ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 45, Number 2, 2015

CHARACTER SUMS DETERMINED BY LOW DEGREE ISOGENIES OF ELLIPTIC CURVES

DUSTIN MOODY AND CHRISTOPHER RASMUSSEN

ABSTRACT. We generalize the character sum formulas of McLeman-Rasmussen attached to isogenies of elliptic curves in positive characteristic. Two improvements are given: sums are evaluated for isogenies of degree greater than two, and over arbitrary finite fields. We prove a transfer formula to evaluate such sums quickly over the domain curve and use this to evaluate the character sums attached to several standard families of isogenies of low degree.

1. Introduction.

Let $p > 3$ be prime, and let h_p denote the class number of $\mathbb{Q}(\sqrt{-p})$. For convenience, let h_p^* denote either 0 or h_p, as $p \pmod 4$ is congruent to 1 or 3, respectively. A well-known consequence of Dirichlet's class number formula is the relation

$$\sum_{x=1}^{p-1} x \left(\frac{x}{p} \right) = -p h_p^*. \tag{1}$$

In the recent article **[3]**, McLeman and Rasmussen reinterpreted this sum in the following way. Let $\mathbb{G}_m$ denote the multiplicative group, and let $\varphi_2 \colon \mathbb{G}_m \to \mathbb{G}_m$ be the squaring homomorphism. Then the Legendre symbol $(\frac{\cdot}{p})$ is simply the cokernel character of the group homomorphism $\varphi_2\big|_{\mathbb{G}_m(\mathbb{F}_p)} \colon \mathbb{G}_m(\mathbb{F}_p) \to \mathbb{G}_m(\mathbb{F}_p)$. Now, the left hand side of (1) may be rewritten $\sum_{x \in \mathbb{G}_m(\mathbb{F}_p)} \{x\} (\frac{x}{p})$, where $\{\cdot\}$ denotes an appropriately chosen lift $\mathbb{F}_p \to \mathbb{Z}$. So this character sum attached to the homomorphism φ_2 is divisible by p, and the quotient by p computes h_p when $p \equiv 3 \pmod 4$.

McLeman and Rasmussen then applied this view to isogenies of elliptic curves. Let $a, b \in \mathbb{Z}$ be chosen such that the following equations

---

2010 AMS *Mathematics subject classification.* Primary 145H2, Secondary 11T24, 14K02.

Received by the editors on October 11, 2012, and in revised form on February 8, 2013.

DOI:10.1216/RMJ-2015-45-2-623

give nonsingular Weierstrass models for elliptic curves over $\mathbb{Q}$:

$$E_1\colon y^2 = x^3 + ax^2 + bx,$$
$$E_2\colon y^2 = x^3 - 2ax^2 + (a^2 - 4b)x.$$

Let $\tau\colon E_1 \to E_2$ denote the 2-isogeny $(x, y) \mapsto (\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2})$. For any prime p of good reduction, this descends to an isogeny on the reduced curves, $\widetilde{\tau}$, and further to a homomorphism of abelian groups, $\widetilde{\tau}\colon \widetilde{E}_1(\mathbb{F}_p) \to \widetilde{E}_2(\mathbb{F}_p)$. Let $\chi_\tau\colon \widetilde{E}_2(\mathbb{F}_p) \to \{\pm 1\}$ denote the associated cokernel character, and define

$$S_{\tau,p} := \sum_{\substack{P \in \tilde{E}_2(\mathbb{F}_p) \\ P \neq \infty}} \{x(P) - a\}\chi_\tau(P).$$

Theorem (McLeman-Rasmussen, [**3,** Theorem 9]). *For any prime $p > 3$ of good reduction, $S_{\tau,p}$ is divisible by p. Moreover, $S_{\tau,p}$ approximates $-ph_p^*$ in the following uniform sense: the difference $|-\frac{1}{p}S_{\tau,p} - h_p^*|$ is bounded by a constant, independent of p.*

In fact, for most isogenies, the difference is zero for a positive density of primes; see [**3**] for details.

