CLASS NUMBERS VIA 3-ISOGENIES AND ELLIPTIC SURFACES

CAM MCLEMAN AND DUSTIN MOODY

Abstract. We show that a character sum attached to a family of 3-isogenies defined on the fibers of a certain elliptic surface over $\mathbb{F}_p$ relates to the class number of the quadratic imaginary number field $\mathbb{Q}(\sqrt{-p})$. In this sense, this provides a higher-dimensional analog of the class number formula given in [6].

1. Introduction

From the days of Diophantus, elliptic curves have long attracted the interest of mathematicians. More recently, elliptic curves have found applications in diverse areas such as the proof of Fermat's last theorem, factoring large integers, and in cryptography. Researchers have also found reasons to study various character sums on the points of an elliptic curve. These reasons include showing the uniformity of distribution of certain points on elliptic curves, summing up primes, finding generators for elliptic curve groups and determining the structure of that group (see, for example, [1], [2], [3], [4], [5], [8], [9], [11]), etc. A new direction in this area has been to examine integer-weighted character sums over elliptic curves [6], [7]. In this vein we recall two results, whose interplay motivates the main result of this paper.

First, to certain 2-isogenies τ of elliptic curves defined over $\mathbb{F}_p$, Rasmussen and McLeman attach an integer-valued character sum S_τ (to be defined shortly). This character sum is shown to be divisible by p in [6]. The subsequent analysis of the quotient S_τ/p turns out to be of arithmetic significance, providing a new class number formula strikingly similar to a classical result of Dirichlet's. Namely, we have

$$-\tfrac{1}{p}\, S_\tau = h_p^*, \tag{1}$$

where

$$h_p^* = \begin{cases} h(\mathbb{Q}(\sqrt{-p})) & \text{if } p \equiv 3 \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Here p is a prime and $h(\mathbb{Q}(\sqrt{-p}))$ denotes the class number of $\mathbb{Q}(\sqrt{-p})$.

A second family of results from [7], computes the mod-p value of a much larger class of analogous character sums attached to isogenies of larger degree, and specifically, finds several new classes of character sums which are also evenly divisible by p. In light of the above class number formula, it seems of interest to determine the analogous quotients. The current article addresses the analysis of such quotients, focusing on one particular family of 3-isogeny sums satisfying precisely this divisibility condition. We show that when this family of character sums is viewed as a single character sum over an elliptic *surface*, these quotients also compute class numbers of quadratic imaginary number fields. In this sense, this can be viewed as a higher-dimensional analog of (1).

Statement of Results – We begin with some notation. Let p and ℓ be primes, with $p \equiv 1 \pmod{\ell}$. Let $\tau\colon E \to E'$ be an ℓ-isogeny of elliptic curves defined over the finite field $\mathbb{F}_p$. Let $\zeta = \zeta_\ell$ denote a fixed primitive complex ℓ-th root of unity, and choose a point $Q \in E'(\mathbb{F}_p) - \tau(E(\mathbb{F}_p))$. From the isomorphism $E'(\mathbb{F}_p)/\tau(E(\mathbb{F}_p)) \cong \mathbb{Z}/\ell\mathbb{Z}$, for each $P \in E'(\mathbb{F}_p)$ we have $P - kQ \in \tau(E(\mathbb{F}_p))$ for a unique $0 \le k \le \ell - 1$. We define the *character* χ_τ *attached to* τ by:

$$\chi_\tau(P) = \zeta^k, \qquad \text{where } P - kQ \in \tau(E(\mathbb{F}_p)).$$

In particular, $\chi_\tau(P) = 1$ if and only if P is in the image of τ.

We adopt the following notation for lifting from $\mathbb{F}_p$ to $\mathbb{Z}$: for $a \in \mathbb{F}_p$, let $\{a\}$ denote the unique integer $0 \le \{a\} \le p-1$ such that $\{a\} \bmod p = a$. For the remainder of this paper we will use $E(\mathbb{F}_p)$ to denote the set of affine $\mathbb{F}_p$-rational points on the curve. That is, we do not include the point ∞ in $E(\mathbb{F}_p)$. Finally, given a point $P \in E(\mathbb{F}_p)$, let $x(P)$ be the x-coordinate of P.

