cdot 7 \cdot 11 \cdot 19 \cdot 127 \cdot 163^2 a^3 \),

where \( 0 \neq a \in \mathbb{Z} \), see Theorem 4. The CM elliptic curve \( E: y^2 = f_n(x) \) and its quadratic twisted curve \( E': sy^2 = f_n(x) \), where \( s \) is a quadratic nonresidue are closely linked to exponential sums \( S(f_n) \) in question. Each of these elliptic curve has complex multiplication by the ring of integers \( \mathbb{Z}[(\sqrt{-n})] \) or \( \mathbb{Z}[(1+\sqrt{-n})/2] \) in the quadratic field \( \mathbb{Q}(\sqrt{-n}) \).

The new evaluations are derived from the nine classes of cubic polynomials and a few other polynomials.
The new nine classes of polynomials derived from \( f_n(x) \) are the following.

1. \( g_1(x) = x^4 + a \),
2. \( g_2(x) = x^4 + 4ax^2 + 2a^2 \),
3. \( g_3(x) = x^6 + a \),
4. \( g_7(x) = x^6 + 21ax^2 + 112a^2 \),
5. \( g_{11}(x) = x^6 - 2^5 \cdot 3 \cdot 11a^2 x^2 + 2^4 \cdot 7 \cdot 11a^3 \),
6. \( g_{19}(x) = x^6 - 2^3 \cdot 19a^2 x^2 + 2 \cdot 19^2 a^3 \),
7. \( g_{43}(x) = x^6 - 2^4 \cdot 5 \cdot 43a^2 x^2 + 2 \cdot 3 \cdot 7 \cdot 43a^3 \),
8. \( g_{67}(x) = x^6 - 2^3 \cdot 5 \cdot 11 \cdot 67a^2 x^2 + 2 \cdot 7 \cdot 31 \cdot 67a^3 \),
9. \( g_{163}(x) = x^6 - 2^4 \cdot 5 \cdot 23 \cdot 29 \cdot 163a^2 x^2 + 2 \cdot 7 \cdot 11 \cdot 19 \cdot 127 \cdot 163a^3 \).

These polynomials are associated with the hyperelliptic curves \( E_n : y^2 = g_n(x) \), and the associated exponential sums \( S(g_n) \). The new closed form evaluations are the following.

**Theorem 1.** (1) If \( n = 1, 2, \) or 7, then

\[
S(g_n) = \sum_{x=1}^{p-1} \left( \frac{g_n(x)}{p} \right) = \begin{cases} A & \text{if } p \text{ is inert,} \\ A + \left( \frac{a}{p} \right) u & \text{if } 4p = u^2 + nv^2, \end{cases}
\]

where the integer \( u \) is uniquely determined by quadratic symbol relation \(( u \mid n ) = ( 2 \mid p )\), and the quadratic exponential sum

\[
A = \sum_{x=0}^{p-1} \left( \frac{f_n(x)/x}{p} \right).
\]

(2) If \( n = 3, 11, 19, 43, 67, \) or 163, then

\[
S(g_n) = \sum_{x=1}^{p-1} \left( \frac{g_n(x)}{p} \right) = \begin{cases} B & \text{if } p \text{ is inert,} \\ B + \left( \frac{a}{p} \right) u & \text{if } 4p = u^2 + nv^2, \end{cases}
\]

where the integer \( u \) is uniquely determined by \(( u \mid n ) = ( 2 \mid p )\), \( g_n(x) = (x + a_1)(x + a_2)(x + a_3)(x + a_4) \in \mathbb{F}_p[x] \), and

\[
B = -1 - \left( \frac{\alpha}{p} \right) (H(\beta) \mod p) \quad \text{with} \quad \alpha \equiv (a_1 - a_4)(a_2 - a_3), \quad \beta \equiv (a_1 - a_4)(a_2 - a_3) \mod p,
\]

and \( H(x) \) is the Hasse invariant.

The proof, which is built up from the simpler closed form evaluations, appears in Section 3.1.

Other widely used families of nonCM elliptic curves of genus \( g = 1 \) are the following:

10. \( F_\beta(x) = x(x - 1)(x - \beta), \) or \( F_\beta(x) = (x^2 - 1)(x^2 - \beta) \), where \( 0, 1 \neq \beta \in \mathbb{Z}, \) Legendre form.
11. \( G_\beta(x) = (k^2 x^2 - 1)(x^2 - \beta), \) \( 0, \pm 1 \neq \beta \in \mathbb{Z}, \) and \( k \neq 0, \) Newton form.
(12) \( H_d(x) = (x^2 - c^2)(c^2dx^2 - 1) \), \( c, d \in \mathbb{Z} \), and \( cd(1 - c^4d) \neq 0 \), Edward form.

The closed form evaluations of these exponential sums are discussed in Section 3.2.