1.1. Isogenies of higher degree. It is natural to consider other isogenies over finite fields to see if the analogous character sums also carry arithmetic information. Already some progress has been made in this direction; McLeman and Moody [**2**] have demonstrated a similar phenomenon occurring in a family of 3-isogenies of elliptic curves with complex multiplication.

In this paper, we consider the case of cyclic m-isogenies of elliptic curves. Here, there is some divergence between the case of elliptic curves and the case of an endomorphism of $\mathbb{G}_m$; this is in fact what makes the generalization interesting. For example, take $m > 2$ odd and suppose $p \equiv 1 \pmod{m}$ is prime. The m-th power map $\varphi_m\colon \mathbb{G}_m \to \mathbb{G}_m$ induces an endomorphism on $\mathbb{G}_m(\mathbb{F}_p)$ whose cokernel character is the m-th order residue symbol $(\frac{\cdot}{p})_m$. However, the analogous character sum

$$\sum_{x \in \mathbb{G}_m(\mathbb{F}_p)} \{x\} \left(\frac{x}{p}\right)_m$$

vanishes always (an immediate consequence of the observation that -1 is an m-th power in $\mathbb{F}_p^\times$).

However, in the case of an m-isogeny π of elliptic curves defined over $\mathbb{F}_p$ ($m > 2$), the situation is more complicated. Experimentally, one observes that the sum does not collapse to 0 (even under the additional condition $p \equiv 1 \pmod{m}$). One suspects these sums also contain arithmetic information, and this idea is already corroborated by the recent work of McLeman-Moody for $m = 3$. In the current article, we present new results on the behavior of these character sums attached to isogenies of degree greater than two.

Theorem 1.1. *Let $\pi\colon E_1 \to E_2$ be a Vélu isogeny (as defined below) of Weierstrass elliptic curves defined over $\mathbb{F}_q$ of degree m. Let $\zeta \in \overline{\mathbb{F}_p}$ be a primitive m-th root of unity. Suppose $P \in E_1(\mathbb{F}_p)$ generates the kernel of π, and let χ denote the cokernel character of the restriction $\pi\big|_{E_1(\mathbb{F}_p)}\colon E_1(\mathbb{F}_p) \to E_2(\mathbb{F}_p)$. Then the weighted character sum $\sum_{Q\in E_2(\mathbb{F}_p)} x(Q)\chi(Q)$ over points of E_2 coincides with the sum $\sum_{j=1}^{m-1} \zeta^j x(jP)$, taken over certain points of E_1.*

In fact, any non-constant separable isogeny may be realized as a Vélu isogeny. Note that the number of terms in the second sum does not grow with p.

As an application, we take standard families of isogenies of small degree over finite fields, and compute the associated character sum explicitly. Sadly, we cannot provide a characteristic zero result in the spirit of [**2, 3**]; in those papers, the cokernel character could be written explicitly in terms of the Weierstrass models of the elliptic curves, by exploiting the properties of the Tate pairing. There is some hope that a combination of these methods, and those of the present article, may yet yield a similar result for larger values of m. In contrast to [**2, 3**], however, the results hold over arbitrary finite fields (not just prime fields), and do not require the condition $p \equiv 1 \pmod{m}$.

This paper is organized as follows. In Section 2, we deduce an exact sequence related to isogenies of elliptic curves over finite fields. In Section 3 we generalize the character sum from [**3**] to higher degree isogenies and prove the main theorem, a relation that transports character sums across a normalized isogeny. In Section 4, we apply the result to several well-known families of isogenies of small degree and obtain congruence relations for the character sums in question.

1.2. Notation. We set some notation and recall some facts about elliptic curves. Let k be a field. An elliptic curve over k is a nonsingular genus 1 curve over k with a k-rational base point. For any k'/k, the set $E(k')$ is naturally an abelian group with the base point as an identity. Any elliptic curve over k is isomorphic to a nonsingular plane cubic in $\mathbb{P}^2$ which possesses an affine model in the form of a Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in k. \tag{2}$$

By a Weierstrass elliptic curve, we mean a nonsingular projective cubic curve $E \subset \mathbb{P}^2$ of the form (2). We let ∞ denote the base point. We will at times refer to Weierstrass elliptic curves $E', E'', \ldots$ of the same form, replacing the coefficients a_i of (2) with $a_i', a_i'', \ldots$, respectively.

