QUOTIENTS OF ELLIPTIC CURVES OVER FINITE FIELDS

JEFFREY D. ACHTER AND SIMAN WONG

Abstract. Fix a prime ℓ, and let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \pmod{\ell}$ elements. If $\ell > 2$ and $q \gg_\ell 1$, we show that asymptotically $(\ell-1)^2/2\ell^2$ of the elliptic curves $E/\mathbb{F}_q$ with complete rational ℓ-torsion are such that $E/\langle P\rangle$ does not have complete rational ℓ-torsion for any point $P \in E(\mathbb{F}_q)$ of order ℓ. For $\ell = 2$ the asymptotic density is 0 or 1/4, depending whether $q \equiv 1 \pmod 4$ or $3 \pmod 4$. We also show that for any ℓ, if $E/\mathbb{F}_q$ has an $\mathbb{F}_q$-rational point R of order ℓ^2, then $E/\langle \ell R\rangle$ always has complete rational ℓ-torsion.

1. Introduction

By Tate's isogeny theorem [14, p. 139], two elliptic curves over a finite field k are k-isogenous if and only if they have the same number of k-rational points. However, the isogeny need not preserve the group structure of the k-rational points of the respective curves. For example, for $E : y^2 = x(x-1)(x+1)$ we have $E(\mathbb{F}_5) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. By explicit computations (cf. [15], [13, p. 70]), we find that $E/\langle(0,0)\rangle$ is $\mathbb{F}_5$-isomorphic to E as elliptic curves (*not* via the quotient map, of course), but that the group of $\mathbb{F}_5$-rational points of both $E/\langle(1,0)\rangle$ and $E/\langle(-1,0)\rangle$ are cyclic. In this paper we investigate the problem of how often the quotient map by a k-rational torsion point preserves the group structure. Note that the group homomorphism induced by an isogeny ϕ is an isomorphism on the prime-to-deg(ϕ) part of the group of rational points, so it suffices to focus on the k-rational deg(ϕ)-torsion.

Let ℓ be a prime, and let E/K be an elliptic curve over a field. Denote by $[\ell] : E \to E$ the multiplication-by-ℓ isogeny on E, and denote by $E[\ell](K)$ the K-rational points of the kernel of this isogeny. For the rest of this paper, we take K to be $\mathbb{F}_q$, a finite field of size q with $q \equiv 1 \pmod{\ell}$. This condition is necessary for the set

$$S(\mathbb{F}_q, \ell) := \text{the set of } \mathbb{F}_q\text{-isomorphism classes of elliptic curves } E \text{ with } E[\ell](\mathbb{F}_q) = E[\ell](\overline{\mathbb{F}}_q)$$

to be non-empty; this follows from properties of the Weil pairing ([13, p. 96]; see also Thm 2.1(c)). If $\ell = 2$ then q is odd, so $y^2 = x(x-1)(x+1)$ belongs to $S(\mathbb{F}_q, 2)$; in particular $S(\mathbb{F}_q, 2)$ is not empty. In general, $S(\mathbb{F}_q, \ell)$ is not empty for $q \geq \ell^4$ (see Lemma 2.2). We also define

$$\begin{aligned} S_0(\mathbb{F}_q, \ell) &= \{E \in S(\mathbb{F}_q, \ell) : E/\langle P\rangle \notin S(\mathbb{F}_q, \ell) \text{ for every non-zero point } P \in E[\ell]\,\}, \\ S_*(\mathbb{F}_q, \ell) &= \{E \in S(\mathbb{F}_q, \ell) : E/\langle P\rangle \in S(\mathbb{F}_q, \ell) \text{ for every non-zero point } P \in E[\ell]\,\}. \end{aligned}$$

and ratios

$$R_0(\mathbb{F}_q, \ell) = \frac{\#S_0(\mathbb{F}_q, \ell)}{\#S(\mathbb{F}_q, \ell)} \text{ and } R_*(\mathbb{F}_q, \ell) = \frac{\#S_*(\mathbb{F}_q, \ell)}{\#S(\mathbb{F}_q, \ell)}.$$

1991 *Mathematics Subject Classification.* Primary 11G20; Secondary 11G25, 14H10.

Key words and phrases. Elliptic curves, finite fields, isogeny, moduli, monodromy, quotients.

Jeffrey Achter's work is supported in part by a grant from the Simons foundation (204164).

Siman Wong's work is supported in part by NSF grant DMS-0901506.

Theorem 1.1. (a) *Let ℓ be an odd prime. For all $q \equiv 1 \pmod{\ell}$, we have*

$$\left| R_0(\mathbb{F}_q, \ell) - \frac{(\ell-1)^2}{2\ell^2} \right| < \frac{\ell^7}{q^{1/2}}, \qquad \left| R_*(\mathbb{F}_q, \ell) - \frac{1}{\ell^3} \right| < \frac{\ell^7}{q^{1/2}}.$$

(b) *Suppose $\ell = 2$. For $1 \leq j \leq 3$, define*

$$S_j(\mathbb{F}_q, 2) = \left\{ E \in S(\mathbb{F}_q, 2) : \begin{array}{l} E/\langle P \rangle \in S(\mathbb{F}_q, 2) \text{ for at least } j \\ \text{distinct points } P \in E \text{ of order } 2 \end{array} \right\}.$$

Then the ratio $R_j(\mathbb{F}_q, 2) = \#S_j(\mathbb{F}_q, 2)/\#S(\mathbb{F}_q, 2)$ is given by

$q \pmod 4$	$R_0(\mathbb{F}_q, 2)$	$R_1(\mathbb{F}_q, 2)$	$R_2(\mathbb{F}_q, 2)$	$R_3(\mathbb{F}_q, 2)$
1	0	1	$\frac{1}{4} + \frac{\epsilon_1(q)}{q}$	$\frac{1}{4} + \frac{\epsilon_1(q)}{q}$
3	$\frac{1}{4} - \frac{\epsilon_2(q)}{q}$	$\frac{3}{4} + \frac{\epsilon_2(q)}{q}$	$\frac{3}{4} + \frac{\epsilon_2(q)}{q}$	0

where each $|\epsilon_i(q)| \leq 23/12$ and depends on $q \pmod{24}$ only.