2. Preliminary

Let \( f(x) \in \mathbb{F}_p[x] \) be a polynomial of degree \( \deg(f) = d > 0 \), and let \( \chi(x) = (x \mid p) \) be the quadratic character. Any exponential sum \( S(f) \) has a closed form evaluation in terms of the characteristics of the continued fractions \([A_0, A_1, \ldots, A_s]\) and \([a_0, a_1, \ldots, a_t]\) of the rational functions \( (f(x) - 1)/(x^p - x) \) and \( (f(x) + 1)/(x^p - x) \) as

\[
S(f) = \sum_{x=0}^{p-1} \chi(f(x)) = \sum_{x=0}^{p-1} \left( \frac{f(x)}{p} \right) = \begin{cases} \text{deg}(a_i) & \text{if } n_f = t, \\ \text{deg}(A_s) & \text{if } n_f = s, \end{cases}
\]

see [LN, p. 236] for the exact analysis. However, only a handful of classes of exponential sums \( S(f) \) have been evaluated in terms of the characteristics of the coefficients of the polynomials \( f(x) \) and the primes \( p \).

This section recalls a few basic results to facilitate the proofs. The evaluations of the quadratic character sum, cubic sum, and a few other cases in terms of the characteristics of the polynomials \( f(x) \) and the primes \( p \).

2.1. The Number of Points on A Curve.
The exponential sums \( S(f) \) under investigation arise in the calculations of the number of points

\[
\#C(\mathbb{F}_p) = \# \{ (x, y) : y^2 = f(x) = 0, \text{ and } x, y \in \mathbb{F}_p \} = p + 1 + S(f(x))
\]

of then algebraic curves \( C : y^2 = f(x) \) of genus \( g \geq 0 \). In terms of the characteristic of the prime \( p \), this is written as

\[
\#C(\mathbb{F}_p) = 1 + \sum_{x=0}^{p-1} \left( 1 + \left( \frac{f(x)}{p} \right) \right) = p + 1 + \sum_{x=0}^{p-1} \left( \frac{f(x)}{p} \right) = p + 1 - \pi - \pi^\prime,
\]

where the trace \( Tr(\pi) = -\pi - \pi^\prime = S(f) \), and \( p = \pi \pi^\prime \) in the quadratic field \( \mathbb{Q}(\sqrt{-n}) \).

2.2. Simple Exponential Sums and Identities.

**Lemma 2.** Let \( t \in \mathbb{F}_p \). Then

\[
\sum_{x \in \mathbb{F}_p} x^t =\begin{cases} 0 & \text{if } q - 1 \not\equiv 0 \pmod{t}, \\ q - 1 & \text{if } q - 1 \equiv 0 \pmod{t}. \end{cases}
\]

To confirm this statement, let \( \theta \) be a generator of the multiplicative group of \( \mathbb{F}_p \), and examine the sum of the geometric progression \( 1, \theta, \theta^2, \ldots, \theta^{p-2} \). The convention \( \theta^0 \equiv 0 \pmod{p} \) in finite fields of characteristic \( p \) is observed.

The linear exponential sum \( S(ax + b) \) is identically zero: A simple change of variables, and the fact that the finite field has equal number of quadratic residues and quadratic nonresidues lead to
For the simpler cubic exponential sums various special cases are given in several papers, for starter, see [LN], [BT], [PD], [SK], and [MN]. This is the culmination of many decades of works on the cubic exponential sums by various workers. The proofs of Lemma 2.4. Transformation and Reduction Formulae.

Several classes of transformations and degree reduction formulae are known for evaluating character sums of degree \(d \geq 3\) in terms of simpler ones of degrees \(<d\). Two of these transformation formulae are explored here.

**Lemma 3.** Let \(p > 2\) be a prime and let \(f(x) = ax^2 + bx + c \in \mathbb{F}_p[x]\), then

\[
S(f) = \sum_{x=0}^{p-1} \left( \frac{ax^2 + bx + c}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x^2}{p} \right) = 0. \tag{10}
\]

**Quadratic Exponential Sums.** The quadratic exponential sum \(S(ax^2 + bx + c)\) has a closed form evaluation for every polynomial. The analysis is a straightforward algebraic manipulation.

**Lemma 3.** Let \(p > 2\) be a prime and let \(f(x) = ax^2 + bx + c \in \mathbb{F}_p[x]\), then

\[
S(f) = \sum_{x=0}^{p-1} \left( \frac{ax^2 + bx + c}{p} \right) = \left( \frac{a}{p} \right)^{-1} \begin{cases} 0 & \text{if } b^2 - 4ac \neq 0, \\ \frac{a}{p}u & \text{if } b^2 - 4ac = 0. \end{cases} \tag{11}
\]

The proof appears in [LN, 230].

**2.3. Cubic Exponential Sums.** The analysis of the cubic exponential sums dates back about a century. The simplest cases \(S(x^3 + a)\) and \(S(x^3 + ax)\) were studied by Jacobsthal and Schrutka in the early 1900, see [WS], [LN], and similar references.

**Theorem 4.** ([PD]) Let \(n = 1, 2, 3, 7, 11, 19, 43, 67, 163\), and suppose that \(y^2 = f_n(x)\) has good reduction at \(p\), exempli gratia, \(p \nmid 2an\), then

\[
S\left( f_n \right) = \sum_{x=0}^{p-1} \left( \frac{f_n(x)}{p} \right) = \begin{cases} 0 & \text{if } p \text{ is inert,} \\ \left( \frac{a}{p} \right)u & \text{if } 4p = u^2 + nv^2, \end{cases} \tag{12}
\]

or \(p = u^2 + nv^2\), where the integer \(u\) is uniquely determined by quadratic symbol relation \((u \mid n) = (2 \mid p)\).