On any elliptic curve, the set of holomorphic and non-vanishing differentials (together with 0) is a one-dimensional $\overline{k}$-vector space. For a Weierstrass elliptic curve E, there is a distinguished generator for this space, the invariant differential

$$\omega = \frac{dx}{2y + a_1x + a_3}. \tag{3}$$

Throughout the paper, we denote the invariant differentials of Weierstrass elliptic curves $E, E', \ldots$, by ω, $\omega', \ldots$, respectively.

A curve morphism $\varphi\colon E \to E'$ which sends the base point of E to the base point of E' is called an isogeny; it is always a group homomorphism. If an isogeny φ is defined over k', then it restricts to a homomorphism $E(k') \to E'(k')$ of abelian groups, denoted $\varphi_{k'}$.

If φ is an isogeny of two Weierstrass elliptic curves, and ω' is the invariant differential of E', then $\varphi^*\omega'$ is again a holomorphic and non-vanishing differential on E. Hence, there exists $c_\varphi \in \overline{k}$ such that $\varphi^*\omega' = c_\varphi\omega$. If $c_\varphi = 1$, we say that φ is a normalized isogeny.

2. A useful exact sequence. Let E/k be an elliptic curve. For any finite subgroup $\mathcal{F} \leq E(\overline{k})$, there exists an elliptic curve E' and a separable isogeny $\pi\colon E \to E'$ whose kernel is precisely $\mathcal{F}$ ([**6,** III.4.12]). The curve E' is unique up to isomorphism.

Proposition 2.1. *Let k be a finite field, E/k an elliptic curve, and let $\pi\colon E \to E'$ be a separable isogeny with kernel $\mathcal{F} \leq E(k)$. Then there exists a k-rational isogeny $\pi'\colon E' \to E$ such that the sequence*

$$0 \longrightarrow \mathcal{F} \longrightarrow E(k) \xrightarrow{\pi_k} E'(k) \xrightarrow{\pi'_k} \mathcal{F} \longrightarrow 0$$

is exact.

Proof. Let Fr_E and $\mathrm{Fr}_{E'}$ denote the Frobenius endomorphisms $(x, y) \mapsto (x^q, y^q)$ on E and E', respectively. Since $\ker \pi = \mathcal{F} \leq E(k) = \ker(1 - \mathrm{Fr}_E)$, there exists, up to isomorphism, a unique isogeny $\pi'\colon E' \to E$ such that $1 - \mathrm{Fr}_E = \pi' \circ \pi$ (**[6,** III.4.11]); π' is necessarily defined over k since both π and $1 - \mathrm{Fr}_E$ are. Set $\mathcal{G} = \operatorname{im} \pi'_k$.

We have $\pi'_k \circ \pi_k = 0$; so $\operatorname{im} \pi_k \leq \ker \pi'_k$. Let $P' \in \ker \pi'_k$. As π is surjective, there exists $P \in E(\overline{k})$ such that $\pi(P) = P'$. Then $P \in \ker(1 - \mathrm{Fr}_E) = E(k)$, and $P' = \pi_k(P) \in \operatorname{im} \pi_k$. Thus, $\ker \pi'_k = \operatorname{im} \pi_k$, and it remains only to show $\mathcal{F} = \mathcal{G}$.

Since π is defined over k, it commutes with the Frobenius endomorphisms (i.e., $\pi \circ \mathrm{Fr}_E = \mathrm{Fr}_{E'} \circ \pi$). Thus, we have

$$\begin{aligned}(\pi \circ \pi') \circ \pi &= \pi \circ (\pi' \circ \pi)\\ &= \pi \circ (1 - \mathrm{Fr}_E) = (1 - \mathrm{Fr}_{E'}) \circ \pi.\end{aligned}$$

