Bull. London Math. Soc. 44 (2012) 1221–1236
doi:10.1112/blms/bds049

Class number formulas via 2-isogenies of elliptic curves

Cam McLeman and Christopher Rasmussen

Abstract

A classical result of Dirichlet shows that certain elementary character sums compute class numbers of quadratic imaginary number fields. We obtain analogous relations between class numbers and a weighted character sum associated to a 2-isogeny of elliptic curves.

1. *Introduction*

We begin by recalling a famous result of Dirichlet that calculates the class number of a quadratic imaginary number field of prime discriminant via a finite sum. Throughout, we let $p > 3$ denote a prime number. Let $(\cdot/p)$ denote the usual Legendre symbol on $\mathbb{F}_p^\times$:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & a \in \mathbb{F}_p^{\times 2}, \\ -1, & a \notin \mathbb{F}_p^{\times 2}. \end{cases}$$

The symbol is extended to all of $\mathbb{Z}$ via the reduction map $\mathbb{Z} \to \mathbb{F}_p$, and the definition $(a/p) = 0$ when $(a, p) > 1$. We let h_p denote the class number of $\mathbb{Q}(\sqrt{-p})$. For notational convenience, we set

$$h_p^* := \begin{cases} 0, & p \equiv 1 \pmod 4, \\ h_p, & p \equiv 3 \pmod 4. \end{cases}$$

The following consequence of Dirichlet's class number formula (for example, [2, Chapter 6]) is well known.

Theorem 1 (Dirichlet). *For any prime $p > 3$,*

$$-\frac{1}{p}\sum_{x=1}^{p-1} x\left(\frac{x}{p}\right) = h_p^*. \tag{1.1}$$

We consider the following point of view for Dirichlet's result. The $\mathbb{F}_p$-rational morphism $\phi\colon \mathbb{G}_m \to \mathbb{G}_m$ defined by $\phi(x) = x^2$ partitions the points of $\mathbb{G}_m(\mathbb{F}_p) \cong \mathbb{F}_p^\times$ into two sets, those that are the image of an $\mathbb{F}_p$-rational point of the domain (that is, the quadratic residues) and those that are not (the non-residues). The character $\chi_\phi := (\cdot/p)$ is now precisely the natural identification of the cokernel of ϕ with $\{\pm 1\}$ which makes the following sequence exact:

$$\mathbb{G}_m(\mathbb{F}_p) \xrightarrow{\phi} \mathbb{G}_m(\mathbb{F}_p) \xrightarrow{\chi_\phi} \{\pm 1\} \longrightarrow 0\ .$$

Note that it is the properties of ϕ, not the underlying algebraic group $\mathbb{G}_m$, which allow this construction. This paper demonstrates that an analogous procedure, arising from a different morphism of algebraic groups, yields new character sums with similar arithmetic properties.

Received 27 August 2010; revised 2 September 2011; published online 10 May 2012.

2010 *Mathematics Subject Classification* 11G05 (primary), 11R29, 11L99, 11G20 (secondary).

The first author was supported in part by the Van Vleck Fund at Wesleyan University.

Let τ be a degree 2 isogeny of elliptic curves defined over $\mathbb{F}_p$. We define a weighted character sum S_τ, analogous to the sum appearing in (1.1). The quantity S_τ is shown to be divisible by p, and a strong relationship between S_τ and h_p^* is established.

REMARK 1. Throughout this article, we study sums of the form $\sum g(x)\chi(x)$, where *a priori* the values of $g(x)$ lie in the finite field $\mathbb{F}_p$. We use the following convention, so as to view the value of the sum as an integer: Each summand is the scaling of the character value $\chi(x) \in \boldsymbol{\mu}_2(\mathbb{C}) = \{\pm 1\}$ by the unique integral lift of $g(x)$ in the range $[0, p)$. For clarity, we use braces $\{\cdot\}$ to denote the lifting $\mathbb{F}_p \to \mathbb{Z} \cap [0, p)$ explicitly.

In some proofs, it will be convenient to view sums of the form $\sum_{x=0}^{p-1}$ interchangeably as sums over $\mathbb{F}_p$ or as sums over the range $[0, p)$ of integers. Consequently, there will occasionally be a mild abuse of notation, for example, given $a \in \mathbb{Z}$, we may write $\{a\}$ to mean $\{\bar{a}\}$, where $\bar{a}$ is the reduction of a mod p.

1.1. *Complex multiplication example*

We begin with two typical results, both special cases of the Main Theorem. Consider first the elliptic curve

$$E/\mathbb{Q}\colon y^2 = (x+2)(x^2-2), \tag{1.2}$$

which possesses complex multiplication by $\mathbb{Z}[\sqrt{-2}]$. As this ring possesses elements of absolute norm 2, there exist endomorphisms of degree 2 on E. These endomorphisms admit reductions defined over $\mathbb{F}_p$ whenever p is a prime of good and ordinary reduction (equivalently, $(-2/p) = 1$). For a specific choice of τ (see § 4), we set

$$\chi_\tau(P) = \begin{cases} +1, & P \in \tau(E(\mathbb{F}_p)), \\ -1, & P \notin \tau(E(\mathbb{F}_p)). \end{cases} \tag{1.3}$$

This defines a character on $E(\mathbb{F}_p)$, and the following sequence is exact:

$$E(\mathbb{F}_p) \xrightarrow{\tau} E(\mathbb{F}_p) \xrightarrow{\chi_\tau} \boldsymbol{\mu}_2 \longrightarrow 0\,.$$

The following is a consequence of the Main Theorem.

PROPOSITION 2. *Let $p > 3$ be a prime of good and ordinary reduction for the elliptic curve E given in (1.2). Then*

$$-\frac{1}{p} \sum_{\substack{P \in E(\mathbb{F}_p) \\ P \neq \infty}} \{x(P)\}\chi_\tau(P) = h_p^*. \tag{1.4}$$

REMARK 2. It is not *a priori* clear that the sum in (1.4) (or the sum in (1.1), for that matter) is divisible by p. We note that the two sums appearing in (1.1) and (1.4) are *not* the same expressions, even though they both compute h_p^*. This is immediate from the observation that E and $\mathbb{G}_m$ need not have the same number of points over $\mathbb{F}_p$. Here is an explicit example: When $p = 11$, one has

$$E(\mathbb{F}_{11}) = \{\infty, (7, \pm 4), (8, \pm 2), (9, 0)\}, \quad \tau(E(\mathbb{F}_{11})) = \{\infty, (7, \pm 4)\}.$$