This is the culmination of many decades of works on the cubic exponential sums by various workers. The proofs of various special cases are given several papers, for starter, see [LN], [BT], [PD], [SK], and [MN].

For the simpler cubic exponential sums \(S(x^3 + a)\) and \(S(x^3 + ax)\), finer analysis are available, see [BT, p 190], [RS].

The elliptic curve \(E_n : y^2 = f_n(x)\) has complex multiplication by the full ring of algebraic integers \(\mathbb{Z}[\sqrt{-n}]\) or \(\mathbb{Z}\left((1 + \sqrt{-n})/2\right)\), \(n = 1, 2, 3, 7, 11, 19, 43, 67, 163\). The group of points on an algebraic curve \(E : y^2 = f(x)\) is defined by \(E(F_p) = \{(x, y) : f(x) - y^2 = 0\}\) and its cardinality is given by \(#E(F_p) = p + 1 + S(f)\). Similarly, the twisted curve \(E' : sy^2 = f(x)\) has the group of points \(E'(F_p) = \{(x, y) : f(x) - sy^2 = 0\}\) and its cardinality is given by \(#E'(F_p) = #E(F_p) + #E(F_p) = 2p + 2\).

**2.4. Transformation and Reduction Formulae.** Several classes of transformations and degree reduction formulae are known for evaluating character sums of degree \(d \geq 3\) in terms of simpler ones of degrees \(<d\). Two of these transformation formulae are explored here.

**Lemma 5.** Let \(f(x) \in \mathbb{F}_p[x]\) be a polynomial. Then

\[
\sum_{x=0}^{p-1} \left( \frac{f(x^2)}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{xf(x)}{p} \right) + \sum_{x=0}^{p-1} \left( \frac{f(x)}{p} \right). \tag{13}
\]
The more general version of this transformation identity is given in [WS]. The degree reduction formula below for evaluating character exponential sums of degree $d > 3$ in terms of simpler ones of degrees $< d$ is given [BT, p. 207]. The special case of degree $d = 4$ is as follows.

**Lemma 6.** Let $p$ be a prime and let $f(x) = (x + a_1)(x + a_2)(x + a_3)(x + a_4)$, then

$$S(f) = \sum_{x=0}^{p-1} \frac{(x+a_1)(x+a_2)(x+a_3)(x+a_4)}{p} = -1 \left( \frac{\alpha}{p} \right) S(F_{\beta}),$$

(14)

where $F_{\beta}(x) = x(x-1)(x-\beta)$, $0, 1 \neq \beta \in \mathbb{Z}$, and the parameters $\alpha$ and $\beta$ are

$$\alpha \equiv (a_1 - a_4)(a_2 - a_3) \mod p, \quad \beta \equiv \frac{(a_1 - a_3)(a_2 - a_4)}{(a_1 - a_4)(a_2 - a_3)} \mod p.$$

(15)

The parameters $\alpha$ and $\beta$ are not independent of the permutation of the roots $a_{\pi(1)}, a_{\pi(2)}, a_{\pi(3)}, a_{\pi(4)}$, where $\pi \in \text{Sym}(n)$ is a permutation of $n$ elements. So the evaluation of the exponential sum $S(f)$ is given up to a permutation of the roots of the polynomial $f(x)$. As the permutation map $\pi \in \text{Sym}(4)$ varies, there are six possible values of each parameter $\alpha \in \{ \pm \alpha_1, \pm \alpha_2, \pm \alpha_3 \}$ and $\beta \in \{ \beta_1^{\pm 1}, \beta_2^{\pm 1}, \beta_3^{\pm 1} \}$, where $0 \neq \alpha, \beta \in \mathbb{F}_p$.

The polynomial $F_{\beta}(x) = x(x-1)(x-\beta)$, $0, 1 \neq \beta \in \mathbb{Z}$, satisfies the identities

(i) $F_{\beta}(x) = F_{1/\beta}(x)$,

(ii) $F_{\beta}(x) = \left( -1/p \right) F_{1-\beta}(x)$,

(iii) $F_{\beta^2}(x) = \left( \beta/p \right) F_{(1-\beta)^2/4}(x)$.

The application of the reduction formula requires information about the reducibility/irreducibility of certain cubic polynomials. The discriminant test can be used to help identify the reducibility/irreducibility of any cubic polynomial $f(x) = x^3 + ax^2 + bx + c$ of discriminant $D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$ over the prime field $\mathbb{F}_p$ or an extension of it. The information is extracted from the value of the quadratic symbol test $\left( \frac{D}{p} \right) = (-1)^s$, where $s$ is the number of irreducible factors in $f(x)$ over $\mathbb{F}_p$. More precise criteria are given in [SP].

2.5. **Hasse Invariant.** Given a prime $p = 2n + 1$, the Hasse polynomial (or Hasse invariant) is defined by

$$H(x) = (-1)^s \sum_{k=0}^{n} \binom{n}{k} x^k,$$

(16)

confer [HR, p. 261], [SN, p. 141], etc. The Hasse polynomial is a solution of the differential equation

$$4x(1-x) \frac{d^2}{dx^2} y + 4(1-2x) \frac{d}{dx} y - 1 = 0$$

in the ring of polynomials $\mathbb{F}_q[x]$, see [SN, P. 142]. It is linked to the $n$th Legendre polynomial $P_n(x)$ by the formula $\pm H(x) = (1-x)^n P_n((1+x)/(1-x))$.