If a curve in $S(\mathbb{F}_q, \ell)$ belongs to $S_0(\mathbb{F}_q, \ell)$, then some quotient of this curve by an ℓ-torsion point must have an $\mathbb{F}_q$-rational point of order ℓ^2. Apply the dual isogeny and we are led to ask how often an elliptic curve $E/\mathbb{F}_q$ with an $\mathbb{F}_q$-rational point R of order ℓ^2 is such that $E/\langle [\ell]R \rangle$ is in $S(\mathbb{F}_q, \ell)$. The answer is surprisingly simple and uniform.

Theorem 1.2. *Let ℓ be a prime, and let $\mathbb{F}_q$ be a finite field of cardinality $q \equiv 1 \pmod{\ell}$. Let E be an elliptic curve over $\mathbb{F}_q$ with an $\mathbb{F}_q$-rational point R of order ℓ^2. Then $E/\langle [\ell]R \rangle$ has complete $\mathbb{F}_q$-rational ℓ-torsion.*

Theorem 1.2 implies that if $S(\mathbb{F}_q, \ell)$ is empty then no elliptic curve over $\mathbb{F}_q$ has an $\mathbb{F}_q$-point of order ℓ^2. This already follows essentially from Deuring's work on complex multiplication [2]; see Theorem 2.1 below. In fact, from these classical works we can derive closed form expressions (Theorem 5.3) for $S(\mathbb{F}_q, \ell)$ and $S_*(\mathbb{F}_q, \ell)$. While it is not clear (to us) how to use these expressions to prove Theorem 1.1, we can use them to test how sharp the estimates are in the Theorem. See Section 5 for more details.

In Section 2, we collect useful, classical facts about elliptic curves over finite fields. In Section 3, we prove Theorem 1.2; combined with an equidistribution argument, this allows us to prove the asymptotic result Theorem 1.1(a). Section 4 takes up the analysis of 2-torsion, and in particular proves Theorem 1.1(b). In Section 5, we follow the suggestion (indeed, detailed sketch) of the referee to derive and interpret formulae for $S(\mathbb{F}_q, \ell)$, $S_0(\mathbb{F}_q, \ell)$ and $S_*(\mathbb{F}_q, \ell)$ in terms of class numbers. Finally, many of our results, especially those of Section 3, generalize readily to abelian varieties of arbitrary dimension. This is explained in greater detail in Section 6.

2. Existence of curves with split torsion

In this section we prove Lemma 2.2 which is stated in the introduction. It is in fact an immediate consequence of the work of Schoof [9], which in turn is based on Deuring's work on complex multiplication [2]. We now summary the relevant parts of Schoof's work, concentrating on the case of ordinary curves in view of the discussion in Section 5. First, we introduce some notation.

Given a binary quadratic form $ax^2 + bxy + cy^2$, its discriminant is defined to be $b^2 - 4ac$, and we say that it is primitive if $\gcd(a, b, c) = 1$. Fix a negative integer $\Delta \equiv 0$ or $1 \pmod 4$. Denote by[1] $H(\Delta)$ (resp. $h(\Delta)$) the number of $SL_2(\mathbb{Z})$-equivalent classes of binary quadratic forms (resp. primitive binary quadratic forms) of discriminant Δ. We have the classical relation (cf. [9, Prop. 2.2])

$$H(\Delta) = \sum_d h(\Delta/d^2), \tag{2.1}$$

where d run through all positive integers such that $d^2|\Delta$ and that $\Delta/d^2 \equiv 0$ or $1 \pmod 4$. In particular, $h(\Delta)$ is the usual class number of $\mathcal{O}(\Delta)$, the unique complex quadratic order of discriminant Δ.

For any integer $t^2 \leq 4q$, denote by $I(\mathbb{F}_q, t)$ the set of $\mathbb{F}_q$-isomorphism classes of elliptic curves with $q+1-t$ $\mathbb{F}_q$-rational points. Either each elliptic curve in the isogeny class $I(\mathbb{F}_q, t)$ is supersingular, or each is ordinary; the isogeny class is ordinary if and only if $\gcd(t, q) = 1$.

For a prime number ℓ, let $S(\mathbb{F}_q, \ell, t) = S(\mathbb{F}_q, \ell) \cap I(\mathbb{F}_q, t)$, and define $S_*(\mathbb{F}_q, \ell, t)$ and $S_0(\mathbb{F}_q, \ell, t)$ analogously.

The following results are taken verbatim from [9].

Theorem 2.1 (Schoof). *Let q be a prime power and let t be an integer such that $t^2 \leq 4q$ and* $\gcd(t, q) = 1$.

(a) [9, Thm. 4.3(i)] *We have $E \in I(\mathbb{F}_q, t)$ if and only if $\mathcal{O}(t^2 - 4q) \subset \mathrm{End}_{\mathbb{F}_q}(E)$.*

(b) [9, Thm. 4.3(i) and Thm. 4.5(i)] *Let $\mathcal{O}$ be a complex quadratic order that contains $\mathcal{O}(t^2 - 4q)$. Then there are $h(\mathcal{O})$ isomorphism classes of elliptic curves $E \in I(\mathbb{F}_q, t)$ such that $\mathrm{End}_{\mathbb{F}_q}(E) \cong \mathcal{O}$.*

(c) [9, Prop. 3.7] *Let ℓ be a prime number such that* $\gcd(\ell, q) = 1$. *We have $E \in S(\mathbb{F}_q, \ell, t)$ if and only if $q + 1 - t \equiv 0 \bmod \ell^2$ and $\mathcal{O}(\frac{t^2-4q}{\ell^2}) \subset \mathrm{End}_{\mathbb{F}_q}(E)$.*

Lemma 2.2. *Let n be an odd integer with $q \equiv 1 \pmod n$. Then there exists an ordinary elliptic curve $E \in S(\mathbb{F}_q, n)$ if $q \geq n^4$.*

Proof. We can find an integer $t \in [0, n^2]$ such that $t \equiv q + 1 \pmod{n^2}$. Replace t by $t + n^2$ if necessary, we can further require that $\gcd(t, q) = 1$ and $t^2 \leq (t + n^2) \leq 4n^2 \leq 4q$. Apply Theorem 2.1 and we are done. □

Remark 2.3. For odd ℓ, the curves in $S(\mathbb{F}_q, \ell)$ are parameterized by the $\mathbb{F}_q$-points of the fine moduli $Y(\ell)$. The modular curve $X(\ell)$ has genus $1 + (\ell^2 - 1)(\ell - 6)/24$, so the Riemann hypothesis implies that $X(\ell)(\mathbb{F}_q)$ is not empty for $q \gg \ell^6$, which is weaker than Lemma 2.2.