Notation in hand, we turn to more precise formulations of the two aforementioned motivating results. The first is the definition of the character sum S_τ appearing in (1). Let $\tau\colon E \to E'$ be a 2-isogeny defined over $\mathbb{F}_p$, and let χ_τ be the character attached to τ as described above. To such a τ, we introduce the integer-valued character sum

$$S_\tau := \sum_{P \in E'(\mathbb{F}_p)} \{x(P)\}\chi_\tau(P). \tag{2}$$

For a concrete example of a situation in which (1) holds, one can take ([6], Proposition 2) E and E' to both be the curve $y^2 = (x+2)(x^2-2)$ over the finite field $\mathbb{F}_p$ for any prime $p > 3$ of good and ordinary reduction, and τ a degree-2 endomorphism of E arising from complex multiplication on E (by $\mathbb{Z}[\sqrt{-2}]$). If we let $p = 131$, for example, then it can be checked that $S_\tau = -655$, and indeed $655/131 = 5$ is the class number of $\mathbb{Q}(\sqrt{-131})$.

The second motivating result concerns a second class of isogenies τ which give character sums divisible by p, but for which we do *not* know the analogous value of S_τ/p. To wit, let $p \equiv 1 \pmod 3$, and let $E_d/\mathbb{F}_p$ be the elliptic curve given by $y^2 = x^3 + d$. If we set $d' = -27d \in \mathbb{F}_p$, the function

$$\tau_d(x,y) := \left(\frac{y^2+3d}{x^2}, \frac{y(x^3-8d)}{x^3}\right)$$

defines a 3-isogeny from E_d to $E_{d'}$. Let us further suppose that $\left(\frac{d}{p}\right) = 1$ to isolate the interesting cases of the character sum[1]. Then we have the following divisibility result:

[1] If d is a non-square mod p, then E_d has a $\mathbb{F}_p$-rational subgroup of order 3 but no $\mathbb{F}_p$-rational 3-torsion point. The isogeny τ corresponding to this subgroup is now surjective, and the character χ_τ degenerates to the trivial character.

Theorem 1. *Let p and $\tau_d \colon E_d \to E_{d'}$ be as above, with character χ_{τ_d}. Then*

$$S_{\tau_d} := \sum_{P \in E_{d'}(\mathbb{F}_p)} \{x(P)\} \chi_{\tau_d}(P)$$

is an integer divisible by p.

This theorem can also be established using the techniques in [7]. We include a proof in this work, as it is a stepping stone to prove our main result. Worth mentioning is the following corollary of Theorem 1.

Corollary 2. *Since $S_{\tau_d} \in \mathbb{Z}$, we note that S_{τ_d} is independent of the choice of the point $Q \in E_{d'}(\mathbb{F}_p) - \tau_d(E_d(\mathbb{F}_p))$ used to define χ_{τ_d}.*

Unlike the sum in (1), however, there does not seem to be a direct relationship between the individuals sums S_{τ_d} and any relevant class number. Instead, we will see that class numbers arise as a *sum* of quotients S_{τ_d}/p as d runs over the set of all quadratic residues mod p. In fact, the process of summing over all such d permits a concise reformulation in terms of elliptic surfaces, which we describe now. We begin with the substitution $d = z^2$, so that running over all $z \in \mathbb{F}_p^\times$ is equivalent to running over all square d twice. After the substitution, we arrive at the algebraic surface

$$\widetilde{\mathcal{E}}/\mathbb{F}_p\colon \quad y^2 = x^3 + z^2.$$

More specifically, $\widetilde{\mathcal{E}}$ is an *elliptic* surface, as the projection $\pi : \mathcal{E} \to \mathbb{A}^1_z$ from $\mathcal{E}$ on to the affine z-line provides the surface with a natural elliptic fibration, with a single singular fiber over $z = 0$. Let $\mathcal{E} = \widetilde{\mathcal{E}} - E_0$ denote the complement of the singular fiber. The above isogenies $\tau_d = \tau_{z^2}$ can now be interpreted as maps from one fiber of $\mathcal{E}$ to another, namely from the fiber over z to the fiber over $-27z$. We patch these fiberwise-defined isogenies together to give a global endomorphism $\tau\colon \mathcal{E} \to \mathcal{E}$ which respects the fibration in the sense that $\pi(P_1) = \pi(P_2)$ implies $\pi(\tau(P_1)) = \pi(\tau(P_2))$ for points $P_1, P_2 \in \mathcal{E}(\mathbb{F}_p)$. We simply set

$$\tau(x, y, z) = \left(\frac{y^2 + 3z^2}{x^2}, \frac{y(x^3 - 8z^2)}{x^3}, -27z \right).$$