**Lemma 7.** The Hasse polynomial $H(x)$ has simple roots in its splitting field $\mathbb{F}_q$ or a quadratic extension $\mathbb{F}_q[\theta]$ of $\mathbb{F}_q$.

**Lemma 8.** ([BM]) For a prime $p > 3$, the following hold:
(i) The number of linear factors of $H(x) \in \mathbb{F}_q[x]$ is $N_1 = \begin{cases} 0 & \text{if } p \equiv 1 \text{ mod } 4, \\ 3h(-p) & \text{if } p \equiv 3 \text{ mod } 4. \end{cases}$

(ii) The number of quadratic factors of $H(x) \in \mathbb{F}_q[x]$ is $N_2 = \begin{cases} h(-p)/2 & \text{if } p \equiv 1 \text{ mod } 4, \\ (3h(-p)-1)/2 & \text{if } p \equiv 3 \text{ mod } 8, \\ (h(-p)-1)/2 & \text{if } p \equiv 7 \text{ mod } 8, \end{cases}$

where $h(-p)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{-p})$.

The first formula for the number $N_1(p)$ of roots of $H(x) \in \mathbb{F}_p[x]$ in $\mathbb{F}_p$ appeared earlier in [YM]. From these formulas it immediately follows that if the polynomial $H(x) \in \mathbb{F}_p[x]$ does not factor completely in $\mathbb{F}_p$, then it has less than $\log_2 h(-p) = O(p^{1/2})$ roots in $\mathbb{F}_p$. The Hasse invariant is used to evaluate the character sum $S(F_{\beta})$ connected with the polynomial $F_{\beta}(x) = x(x-1)(x-\beta)$.

**Lemma 9.** Let $F_{\beta}(x) = x(x-1)(x-\beta)$, $\beta \neq 0$, $1 \in \mathbb{F}_p$, $p = 2m + 1$. Then

$$S(F_{\beta}) = \sum_{x=0}^{p-1} \left( \frac{x(x-1)(x-\beta)}{p} \right) \equiv (-1)^m \sum_{k=0}^{m} \left( \frac{m}{k} \right)^2 \beta^k \mod p \equiv H(\beta) \mod p. \quad (17)$$

Proof: Compute the expression

$$S(F_{\beta}) = \sum_{x=0}^{p-1} \left( \frac{x(x-1)(x-\beta)}{p} \right) \equiv \sum_{x=0}^{p-1} (x(x-1)(x-\beta))^{(p-1)/2} \mod p \equiv H(\beta) \mod p, \quad (18)$$

refer to [HR, p. 251], and [SN, p. 140].

For $p > 2$, supersingular elliptic curves are characterized by the condition $H(\beta) \equiv 0 \text{ mod } p$, see [HR] and [SN] for other equivalent criteria. Elliptic curves with complex multiplication are supersingular for every prime $p \equiv 3 \text{ mod } 4$, and ordinary for every prime $p \equiv 1 \text{ mod } 4$, confer [SN, p. 144].

As an example, Lemma 8 implies that the elliptic curve $E$: $y^2 = F_{\beta}(x) = x(x-1)(x-\beta)$, $0, 1 \neq \beta$, is not supersingular for any $\beta \in \mathbb{F}_p$, whenever the prime $p = 4m + 1$.

**Theorem 10.** (Manin) Let $E$: $y^2 = F_{\beta}(x) = x(x-1)(x-\beta)$, $0, 1 \neq \beta$, be an elliptic curve over the rational numbers $\mathbb{Q}$ with good reduction at a prime $p$, and let $a_p = -S(F_{\beta})$ be the trace of Frobenius at $p$, then $H(\beta) \equiv a_p \mod p$. In particular,

$$\#E(\mathbb{F}_p) = \# \{ (x, y) : y^2 - F_{\beta}(x) = 0, \text{ and } x, y \in \mathbb{F}_p \} = p + 1 + (H(\beta) \mod p).$$

More generally, for an elliptic curve $E$: $y^2 = f(x)$, the number of points satisfies $\#E(\mathbb{F}_q) \equiv 1 - H(\beta)^{(q-1)\mod (p-1)} \mod p$.

**2.6. Other Exponential Sums.** Several other related evaluations of character sums are included in this section.

**Definition 11.** If $p - 1 \equiv 0 \mod k$, and $a \neq 0$, the Jacobson sums are defined by
\[ \phi_k(a) = \sum_{x=0}^{p-1} \left( \frac{x^{k} + a}{p} \right) \text{ and } \psi_k(a) = \sum_{x=0}^{p-1} \left( \frac{x^{k+a}}{p} \right). \]

**Proposition 12.** If \( p \equiv k + 1 \mod 2k \) then \( \phi_k(a) = 0 \), and \( \phi_{2k}(a) = 0 \).

Proof: As \( (p-1)/k \) is odd number, the set \( \{ x^{k} p : 0 < x < p \} \) of residues modulo \( p \) is just a permutation of the set \( \{ x^{2k} p : 0 < x < p \} \), see [B, p. 184] for more details. \( \blacksquare \)

**Theorem 13.** Let \( k > 1 \) and let \( p \) be a prime such that \( p - 1 \equiv 0 \mod k \), then

(i) \( \psi_k(a) = 0 \) if \( \gcd(k, p-1) = 1 \). 
(ii) \( \psi_k(a) = \sum_{x=0}^{p-1} \left( \frac{x^{k} + a}{p} \right) \equiv -\sum_{x=0}^{k-2} \left( \frac{a^{f(k-2i)}}{2} \right) a^{f(k-2i)} \mod p \) if \( \gcd(p - 1, k) \neq 1 \).