As π is surjective, $\pi \circ \pi' = 1 - \mathrm{Fr}_{E'}$. Thus, $\pi_k \circ \pi'_k = 0$, and so $\mathcal{G} = \operatorname{im} \pi'_k \leq \ker \pi_k = \mathcal{F}$. On the other hand, k-isogenous elliptic curves have the same number of points over k (**[8,** Theorem 1(c)]) and $\operatorname{im} \pi_k = \ker \pi'_k$. Thus,

$$\#\mathcal{G} = \frac{\#E'(k)}{\#\ker \pi'_k} = \frac{\#E(k)}{\#\operatorname{im} \pi_k} = \#\mathcal{F}, \tag{4}$$

so $\mathcal{G} = \mathcal{F}$ and the sequence is exact, as claimed. □

2.1. Vélu's formula. Let E be a Weierstrass elliptic curve defined over an arbitrary field k, and let $\mathcal{F} \leq E(\overline{k})$ be a finite subgroup. Let $\mathcal{F}^* = \mathcal{F} - \{\infty\}$. Then there exists an elliptic curve E' and a separable isogeny $E \to E'$ whose kernel is $\mathcal{F}$. For any choice of E and $\mathcal{F}$, Vélu has given explicit formulas for both a Weierstrass elliptic curve E' and an isogeny $V\colon E \to E'$ with kernel $\mathcal{F}$. Let us write $P = (x_P, y_P)$ for the affine coordinates of any point on E. If $P \notin \mathcal{F}$, the coordinates of V are given by

$$x_{V(P)} = x_P + \sum_{Q\in\mathcal{F}^*} (x_{P+Q} - x_Q),$$
$$y_{V(P)} = y_P + \sum_{Q\in\mathcal{F}^*} (y_{P+Q} - y_Q). \tag{5}$$

If E has the form (2), then the Weierstrass equation for E' is

$$E'\colon y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6',$$

where $a_i' = a_i$ for $1 \le i \le 3$, and $a_4', a_6' \in \overline{k}$ are determined explicitly by the points of $\mathcal{F}$. The formulas in **[9]** make it clear, as expected, that $a_4', a_6' \in k$ if $\mathcal{F}$ is a k-rational subgroup of $E(\overline{k})$ (i.e., invariant under the action of $\mathrm{Gal}(\overline{k}/k)$). Moreover, it follows directly from the formulas (for example, see **[5]**) that V is always a normalized isogeny. Throughout this article, we will refer to an isogeny of the form V as a Vélu isogeny.

Let $\varphi\colon C \to C'$ be a separable isogeny of elliptic curves, and fix an isomorphism $\eta\colon C \to E$ identifying C with a Weierstrass elliptic curve E. Let $V\colon E \to E'$ denote the Vélu isogeny with kernel $\eta(\ker\varphi)$. Then there exists ([**6,** III.4.11]) an isomorphism $\eta'\colon C' \to E'$ such that $\eta'\varphi = V\eta$. In this way, any separable isogeny may be realized as a Vélu isogeny of Weierstrass elliptic curves, a fact we will use in the sequel.

2.2. Normalization. Consider again the setting of Proposition 2.1. The purpose of the current section is to verify the following fact: if E and E' are Weierstrass elliptic curves and π is a Vélu isogeny, then π' is also a Vélu isogeny.

Lemma 2.2. *Suppose $\varphi\colon E \to E'$ is a separable isogeny of Weierstrass elliptic curves defined over k, and let $V\colon E \to E''$ denote Vélu's isogeny which has the same domain and kernel as φ. Then $\varphi = V$ if and only if φ is normalized and $a_i' = a_i$ for $1 \le i \le 3$.*

Proof. One direction is immediate from the properties of V. For the other, suppose $\varphi^*\omega' = \omega$ and $a_i' = a_i$ for $1 \le i \le 3$. By [**6,** III.4.11], there exists an isogeny η such that $\varphi = \eta \circ V$. Comparing degrees, η is an isomorphism of Weierstrass elliptic curves, and so has the form

$$\eta(x,y) = \big(u^{-2}(x-r), u^{-3}(y-sx+rs-t)\big), \quad r,s,t \in k,\ u \in k^{\times}.$$