We also extend the character χ_{τ_d}, defined *a priori* on each fiber to a global function on $\mathcal{E}$: For $P = (x, y, z) \in \mathcal{E}$, we have $(x, y) \in E_{z^2}$, and hence it is sensible to write

$$\chi_\tau(P) = \chi_{\tau_{z^2}}(x, y).$$

Note that, as before, $\chi_\tau(P) = 1$ if and only if P is in the image of τ. Finally, we construct the higher-dimensional character sum. Define

$$\mathcal{S}_\tau = \sum_{P \in \mathcal{E}} \{x(P)\} \chi_\tau(P).$$

The principal result of this work is the following theorem.

Main Theorem. *Let $p \equiv 1 \pmod 3$, and let $\mathcal{E}$, τ, χ_τ, and $\mathcal{S}_\tau$ be as above. Then*

$$\tfrac{1}{p}\, \mathcal{S}_\tau = h_p^* - \tfrac{p-1}{2}.$$

Our technique for calculating the sum $\mathcal{S}_\tau$ defined on $\mathcal{E}$ is essentially a division of labor between two approaches. We will independently sum "vertically" (over fibers) and "horizontally" (over sections) over our surface. Section 2 deals with the former, analyzing the fiber-wise isogenies τ_d defined in the introduction, and we address the global calculation of $\mathcal{S}_\tau$ in Section 3.

2. Fiberwise-sums and the Tate pairing

We maintain the notation established in the introduction. Namely, we have $p \equiv 1 \pmod 3$, a value $d \in \mathbb{F}_p^*$ with $\left(\frac{d}{p}\right) = 1$, and the 3-isogeny of $\mathbb{F}_p$-curves $\tau_d : E_d \to E_{d'}$. Note that the conditions on p and d imply

$$\left(\frac{d}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{-3d}{p}\right) = 1.$$

We begin with an analysis of the contribution to $\mathcal{S}_\tau$ coming from a given fiber. Set

$$S_{\tau_d} := \sum_{P \in E_{d'}(\mathbb{F}_p)} \{x(P)\}\chi_{\tau_d}(P),$$

so that $\mathcal{S}_\tau = 2 \sum_{\substack{d=0 \\ \left(\frac{d}{p}\right)=1}}^{p-1} S_{\tau_d}$. As in [6], the first step in evaluating S_{τ_d} is to use the Tate pairing to provide explicit formulas for the computation of χ_{τ_d}.

Let us briefly recall the construction of the (complex-valued) Tate pairing attached to τ_d, and its connection to the character χ_{τ_d}. Let $\widehat{\tau_d}$ be the dual isogeny to τ_d and consider the point $T = (0, 3\sqrt{-3d})$, which generates of the group $E_{d'}[\widehat{\tau_d}](\mathbb{F}_p)$. One begins by finding a pair of functions f_T and g_T such that $\operatorname{div}(f_T) = 3[T] - 3[\infty]$ and $f_T \circ \tau_d = g_T^3$. The Tate pairing

$$\psi_{\tau_d} \colon \frac{E_{d'}(\mathbb{F}_p)}{\tau(E_d(\mathbb{F}_p))} \times E_{d'}[\widehat{\tau_d}](\mathbb{F}_p) \longrightarrow \mu_3(\mathbb{C}),$$

is the (bilinear and non-degenerate) pairing given by the composite

$$\psi_{\tau_d}([P], kt) = \left(\frac{\psi'_{\tau_d}([P], kT)}{p}\right)_3,$$

where $[P]$ denotes the image of P in the quotient $E_{d'}(\mathbb{F}_p)/\tau_d(E_d(\mathbb{F}_p))$, and after choosing an arbitrary point $Q \in E_{d'}(\mathbb{F}_p) - \langle T \rangle$, we set

$$\psi'_{\tau_d}([P], kT) := \begin{cases} f(P)^k & [P] \notin \langle [T] \rangle \\ \left(\frac{f(P+Q)}{f(Q)}\right)^k & [P] \in \langle [T] \rangle. \end{cases} \tag{3}$$

We use $\mu_3(\mathbb{C})$ to denote the set of cubic roots of unity in $\mathbb{C}$, and $\left(\frac{\cdot}{p}\right)_3$ to denote the cubic residue symbol mod p.