Proof: Take \( p = 2kf + 1 \). Routine calculations show that

\[ \psi_k(a) = \sum_{x=0}^{p-1} \left( \frac{x^{k} + a}{p} \right) \equiv \sum_{x=0}^{p-1} (x^{k} + a)^{(p-1)/2} \mod p \equiv \sum_{x=0}^{p-1} (kf) a^{f(k-2i)} \mod p \]

The inner sum vanishes for \( kd \not\equiv 0 \mod p - 1 \), but equals \(-1\) for \( kd \equiv 0 \mod p - 1 \), see Lemma 2. Hence,

\[ \psi_k(a) \equiv -\sum_{d=0, kd \equiv 0 \mod p - 1}^{k} \left( \frac{a^{f(k-2i)}}{2} \right) a^{f(k-2i)} \mod p, \]

where the index \( i \) runs over the solutions of \( kd = (p - 1)i = 2k\), and \( 0 \leq d \leq kf \). \( \blacksquare \)

**Theorem 14.** Let \( k \geq 1 \) and let \( p = 2kf + 1 \) be a prime, then

\[ \phi_k(a) = \sum_{x=0}^{p-1} \left( \frac{x^{k} + a}{p} \right) \equiv -\sum_{i=0}^{(k+1)/2} \left( \frac{kf}{(2i - 1)f} \right) a^{f(k-2i+1)} \mod p. \]

Proof: Routine calculations show that

\[ \phi_k(a) = \sum_{x=0}^{p-1} \left( \frac{x^{k} + a}{p} \right) \equiv \sum_{x=0}^{p-1} (x^{k} + a)^{(p-1)/2} \mod p \equiv \sum_{d=0}^{k} \left( \frac{kf}{d} \right) a^{f(k-2i)} \sum_{x=0}^{p-1} x^{k(f+d)} \mod p. \]

The inner sum vanishes for \( k(f + d) \not\equiv 0 \mod p - 1 \), see Lemma 2, but equals \(-1\) for \( k(f + d) \equiv 0 \mod p - 1 \). Hence

\[ \phi_k(a) \equiv -\sum_{d=0, p-1 \equiv 0 \mod (f + d)}^{k} \left( \frac{kf}{d} \right) a^{f(k-2i)} \mod p \equiv -\sum_{i=0}^{(k+1)/2} \left( \frac{kf}{(2i - 1)f} \right) a^{f(k-2i+1)} \mod p, \]

where the index \( i \) runs over the solutions of \( k(f + d) = (p - 1)i = 2k\), and \( 0 \leq d \leq kf \). \( \blacksquare \)
Note: The binomial coefficient vanishes in the two cases: \( \binom{n}{-k} = 0 \) for \( k > 0 \), and \( \binom{n}{k} = 0 \) for \( k > n \geq 1 \).

**Lemma 15.** Let \( C : y^2 = x^k + a, \ k > 4 \), Then
(i) The group of automorphism \( \text{Aut}(C) = \mu_k \times \mu_2 \), and defined by \( (x, y) \rightarrow (\omega x, \pm y) \), where \( \omega \in \mu_k \) is the group of \( k \)th root of unity.
(ii) The algebraic curve \( C \) has complex multiplication by \( \mathcal{G} = \mu_k \times \mu_2 \), and defined by \( (x, y) \rightarrow (\omega x, \pm y) \), where \( \omega \in \mu_k \) is the group of \( k \)th root of unity.

3. Closed Form Evaluations
The method for evaluating the exponential sums \( S(g_n(x)) \) in closed form uses the values of simpler exponential quadratic exponential sum \( S(ax^2 + bx + c) \) and cubic exponential sum \( S(f_n(x)) \) of lower degrees to derive the values of the exponential sums \( S(g_n(x)) \) of higher degree. A different but related method was employed in [WS] to evaluate several classes of quartic exponential sums, including \( S(g_n(x)), n = 1, 2, \) and 7.