As V and φ are both normalized, η is also. But $\eta^*\omega'' = u\omega'$, so $u = 1$. The well-known formulas relating a_i' and a_i'' ([**6,** pg. 45]), together with the equalities $a_i' = a_i = a_i''$ for $1 \le i \le 3$, now force $r = s = t = 0$. Thus, η is the identity, $E' = E''$, and $V = \varphi$. $\square$

Corollary 2.3. *Take the hypotheses of Proposition* 2.1*. If E and E' are Weierstrass elliptic curves and π is a Vélu isogeny, then π' is also a Vélu isogeny.*

Proof. As the Frobenius map is inseparable, we have $\mathrm{Fr}_E^*\omega = 0$; it follows that $\pi' \circ \pi = 1 - \mathrm{Fr}_E$ is normalized. As π is normalized by assumption, π' must be normalized also. But we already have $a_i = a_i'$ for $1 \le i \le 3$, and so we are done by the previous lemma. $\square$

3. A character sum determined by an isogeny. We now consider a higher degree analogue of the character sums in [**3**], where the isogenies had degree $m = 2$. Fix a prime p, and set $q = p^r$ for some $r > 0$. Let $m \ge 2$ satisfy $(p,m) = 1$. (Note, however, that we do not require $p \equiv 1 \pmod{m}$ as in [**2**] or even [**3,** Section 2].) Suppose $E_1/\mathbb{F}_q$ is a Weierstrass elliptic curve and $P \in E_1(\mathbb{F}_q)$ has exact order m. Let $V\colon E_1 \to E_2$ denote the Vélu isogeny with kernel $\langle P\rangle$. By Corollary 2.3,

$$0 \longrightarrow \langle P\rangle \longrightarrow E_1(\mathbb{F}_q) \xrightarrow{V_{\mathbb{F}_q}} E_2(\mathbb{F}_q) \xrightarrow{V'_{\mathbb{F}_q}} \langle P\rangle \longrightarrow 0$$

is exact, where $V'\colon E_2 \to E_1$ is the Vélu isogeny with kernel $V(E_1(\mathbb{F}_q))$. Thus, $V'_{\mathbb{F}_q}$ induces an isomorphism $E_2(\mathbb{F}_q)/V(E_1(\mathbb{F}_q)) \overset{\cong}{\to} \langle P\rangle$. Fix $Q \in E_2(\mathbb{F}_q)$ such that $V'(Q) = P$. (Of course, if m is prime and we allow ourselves to replace P with another generator of $\langle P\rangle$, then we may choose any $Q \in E_2(\mathbb{F}_q) - V(E_1(\mathbb{F}_q))$.)

Let ζ denote a primitive m-th root of unity in $\overline{\mathbb{F}_q}$. The cokernel character for $V_{\mathbb{F}_q}$ may be realized explicitly as $\chi_{\zeta,P}\colon E_2(\mathbb{F}_q) \to \mu_m(\overline{\mathbb{F}_q})$, defined for any $R \in E_2(\mathbb{F}_q)$ by

$$\chi_{\zeta,P}(R) := \zeta^j, \quad j \text{ chosen such that } R - jQ \in V(E_1(\mathbb{F}_q)).$$

The definition does not depend on the choice of Q; if $V'(Q_1) = V'(Q) = P$, then $R - jQ_1$ and $R - jQ$ differ by an element of $\ker V'_{\mathbb{F}_q} = \operatorname{im} V_{\mathbb{F}_q}$. The definition does depend on both the choice of generator P for the kernel of V and also the choice of generator ζ of μ_m, but these choices are related as follows. If $\langle P' \rangle = \langle P \rangle$, then there exists a, $(a, m) = 1$, such that $P' = aP$. Further, there exists $\zeta' \in \mu_m$ such that $\zeta'^a = \zeta$. The point $Q' = aQ$ satisfies $V'(Q') = P'$, and for any R we have $R - jQ' = R - jaQ$. Thus, if $\chi_{\zeta,P'}(R) = \zeta^j$, then $R - jaQ \in V(E_1(\mathbb{F}_q))$, and $\chi_{\zeta',P}(R) = \zeta'^{aj} = \chi_{\zeta,P'}(R)$.