Remark 3. The definition of the Tate pairing in (3) actually outputs a value in $\mathbb{F}_p^*/(\mathbb{F}_p^*)^3$, so we compose this version of the Tate pairing with an isomorphism $\mathbb{F}_p^*/(\mathbb{F}_p^*)^3 \cong \mu_3(\mathbb{C})$. In the proof of Theorem 5, we will choose the isomorphism which forces the Tate pairing to coincide with our character χ_{τ_d}.

Proposition 4. *Letting E_d, $E_{d'}$, τ_d, and T as above, we can take*

$$f_T = y - 3\sqrt{-3d} \qquad \text{and} \qquad g_T = \frac{y-\sqrt{-3d}}{x}$$

in the definition of the Tate pairing.

Proof. We easily check that f_T is of degree 3 and vanishes only at T, so $\operatorname{div}(f_T) = 3[T] - 3[\infty]$. Now we need only to verify that as functions on $E_{d'}$, $f_T \circ \tau_d$ is the cube of g_T. For a point $P = (x, y) \in E_1(\mathbb{F}_p)$ (i.e., satisfying $x^3 = y^2 - d$), we have

$$\begin{aligned} f \circ \tau(P) &= \frac{y(x^3 - 8d)}{x^3} - 3\sqrt{-3d} \\ &= \frac{y(y^2 - 9d) - 3\sqrt{-3d}(y^2 - d)}{x^3} \\ &= \left(\frac{y - \sqrt{-3d}}{x}\right)^3, \end{aligned}$$

as desired. □

Theorem 5. *With E_d, τ_d, and T as above, we have the following explicit formulas for the character χ_{τ_d}:*

$$\chi_{\tau_d}(P) = \psi_{\tau_d}([P], T) = \begin{cases} \left(\frac{-4d}{p}\right)_3^k & \text{if } [P] = [kT],\ k = 0, 1, 2, \\ \left(\frac{y-3\sqrt{-3d}}{p}\right)_3 & \text{otherwise.} \end{cases} \tag{4}$$

Note in particular that $\chi_{\tau_d}(P) = 1$ if and only if $P \in \tau_d(E_1(\mathbb{F}_p))$.

Proof. Let us abbreviate $\tau = \tau_d$ for the duration of the proof. For the statement that $\chi_\tau(\cdot) = \psi_\tau([\cdot], T)$, we first show that a point $P \in E_{d'}(\mathbb{F}_p)$ is in the image of τ if and only if $\psi_\tau([P], T) = 1$. By bilinearity, $\psi_\tau([P], kT) = \psi_\tau([P], T)^k$. As $E_2[\hat{\tau}]$ is generated by T, P pairs trivially with T 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 $E_2(\mathbb{F}_p)/\tau(E_1(\mathbb{F}_p))$, i.e., P is in the image of τ. This shows that $\chi_\tau(\cdot) = \psi_\tau([\cdot], P)$ or $\chi_\tau(\cdot) = \psi_\tau^{-1}([.], P)$. As in Remark 3, we now choose the correct isomorphism to achieve equality.

We proceed to the second equality in the statement of the theorem. Since the bottom case is the definition of the Tate pairing for such points (given the calculation of f_T from the previous proposition), we only need to address the top case. For this it suffices to show that $\chi_\tau(T) = 1$ if and only if $\left(\frac{-4d}{p}\right)_3 = 1$. Let α be a square root of $-3d$ in $\mathbb{F}_p$, such that $T = (0, 3\alpha)$. Suppose first $\left(\frac{-4d}{p}\right)_3 = 1$, so that we have some $\delta \in \mathbb{F}_p$ with $\delta^3 = -4d$. Then

$$\begin{aligned} \tau(\delta, \alpha) &= \left(\frac{\alpha^2 + 3d}{\delta^2}, \frac{\alpha(\delta^3 - 8d)}{\delta^3}\right) \\ &= \left(0, \frac{-12d\alpha}{-4d}\right) \\ &= T, \end{aligned}$$

which shows that $\chi_\tau(T) = 1$.