3. The case of ℓ odd

3.1. **Pointwise results.** Throughout this section we consider an elliptic curve E over a field K in which the odd, rational prime ℓ is invertible. Consequently, for each n, each element of $E[\ell^n](\overline{K})$ is actually defined over a separable extension of K. In particular, $E[\ell^n](\overline{K})^{\mathrm{Gal}(K)} = E[\ell^n](K)$.

[1] This is closely related to but different from the *weighted* Kronekcer class number in [10, p. 165] (also denoted $H(\Delta)$ in [10]); see Remark 5.4 for more details.

Lemma 3.1. *Suppose that $E[\ell](K) \cong \mathbb{Z}/\ell \oplus \mathbb{Z}/\ell$, with generators P and Q. Then K contains a primitive ℓ^{th} root of unity.*

Suppose $R \in E(K)$ satisfies $[\ell]R = P$. Let $E' = E/\langle P\rangle$, and let R' and Q' be the images of R and Q in $E'(K)$. Then $E'[\ell](K)$ is generated by R' and Q'.

Proof. The existence of $\zeta_\ell \in K$ comes from the $\mathrm{Gal}(K)$-equivariance of the Weil pairing, cf. [13, p. 96]. For the second claim, since

$$E'[\ell](\overline{K}) = \{S \in E(\overline{K}) : [\ell]S \in \langle P\rangle\}/\langle P\rangle,$$

it is clear that $R', Q' \in E'[\ell](K)$; it remains to show that they are linearly independent.

Suppose otherwise; then there is some $a \in \mathbb{F}_\ell$ with $R' = [a]Q'$, i.e., $R - [a]Q \in \langle P\rangle$. However, $[\ell](R - aQ) = P \neq 0_E$, while $[\ell]\langle P\rangle = \{0_E\}$. □

Lemma 3.2. *Let E/K be an elliptic curve, and suppose that K contains a primitive ℓ^{th} root of unity. Suppose that $P \in E[\ell](K)$ is a point of order ℓ and $R \in E(\overline{K})$ satisfies $[\ell]R = P$. Let $E' = E/\langle P\rangle$.*

(a) *Then $E'[\ell](K) \cong \mathbb{Z}/\ell \oplus \mathbb{Z}/\ell$ if and only if the coset*

$$R + \langle P\rangle = \{R, R+P, \cdots, R + [\ell-1]P\}$$

is stable under $\mathrm{Gal}(K)$.

(b) *Suppose further $E[\ell](K) \cong \mathbb{Z}/\ell \oplus \mathbb{Z}/\ell$. Then $R + \langle P\rangle \in E'$ is* $\mathrm{Gal}(K)$*-stable if and only if $T + \langle P\rangle \in E'$ is* $\mathrm{Gal}(K)$*-stable for each $T \in E(\overline{K})$ with $[\ell]T = P$.*

Proof. Choose $Q \in E[\ell](\overline{K})$ so that $\{P, Q\}$ is a basis for $E[\ell](\overline{K})$. By Lemma 3.1, the images R' and Q' of R and Q in $E'[\ell](\overline{K})$ are a basis for $E'[\ell](\overline{K})$; it remains to verify that R' and Q' are actually defined over K.

The hypothesis on K, combined with the $\mathrm{Gal}(K)$-equivariance of the Weil pairing, means that for each $\sigma \in \mathrm{Gal}(K)$ one has $\sigma(Q) = Q + [a_\sigma]P$ for some $a_\sigma \in \mathbb{Z}/\ell$. Consequently, $\sigma(Q) \equiv Q \bmod \langle P\rangle$, and $Q' \in E(K)$. Therefore, $E'[\ell](K) \cong \mathbb{Z}/\ell \oplus \mathbb{Z}/\ell$ if and only if the coset $R + \langle P\rangle/\langle P\rangle$ is $\mathrm{Gal}(K)$-stable.

For (b), use the fact that $[\ell]^{-1}(P)$ is a torsor under $E[\ell](K)$. More explicitly, if R and T satisfy $[\ell]R = [\ell]T = P$, then $T = R + Q$ for some $Q \in E[\ell](K)$. □

Proof of Theorem 1.2. If $R \in E(\mathbb{F}_q)$ has order ℓ^2, then with $P := [\ell]R$ the hypothesis of Lemma 3.1(a) is satisfied, and Theorem 1.2 follows. □

We end this section with the following application of Lemma 3.1; it will be useful for the proof of Theorem 1.1(a).

Lemma 3.3. *Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field such that $q \equiv 1 \bmod \ell$. Suppose that $E[\ell](\mathbb{F}_q) \cong \mathbb{Z}/\ell \oplus \mathbb{Z}/\ell$.*

(a) *After a choice of basis for $E[\ell^2](\overline{\mathbb{F}}_q)$, the action of $\mathrm{Fr}_{E/\mathbb{F}_q}$ on the ℓ^2-torsion is given by a matrix $\alpha = 1 + \ell\beta \in \mathrm{GL}_2(\mathbb{Z}/\ell^2)$, where $\beta \in \mathrm{Mat}_2(\mathbb{Z}/\ell)$.*

(b) *The following are equivalent:*
   (i) *For each $P \in E[\ell](\mathbb{F}_q)$ of order ℓ, $(E/\langle P\rangle)[\ell](\mathbb{F}_q) \cong \mathbb{Z}/\ell$;*
   (ii) *The matrix β has no $\mathbb{F}_\ell$-rational eigenspace.*

(c) *The following are equivalent:*
   (i) *For each $P \in E[\ell](\mathbb{F}_q)$ of order ℓ, $(E/\langle P\rangle)[\ell](\mathbb{F}_q) \cong \mathbb{Z}/\ell \oplus \mathbb{Z}/\ell$;*
   (ii) *The matrix β is scalar.*

Proof. If $R \in E[\ell^2](\overline{\mathbb{F}}_q)$, then $[\ell]R \in E[\ell](\overline{\mathbb{F}}_q) = E[\ell](\mathbb{F}_q)$. Therefore, for each R, $\mathrm{Fr}_{E/\mathbb{F}_q,\ell^2}([\ell]R) = [\ell]R$, and in particular $\mathrm{Fr}_{E/\mathbb{F}_q,\ell^2}(R) \equiv R \bmod \ell$. This proves (a).