So we fix, once and for all, a generator ζ for μ_m, and write χ_P for $\chi_{\zeta,P}$. We define an associated character sum over the $\mathbb{F}_q$-points of E_2:

$$S_P := \sum_{\substack{R \in E_2(\mathbb{F}_q) \\ R \neq \infty}} \chi_P(R) x_R.$$

The main result of this paper is that S_P is determined by a simpler weighted sum over the x-coordinates of points in $\langle P \rangle$.

Theorem 3.1. *With the above notation,*

$$S_P = \sum_{j=1}^{m-1} \zeta^j x_{jP}.$$

Thus, the task of computing the sum S_P, a priori involving roughly $q \approx \#E_2(\mathbb{F}_q)$ terms, in fact only involves summing $m - 1$ terms, and one does not even need to know E_2 explicitly in order to do it!

Proof of Theorem 3.1. Let $\mathcal{T} = V(E_1(\mathbb{F}_p))$, and set $\mathcal{T}^* = \mathcal{T} - \{\infty\}$. If $m = 2k$ is even, then

$$S_P = \sum_{R \in \mathcal{T}^*} x_R + \sum_{j=1}^{k-1} \left(\sum_{R \in \mathcal{T}} (\zeta^j + \zeta^{-j}) x_{jQ+R} \right) + \sum_{R \in \mathcal{T}} \zeta^k x_{kQ+R}.$$

The kernel of V' is $\mathcal{T}$. So, from Vélu's formula (5) (and noting $\zeta^k = -1$), we have

$$S_P = -x_{kQ} + \sum_{R \in \mathcal{T}^*} (x_R - x_{kQ+R}) + \sum_{j=1}^{k-1} \left(\sum_{R \in \mathcal{T}} (\zeta^j + \zeta^{-j}) x_{jQ+R} \right)$$

$$
\begin{aligned}
&= -x_{kV'(Q)} + \sum_{j=1}^{k-1}\left(\sum_{R\in\mathcal{T}}(\zeta^j+\zeta^{-j})x_{jQ+R}\right)\\
&= -x_{kP} + \sum_{j=1}^{k-1}(\zeta^j+\zeta^{-j})\sum_{R\in\mathcal{T}}x_{jQ+R}\\
&= -x_{kP} + \sum_{j=1}^{k-1}(\zeta^j+\zeta^{-j})\left(\sum_{R\in\mathcal{T}}x_{jQ+R} - \sum_{R\in\mathcal{T}^*}x_R + \sum_{R\in\mathcal{T}^*}x_R\right)\\
&= -x_{kP} + \sum_{j=1}^{k-1}(\zeta^j+\zeta^{-j})\left(x_{V'(jQ)} + \sum_{R\in\mathcal{T}^*}x_R\right)\\
&= -x_{kP} + \sum_{j=1}^{k-1}(\zeta^j+\zeta^{-j})x_{jP} + \sum_{j=1}^{k-1}(\zeta^j+\zeta^{-j})\sum_{R\in\mathcal{T}^*}x_R\\
&= -x_{kP} + \sum_{j=1}^{k-1}(\zeta^j+\zeta^{-j})x_{jP} - (\zeta^k+1)\sum_{R\in\mathcal{T}^*}x_R\\
&= -x_{kP} + \sum_{j=1}^{k-1}(\zeta^j+\zeta^{-j})x_{jP} = \sum_{j=1}^{m-1}\zeta^j x_{jP}.
\end{aligned}
$$