3.1 The Proof of Theorem 1.

**Theorem 1.** (1) If \( n = 1, 2, \) or 7, then
\[
S(g_n) = \sum_{x=0}^{p-1} \left( \frac{g_n(x)}{p} \right) = \begin{cases} A & \text{if } p \text{ is inert}, \\ A + \left( \frac{a}{p} \right) u & \text{if } 4p = u^2 + nv^2, \end{cases}
\] (24)

where the integer \( u \) is uniquely determined by quadratic symbol relation \( (u | n) = (2 | p) \), and the quadratic exponential sum
\[
A = \sum_{x=0}^{p-1} \left( \frac{f_n(x)/x}{p} \right). \tag{25}
\]

(2) If \( n = 3, 11, 19, 43, 67, \) or 163, then
\[
S(g_n) = \sum_{x=0}^{p-1} \left( \frac{g_n(x)}{p} \right) = \begin{cases} B & \text{if } p \text{ is inert}, \\ B + \left( \frac{a}{p} \right) u & \text{if } 4p = u^2 + nv^2, \end{cases}
\] (26)

where the integer \( u \) is uniquely determined by \( (u | n) = (2 | p) \), \( g_n(x) = (x + a_1)(x + a_2)(x + a_3)(x + a_4) \in \mathbb{F}_p[x] \),
and
\[
B = -1 \left( \frac{\alpha}{p} \right) (H(\beta) \mod p) \quad \text{with} \quad \alpha = (a_1 - a_2)(a_2 - a_3), \quad \beta = \frac{(a_1 - a_2)(a_2 - a_3)}{(a_1 - a_4)(a_2 - a_3)} \mod p, \tag{27}
\]
and \( H(x) \) is the Hasse invariant.
Proof: To verify the first case, it is sufficient to consider \( f_1(x) = x^3 + ax \), and \( g_1(x) = f_1(x^2) = x^4 + a \), the singular part is removed since the quadratic symbol annihilates it. Apply the transformation formula, Lemma 5, to \( f_1(x) \) to obtain
\[
\sum_{x=0}^{p-1} \left( \frac{x^6 + ax^2}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x(x^3 + ax)}{p} \right) + \sum_{x=0}^{p-1} \left( \frac{x^3 + ax}{p} \right).
\]
(28)

Now, substituting the known values of the exponential sums \( A = S(f_1(x)/x) \), see Lemma 3, and \( S(f_1(x)) \), see Theorem 4, and simplifying return
\[
\sum_{x=0}^{p-1} \left( \frac{x^4 + a}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x^2 + a}{p} \right) + \sum_{x=0}^{p-1} \left( \frac{x^3 + ax}{p} \right) = \begin{cases} A & \text{if } p \text{ is inert,} \\ A + \left( \frac{a}{p} \right) u & \text{if } 4p = u^2 + nv^2. \end{cases}
\]
(29)

To verify the second case, it is sufficient to consider the polynomials \( f_{11}(x) = x^3 - 2^5 \cdot 3 \cdot 11 a^2 x + 2^4 \cdot 7 \cdot 11^2 a^3 \), and \( g_{11}(x) = f_{11}(x^2) \). Apply the transformation formula, Lemma 5, to \( f_{11}(x) \) to obtain
\[
\sum_{x=0}^{p-1} \left( \frac{f_{11}(x^2)}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{xf_{11}(x)}{p} \right) + \sum_{x=0}^{p-1} \left( \frac{f_{11}(x)}{p} \right).
\]
(30)

To apply the reduction formula, Lemma 6, factor the polynomial as
\[
xf_{11}(x) = x(x^3 - 2^5 \cdot 3 \cdot 11 a^2 x + 2^4 \cdot 7 \cdot 11^2 a^3) = (x + a_1)(x + a_2)(x + a_3)(x + a_4) \in \mathbb{F}_p[x],
\]
(31)

where \( a_1 = 0 \), and put \( \alpha = (a_1 - a_4)(a_3 - a_2) \), \( \beta = ((a_1 - a_2)(a_2 - a_3))^{-1}(a_1 - a_3)(a_2 - a_4) \mod p \). Next, substitute the known values of the cubic exponential sum \( S(f_{11}(x)) \), see Theorem 4, and the quartic exponential sum \( S(xf_{11}(x)) \), Lemmas 6 and 9, to arrive at
\[
\sum_{x=0}^{p-1} \left( \frac{f_{11}(x^2)}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{xf_{11}(x)}{p} \right) + \sum_{x=0}^{p-1} \left( \frac{f_{11}(x)}{p} \right) = \begin{cases} B & \text{if } p \text{ is inert,} \\ B + \left( \frac{a}{p} \right) u & \text{if } 4p = u^2 + nv^2, \end{cases}
\]
(32)

where
\[
B = \sum_{x=0}^{p-1} \left( \frac{xf_{11}(x)}{p} \right) = -1 \left( \frac{\alpha}{p} \right) (H(\beta) \mod p),
\]
(33)

and the polynomial \( H(x) \) is the Hasse invariant, see Lemma 9.

\[ \blacksquare \]

**Note:** The last formula works over the splitting field of a polynomial \( f(x) = (x + a_1)(x + a_2)(x + a_3)(x + a_4) \). If it does not split over the prime field \( \mathbb{F}_p \), then splitting field of \( f(x) \) is either \( \mathbb{F}_{p^2} \), \( \mathbb{F}_{p^4} \), or \( \mathbb{F}_{p^8} \).

The new polynomials \( g_n(x) \) are connected with algebraic curves of genus \( g = 1, 2 \). These curves are as follows.

1. The elliptic curve \( C_n : y^2 = g_n(x) \), with the parameters \( n = 1, 2, 7, \) and \( g = 1 \).
(2) The hyperelliptic curve $C_n: y^2 = g_n(x)$, with the parameters $n = 3, 11, 43, 67, 163,$ and $g = 2$.