For the converse, we assume there exists $x, y \in \mathbb{F}_p$, with $\tau(x, y) = (0, 3\alpha)$. This requires that $\frac{y^2+3d}{x^2} = 0$ and $\frac{y(x^3-8d)}{x^3} = 3\alpha$. From the first of these equations we see that $y^2 = -3d$. As the point (x, y) is on the curve $y^2 = x^3 + d$, it follows that $x^3 = -4d$, so $\frac{-4d}{p}{}_3 = 1$. $\square$

With these explicit formulas for χ_{τ_d} in hand, we now prove Theorem 1.

Theorem 1. *Let p, E_d, $E_{d'}$, and τ_d be as above. Then*

$$S_{\tau_d} := \mathop{}_{P\in E_{d'}(\mathbb{F}_p)} \{x(P)\}\chi_{\tau_d}(P)$$

is an integer divisible by p.

Proof. Since the values of $\{x(P)\}$ are 0 for $P \in \langle T\rangle$, they contribute trivially to the sum (no matter the value of $\chi_{\tau_d}(P)$). This allows us to avoid breaking the sum into cases based on the results of the Tate pairing. We have

$$\begin{aligned}\sum_{P\in E_{d'}(\mathbb{F}_p)} \{x(P)\}\chi_\tau(P) &= \sum_{P\in E_{d'}(\mathbb{F}_p)} \{x(P)\} \left(\frac{y(P) - 3\sqrt{-3d}}{p}\right)_3 \\ &= \sum_{y=0}^{p-1} \sum_{\substack{x=0 \\ x^3\equiv y^2+27d}}^{p-1} x \left(\frac{y - 3\sqrt{-3d}}{p}\right)_3 \\ &= \sum_{y=0}^{p-1} \left(\frac{y - 3\sqrt{-3d}}{p}\right)_3 \sum_{\substack{x=0 \\ x^3\equiv y^2+27d}}^{p-1} x.\end{aligned}$$

Now each inner summand here is the sum of the lifts of the mod-p cube roots of $y^2 + 27d$. This sum is necessarily zero mod p since the coefficient of x^2 in the polynomial $x^3 - (y^2 + 27d)$ is trivial. Thus the whole sum is divisible by p, as desired. $\square$

3. The Global Sum

We recall the global setting from the introduction. The surface $\mathcal{E}$ is the complement of the singular fiber over $z = 0$ in the elliptic surface defined over $\mathbb{F}_p$ by $y^2 = x^3 + z^2$. As such, $\mathcal{E}$ is the union of fibers over z for non-zero $z \in \mathbb{F}_p$. For $P = (x, y, z) \in \mathcal{E}$, we have $(x, y) \in E_{z^2}$, and we glue together the fiber-wise isogenies τ_d to a global function τ and global character χ_τ by defining

$$\chi_\tau(P) = \chi_{\tau_{z^2}}(x, y).$$

The global sum $\mathcal{S}_\tau$ from the main theorem now decomposes as (twice) the sum of the fiberwise-sums addressed in the previous section:

$$\mathcal{S}_\tau := \mathop{}_{P\in\mathcal{E}} \{x(P)\}\chi_\tau(P) = 2 \mathop{}_{\substack{d\in\mathbb{F}_p \\ \left(\frac{d}{p}\right)=1}} S_{\tau_d}.$$

As an immediate corollary of Theorem 1, we have the divisibility of the global sum.