If $m = 2k+1$ is odd, the argument is similar. We have

$$
\begin{aligned}
S_P &= \sum_{R\in\mathcal{T}^*}x_R + \sum_{j=1}^{k}\left(\sum_{R\in\mathcal{T}}(\zeta^j+\zeta^{-j})x_{jQ+R}\right)\\
&= \sum_{R\in\mathcal{T}^*}x_R + \sum_{j=1}^{k}(\zeta^j+\zeta^{-j})\left(\sum_{R\in\mathcal{T}}x_{jQ+R} - \sum_{R\in\mathcal{T}^*}x_R + \sum_{R\in\mathcal{T}^*}x_R\right)\\
&= \sum_{R\in\mathcal{T}^*}x_R + \sum_{j=1}^{k}(\zeta^j+\zeta^{-j})\left(x_{V'(jQ)} + \sum_{R\in\mathcal{T}^*}x_R\right)\\
&= \left(1+\sum_{j=1}^{k}(\zeta^j+\zeta^{-j})\right)\sum_{R\in\mathcal{T}^*}x_R + \sum_{j=1}^{k}(\zeta^j+\zeta^{-j})x_{jP}\\
&= \sum_{j=1}^{k}(\zeta^j+\zeta^{-j})x_{jP} = \sum_{j=1}^{m-1}\zeta^j x_{jP},
\end{aligned}
$$

as claimed. □

TABLE 1. S_P for various m

$\phi(m)$	m	S_P
1	2	$-x_P$
2	3	$-x_P$
	4	$-x_{2P}$
	6	$-x_{3P}$
4	5	$\lambda_1 x_P + \lambda_2 x_{2P}$
	8	$\lambda_1(x_P - x_{3P}) - x_{4P}$
	10	$\lambda_1(x_P - x_{4P}) + \lambda_2(x_{2P} - x_{3P}) - x_{5P}$
	12	$\lambda_1(x_P - x_{5P}) + x_{2P} - x_{4P} - x_{6P}$
6	7	$\lambda_1 x_P + \lambda_2 x_{2P} + \lambda_3 x_{3P}$
	9	$\lambda_1 x_P + \lambda_2 x_{2P} - x_{3P} + \lambda_4 x_{4P}$

4. Applications.

4.1. General formulas for small m. As discussed in the previous section, the value of S_P is dependent on the choice of generator ζ for μ_m. Hence, there may be up to $\phi(m)$ possible values for the sum. In fact, as $x_{-P} = x_P$ for every point P on a Weierstrass elliptic curve, there are only $\phi(m)/2$ distinct values for S_P for $m > 2$.

Let $\lambda_i = \zeta^i + \zeta^{-i}$; then we may rewrite Theorem 3.1 as

$$S_P = \begin{cases} \sum_{j=1}^{k} \lambda_j x_{jP} & m = 2k+1 \\ -x_{kP} + \sum_{j=1}^{k-1} \lambda_j x_{jP} & m = 2k. \end{cases}$$

For any particular value of m, the expression may simplify further due to the symmetries of μ_m. For example, when $m = 8$, $\lambda_2 = 0$ and $\lambda_3 = -\lambda_1$. In Table 1, we catalog these expressions for S_P for various small m.

4.2. Parametrized families of isogenies. For the values of m given in Table 1, there are explicit parametrizations of Weierstrass elliptic curves with a rational point of order m; thus, each such curve is the domain of a Vélu isogeny of degree m which satisfies the hypotheses of Proposition 2.1. Consequently, we may compute P, and hence S_P, directly from the coefficients of the Weierstrass equation.

TABLE 2. S_P for parametrized families.

$m = 2$	$E\colon y^2 = x(x^2 + \alpha x + \beta)$; $P = (0, 0)$ $S_P = 0$
$m = 3$	$E\colon y^2 + \alpha xy + \beta y = x^3$; $P = (0, 0)$ $S_P = 0$
$m = 4$	$E\colon y^2 + xy - \alpha y = x^3 - \alpha x^2$; $P = (0, 0)$ $S_P = -\alpha$
$m = 4$ [**4,** Lemma 3.1]	$E\colon y^2 = x^3 + (1 - 2\alpha)x^2 + \alpha^2 x$; $P = (\alpha, \alpha)$ $S_P = 0$
$m = 6$	$E = E(\alpha + \alpha^2, \alpha)$; $P = (0, 0)$ $S_P = -\alpha(\alpha + 2)$
$m = 5$	$E = E(\alpha, \alpha)$; $P = (0, 0)$ $S_P = \lambda_2 \alpha$
$m = 8$	$E = E(\beta, \gamma)$; $P = (0, 0)$ $\beta = (2\alpha - 1)(\alpha - 1)$, $\gamma = \beta/\alpha$ $S_P = -\alpha^{-1}(\alpha - 1)(\alpha^2 + 2\lambda_1 \alpha - \lambda_1)$

As a final application, we find these values of S_P for parametrized families for $m \in \{2, 3, 4, 5, 6, 8\}$. The results are given in Table 2. This corresponds to the computation of $S_{\tau,p}$ in [**3**] for families of degree 2 isogenies, although our sums here are only valid in positive characteristic. Even in the case $m = 2$, however, the present result generalizes [**3**], where the characteristic p formulas were only established over the prime field $\mathbb{F}_p$.