Hence, (1.4) may be evaluated as

$$-\tfrac{1}{11}(7 + 7 - 8 - 8 - 9) = 1,$$

whereas the classical expression (1.1) yields

$$-\tfrac{1}{11}(1-2+3+4+5-6-7-8+9-10)=1.$$

1.2. *Non-complex multiplication example*

This connection between weighted character sums and class numbers is not unique to isogenies arising from complex multiplication. Consider the elliptic curves

$$E_1/\mathbb{Q}\colon y^2=x^3+2x^2-x,$$
$$E_2/\mathbb{Q}\colon y^2=x^3-4x^2+8x,$$

and the following isogeny of degree 2:

$$\tau\colon E_1\to E_2,\quad \tau(x,y)=\left(\frac{y^2}{x^2},-\frac{y(1+x^2)}{x^2}\right).$$

The curves E_1 and E_2 have good reduction away from 2. For any odd prime p, τ induces an isogeny between the reductions of E_1 and E_2 over $\mathbb{F}_p$, and this morphism is in fact $\mathbb{F}_p$-rational. Hence, there exists a homomorphism $\tau\colon E_1(\mathbb{F}_p)\to E_2(\mathbb{F}_p)$. As in the previous example, we consider the character

$$\chi_\tau\colon E_2(\mathbb{F}_p)\longrightarrow\{\pm1\},$$

where $\chi_\tau(P)=+1$ if and only if $P\in\tau(E_1(\mathbb{F}_p))$. Again we find a strong relationship between h_p^* and the weighted character sum

$$S_\tau:=\sum_{\substack{P\in E_2(\mathbb{F}_p)\\ P\neq\infty}}\{x(P)-2\}\chi_\tau(P).$$

The following is a special case of the Main Theorem (see § 4, Example 1).

PROPOSITION 3. *With E_1, E_2 and τ as above, and any prime $p>3$, we have $-(1/p)S_\tau=h_p^*$.*

1.3. *Main result*

The Main Theorem generalizes the previous examples, each of which relates h_p^* to a weighted character sum. Suppose $E_1/\mathbb{Q}$, $E_2/\mathbb{Q}$ are elliptic curves and $\tau\colon E_1\to E_2$ is a $\mathbb{Q}$-rational 2-isogeny. For any prime p of good reduction, there is an $\mathbb{F}_p$-rational isogeny $\tau_p\colon E_1/\mathbb{F}_p\to E_2/\mathbb{F}_p$. Hence, τ induces a family of isogenies $\{\tau_p\}$, indexed by the primes of good reduction. To each of these isogenies, there is an associated character $\chi_\tau=\chi_{\tau,p}$, and an associated weighted character sum $S_{\tau,p}$ (defined below). As in the above examples, the quotient $-(1/p)S_{\tau,p}$ always approximates h_p^* well, in the sense that there is an absolute bound for the error as p varies among all primes of good reduction.

Concretely, let $a,b\in\mathbb{Z}$, and let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be the elliptic curves given by the following Weierstrass models:

$$\begin{aligned}E_1&\colon y^2=x^3+ax^2+bx,\\ E_2&\colon y^2=x^3-2ax^2+(a^2-4b)x.\end{aligned}\tag{1.5}$$

Let $\tau\colon E_1\to E_2$ be the explicit isogeny given in (2.2).

MAIN THEOREM. *Let E_1, E_2 and τ be as above, and let $p>3$ be a prime of good reduction for E_1 and E_2.*

(a) *For all such p, the weighted character sum*

$$S_{\tau,p} := \sum_{\substack{P \in E_2(\mathbb{F}_p) \\ P \neq \infty}} \big\{x(P) - a\big\}\chi_\tau(P)$$

is divisible by p.

(b) *The sum $S_{\tau,p}$ approximates $-ph_p^*$ in the following sense: the quantity*

$$R_{a,b}(p) = -\frac{1}{p}S_{\tau,p} - h_p^*$$

is bounded in absolute value by a constant C_τ, independent of p.

(c) *If there exists one $p > |a|$ such that $R_{a,b}(p) = 0$, then there exists a set of primes of positive density for which $S_{\tau,p} = h_p^*$, determined by explicit congruence conditions.*

The remainder of the paper is organized as follows. In § 2, we collect relevant facts about 2-isogenies over finite fields, and compute the cokernel character χ_τ in terms of the Tate pairing. In § 3, we prove the Main Theorem. The proof combines classical techniques for evaluating character sums with formulas deduced from the Tate pairing. In § 4, we extend the theorem to isogenies not specifically of the form (2.2), in particular the degree 2 endomorphisms existing on elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{-7}]$. An analogous result for the dual isogeny $\hat{\tau}$ of (2.2) is given in the Appendix.

2. *Preliminaries*

Our strategy for the proof of the Main Theorem will be to convert the characters in § 1 into explicitly computable Legendre symbols. For this, we recall some facts about isogenies of degree 2 and the mechanics of the Tate pairing attached to an isogeny.

2.1. *Degree 2 isogenies*

Let K be an arbitrary field with $\operatorname{char} K \neq 2$, and let E_1 and E_2 be elliptic curves defined over K. Let $\phi\colon E_1 \to E_2$ be an isogeny of degree 2 defined over K. Necessarily, this implies that both E_1 and E_2 possess K-rational points of order 2 (generating the kernels of ϕ and the dual $\hat{\phi}$, respectively). Hence, by appropriate changes of coordinates, E_1 and E_2 are isomorphic over K to elliptic curves E_1' and E_2', respectively, each of which possesses a Weierstrass equation of the form $y^2 = f_i(x)$, with $f_1(0) = f_2(0) = 0$. In fact, we may always simultaneously choose isomorphisms $\alpha_i\colon E_i \to E_i'$ such that

(i) E_1' has the Weierstrass model $y^2 = x^3 + ax^2 + bx$ with $a, b \in K$;
(ii) E_2' has the Weierstrass model $y^2 = x^3 - 2ax^2 + rx$, with $r = a^2 - 4b$;
(iii) there exists a K-rational 2-isogeny $\tau\colon E_1' \to E_2'$ such that the following diagrams commute:

$$\begin{array}{ccc} E_1 & \xrightarrow{\alpha_1} & E_1' \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\tau} \\ E_2 & \xrightarrow[\alpha_2]{} & E_2' \end{array} \qquad \begin{array}{ccc} E_2 & \xrightarrow{\alpha_2} & E_2' \\ {\scriptstyle\hat{\phi}}\downarrow & & \downarrow{\scriptstyle\hat{\tau}} \\ E_1 & \xrightarrow[\alpha_1]{} & E_1' \end{array} \tag{2.1}$$

The explicit formulas for τ and its dual are well known [7, III.4.5]:

$$\tau(x,y) = \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right), \quad \hat{\tau}(x,y) = \left(\frac{y^2}{4x^2}, \frac{y(r-x^2)}{8x^2}\right). \tag{2.2}$$

Placing the isogeny in this form will simplify the computations involving the Tate pairing. We will show how to treat more general 2-isogenies in § 4.