Corollary 6. *With notation as previously defined, $p \mid \mathcal{S}_\tau$.*

We now let β denote a fixed square root of $-27 \pmod{p}$, and introduce the characteristic function

$$e(x,y,z) := \begin{cases} 1 & \text{if } y^2 \equiv x^3 - 27z^2 \pmod{p}, \\ 0 & \text{otherwise} \end{cases}$$

on points $(x,y,z) \in \mathbb{F}_p^3$. The explicit computation of the Tate pairing, using the function $f_T = y - 3\sqrt{-3}\,z = y - \beta z$ in the fiber E_{z^2} provides the following formula for $\mathcal{S}_\tau$.

$$\begin{aligned} \mathcal{S}_\tau &= \sum_{z=1}^{p-1} \sum_{y=0}^{p-1} \sum_{\substack{x=1 \\ x^3 \equiv y^2+27z^2}}^{p-1} x \left(\frac{y-\beta z}{p}\right)_3 \\ &= \sum_{z=1}^{p-1} \sum_{y=0}^{p-1} \sum_{x=1}^{p-1} x \left(\frac{y-\beta z}{p}\right)_3 e(x,y,z). \end{aligned} \tag{5}$$

We re-arrange the orders of summation and use symmetries of the function $e(x,y,z)$ to simplify the sum. First, we write the sum as

$$\sum_{x=1}^{p-1} x \sum_{y=0}^{p-1} \sum_{z=1}^{p-1} \left(\frac{y-\beta z}{p}\right)_3 e(x,y,z),$$

and for a fixed x and y we address the innermost sum

$$s(x,y) = \sum_{z=1}^{p-1} \left(\frac{y-\beta z}{p}\right)_3 e(x,y,z).$$

Note for a fixed x and y, there exists a z (with $1 \le z \le p-1$) such that $e(x,y,z) = 1$ if and only if $\frac{y^2-x^3}{-27}$ is a square mod p. In this case there are precisely two such z's, which we will denote by $\pm z_0$. We then have

$$\begin{aligned} s(x,y) &= \left(\frac{y-\beta z_0}{p}\right)_3 + \left(\frac{y+\beta z_0}{p}\right)_3 \\ &= \begin{cases} 1+1 = 2 & \text{if } \left(\frac{y-\beta z_0}{p}\right)_3 = 1, \\ \zeta + \zeta^{-1} = -1 & \text{otherwise.} \end{cases} \end{aligned}$$

Here we have used that $\left(\frac{y-\beta z_0}{p}\right)_3$ and $\left(\frac{y+\beta z_0}{p}\right)_3$ are multiplicative inverses by the calculation

$$\left(\frac{y-\beta z_0}{p}\right)_3 \left(\frac{y+\beta z_0}{p}\right)_3 = \left(\frac{y^2+27z_0^2}{p}\right)_3 = \left(\frac{x^3}{p}\right)_3 = 1.$$

Note that $z_0 = z_0(x,y)$ can be written (only slightly abusively) as $\sqrt{\frac{y^2-x^3}{-27}}$, and so we have $\beta z_0 = \pm\sqrt{y^2-x^3}$. To summarize, the innermost sum $s(x,y)$ evaluates as one of three possible cases depending on x and y:

$$s(x,y) = \begin{cases} 0 & \text{if } \left(\frac{y^2-x^3}{p}\right) \neq 1, \\ 2 & \text{if } \left(\frac{y^2-x^3}{p}\right) = 1 \text{ and } \left(\frac{y\pm\sqrt{y^2-x^3}}{p}\right)_3 = 1, \\ -1 & \text{if } \left(\frac{y^2-x^3}{p}\right) = 1 \text{ and } \left(\frac{y\pm\sqrt{y^2-x^3}}{p}\right)_3 \neq 1. \end{cases} \tag{6}$$

Recall from equation (5)

$$\mathcal{S}_\tau = \sum_{x=1}^{p-1} x \sum_{y=0}^{p-1} s(x,y). \tag{7}$$

Before we evaluate the new inner-most sum, we need a technical result.