Most parametrizations are given in [**1,** Table 3]; in one other case, a reference is listed in the table. As in [**1**], we let $E(\beta, \gamma)$ denote the Weierstrass elliptic curve

$$E(\beta, \gamma)\colon y^2 + (1 - \gamma)xy - \beta y = x^3 - \beta x^2.$$

The parameters β and γ are constrained only by the condition that the resulting equation must be nonsingular. For each family, we identify a point P of order m and the value(s) of S_P for the Vélu isogeny of kernel $\langle P \rangle$. Of course, this computation can be done for any parametrized family, although the corresponding formulas are no longer particularly informative as m gets large. For example, when $m = 10$, Kubert provides the parametrization ([**1,** Table 3]):

$$E = E(\beta, \gamma), \quad \delta = \alpha(\alpha - 1) - 1, \gamma = \alpha(\delta - 1), \beta = \gamma\delta,$$

which possesses $P = (0, 0)$ as a point of order 10. For this curve, we find

$$\begin{aligned} S_P = \lambda_2\alpha^5 - (3\lambda_2 + 2)\alpha^4 - (\lambda_2 - 4)\alpha^3 \\ + (6\lambda_2 + 2)\alpha^2 + (\lambda_2 - 4)\alpha - (2\lambda_2 + 2). \end{aligned}$$

5. Future work. As previously noted, when $\phi(m) = 2$, the value of S_P is well-defined and we have explicit expressions for it. These cases ($m = 3, 4, 6$) are naturally the easiest to research if relations can be found between the quotient S_p/p and the class number h_p. The authors are currently investigating the cases $m = 4$ and $m = 6$. In another direction, we ask whether any of the results generalize to character sums attached to isogenies of higher dimensional abelian varieties.

Acknowledgments. We acknowledge the contribution of SAGE [**7**], which facilitated the construction of examples which were helpful in discovering the main theorems of this work. The first author would also like to thank Daniel Shumow for conversations which led to a better understanding of normalized isogenies. Finally, we greatly appreciate the comments of an anonymous reviewer for many useful suggestions, including comments that greatly improved the presentation in Section 2. This research was partially supported by the National Institute of Standards and Technology.

REFERENCES

1. D.S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. Lond. Math. Soc. **33** (1976), 193–237.

2. C. McLeman and D. Moody, *Class numbers via* 3*-isogenies and elliptic surfaces*, Int. J. Num. Theor., 2012.

3. C. McLeman and C. Rasmussen, *Class number formulas via* 2*-isogenies of elliptic curves*, Bull. Lond. Math. Soc., 2012.

4. R. Rezaeian Farashahi, D. Moody and H. Wu, *Isomorphism classes of Edwards curves over finite fields*, Finite Fields Appl. **18** (2012), 597–612.

5. D. Shumow, *Isogenies of elliptic curves*: *A computational approach*, Master's thesis, University of Washington, 2010.

6. J.H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts Math. **106**, Springer, Dordrecht, 2009.

7. W. Stein, et al., *Sage mathematics software*, (Version 4.7), The Sage Development Team, 2011, `http://www.sagemath.org`.

8. J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

9. J. Vélu, *Isogénies entre courbes elliptiques*, C.R. Acad. Sci. **273** (1971), A238–A241.

National Institute of Standards and Technology (NIST), 100 Bureau Drive–Stop 8930, Gaithersburg, MD, 20899
Email address: **dustin.moody@nist.gov**

Department of Mathematics & Computer Science, Wesleyan University, Middletown, CT 06459
Email address: **crasmussen@wesleyan.edu**