2.2. *The Tate pairing*

Let ℓ and p be prime numbers such that $p \equiv 1 \pmod{\ell}$, and let E_1 and E_2 be elliptic curves defined over $\mathbb{F}_p$. Let $\tau\colon E_1 \to E_2$ be an isogeny of degree ℓ defined over $\mathbb{F}_p$, and let $\hat{\tau}$ denote the dual isogeny. Let us assume that $E_1[\tau] \subseteq E_1(\mathbb{F}_p)$ and $E_2[\hat{\tau}] \subseteq E_2(\mathbb{F}_p)$, and let T_1 and T_2 generate the groups $E_1[\tau]$ and $E_2[\hat{\tau}]$, respectively. The Tate pairing associated to τ is a function

$$\psi_\tau\colon \frac{E_2(\mathbb{F}_p)}{\tau(E_1(\mathbb{F}_p))} \times E_2[\hat{\tau}] \longrightarrow \mathbb{F}_p^\times/\mathbb{F}_p^{\times\ell},$$

which is bilinear and non-degenerate on the left. (See, for example, [7, X.1.1], which develops the properties of $\psi_{[m]}$. The proofs for ψ_τ are essentially identical.) We can explicitly compute ψ_τ as follows. The points T_1 and T_2 are of exact order ℓ, as is any $R \in \tau^{-1}(T_2)$. Thus, there exist functions f on E_2 and g on E_1 whose divisors are

$$\begin{aligned}(f) &= \ell(T_2) - \ell(\infty),\\ (g) &= \tau^*((T_2) - (\infty)) = \sum_{i=0}^{\ell-1}(R + iT_1) - \sum_{i=0}^{\ell-1}(iT_1).\end{aligned} \tag{2.3}$$

Scaling either f or g by a constant if necessary, we have an equality of functions $f \circ \tau = g^\ell$. For a point $S \in E_2(\mathbb{F}_p)$, let $[S]$ denote its image in $E_2(\mathbb{F}_p)/\tau(E_1(\mathbb{F}_p))$. If $S \in E_2(\mathbb{F}_p)$ and $[S] \neq [T_2], [\infty]$, then we define

$$\psi_\tau([S], T_2) := f(S) \pmod{\mathbb{F}_p^{\times\ell}}.$$

In case $[S] \in \{[T_2], [\infty]\}$, we choose a point $Q \notin \{T_2, \infty\}$ on E_2 and set

$$\psi_\tau([S], T_2) := \frac{f(S+Q)}{f(Q)} \pmod{\mathbb{F}_p^{\times\ell}}.$$

As $E_2[\hat{\tau}]$ is generated by T_2, we may recover the entire pairing by bilinearity, since we have $\psi_\tau([S], kT_2) = \psi_\tau([S], T_2)^k$. Thus, the following definition is complete:

$$\psi_\tau([S], kT_2) := \begin{cases} f(S)^k, & [S] \notin \{[T_2], [\infty]\},\\ \left(\dfrac{f(S+Q)}{f(Q)}\right)^k, & [S] \in \{[T_2], [\infty]\}.\end{cases}$$

2.3. *Formulas for 2-isogenies*

We now specialize to the case of the degree 2 isogenies τ and $\hat{\tau}$ given in (2.2).

Definition 4. Define a character $\chi_\tau\colon E_2(\mathbb{F}_p) \to \boldsymbol{\mu}_2$ by

$$\chi_\tau(P) = \begin{cases} +1, & P \in \tau(E_1(\mathbb{F}_p)),\\ -1, & P \notin \tau(E_1(\mathbb{F}_p)).\end{cases}$$

We compute this character explicitly in terms of the pairing ψ_τ. This allows us to replace χ_τ with expressions involving the Legendre symbol, and so evaluate the weighted character sum S_τ from § 1. We let T_1 and T_2, respectively, denote the point $(0,0) \in E_1(\mathbb{F}_p)$, which generates $E_1[\tau]$, and the point $(0,0) \in E_2(\mathbb{F}_p)$, which generates $E_2[\hat{\tau}]$.

PROPOSITION 5. *Suppose* $\tau\colon E_1 \to E_2$ *is of the form* (2.2), *and let* $P = (x, y) \in E_2(\mathbb{F}_p)$. *Then*

$$\chi_\tau(P) = \psi_\tau([P], T_2) = \begin{cases} \left(\dfrac{x}{p}\right), & [P] \neq [T_2], [\infty], \\ \left(\dfrac{r}{p}\right), & [P] = [T_2], \\ 1, & [P] = [\infty], \end{cases}$$

where in the second equality we canonically identify $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ *with* $\boldsymbol{\mu}_2$ *via the Legendre symbol.*

Proof. For the statement that $\chi(\cdot) = \psi_\tau(\cdot, T_2)$, we must show that a point $P \in E_2(\mathbb{F}_p)$ is in the image of τ if and only if $\psi_\tau([P], T_2) = 1$. By bilinearity, $\psi_\tau([P], kT_2) = \psi_\tau([P], T_2)^k$. As $E_2[\hat{\tau}]$ is generated by T_2, P pairs trivially with T_2 if and only if it pairs trivially with every element of $E_2[\hat{\tau}]$. By the left non-degeneracy of ψ_τ, this occurs if and only if $[P]$ represents the trivial class of $E_2(\mathbb{F}_p)/\tau(E_1(\mathbb{F}_p))$, that is, P is in the image of τ.

To prove the second equality, we now compute $\psi_\tau([P], T_2)$ explicitly. Functions f and g whose divisors are given in (2.3) are $f(x, y) = x$, $g(x, y) = y/x$. No scaling is necessary, as we have

$$f(\tau(P)) = x(\tau(P)) = \frac{y^2}{x^2} = g^2(P).$$

Thus, $\psi_\tau([P], T_2)$ is a square in $\mathbb{F}_p^\times$ if and only if $(x/p) = 1$. This proves the second equality when $[P] \neq [T_2], [\infty]$. The result is trivial for $[P] = [\infty]$. It remains to prove $\psi_\tau([T_2], T_2) = (r/p)$. Note that $T_2 \in \tau(E_1(\mathbb{F}_p))$ if and only if $E_1[2] \subseteq E_1(\mathbb{F}_p)$. From this, we see

$$\begin{aligned} \psi_\tau([T_2], T_2) = +1 &\iff E_1[2] \subseteq E_1(\mathbb{F}_p) \\ &\iff x^2 + ax + b \text{ splits in } \mathbb{F}_p[x] \\ &\iff r = a^2 - 4b \equiv \square \pmod{p} \\ &\iff \left(\frac{r}{p}\right) = +1. \end{aligned}$$

□

REMARK 3. In fact, $[T_2] = [\infty]$ if and only if $(r/p) = 1$.