Given Lemma 3.2(a), condition (b)(i) is equivalent to the statement that, for each $R \in E(\overline{\mathbb{F}}_q)$ of order ℓ^2, the subgroup $\langle R\rangle \subset E[\ell^2](\overline{\mathbb{F}}_q)$ is not $\mathrm{Gal}(\mathbb{F}_q)$-stable. Equivalently, $\mathrm{Fr}_{E/\mathbb{F}_q,\ell^2}$ stabilizes no rank one summand of $E[\ell^2](\overline{\mathbb{F}}_q)$. Thanks to the calculation in (a), this is readily seen to be equivalent to the condition that β has no nonzero eigenvector.

The argument for (c) is similar. Thanks to Lemma 3.2(b), condition (c)(i) holds if and only if *every* rank one summand of $E[\ell^2](\overline{\mathbb{F}}_q)$ is $\mathrm{Gal}(\mathbb{F}_q)$-stable. □

3.2. **Results in families.** We start by recalling the definition of relevant modular curves. Fix an integer $N \geq 3$, and briefly work in the category of schemes over $\mathbb{Z}[\zeta_N, 1/N]$; in particular, each scheme is equipped with a canonical choice of a primitive N^{th} root of unity. There is a relative curve $Y(N) \to \operatorname{Spec}\mathbb{Z}[\zeta_N, 1/N]$ whose S-points are isomorphism classes of pairs (E, ϕ), where E/S is an elliptic curve and $\phi : (\mathbb{Z}/N)_S^{\oplus 2} \xrightarrow{\sim} E[N]$ is a trivialization of the N-torsion of E such that, if $\langle\cdot,\cdot\rangle$ denotes the Weil pairing, then

$$\langle \phi((1,0)), \phi((0,1))\rangle = \zeta_N.$$

It is a classical fact (e.g., [4, Cor. 10.9.2]) that each fiber of $Y(N) \to \operatorname{Spec}\mathbb{Z}[1/N, \zeta_N]$ is a smooth, geometrically irreducible affine curve. Let $X(N)$ be its compactification; since we have inverted N, $X(N)$ has smooth, projective fibers.

Let

$$d_N = \frac{N^3}{2}\prod_{p|N}\left(1 - \frac{1}{p^2}\right)$$

be the degree of the modular map $X(N) \to X(1) \cong \mathbb{P}^1$. By [11, p. 23], the genus of $X(N)$ is $1 + \frac{d_N(N-6)}{12N}$, while the Euler characteristic of $Y(N)$ is

$$\begin{aligned}\chi(Y(N)) &= 2 - 2g(X(N)) - \#(X(N) - Y(N))\\ &= \frac{-d_N}{6}.\end{aligned}$$

Let $(\mathcal{E}, \Phi)$ be the universal elliptic curve over $Y(N)$ with trivialized N-torsion. For any natural number M and field K equipped with a morphism $\mathbb{Z}[1/MN, \zeta_N] \to K$, and geometric point s of $Y(N)_K$, there is a monodromy representation

$$\pi_1(Y(N)_K, s) \longrightarrow Aut(\mathcal{E}_s[M]) \cong \mathrm{GL}_2(\mathbb{Z}/M).$$

We will need to compute the image of this representation in the case where $(N, M) = (\ell, \ell^2)$. To express the answer, the following notation is convenient. Let

$$\begin{aligned} G_\ell &= \{\alpha \in \mathrm{GL}_2(\mathbb{Z}/\ell^2) : \alpha \equiv \mathrm{id} \bmod \ell\}\\ &\cong \mathrm{Mat}_2(\mathbb{Z}/\ell); \end{aligned} \tag{3.1}$$

for each natural number r, let

$$\begin{aligned} G_\ell^{(r)} &= \{\alpha \in G_\ell : \det(\alpha) \equiv r \bmod \ell^2\}\\ &\cong \{\beta \in \mathrm{Mat}_2(\mathbb{Z}/\ell) : \mathrm{tr}(\beta) \equiv r \bmod \ell\} \qquad \text{with respect to (3.1).} \end{aligned} \tag{3.2}$$

If $W \subseteq G_\ell$ is any subset, let

$$W^{(r)} = W \cap G_\ell^{(r)}. \tag{3.3}$$

Lemma 3.4. *Let ℓ be an odd prime, let K be an algebraically closed field equipped with a primitive ℓ^{th} root of unity, and let s be a geometric point of $Y(\ell)_K$. The image of the monodromy representation $\pi_1(Y(\ell)_K, s) \to Aut(\mathcal{E}_s[\ell^2])$ is*

$$G_\ell^{(0)} = \{\alpha \in \mathrm{SL}_2(\mathbb{Z}/\ell^2) : \alpha \equiv \mathrm{id} \bmod \ell\}.$$

Proof. Fix a compatible choice of primitive root of unity of order ℓ^2. Since, for an elliptic curve E, a trivialization of $E[\ell^2]$ determines a trivialization of $E[\ell]$, there is a morphism of fine moduli schemes $Y(\ell^2) \to Y(\ell)$. The fiber over a point of $Y(\ell)$ is a torsor under the automorphisms of $(\mathbb{Z}/\ell^2)^{\oplus 2}$ that are congruent to the identity and preserve the determinant. Consequently, $Y(\ell^2) \to Y(\ell)$ is étale and Galois, with covering group $G_\ell^{(0)}$.

Since $Y(\ell^2)_K$ is irreducible, it corresponds to a surjection $\pi_1(Y(\ell)_K, s) \to G_\ell^{(0)}$. In particular, every automorphism of $\mathcal{E}_s[\ell^2]$ of determinant one and congruent to one modulo ℓ is realized by some element of the fundamental group of $Y(\ell)_K$; this is exactly the desired statement. □

If $E/\mathbb{F}_q$ has full rational ℓ-torsion, then (after a choice of basis for $E[\ell](\mathbb{F}_q)$) its Frobenius determines an element $\mathrm{Fr}_{E/\mathbb{F}_q, \ell^2} \in G_\ell$; the conjugacy class of $\mathrm{Fr}_{E/\mathbb{F}_q, \ell^2}$ is independent of this choice.