**Corollary 16.** The number of points on the hyperelliptic curve $C_n: y^2 = g_n(x)$ is $\# C_n(F_p) = p + 1 + S(g_n(x))$. 

**Corollary 17.** Let $g_n(x) = f_n(x^2)$, then

$$\left| \sum_{x=0}^{p-1} \left( \frac{g_n(x)}{p} \right) \right| \leq 2\sqrt{p}.$$  

(34)

Proof: Since $H(\beta) \mod p \equiv a_p < 2g\sqrt{p}$, where $g > 0$ is the genus of the curve, the absolute value of $H(d) \mod p$ is the same as the absolute value of the trace of Frobenius $a_p = -S(F_d)$ at $p$. 

This improves the Weil estimate $|S(f)| \leq (n-1)\sqrt{p}$, 4 ≤ $n$ ≤ 6, for the polynomials $f(x) = g_n(x)$, and their twisted polynomials $g(x) = sg_n(x)$, $s \in F_p$.

### 3.2. More Closed Form Evaluations.

Other widely used families of nonCM elliptic curves of genus $g = 1$ are the followings:

1. $F_{\beta}(x) = x(x-1)(x-\beta)$, or $F_{\beta}(x) = (x^2 - 1)(x^2 - \beta)$, where 0, 1 $\neq \beta \in \mathbb{Z}$,  
   Legendre form.

2. $G_{\beta}(x) = (k^2x^2 - 1)(x^2 - \beta)$, 0, ±1 $\neq \beta \in \mathbb{Z}$, and $k \neq 0$,  
   Newton form.

3. $H_d(x) = (x^2 - c^2)(c^2dx^2 - 1)$, $c, d \in \mathbb{Z}$, and $cd(1 - c^4d) \neq 0$,  
   Edward form.

The Edward form $H_d(x) = (x^2 - c^2)(c^2dx^2 - 1)$ is derived from the elliptic curve $E: x^2 + y^2 = c^2(1 + dx^2y^2)$ or its quadratic twist $E': sx^2 + y^2 = 1 + dx^2y^2$, see [ES], and [BL]. Basically, the Newton form $E: y^2 = x^4 - ax^2 + 1$, and Jacobi elliptic curve $E: y^2 = x^3 + ax + b$ are special cases of the Edward form.

Since the Edward form $H_d(x) = (x^2 - c^2)(c^2dx^2 - 1) = (x + a_1)(x + a_2)(x + a_3)(x + a_4) \in F_p[x]$ or over a quadratic extension $F_q$ of $F_p$, where $a_1 = c, a_2 = -c, a_3 = -1/c\sqrt{d}, a_4 = 1/c\sqrt{d}$, an elliptic curve $E: y^2 = x^3 + ax + b$, with 2-torsion points is isogenous to an Edward form.

Similarly, an arbitrary elliptic curve $E: y^2 = f(x)$ is isogenous to the Legendre form $E': y^2 = F_{\beta}(x)$, or one of the other forms over some finite extension $F_q$ of $F_p$, it appears that the associated exponential sum $S(f)$ can be evaluated in closed form in terms of simpler exponential sums such as $S(F_{\beta})$ and quadratic exponential sums $S(ax^2 + bx + c)$. A new paper, see [OG], develops the rational maps between the Legendre forms and the Edward forms of elliptic curves.

**Theorem 18.** Let $F(x) = F_{\beta}(x)$, $G_{\beta}(x)$, or $H_d(x)$, then

$$S(F) = \sum_{x=0}^{p-1} \left( \frac{F(x)}{p} \right) = -1 - \left( \frac{\alpha}{p} \right)(H(\beta) \mod p).$$  

(35)

where $-a_1, -a_2, -a_3, -a_4$ are the roots of the polynomial $F(x)$, and $\alpha \equiv (a_1 - a_3)(a_3 - a_2)$, and $\beta \equiv ((a_1 - a_4)(a_2 - a_3))^{-1} a_3(a_2 - a_4) \mod p$.

Proof: Factor the polynomial as $F(x) = (x + a_1)(x + a_2)(x + a_3)(x + a_4) \in F_q[x]$, and put
Classes of Exponential Sums And Curves

\[ \alpha \equiv (a_1 - a_4)(a_2 - a_3), \quad \text{and} \quad \beta \equiv \frac{(a_1 - a_3)(a_2 - a_4)}{(a_1 - a_4)(a_2 - a_3)} \mod p. \]  \hspace{1cm} (36)

By Lemmas 6 and 9,

\[ S(F) = \frac{1}{p} \sum_{x=0}^{p-1} \left( \frac{F(x)}{p} \right) = -1 - \left( \frac{\alpha}{p} \right) S(F_\beta). \]  \hspace{1cm} (37)

Next, substitute the known value of the exponential sum \( S(F_\beta(x)) \equiv H(\beta) \mod p \), Lemma 9, and simplify. The evaluations are correct up to a permutation of the roots \( a_{\pi(1)}, a_{\pi(2)}, a_{\pi(3)}, a_{\pi(4)} \), where \( \pi \in \text{Sym}(4) \) is a permutation of 4 elements, of the roots of the polynomial \( F(x) \).