Lemma 7. *Let $x \neq 0$ be a fixed element of $\mathbb{F}_p$. Then*

$$\left|\left\{ y \in \mathbb{F}_p : \left(\frac{y^2-x^3}{p}\right) = 1 \right\}\right| = \begin{cases} (p-1)/2 & \text{if } x \text{ is non-square in } \mathbb{F}_p, \\ (p-3)/2 & \text{if } x \text{ is a square in } \mathbb{F}_p. \end{cases}$$

Proof. It is easy to see the number of $u, v \in \mathbb{F}_p$ with $uv = x^3$ is $p-1$: for any non-zero u, let $v = x^3/u$. For each such solution, let $y = (u+v)/2$ and $c = (u-v)/2$, which is equivalent to $u = y + c$ and $v = y - c$. Thus, the number of solutions to $(y+c)(y-c) = y^2 - c^2 = x^3$ is also $p-1$. We may rewrite this equation as $y^2 - x^3 = c^2$.

Now suppose first x is not a square in $\mathbb{F}_p$. Then x^3 is not a square, and so there are no values of y such that $y^2 - x^3 = 0$. As c and $-c$ are distinct and both lead to c^2, then in this case there are $(p-1)/2$ values of y for which $y^2 - x^3$ is a (non-zero) square.

If instead x is square, then so also is x^3 and there will be two values of y for which $y^2 - x^3 = 0$. This leaves $p-3$ solutions to $y^2 - x^3 = c^2$, with $c \neq 0$. Again, as $\pm c$ both lead to the same value of c^2, we find there are thus $(p-3)/2$ values of y for which $y^2 - x^3$ is a non-zero square in $\mathbb{F}_p$. $\square$

With Lemma 7, we can now easily establish the following lemma.

Lemma 8. *For a fixed $x \neq 0$,*

$$\sum_{y=0}^{p-1} s(x,y) = -1 - \left(\frac{x}{p}\right).$$

Proof. Suppose first that x is not a square. We can ignore the values of y for which $\left(\frac{y^2-x^3}{p}\right) \neq 1$, as then $s(x,y) = 0$ and they do not contribute to the overall sum. So we assume $y^2 - x^3$ is a non-zero square in $\mathbb{F}_p$. We now claim that as we run over these values of y, the values $y \pm \sqrt{y^2 - x^3}$ are distinct. If this were not the case, then there would exist a y_1 and y_2 such that

$$y_1 \pm \sqrt{y_1^2 - x^3} = y_2 \pm \sqrt{y_2^2 - x^3}.$$

Squaring both sides of this equation and simplifying, we see

$$y_1(y_1 \pm \sqrt{y_1^2 - x^3}) = y_2(y_2 \pm \sqrt{y_2^2 - x^3}).$$

As $x = 0$, then $y_1 \pm \sqrt{y_1^2 - x^3} = 0$, and similarly for y_2. By assumption, $y_1 \pm \sqrt{y_1^2 - x^3} = y_2 \pm \sqrt{y_2^2 - x^3}$, and as this is non-zero we can divide through by it to see that $y_1 = y_2$.

From Lemma 7, there are $(p-1)/2$ values of y with $\left(\frac{y^2-x^3}{p}\right) = 1$. Substituting these values into $y \pm \sqrt{y^2 - x^3}$ will result in $p - 1$ distinct non-zero values in $\mathbb{F}_p$. It follows that there are $(p-1)/6$ values of y such that $\left(\frac{y\pm\sqrt{y^2-x^3}}{p}\right)_3 = 1$ (or ζ or ζ^2). So in this case, using (6) we see that

$$\begin{aligned}\sum_{y=0}^{p-1} s(x,y) &= 2\left(\frac{p-1}{6}\right) - \left(\frac{p-1}{3}\right)\\ &= 0\\ &= -1 - \left(\frac{x}{p}\right).\end{aligned}$$

We similarly examine the case when x is a square in $\mathbb{F}_p$. By Lemma 7 again, there are $(p-3)/2$ values of y with $\left(\frac{y^2-x^3}{p}\right) = 1$. These are the only values for which $s(x,y) = 0$. As we run over them, then $y \pm \sqrt{y^2 - x^3}$ will run over $p - 3$ distinct non-zero values in $\mathbb{F}_p$. The two values not obtained are when $y = \pm x\sqrt{x}$, as then $y^2 = x^3$ and so $\left(\frac{y^2-x^3}{p}\right) = 0$. But note that then $y \pm \sqrt{y^2 - x^3}$ just equals y, and $y = (\pm\sqrt{x})^3$. In short, the values of $\left(\frac{y\pm\sqrt{y^2-x^3}}{p}\right)_3$ will be equidistributed amongst 1, ζ, and ζ^2, except for the two values in $\mathbb{F}_p^*$, both of which have it equaling 1. So then,

$$\begin{aligned}\sum_{y=0}^{p-1} s(x,y) &= 2\left(\frac{p-1}{6} - 1\right) - \left(\frac{p-1}{3}\right)\\ &= -2\\ &= -1 - \left(\frac{x}{p}\right).\end{aligned}$$

This completes the proof. $\square$

Finally, we can complete the proof of the main result.