Lemma 3.5. *Let $W \subset \mathrm{GL}_2(\mathbb{Z}/\ell^2)$ be a subset that is stable under conjugation. Then for each $q > (\ell^3 - \ell + 12)^2/9$ with $q \equiv 1 \bmod \ell$,*

$$\left| \frac{\#\{s \in Y(\ell)(\mathbb{F}_q) : \mathrm{Fr}_{\mathcal{E}_s/\mathbb{F}_q, \ell^2} \in W^{(q)}\}}{\#Y(\ell)(\mathbb{F}_q)} - \frac{\#W^{(q)}}{G_\ell^{(q)}} \right| < \frac{\ell^4(\ell^2-1)|\ell - 6|}{6\sqrt{q}}. \tag{3.4}$$

Note that if $q \not\equiv 1 \bmod \ell$, then $G_\ell^{(q)}$ and $Y(\ell)(\mathbb{F}_q)$ are both empty.

Proof. Fix a geometric point $\eta \in Y(\ell)$ whose characteristic is that of $\mathbb{F}_q$; by Lemma 3.4, the image of the (geometric) monodromy representation

$$\pi_1(Y(\ell), \eta) \longrightarrow Aut(\mathcal{E}_\eta[\ell^2])$$

is all of $G_\ell^{(0)}$. Since ℓ is relatively prime to the characteristic of the base field, the cover $X(\ell^2)_\eta \to X(\ell)_\eta$ is tamely ramified. Katz's equidistribution theorem [5, Thm. 9.7.13] then asserts that, if $q > 4(h_c^0(Y(\ell)_\eta, \mathbb{Q}_{\ell'}) + h_c^1(Y(\ell)_\eta, \mathbb{Q}_{\ell'}))^2$, then the quantity on the left-hand side of (3.4) is bounded by $2|\chi(Y(\ell)_\eta)|\#G_\ell/\sqrt{q}$. □

Now let

$$W_0 = \{\alpha = 1 + \ell\beta \in G_\ell : \beta \text{ has no } \mathbb{F}_\ell\text{-rational eigenvalue}\}$$
$$W_* = \{\alpha = 1 + \ell\beta \in G_\ell : \beta \text{ is scalar}\};$$

each is stable under conjugation. For $t \in \mathbb{F}_\ell$, let

$$N_t = \{\beta \in \mathrm{Mat}_2(\mathbb{F}_\ell) : \mathrm{tr}(\beta) = t \text{ and } \beta \text{ has no } \mathbb{F}_\ell\text{-rational eigenvalue}\}$$

Lemma 3.6. *Suppose ℓ is odd. Then $\#N_t = \ell(\ell-1)^2/2$.*

Proof. As is usual, identify $\mathbb{F}_{\ell^2}^\times$ with a maximal nonsplit torus T in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Then each element of N_t is conjugate to one of the $\ell-1$ elements of $\mathbb{F}_{\ell^2}^\times$ of trace t, and the orbit of $\alpha \in \mathbb{F}_{\ell^2}^\times$ under the normalizer of T in $\mathrm{GL}_2(\mathbb{F}_\ell)$ consists of α and its conjugate. The centralizer of each α is T, and thus $\#N_t = \frac{\#T}{2} \cdot \frac{\#\mathrm{GL}_2(\mathbb{F}_\ell)}{\#T}$, as claimed. □

Lemma 3.7. *If $q \equiv 1 \bmod \ell$, then $\#W_0^{(q)} = \frac{\ell(\ell-1)^2}{2}$ and $\#W_*^{(q)} = 1$.*

Proof. As explained above, $W_0^{(q)}$ coincides with the set N_q, whose cardinality is given by Lemma 3.6. For $W_*^{(q)}$, since ℓ is odd it is clear that there is a unique scalar matrix with given trace. □

Proof of Theorem 1.1(a). Consider the set $S(\mathbb{F}_q,\ell)$ of $\mathbb{F}_q$-isomorphism classes of elliptic curves with full rational ℓ-torsion. Since $\ell \geq 3$, each elliptic curve E in $S(\mathbb{F}_q,\ell)$ is represented by exactly $\#\mathrm{SL}_2(\mathbb{Z}/\ell)$ points $(E,\{P,Q\}) \in Y(\ell)(\mathbb{F}_q)$. Moreover, $\mathrm{Fr}_{E/\mathbb{F}_q,\ell^2} \in W_0$ if and only if $E \in S_0(\mathbb{F}_q,\ell)$ (Lemma 3.3(b)). Therefore, $\#S_0(\mathbb{F}_q,\ell)/\#S(\mathbb{F}_q,\ell)$ is exactly the proportion of points $s \in Y(\ell)(\mathbb{F}_q)$ for which $\mathrm{Fr}_{\mathcal{E}_s/\mathbb{F}_q,\ell^2} \in W_0^{(q)}$. This proportion is calculated in Lemmas 3.5 and 3.7; the result for $\#S_*(\mathbb{F}_q,\ell)/\#S(\mathbb{F}_q,\ell)$ is deduced in an entirely analogous fashion. □

4. The case of $\ell = 2$

Let $\mathbb{F}_q$ be a finite field of odd cardinality. Then every elliptic curve in $S(\mathbb{F}_q,2)$ is given either by a Legendre curve $y^2 = y(x-1)(x-\lambda)$ with $\lambda \in \mathbb{F}_q - \{0,1\}$ or a quadratic twist of such. In particular, every curve in $S(2,\mathbb{F}_q)$ has a model of the form

$$E_{\lambda,D} : \ y^2 = x(x-D)(x-D\lambda) \quad \text{with } D \in \mathbb{F}_q - \{0\}, \lambda \in \mathbb{F}_q - \{0,1\}. \tag{4.1}$$

Set

$$P_1 = (0,0), \ \ P_2 = (D,0), \ \ P_3 = (D\lambda,0).$$

Using the explicit formula in [15] (cf. also [13, p. 70]) we obtain the following equations for the quotient curves $E_{\lambda,D,i} := E_\lambda/\langle P_i\rangle$:

$$\begin{aligned}
E_{\lambda,D,1} : &\ \ Y^2 = (X - D(\lambda+1))(X^2 - 4D^2\lambda),\\
E_{\lambda,D,2} : &\ \ Y^2 = (X - D(\lambda-1))(X^2 - 2DX + 4D^2\lambda - 3D^2),\\
E_{\lambda,D,3} : &\ \ Y^2 = (X - D(1-\lambda))(X^2 - 2D\lambda X - (3D^2\lambda^2 - 4D^2\lambda)).
\end{aligned}$$

Note that $S_0(\mathbb{F}_q,2)$ is the complement of $S_1(\mathbb{F}_q,2)$ in $S(\mathbb{F}_q,2)$. So to prove Theorem 1.1(b) it suffices to consider the sets $S_j(\mathbb{F}_q,2)$ for $1 \leq j \leq 3$.