2.4. *Dual isogeny formulas*

Finally, we note that we can provide an equally explicit result for the pairing attached to the dual $\hat{\tau}$. The cokernel character $\chi_{\hat{\tau}}$ is defined by

$$\chi_{\hat{\tau}}(P) = \begin{cases} +1, & P \in \hat{\tau}(E_2(\mathbb{F}_p)), \\ -1, & P \notin \hat{\tau}(E_2(\mathbb{F}_p)). \end{cases}$$

Let $\hat{f}$ and $\hat{g}$ be the functions on E_1 whose divisors are

$$\begin{aligned} (\hat{f}) &= 2(T_1) - 2(\infty), \\ (\hat{g}) &= \hat{\tau}^*((T_1) - (\infty)). \end{aligned}$$

For example, take $\hat{f}(x, y) = x$, and $\hat{g}(x, y) = y/2x$. Then the associated pairing

$$\psi_{\hat{\tau}}\colon \frac{E_1(\mathbb{F}_p)}{\hat{\tau}(E_2(\mathbb{F}_p))} \times E_1[\tau] \longrightarrow \frac{\mathbb{F}_p^\times}{\mathbb{F}_p^{\times 2}}$$

may be computed via

$$\psi_{\hat{\tau}}([S], kT_1) = \begin{cases} \hat{f}(S)^k, & [S] \notin \{[T_1], [\infty]\}, \\ \left(\dfrac{\hat{f}(S+Q)}{\hat{f}(Q)} \right)^k, & [S] \in \{[T_1], [\infty]\}. \end{cases}$$

PROPOSITION 6. *For any $P = (x, y) \in E_1(\mathbb{F}_p)$,*

$$\chi_{\hat{\tau}} = \psi_{\hat{\tau}}([P], T_1) = \begin{cases} \left(\dfrac{x}{p} \right), & [P] \neq [T_1], [\infty], \\ \left(\dfrac{b}{p} \right), & [P] = [T_1], \\ 1, & [P] = [\infty]. \end{cases}$$

Proof. The argument parallels Proposition 5 exactly. □

3. *Weighted character sums*

There are well-established connections between arithmetic data and character sums arising from elliptic curves. If $y^2 = f(x)$ is an integral model for an elliptic curve over $\mathbb{Q}$ with complex multiplication, and p is a prime of good reduction, then the work of Deuring [**3**] demonstrates that character sums of the form

$$\sum_{x=1}^{p-1} \left(\frac{f(x)}{p} \right)$$

can be computed in terms of the trace of Frobenius and the splitting of p in the endomorphism ring of the curve. Similar results have been established by many different authors. We mention, for example, the works of Williams [**10**], Joux–Morain [**4**] and Padma–Venkataraman [**6**], each of which takes slightly different approaches to such character sums, consolidates many previous results and contains comprehensive bibliographies.

We briefly contrast these character sums to those contained in the present paper. First, the character χ_τ is determined by an isogeny, not an elliptic curve. Second, the terms of the sum are weighted by a non-trivial integer-valued function. (This is necessary if we hope to obtain interesting results, since trivially we have $\sum_P \chi_\tau(P) = 0$.) To the authors' knowledge, these sums have not been extensively studied.

We recall our convention to use $\{\cdot\}$ to denote the lifting $\mathbb{F}_p \to \mathbb{Z} \cap [0, p)$, and introduce a second convention that a primed sum over the points on an elliptic curve will exclude the point at infinity on that curve. Under these conventions, we seek to evaluate the sum

$$\sum_{P \in E_2(\mathbb{F}_p)}{}' \{x(P) - a\} \chi_\tau(P), \tag{3.1}$$

where τ is the isogeny given in (2.2). Here, we are taking E_1, E_2 and τ to be defined over $\mathbb{F}_p$.

We first evaluate a useful character sum. For a given prime p and $k \in \mathbb{Z}$ such that $p \nmid k$, we define

$$\delta_k := \frac{1}{2} \left(1 + \left(\frac{k}{p} \right) \right) = \begin{cases} 1, & k \equiv \square \pmod{p}, \\ 0, & k \not\equiv \square \pmod{p}. \end{cases}$$

LEMMA 7. *For any integer k relatively prime to p,*

$$\sum_{u=1}^{p-1} u\left(\frac{u^2+k}{p}\right) = -p\delta_k. \tag{3.2}$$

Proof. Let S be the sum. Then, by substituting $u \mapsto p-u$, we find

$$S = \sum_{u=1}^{p-1}(p-u)\left(\frac{(p-u)^2+k}{p}\right) = p\sum_{u=1}^{p-1}\left(\frac{u^2+k}{p}\right) - S.$$

Therefore,

$$\begin{aligned}\frac{2S}{p} &= \sum_{u=1}^{p-1}\left(\frac{u^2+k}{p}\right) = -\left(\frac{k}{p}\right) + \sum_{u=0}^{p-1}\left(\frac{u^2+k}{p}\right)\\ &= -\left(\frac{k}{p}\right) - p + \sum_{u=0}^{p-1}\left[1+\left(\frac{u^2+k}{p}\right)\right].\end{aligned} \tag{3.3}$$

Let $C/\mathbb{F}_p$ be the conic $u^2+kw^2=v^2$. The final term in (3.3) counts the number of $\mathbb{F}_p$-rational points on C within the affine region $w \neq 0$. Since $(p,k)=1$, the conic is birational to $\mathbb{P}^1$ and has $p+1$ points. Exactly two of these, $(1:\pm 1:0)$, lie on $w=0$, so the affine region contains $p-1$ points. Thus,

$$S = \frac{p}{2}\left[-\left(\frac{k}{p}\right) - p + (p-1)\right] = -\frac{p}{2}\left(1+\left(\frac{k}{p}\right)\right) = -p\delta_k,$$

which completes the proof. □

REMARK 4. Sums of the form (3.2) will appear in the proof below, with $u = x-a$. This motivates the choice $g = x(P)-a$ as the weight in (3.1). We mention in passing that this function g has an interesting geometric description: If $Q_i = (\alpha_i, 0)$ are the 2-torsion points on E_2 that are not in the kernel of $\hat{\tau}$, then $a = \frac{1}{2}(\alpha_1+\alpha_2)$. That is, we may think of $g=0$ as the unique vertical line which intersects the x-axis at a point equidistant to both Q_1 and Q_2.