The exponential sum \( S(G_\beta(x)) \) for the special case \( G_\beta(x) = (k^2x^2 - 1)(x^2 - \beta), 0, \pm 1 \neq \beta \in \mathbb{Z}, \) for \( k = 1 \), can be computed in a slightly different way as

\[ \sum_{x=0}^{p-1} \left( \frac{(x^2 - 1)(x^2 - \beta)}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x(x-1)(x-\beta)}{p} \right) + \sum_{x=0}^{p-1} \left( \frac{(x-1)(x-\beta)}{p} \right). \]  \hspace{1cm} (38)

Completing the calculations yield

\[ \sum_{x=0}^{p-1} \left( \frac{(x^2 - 1)(x^2 - \beta)}{p} \right) = A_\beta + (H(\beta) \mod p) \]  \hspace{1cm} (39)

where

\[ A_\beta = \sum_{x=0}^{p-1} \left( \frac{(x-1)(x-\beta)}{p} \right) = \begin{cases} -1 & \text{if } (1-\beta)^2 \neq 0, \\ p-1 & \text{if } (1-\beta)^2 = 0, \end{cases} \]  \hspace{1cm} (40)

see Lemma 3.

**Theorem 19.** Let \( F(x) = x^k - a, a \in \mathbb{F}_q \). If \( \gcd(p-1, k) \neq 1 \), then

\[ \sum_{x=0}^{p-1} \left( \frac{x^{2k} - a}{p} \right) = - \sum_{i=0}^{(k+1)/2} \left( \frac{kf}{(2i-1)f} \right) a^{f(k-2i+1)} + \left( \frac{kf}{2f} \right) a^{f(k-2i)} \mod p. \]  \hspace{1cm} (41)

Proof: Using the identity

\[ \sum_{x=0}^{p-1} \left( \frac{g_n(x^2)}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{g_n(x)}{p} \right) + \sum_{x=0}^{p-1} \left( \frac{g_n(x)}{p} \right). \]  \hspace{1cm} (42)

In full details, this is precisely

\[ \sum_{x=0}^{p-1} \left( \frac{x^{2k} + a}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x(x^2 + a)}{p} \right) + \sum_{x=0}^{p-1} \left( \frac{x^2 + a}{p} \right) = \phi_k(a) + \psi_k(a). \]  \hspace{1cm} (43)
where the last two exponential sums are, see Theorem 13, and 14,

\[ \phi_k(a) \equiv \sum_{x=0}^{p-1} \left( x \right) \left( x^k + a \right) \equiv - \sum_{i=0}^{(k+1)/2} \left( \frac{kf}{2i+1} \right) a^{f(k-2i)} \mod p, \tag{44} \]

and

\[ \psi_k(a) = \sum_{x=0}^{p-1} \left( \frac{x^k + a}{p} \right) \equiv - \sum_{i=0}^{k/2} \left( \frac{2f}{k} \right) a^{f(k-2i)} \mod p \text{ if } \gcd(p-1, k) \neq 1. \tag{45} \]
REFERENCES:
[BL] Bernstein, Daniel J.; Birkner, Peter; Joye, Marc; Lange, Tanja; Peters, Christiane Twisted Edwards curves. Progress in cryptology—AFRICACRYPT 2008, 389–405, Lecture Notes in Comput. Sci., 5023, Springer, Berlin, 2008.
[BR] Brillhart, John; Morton, Patrick Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial. J. Number Theory 106 (2004), no. 1, 79–111.
[BT] BC Berndt, RJ Evans, KS Williams, GAUSS AND JACOBI SUMS, Wiley-Interscience, N.Y., 1998.
[ES] Edwards, Harold M. A normal form for elliptic curves. Bull. Amer. Math. Soc. (N.S.) 44 (2007), no. 3, 393–422.
[JM] A Joux, F Morain, Sur les sommes de caractères liees aux courbes elliptiques a multiplication complexe, J. Number Theory 55 (1995), 108-128.
[LN] Lidl, Rudolf; Niederreiter, Harald Finite fields. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997. ISBN: 0-521-39231-4.
[OG] Omran Ahmadi, Robert Granger, On isogeny classes of Edwards curves over finite fields, arXiv:1103.3381.
[OL] Loren Olson, Hasse invariants and anomalous primes for elliptic curves with complex multiplication, J. Number Theory 8, 397-414 (1976).
[PD] R Padma, S Venkataraman, Elliptic Curves with Complex Multiplication and a Character Sum, J. Number Theory 61, 274-282 (1996).
[RS] Rubin, K.; Silverberg, A. Point counting on reductions of CM elliptic curves. J. Number Theory 129 (2009), no. 12, 2903–2923.
[SK] Stark, H. M. Counting points on CM elliptic curves. Symposium on Diophantine Problems (Boulder, CO, 1994). Rocky Mountain J. Math. 26 (1996), no. 3, 1115–1138.
[SP] BK Spearman, KS Williams, The cubic congruence x3 + Ax2 + Bx + C mod p and binary quadratic forms, J. London Math. Soc. (2) 46 (1992) 397-410.
[WS] KS Williams, EVALUATION OF CHARACTER SUMS CONNECTED WITH ELLIPTIC CURVES, Proc. Amer. Math. Soc. Vol. 73, No. 3, 1979, 291-296.
[YM] M Yamuchi, Some identities on the character sum containing x(x - 1)(x - d), Nagoya Math. J., 32 (1971) 109-113.