Lemma 4.1. *Fix $D \in \mathbb{F}_q^\times$. With the notation as above,*

(a) *$E_{\lambda,D,1}$ (resp. $E_{\lambda,D,3}$, $E_{\lambda,D,3}$) belongs to $S(\mathbb{F}_q,2)$ precisely when $\lambda = t_1^2$ (resp. $\lambda = 1-t_2^2$, $\lambda = 1/(1-t_3^2)$) with $t_i \in \mathbb{F}_q - \{0,\pm1\}$. In particular, $E_{\lambda,D,i} \in S(\mathbb{F}_q,2)$ for exactly $(q-3)/2$ of the $\lambda \in \mathbb{F}_q - \{0,1\}$.*

(b) *Denote by $(\frac{-1}{\cdot})$ the usual quadratic character. Then for any two distinct indices $i,j \in \{1,2,3\}$, the pair of quotient curves $E_{\lambda,D,i}, E_{\lambda,D,j}$ are both in $S(\mathbb{F}_q,2)$ for $(q-4-(\frac{-1}{q}))/4$ of the $\lambda \in \mathbb{F}_q - \{0,1\}$.*

(c) *A necessary condition for all three $E_{\lambda,D,i}$ to be in $S(\mathbb{F}_q,2)$ is that -1 is a square in $\mathbb{F}_q$. Under that condition, if any two of the $E_{\lambda,D,i}$ are in $S(\mathbb{F}_q,2)$ then so is the third one.*

(d) *The number of $\lambda \in \mathbb{F}_q - \{0, 1\}$ for which at least one $E_{\lambda,D,i}$ is in $S(\mathbb{F}_q, 2)$ is $q - 2$ if $q \equiv 1 \pmod 4$, and $3(q - 3)/4$ if $q \equiv 3 \pmod 4$.*

(e) *$E_{-1,D}$ belongs to $S_1(\mathbb{F}_q, 2)$ if and only either $(\frac{-1}{q}) = 1$, or $(\frac{2}{q}) = 1$, or if q is an even power of 3, and $E_{-1,D}$ belongs to $S_3(\mathbb{F}_q, 2)$ if and only if either $q \equiv 1 \pmod 8$ or q is an even power of 3.*

(f) *Suppose $\mathbb{F}_q$ contains a root of $\lambda^2 - \lambda + 1 = 0$. Then $E_{\lambda,D} \in S_1(\mathbb{F}_q, 2)$ if and only if either $q \equiv 1 \pmod{12}$ or q is an even power of 3, in which case $E_{\lambda,D} \in S_3(\mathbb{F}_q, 2)$ as well.*

Proof. From the Weierstrass equations for the $E_{\lambda,D,i}$ above we can readily determine the 2-division fields of these quotient curves; these fields turn out to be independent of D:

$$\mathbb{F}_q(E_{\lambda,D,1}[2]) = \mathbb{F}_q(\sqrt{\lambda}),\ \mathbb{F}_q(E_{\lambda,D,2}[2]) = \mathbb{F}_q(\sqrt{1-\lambda}),\ \mathbb{F}_q(E_{\lambda,D,3}[2]) = \mathbb{F}_q(\sqrt{\lambda(\lambda-1)}). \tag{4.2}$$

Part (a) is now immediate.

Next, suppose that both $E_{\lambda,D,1}$ and $E_{\lambda,D,2}$ are in $S(\mathbb{F}_q, 2)$. That means $\lambda = t^2 = 1 - u^2$ for some $t, u \in \mathbb{F}_q - \{0, \pm 1\}$. Since q is odd, the usual parameterization of Pythagorean triples gives $t = t(s) := 2s/(1 + s^2)$ for some $s \in \mathbb{F}_q$. The condition $t, u \notin \{0, \pm 1\}$ becomes $s \notin \{0, \pm 1\}$, and of course s cannot be a primitive 4-th root of unity ζ_4; the latter are in $\mathbb{F}_q$ precisely when $(\frac{-1}{q}) = 1$. Note that

$$\begin{array}{rcl} t(s_1) = \ \ t(s_2) & \Longleftrightarrow & s_1 = \ \ s_2 \quad \text{or} \quad s_1 s_2 = \ \ 1; \\ t(s_1) = -t(s_2) & \Longleftrightarrow & s_1 = -s_2 \quad \text{or} \quad s_1 s_2 = -1. \end{array}$$

Thus $s \mapsto \lambda = t(s)^2$ defines a set map $\mathbb{F}_q^\times - \{s : s^4 = 1\} \to \mathbb{F}_q - \{0, \pm 1\}$ whose fiber above $t(s)$ is $\{\pm s, \pm 1/s\}$. This fiber has size exactly 4 unless $s^2 = \pm 1$. Since we already excluded ± 1 and $\pm \zeta_4$ (if they exist) from the domain of this map, the image of this map has size $(q - 4 - (\frac{-1}{q}))/4$, in other words $E_{\lambda,D,1}$ and $E_{\lambda,D,2}$ are in $S(\mathbb{F}_q, 2)$ for exactly $(q - 4 - (\frac{-1}{q}))/4$ distinct λ. Repeat the same calculation for the other two pairs of $E_{\lambda,D,i}$ and we get the same answer, and Part (b) follows.