As always, let $p>3$ be prime. We have already seen at the start of § 2 that we may transform any $\mathbb{F}_p$-rational 2-isogeny into the isogeny τ of (2.2). Then the isogeny τ is between the curves

$$\begin{aligned}E_1&: y^2 = f_1(x) = x^3+ax^2+bx, \quad a,b \in \mathbb{F}_p,\\ E_2&: y^2 = f_2(x) = x^3-2ax^2+rx, \quad r = a^2-4b.\end{aligned}$$

Recall that $T := (0,0) \in E_2(\mathbb{F}_p)$ generates the kernel of $\hat{\tau}$. Our goal is to evaluate the sum

$$S_\tau := \sum_{P\in E_2(\mathbb{F}_p)}{}' \{x(P)-a\}\chi_\tau(P). \tag{3.4}$$

For convenience, we define an error term:

$$R_{a,b} := \delta_{-b} - \sum_{x=1}^{\{a\}-1}\left(\frac{x}{p}\right).$$

PROPOSITION 8. *Let $p > 3$ be prime, and E_1, E_2, τ and S_τ be as above. Then S_τ is divisible by p and*

$$-\frac{1}{p}S_\tau = h_p^* + R_{a,b}. \tag{3.5}$$

Further, $|R_{a,b}| \leqslant \{a\}$.

Proof. The bound on $R_{a,b}$ is immediate. As h_p^* and $R_{a,b}$ are integers, it remains only to establish (3.5). Applying Proposition 5, we have

$$\begin{aligned}
S_\tau &= \sum_{P\in E_2(\mathbb{F}_p)}{}' \{x(P)-a\}\chi_\tau(P)\\
&= \{x(T)-a\}\chi_\tau(T) + \sum_{\substack{P\in E_2(\mathbb{F}_p)\\ P\neq T,\infty}} \{x(P)-a\}\left(\frac{x(P)}{p}\right)\\
&= \{p-a\}\left(\frac{r}{p}\right) + \sum_{x=1}^{p-1}\{x-a\}\left(\frac{x}{p}\right)\left(1+\left(\frac{x^3-2ax^2+rx}{p}\right)\right)\\
&= \{p-a\}\left(\frac{r}{p}\right) + \sum_{x=1}^{p-1}\{x-a\}\left(\frac{x}{p}\right) + \sum_{x=1}^{p-1}\{x-a\}\left(\frac{(x-a)^2-4b}{p}\right)\\
&= \sum_{x=1}^{p-1}\{x-a\}\left(\frac{x}{p}\right) + \sum_{x=0}^{p-1}\{x-a\}\left(\frac{(x-a)^2-4b}{p}\right).
\end{aligned}$$

We evaluate these two sums in turn. First,

$$\begin{aligned}
\sum_{x=1}^{p-1}\{x-a\}\left(\frac{x}{p}\right) &= \sum_{x=1}^{\{a\}-1}(p+\{x\}-\{a\})\left(\frac{x}{p}\right) + \sum_{x=\{a\}}^{p-1}(\{x\}-\{a\})\left(\frac{x}{p}\right)\\
&= p\sum_{x=1}^{\{a\}-1}\left(\frac{x}{p}\right) + \sum_{x=1}^{p-1}x\left(\frac{x}{p}\right) - a\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\\
&= p\sum_{x=1}^{\{a\}-1}\left(\frac{x}{p}\right) - ph_p^*.
\end{aligned}$$

We note that the second sum is unchanged by making the substitution $u = x - a$. Thus,

$$\sum_{x=0}^{p-1}\{x-a\}\left(\frac{(x-a)^2-4b}{p}\right) = \sum_{u=0}^{p-1}\{u\}\left(\frac{u^2-4b}{p}\right) = -p\delta_{-b}$$

by Lemma 7. Combining the two sums, we have

$$S_\tau = -ph_p^* - p\delta_{-b} + p\sum_{x=1}^{\{a\}-1}\left(\frac{x}{p}\right),$$

which gives (3.5). □

The Main Theorem can be viewed as the global version of Proposition 8. Consider elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ with respective Weierstrass models

$$\begin{aligned}
E_1&\colon y^2 = x^3 + ax^2 + bx,\\
E_2&\colon y^2 = x^3 - 2ax^2 + (a^2-4b)x,
\end{aligned}$$

with $a, b \in \mathbb{Z}$. As always, we let $\tau\colon E_1 \to E_2$ be the explicit $\mathbb{Q}$-rational 2-isogeny given in (2.2).

THEOREM 9. *Let $\tau\colon E_1 \to E_2$ be as above, and let $p > 3$ be a prime of good reduction.*

(a) *For all such p, the weighted character sum*

$$S_{\tau,p} := \sum_{P \in E_2(\mathbb{F}_p)}{}' \{x(P) - a\}\chi_\tau(P)$$

is divisible by p.

(b) *The sum $S_{\tau,p}$ approximates $-ph_p^*$ in the following sense: the quantity*

$$R_{a,b}(p) = -\frac{1}{p}S_{\tau,p} - h_p^*$$

is bounded in absolute value by a constant C_τ, independent of p.

(c) *If there exists one $p > |a|$ such that $R_{a,b}(p) = 0$, then there exists a set of primes of positive density for which $S_{\tau,p} = h_p^*$, determined by explicit congruence conditions.*

Proof. Part (a) is precisely Proposition 8 applied to any prime of good reduction. For part (b), it is enough to bound the number of terms in $R_{a,b}$ independently of p. If $a > 0$, then this is obvious; the sum has exactly $\{a\}$ terms, and $\{a\} \leqslant a$. When $a = 0$, we trivially have $C_\tau = 1$. Now suppose $a < 0$. If $p \leqslant |a|$, then $\{a\} < p \leqslant |a|$, and $|R_{a,b}| \leqslant |a|$. If $p > |a|$, then $\{a\} = p + a$.

$$R_{a,b} = \delta_{-b} - \sum_{x=1}^{\{a\}-1}\left(\frac{x}{p}\right) = \delta_{-b} - \sum_{x=1}^{p}\left(\frac{x}{p}\right) + \sum_{x=\{a\}}^{p}\left(\frac{x}{p}\right) = \delta_{-b} + \sum_{x=p+a}^{p}\left(\frac{x}{p}\right),$$

and so $|R_{a,b}| \leqslant |a| + 2$.

For part (c), suppose $p_0 > |a|$ is a prime for which $R_{a,b}(p_0) = 0$. So $p = p_0$ is a solution to the following:

$$\delta_{-b} = \sum_{x=1}^{\{a\}-1}\left(\frac{x}{p}\right). \tag{3.6}$$

Now, among $p > |a|$, the individual terms of the sum (3.6) never vanish, and so the sum is periodic as a function of p, with respect to some sufficiently large modulus, for example, $N = 4G$, where G is the least common multiple of $\{2, 3, \ldots, |a| - 1\}$. Thus, every prime in the sequence $\{p_0 + kN\}$ also satisfies $R_{a,b}(p) = 0$. □

The analogous result for the dual isogeny $\hat{\tau}$ is proved in the Appendix.