Theorem 9. *We have*

$$\frac{\mathcal{S}_\tau}{p} = h_p^* - \tfrac{p-1}{2}.$$

Proof. By equation (7) and Lemma 8, we see that

$$\begin{aligned}\mathcal{S}_\tau &= \sum_{x=1}^{p-1} x\left(-1 - \left(\frac{x}{p}\right)\right),\\ &= -\sum_{x=1}^{p-1} x\left(\frac{x}{p}\right) - \sum_{x=1}^{p-1} x,\\ &= ph_p^* - \tfrac{p(p-1)}{2}.\end{aligned}$$

We have used Dirichlet's result that

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

This completes the proof. □

4. Conclusion

It would be interesting if other families of elliptic curves (or surfaces) could be found which yield class number formulas similar to the results in this paper. We searched for other families of elliptic curves with 3-isogenies, but were unsuccessful besides families isomorphic to the curves $y^2 = x^3 + d$. It would also be interesting to find analogous formulas for curves with isogenies of degree greater than 3. As mentioned in the Introduction, some divisibility properties have been shown in [7], however not much is known about the corresponding quotients. Finally, we leave it as future work to analyze related character sums, where we weight by other integer valued funtions other than $x(P)$. Preliminary work using $y(P)$ has been shown to have relations with class numbers.

We acknowledge the contribution of SAGE [10], which facilitated the construction of examples which were helpful in discovering the main theorems of this work.

References

[1] O. Ahmadi and I. E. Shparlinski, Bilinear character sums and the sum-product problem on elliptic curves, *Proc. Edinburgh Math. Soc.* 53 (2010), 112.

[2] W. D. Banks, J. B. Friedlander, M. Garaev, I. E. Shparlinski, Double character sums over elliptic curves and finite fields, *Pure Appl. Math. Q. 2* (2006), 179-197.

[3] A. Joux and F. Morain, Sur les sommes de caractères liées aux courbes elliptiques à multiplication complexe. *J. Number Theory*, 55(1):108–128, 1995.

[4] D. Kohel and I. E. Shparlinski, Exponential sums and group generators for elliptic curves over finite fields, in: *Proceedings of the 4th Algorithmic Number Theory Symposium*, Lecture Notes in Comput. Sci. 1838, Springer-Verlag, Berlin, 2000, pp. 395-404.

[5] T. Lange and I. E. Shparlinski, Certain exponential sums and random walks on elliptic curves, *Canad. J. Math.* 57 (2005), 338-350.

[6] C. McLeman and C. Rasmussen, Class Numbers via 2-Isogenies. *Bulletin of the London Mathematical Society(?).*

[7] D. Moody and C. Rasmussen, Character sums determined by low degree isogenies of elliptic curves. *Journal of Number Theory.*

[8] R. Padma and S. Venkataraman, Elliptic curves with complex multiplication and a character sum. *J. Number Theory*, 61(2):274–282, 1996.

[9] I. E. Shparlinski, Bilinear character sums over elliptic curves, *Finite Fields Appl.* 14 (2008), 132-141.

[10] W. A. Stein et al. Sage Mathematics Software (Version 4.7). The Sage Development Team, 2011. Available at `http://www.sagemath.org`.

[11] K. Williams, Evaluation of character sums connected with elliptic curves. *Proc. Amer. Math. Soc.*, 73(3):291–299, 1979.

University of Michigan - Flint, Mathematics Department, Flint, MI 42439, USA.,
E-mail address: `mclemanc@umflint.edu`

National Institute of Standards and Technology (NIST), 100 Bureau Drive, Gaithersburg, MD, 20899, USA,
E-mail address: `dustin.moody@nist.gov`