Finally, suppose all three $E_{\lambda,D,i}$ are in $S(\mathbb{F}_q, 2)$. By (4.2), each of $\lambda, 1 - \lambda, \lambda(\lambda - 1)$ is a square in $\mathbb{F}_q$. Thus -1 is a square in $\mathbb{F}_q$, and so $\zeta_4 \in \mathbb{F}_q$. Since both $E_{\lambda,D,1}, E_{\lambda,D,2}$ are in $S(\mathbb{F}_q)$, as we saw in the argument for Part (b), we get $\lambda = t^2$ with

$$t = 2s/(1 + s^2) \quad \text{for some } s \in \mathbb{F}_q - \{0, \pm 1, \pm \zeta_4\}.$$

Apply the same argument to the pair $E_{\lambda,D,2}, E_{\lambda,D,3}$ now gives (for the same t)

$$\frac{1}{t} = \frac{2r}{1 + r^2} \quad \text{for some } r \in \mathbb{F}_q - \{0, \pm 1, \pm \alpha_4\}.$$

Combine the two relations and we get

$$0 = (1 + r^2)(1 + s^2) - 4rs = (rs + r\zeta_4 - s\zeta_4 - 1)(rs - r\zeta_4 + s\zeta_4 - 1),$$

whence

$$r = \frac{1 + s\zeta_4}{s + \zeta_4} \quad \text{or} \quad r = \frac{1 - s\zeta_4}{s - \zeta_4}.$$

This also shows that if $s \notin \{0, \pm 1, \pm \zeta_4\}$ then $r \notin \{0, \pm 1, \pm \zeta_4\}$. Thus if both $E_{\lambda,D,1}, E_{\lambda,D,2}$ are in $S(\mathbb{F}_q, 2)$ then so does $E_{\lambda,D,3}$. A similar calculation shows that if any two of the $E_{\lambda,D,i}$ are in $S(\mathbb{F}_q, 2)$ then so does the third one. Apply Part (b) and Part (c) follows. Part (d) follows by applying the inclusion-exclusion principle, and Part (e) and (f) follows from Part (a). □

Note that $E_{\lambda,D}$ (resp. $E_{\lambda,D,i}$) is the quadratic twist of $E_{\lambda,1}$ (resp. $E_{\lambda,1,i}$) by D. The following result is an immediate consequence of the 2-division fields calculation (4.2) which in turns follows from the explicit form of the quotient curves $E_{\lambda,D,i}$.

Lemma 4.2. *For any $\lambda \in \mathbb{F}_q - \{0,1\}$ and any $D \in \mathbb{F}_q - \{0\}$, the curve $E_{\lambda,D,i}$ is in $S(\mathbb{F}_q, 2)$ if and only if $E_{\lambda,1,i}$ is.* □

Proof of Theorem 1.1(b). Note that $S_0(\mathbb{F}_q, 2)$ is the complement of $S_1(\mathbb{F}_q, 2)$ in $S(\mathbb{F}_q, 2)$, so for the rest of the proof we will concentrate on the sets $S_j(\mathbb{F}_q, 2)$ for $1 \le j \le 3$.

Since $2 \nmid q$, we saw at the beginning of this section that every elliptic curve in $S(\mathbb{F}_q, 2)$ has a model of the form $E_{\lambda,D}$ for some $\lambda \in \mathbb{F}_q - \{0,1\}$ and $D \in \mathbb{F}_q - \{0\}$. Recall that $E_{\lambda,D}$ is the quadratic twist of $E_{\lambda,1}$ by D, so by [13, p. 50],

$$E_{\lambda,D}, E_{\lambda',D} \text{ have the same } j\text{-invariant} \Leftrightarrow \lambda' \in \left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{1-\lambda}, \frac{\lambda-1}{\lambda}\right\}. \tag{4.3}$$

Set $\zeta_6 = -1$ if $3|q$, otherwise let $\zeta_6 \in \overline{\mathbb{F}}_q$ be a primitive 6-th root of unity. Then the six values on the right side are pairwise distinct except when

$$\lambda \in \{-1, 2, 1/2\}: \qquad \text{then } j(E_\lambda) = 1728; \tag{4.4}$$

$$\lambda \in \{\zeta_6^{\pm 1}\}: \qquad \text{then } j(E_\lambda) = 0 \tag{4.5}$$

We check that the elements

$$-1, 2, 1/2, \zeta_6^{\pm 1}$$

are pairwise distinct if $3 \nmid q$, and that they become the single element -1 when $3|q$.

Denote by $T_0(\mathbb{F}_q)$ and $T_{1728}(\mathbb{F}_q)$ the subset of curves in $S(\mathbb{F}_q, 2)$ with j-invariant 0 and 1728, respectively, and by $T'(\mathbb{F}_q)$ the set of remaining curves. To prove Theorem 1.1(b) we consider three cases based on whether or not $\zeta_6 \in \mathbb{F}_q$ (and if $3 \nmid q$). We will make frequent use without comment of the following immediate consequence of (4.3) plus Lemma 4.2: if $\lambda \in \mathbb{F}_q$ gives rise to a curve in $S(\mathbb{F}_q, 2)$ (resp. $S_1(\mathbb{F}_q, 2)$, resp. $S_3(\mathbb{F}_q, 2)$) with j-invariant $j_0 \neq 0, 1728$, then there are six values of λ corresponding to two isomorphism classes of curves with the j-invariant j_0.

Case: $\zeta_6 \notin \mathbb{F}_q$

Then $T_0(\mathbb{F}_q)$ is empty. By the comment above,

$$\#T'(\mathbb{F}_q) = \frac{\#(\mathbb{F}_q - \{0, 1, -1, 2, 1/2\})}{3} = \frac{q-5}{3}.$$

Since $\mathrm{char}(\mathbb{F}_q) \neq 2$ or 3, any curve with j-invariant 1728 is of the form $y^2 = x^3 - \delta x$ with $\delta \in \mathbb{F}_q$. Such a curve is in $S(\mathbb{F}_q, 2)$ precisely when $\delta = D^2$ for some $D \in \mathbb{F}_q$, in which case the curve is simply $E_{-1,D}$. Apply Lemma 4.2 again and we see that $\#T_{1728}(\mathbb{F}_q) = 2$. Combine everything and we see that if $q \equiv 2 \pmod 3$ then

$$\#S(\mathbb{F}_q, 2) = (q-5)/3 + 2 = (q+1)/3. \tag{4.6}$$

We now examine how many of these curves have quotients by 2-isogenies that are also in $S(\mathbb{F}_q, 2)$.