REMARK 5. It is natural to ask what happens when the hypothesis in part (c) does not hold. It is possible that the error term is zero for only finitely many p. For example, when $(a, b) = (9, -1)$, the error term vanishes only for $p = 7$. It is even possible that the error term is never zero (see Example 2). Indeed, by the periodicity modulo N, the error term is never zero if it is non-zero for all $p < N$.

REMARK 6. For fixed a and varying p, it is not hard to argue that the uniform bounds constructed in the proof of Theorem 9 are the best possible. However, for a *particular* value of p, better bounds certainly exist. For example, if $a = O(\log p)$, then the estimates of Pólya–Vinogradov (and later improvements by Burgess) may offer substantial improvement. For details, see, for example, [**5**, § 9.4].

3.1. *Examples*

We consider a few examples for illustration. In all cases, the selection of values (a, b) determines elliptic curves E_1, E_2 by (1.5) and an isogeny τ by (2.2).

EXAMPLE 1. Set $(a, b) = (2, -1)$. Then we have $R_{a,b}(p) = 0$ for all primes $p > 3$. Hence, $-S_\tau/p = h_p^*$ for all such p.

EXAMPLE 2. Set $(a, b) = (3, -1)$. We find $R_{a,b} = -(2/p)$, which is non-zero for all $p > 3$.

EXAMPLE 3. Set $(a, b) = (7, 2)$. Then, for $p \neq 5$ ($R_{a,b}(5) \neq 0$ by a separate calculation),

$$R_{a,b} = \delta_{-2} - \sum_{x=1}^{6} \left(\frac{x}{p}\right) = 2 + \delta_{-2} + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \left(\frac{5}{p}\right) + \left(\frac{6}{p}\right).$$

We wish to decide when this sum vanishes. By a parity argument, we must have $\delta_{-2} = 0$, and of the four remaining Legendre symbols, three must evaluate to -1, and one to $+1$. Further, we cannot have $(5/p) = 1$. Otherwise, $R_{a,b} = 0$ implies $(2/p) = (3/p) = (6/p) = -1$, contradicting the multiplicativity of the Legendre symbol. The remaining possibilities each lead to congruence conditions easily determined via quadratic reciprocity. Namely, we find

$$-\frac{S_\tau}{p} = h_p^* \iff p \equiv 17, 43, 67, 83, 107 \text{ or } 113 \mod 120.$$

4. *Complex multiplication*

Having computed the character sums associated to 2-isogenies given in the specific form (2.2), we turn to the analogous computation for other 2-isogenies. The principal technical lemma is that the character sums are unaffected by applying a change of coordinates $x \mapsto x - \varepsilon$ to the curve. This will allow us to change the codomain of an arbitrary 2-isogeny to one of the form in (2.2), and allow us to compute the corresponding character sums. As a primary application, the elliptic curves with complex multiplication by $\sqrt{-1}$, $\sqrt{-2}$ or $\sqrt{-7}$ possess an endomorphism of degree 2, and in this section we will compute the associated weighted character sum. In particular, we deduce Proposition 2.

Suppose that $\phi\colon E_1' \to E_2'$ is a degree 2-isogeny defined over $\mathbb{F}_p$ with $p > 3$. Then there exist $\mathbb{F}_p$-isomorphisms $\alpha_i\colon E_i' \to E_i$ and an isogeny τ of the form (2.2) such that the left square of the following diagram commutes:

$$\begin{array}{ccccc} E_1' & \xrightarrow{\phi} & E_2' & \xrightarrow{\chi_\phi} & \boldsymbol{\mu}_2 \\ {\scriptstyle\alpha_1}\downarrow & & \downarrow{\scriptstyle\alpha_2} & & \Vert{\scriptstyle\mathrm{id}} \\ E_1 & \xrightarrow[\tau]{} & E_2 & \xrightarrow[\chi_\tau]{} & \boldsymbol{\mu}_2 \end{array} \tag{4.1}$$

Here, χ_ϕ and χ_τ are the characters attached to ϕ and τ, respectively.

LEMMA 10. *The right square of the above diagram commutes, that is,* $\chi_\phi(P') = \chi_\tau(\alpha_2(P'))$ *for any* $P' \in E_2'(\mathbb{F}_p)$.

Proof. This is a simple diagram chase. If $\chi_\phi(P') = 1$, then there exists a point $Q' \in E_1'(\mathbb{F}_p)$ such that $\phi(Q') = P'$. Hence, $\alpha_2(P') = \tau(\alpha_1(Q))$, and so $\chi_\tau(\alpha_2(P')) = 1$ also. This argument is easily reversed, and the result follows. □

As a consequence, we demonstrate that the weighted character sum

$$S_\phi := \sum_{P\in E_2'(\mathbb{F}_p)}{}' \{x(P)-\xi\}\chi_\phi(P)$$

equals the sum S_τ of (3.4), provided that α_2 is of a particular form and ξ is chosen appropriately. Let E_2' be the elliptic curve

$$y^2 = (x-\varepsilon)(x^2-2\mu x+\nu), \quad \varepsilon,\mu,\nu\in\mathbb{F}_p \tag{4.2}$$

defined over $\mathbb{F}_p$. Let ϕ be an isogeny such that the kernel of the dual isogeny $\hat\phi$ is generated by $(\varepsilon,0)\in E_2'(\mathbb{F}_p)$. Set $(a,b)=(\mu-\varepsilon,\frac14(\mu^2-\nu))$, and let E_1,E_2,τ be as in (2.2). Then the map

$$\alpha_2(x,y) := (x-\varepsilon,y) \tag{4.3}$$

has the property that $\hat\tau\circ\alpha_2$ and $\hat\phi$ have the same kernel. This guarantees the existence of a unique α_1 satisfying $\hat\tau\circ\alpha_2=\alpha_1\circ\hat\phi$ and, in fact, α_1 completes the diagram (4.1). Now set $\xi=\varepsilon+a$, so that

$$S_\phi = \sum_{P\in E_2'(\mathbb{F}_p)}{}' \{x(P)-\varepsilon-a\}\chi_\phi(P).$$

LEMMA 11. $S_\phi = S_\tau$.

Proof. Let p be a prime of good reduction. Applying the previous lemma, we have

$$\begin{aligned} S_\phi &= \sum_{P\in E_2'(\mathbb{F}_p)}{}' \{x(P)-\varepsilon-a\}\chi_\phi(P)\\ &= \sum_{P\in E_2(\mathbb{F}_p)}{}' \{x(\alpha_2^{-1}(P))-\varepsilon-a\}\chi_\phi(\alpha_2^{-1}(P))\\ &= \sum_{P\in E_2(\mathbb{F}_p)}{}' \{x(P)-a\}\chi_\tau(P) = S_\tau. \end{aligned} \tag{4.4}$$

□

We now address complex multiplication endomorphisms. For each endomorphism ϕ, we select isomorphisms α_i such that $\alpha_2\circ\phi=\tau\circ\alpha_1$, as in diagram (4.1), and such that E_2' and α_2 have the forms (4.2) and (4.3), respectively. Evaluation of S_ϕ now follows from the previous lemma.

4.1. *Complex multiplication by* -1

Consider first the elliptic curve $E/\mathbb{Q}$: $y^2=x^3+x$, which has complex multiplication by $\mathbb{Z}[\sqrt{-1}]$, and possesses the degree 2 endomorphism

$$\phi\colon E\longrightarrow E, \quad \phi(x,y)=\left(\frac{x^2+1}{2ix},\frac{y(x^2-1)}{(2i-2)x^2}\right). \tag{4.5}$$

Let $E'/\mathbb{Q}$ be the elliptic curve with the Weierstrass equation $y^2=x^3-\frac14 x$, and let $\tau\colon E'\to E$ be the isogeny corresponding to $(a,b)=(0,-\frac14)$. If α_2 is the identity and α_1 is the isomorphism

$$\alpha_1(x,y)=(u^{-2}x,u^{-3}y), \quad u=-(1+i),$$

then $\alpha_2\circ\phi=\tau\circ\alpha_1$. Suppose $p>3$ is a prime of good reduction that splits in $\mathbb{Q}(i)$. Each of the morphisms in the above diagram has a well-defined reduction mod p, and the diagram still commutes after reduction. Applying Lemma 10 and Theorem 9, we see

$$S_\phi = S_\tau = -ph_p^* - pR_{0,-\frac14} = -p.$$

This proves the following corollary.

COROLLARY 12. *Let $p > 3$ be a prime, and suppose $p \equiv 1 \pmod 4$. Then*

$$-\frac{1}{p}\sum_{P\in E(\mathbb{F}_p)}{}' \{x(P)\}\chi_\phi(P) = 1.$$

4.2. *Complex multiplication by -2*

Next, we compute the character sum associated to a degree 2 endomorphism on an elliptic curve with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$. One such elliptic curve is

$$E/\mathbb{Q}\colon y^2 = (x+2)(x^2-2).$$

One degree 2 endomorphism on E is

$$\phi(x,y) = \left(\frac{(x+2)^2+2}{-2(x+2)}, \frac{y((x+2)^2-2)}{2\sqrt{-2}(x+2)^2}\right). \tag{4.6}$$

(This may be derived from the formula given in [8, p. 111], but note that we are using a different Weierstrass equation.) Let $p > 3$ be a prime that splits in $\mathbb{Q}(\sqrt{-2})$, so that $(-2/p) = 1$. Equivalently, p is congruent to 1 or 3 (mod 8). For such primes, there is a well-defined reduction for ϕ over $\mathbb{F}_p$, which we will also denote by ϕ. We now prove Proposition 2. Set

$$S_\phi := \sum_{P\in E(\mathbb{F}_p)}{}' \{x(P)\}\chi_\phi(P).$$

COROLLARY 13. *For any prime $p > 3$ such that $p \equiv 1$ or $3 \pmod 8$, $-(1/p)S_\phi = h_p^*$.*

Proof. Let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ denote the elliptic curves corresponding to the choice $(a,b) = (2, \frac{1}{2})$ in (2.2); let τ denote the corresponding 2-isogeny. It is straightforward to find isomorphisms α_i with the requisite properties such that $\tau\circ\alpha_1 = \alpha_2\circ\phi$. Hence, $S_\phi = S_\tau$. By Proposition 8, $-(1/p)S_\tau = h_p^* + R_{2,\frac{1}{2}} = h_p^*$, as $R_{2,\frac{1}{2}} = 0$ if $p \equiv 1, 3 \pmod 8$. □

4.3. *Complex multiplication by -7*

Finally, we compute the character sum associated to a degree 2 endomorphism on a curve with complex multiplication by $\mathbb{Z}[\sqrt{-7}]$. We take the elliptic curve

$$E/\mathbb{Q}\colon y^2 = (x+7)(x^2-7x+14).$$

Let $p > 3$ be a prime that splits in $\mathbb{Q}(\sqrt{-7})$, so $(-7/p) = 1$. Set $\beta = (1+\sqrt{-7})/2$. A degree 2 endomorphism on E is given explicitly by Silverman [8, p. 111]:

$$\phi(x,y) = \left(\beta^{-2}\left(x - \frac{7(1-\beta^4)}{x+\beta^2-2}\right), \beta^{-3}y\left(1 + \frac{7(1-\beta)^4}{(x+\beta^2-2)^2}\right)\right). \tag{4.7}$$

Let E_1 and E_2 be the elliptic curves

$$E_1/\mathbb{Q}(\sqrt{-7})\colon y^2 = x^3 + ax^2 + bx,$$
$$E_2/\mathbb{Q}(\sqrt{-7})\colon y^2 = x^3 - 2ax^2 + rx,$$

where

$$a = \tfrac{3}{2}(\beta - 4), \quad b = \tfrac{7}{16}(3\beta + 14), \quad r = a^2 - 4b.$$

The curves E, E_1 and E_2 are all isomorphic over $\mathbb{Q}(\sqrt{-7})$. Let α_1 and α_2 be the isomorphisms

$$\alpha_1 \colon E \longrightarrow E_1, \quad (x, y) \longmapsto ((\beta - 1)^2 x + \beta + 3, (\beta - 1)^3 y),$$
$$\alpha_2 \colon E \longrightarrow E_2, \quad (x, y) \longmapsto (x + 4 - \beta, y).$$

As before, we have $\tau \circ \alpha_1 = \alpha_2 \circ \phi$, and each morphism reduces to an $\mathbb{F}_p$-rational morphism on the reduced curves, as p splits in $\mathbb{Q}(\sqrt{-7})$. If we define

$$S_\phi := \sum_{P \in E(\mathbb{F}_p)}{}' \{x(P)\} \chi_\phi(P),$$

then $S_\phi = S_\tau$, and we find $-(1/p)S_\phi = h_p^* + R_{a,b}$.

Unlike all previous examples, however, we do not have a uniform bound for the error. Our bound is always in terms of $\{a\}$, but in this situation $a \notin \mathbb{Z}$. Hence, as a function of p, $\{a\}$ is not eventually constant, and the previous results bounding $R_{a,b}$ do not apply.

Appendix. *A proof of a dual isogeny calculation*

Let τ and $\hat{\tau}$ be the isogenies defined in (2.2), with $a, b \in \mathbb{F}_p$ for $p > 3$. Recall that we set $r = a^2 - 4b$. Let $\eta = \{a/2\}$, and define

$$\hat{R}_{a,b} := \delta_{-r} + \sum_{x=1}^{\eta} \left(\frac{-x}{p}\right).$$

We wish to evaluate

$$S_{\hat{\tau}} := \sum_{P \in E_1(\mathbb{F}_p)}{}' \left\{x(P) + \frac{a}{2}\right\} \chi_{\hat{\tau}}(P).$$

THEOREM A.1. *For any odd prime p of good reduction,*

$$-\frac{1}{p} S_{\hat{\tau}} = h_p^* + \hat{R}_{a,b}. \tag{A.1}$$

Proof. By Proposition 6, we first obtain

$$\begin{aligned}
S_{\hat{\tau}} &= \eta \left(\frac{b}{p}\right) + \sum_{\substack{P \in E_1(\mathbb{F}_p) \\ P \neq T_1, \infty}} \left\{x(P) + \frac{a}{2}\right\} \chi_{\hat{\tau}}(P) \\
&= \eta \left(\frac{b}{p}\right) + \sum_{x=1}^{p-1} \left\{x + \frac{a}{2}\right\} \left(\frac{x}{p}\right) \left(1 + \left(\frac{x^3 + ax^2 + bx}{p}\right)\right) \\
&= \eta \left(\frac{b}{p}\right) + \sum_{x=1}^{p-1} \left\{x + \frac{a}{2}\right\} \left(\frac{x}{p}\right) + \sum_{x=1}^{p-1} \left\{x + \frac{a}{2}\right\} \left(\frac{x^2 + ax + b}{p}\right) \\
&= \sum_{x=1}^{p-1} \left\{x + \frac{a}{2}\right\} \left(\frac{x}{p}\right) + \sum_{x=0}^{p-1} \left\{x + \frac{a}{2}\right\} \left(\frac{x^2 + ax + b}{p}\right).
\end{aligned}$$

The first sum evaluates as follows:

$$\sum_{x=1}^{p-1}\left\{x+\frac{a}{2}\right\}\left(\frac{x}{p}\right)=\sum_{x=1}^{p-1-\eta}(\{x\}+\{\eta\})\left(\frac{x}{p}\right)+\sum_{x=p-\eta}^{p-1}(\{x\}+\{\eta\}-p)\left(\frac{x}{p}\right)$$
$$=\sum_{x=1}^{p-1}x\left(\frac{x}{p}\right)+\eta\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)-p\sum_{x=p-\eta}^{p-1}\left(\frac{x}{p}\right)=-ph_p^*-p\sum_{x=1}^{\eta}\left(\frac{-x}{p}\right).$$

As for the second sum, we substitute $u=x+\eta$ and apply Lemma 7 to get

$$\sum_{x=0}^{p-1}\left\{x+\frac{a}{2}\right\}\left(\frac{x^2+ax+b}{p}\right)=\sum_{u=0}^{p-1}\{u\}\left(\frac{u^2-r/4}{p}\right)=-p\delta_{-r/4}=-p\delta_{-r}.$$

Combining the above calculations yields the result. □

We conclude with a brief comment on the 'globalization' of the error term for $S_{\hat{\tau}}$, analogously to Theorem 9 for S_τ. Take E_1, E_2 and τ as in (2.2), with $a,b\in\mathbb{Z}$. For simplicity, suppose $p>a>0$, so that $a=\{a\}$. If a is even, then we have the explicit bound $|\hat{R}_{a,b}|\leqslant a/2+1$ for the error term. If a is odd, the behavior of the error is different. For $p>2a$, we have $\eta=(p-1)/2+(a+1)/2$ exactly, and so the error term has roughly $p/2$ terms. Further, from [1, § 4, Chapter 5], we have

$$\sum_{x=1}^{(p-1)/2}\left(\frac{-x}{p}\right)=\begin{cases}0, & p\equiv 1,5 \pmod 8,\\ -3h_p, & p\equiv 3 \pmod 8,\\ -h_p, & p\equiv 7 \pmod 8.\end{cases}$$

Thus, the term $\hat{R}_{a,b}$ may dwarf h_p! Rather, if we define

$$\hat{\rho}_{a,b}:=\delta_{-r}+\sum_{x=1}^{(a+1)/2}\left(\frac{-(p-1)/2-x}{p}\right),$$

then $|\hat{\rho}_{a,b}|\leqslant(a+3)/2$, and (A.1) can be rewritten:

$$-\frac{1}{p}S_{\hat{\tau}}=\hat{\rho}_{a,b}+\begin{cases}0, & p\not\equiv 3 \pmod 8,\\ -2h_p, & p\equiv 3 \pmod 8.\end{cases}$$

This gives a better description of the behavior of the sum $S_{\hat{\tau}}$ when a is odd.

Acknowledgements. We are grateful to Kirti Joshi for first bringing our attention to the interesting divisibility properties of weighted character sums on elliptic curves, and for many fruitful conversations during our research. We give our thanks to Joe Silverman and Matt Papanikolas for helpful suggestions. We wish to recognize the contribution of W. A. Stein *et al.* [9], which was invaluable for computational experimentation related to this project. Finally, we appreciate the many helpful comments and suggestions of the referee during the revision of this article.

References

1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Pure and Applied Mathematics 20 (Academic Press, New York, 1966). Translated by Newcomb Greenleaf.
2. H. Davenport, *Multiplicative number theory*, 3rd edn, Graduate Texts in Mathematics 74 (Springer, New York, 2000). Revised and with a preface by Hugh L. Montgomery.
3. M. Deuring, 'Die Typen der Multiplikatorenringe elliptischer Funktionenkörper', *Abh. Math. Sem. Hansischen Univ.* 14 (1941) 197–272.
4. A. Joux and F. Morain, 'Sur les sommes de caractères liées aux courbes elliptiques à multiplication complexe', *J. Number Theory* 55 (1995) 108–128.

5. H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics 97 (Cambridge University Press, Cambridge, 2007).
6. R. Padma and S. Venkataraman, 'Elliptic curves with complex multiplication and a character sum', *J. Number Theory* 61 (1996) 274–282.
7. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106 (Springer, New York, 1986).
8. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151 (Springer, New York, 1994).
9. W. A. Stein *et al.*, *Sage mathematics software (Version 4.3.3)*, The Sage Development Team, 2009, http://www.sagemath.org.
10. K. S. Williams, 'Evaluation of character sums connected with elliptic curves', *Proc. Amer. Math. Soc.* 73 (1979) 291–299.

Cam McLeman
Department of Mathematics
University of Michigan-Flint
303 E. Kearsley Street
Flint, MI 48502
USA

mclemanc@umflint.edu

Christopher Rasmussen
Department of Mathematics and Computer Science
Wesleyan University
265 Church Street
Middletown, CT 06459
USA

crasmussen@wesleyan.edu