Subcase: $\zeta_4 \notin \mathbb{F}_q$ This time $E_{-1,D} \notin S_1(\mathbb{F}_q, 2)$, so $S_1(\mathbb{F}_q, 2)$ is made up entirely of curves with non-zero j-invariants. By Lemma 4.1(d),

$$\# S_1(\mathbb{F}_q, 2) = \frac{q-3}{4}.$$

Lemma 4.1(c) says that $S_3(\mathbb{F}_q, 2)$ is empty, and by Lemma 4.1(b) plus inclusion-exclusion,

$$\# S_2(\mathbb{F}_q, 2) = \frac{q-3}{4}.$$

This completes the proof of Theorem 1.1(b). □

5. Class numbers

Deuring's work on elliptic curves over finite fields, such as that summarized in Theorem 2.1, allows an alternative approach to calculating $S_0(\mathbb{F}_q, \ell)$ and $S_\star(\mathbb{F}_q, \ell)$. In this section we supplement this classical knowledge with the more modern perspective of isogeny volcanoes in order to derive explicit formulae ((5.2) and (5.3)) for these quantities. As we noted above in the introduction, this section freely incorporates suggestions and ideas from a referee.

For the moment, fix a prime power q and an integer t such that $t^2 \leq 4q$ and $\gcd(t, q) = 1$. As in Section 2, let $I(\mathbb{F}_q, t)$ denote the isogeny class of elliptic curves over $\mathbb{F}_q$ for which the characteristic polynomial of Frobenius is the polynomial

$$X^2 - tX + q;$$

the assumption $\gcd(t, q) = 1$ is equivalent to the condition that each $E \in I(\mathbb{F}_q, t)$ is ordinary.

Let $\mathcal{O}_{t,q}$ be the order $\mathbb{Z}[X]/(X^2 - tX + q)$, and let $K_{t,q}$ be its splitting field. Let $f_{t,q}$ be the conductor of $\mathcal{O}_{t,q}$, i.e., the index $[\mathcal{O}_{K_{t,q}} : \mathcal{O}_{t,q}]$. Then the discriminant of $\mathcal{O}_{t,q}$ is given by $\Delta_{t,q} = f_{t,q}^2 \Delta_{K_{t,q}}$.

Recall (Theorem 2.1(a)) that an order $\mathcal{O}$ of $K_{t,q}$ arises as the endomorphism ring of an elliptic curve $E \in I(\mathbb{F}_q, t)$ if and only its conductor f satisfies $f | f_{t,q}$. For $E \in I(\mathbb{F}_q, t)$, let f_E be the conductor of the order $\operatorname{End}(E)$.

Now fix a prime ℓ relatively prime to q. An input to the structure theory of isogeny volcanoes is the following collection of observations.

Lemma 5.1 (Kohel). *Let $E \in I(\mathbb{F}_q, t)$ be an elliptic curve.*

(a) *There exists an ℓ-isogeny $E \to E'$ such that $f_E = f_{E'}$ if and only if* $\operatorname{ord}_\ell(f_E) = 0$ *and ℓ is ramified or split in K.*

(b) *There exists an ℓ-isogeny $E \to E'$ such that* $\operatorname{ord}_\ell(f_{E'}) = \operatorname{ord}_\ell(f_E) - 1$ *if and only if* $\operatorname{ord}_\ell(f_E) > 0$.

(c) *There exists an ℓ-isogeny $E \to E'$ such that* $\operatorname{ord}_\ell(f_{E'}) = \operatorname{ord}_\ell(f_E) + 1$ *if and only if* $\operatorname{ord}_\ell(f_E) < \operatorname{ord}_\ell(f_{t,q})$.

Proof. This is a coarse form of [6, Prop. 23]; see also [3, Thm. 21] and [12, Thm. 7]. □

In fact, if $E \to E'$ is an ℓ-isogeny, then $f_E/f_{E'} = \ell^m$ for some $m \in \{-1, 0, 1\}$. Consequently, Lemma 5.1 completely describes the endomorphism rings of elliptic curves ℓ-isogenous to a given elliptic curve.

Lemma 5.2. *Suppose $q \equiv 1 \bmod \ell$, $t \equiv 1 + q \bmod \ell^2$ and $E \in I(\mathbb{F}_q, t)$. Then*

(a) *$E \in S(\mathbb{F}_q, \ell)$ if and only if* $\operatorname{ord}_\ell(f_E) < \operatorname{ord}_\ell(f_{t,q})$;

(b) $E \in S_*(\mathbb{F}_q, \ell)$ *if and only if* $\operatorname{ord}_\ell(f_E) < \operatorname{ord}_\ell(f_{t,q}) - 1$;

(c) $E \in S_0(\mathbb{F}_q, \ell)$ *if and only if* $\operatorname{ord}_\ell(f_E) = 0$, $\operatorname{ord}_\ell(f_{t,q}) = 1$, *and* ℓ *is inert in* K.

Proof. Part (a) is a rephrasing of Theorem 2.1(c). Moreover, the membership of E in $S_*(\mathbb{F}_q, \ell)$ is equivalent to the condition that, for each ℓ-isogeny $E \to E'$, $E' \in S(\mathbb{F}_q, \ell)$. Thus, (b) follows immediately from Lemma 5.1(c). From Lemma 5.1 we further see that $E \in S_0(\mathbb{F}_q, \ell)$ if and only if $\operatorname{ord}_\ell(f_E) > 0$, so that $E \in S(\mathbb{F}_q, \ell)$, and for each ℓ-isogeny $E \to E'$ we have $\operatorname{ord}_\ell(f_{E'}) = \operatorname{ord}_\ell(f_{t,q})$. This proves (c). □

Lemma 5.2 yields an explicit formula, involving class numbers, for quantities like $S(\mathbb{F}_q, \ell)$.

Theorem 5.3. *Let* $q = p^e$ *be a prime power and let* ℓ *be a rational prime such that* $q \equiv 1 \bmod \ell$. *Suppose that* e *is odd, and further suppose that* ℓ *is odd or that* $q \not\equiv 3 \bmod 4$. *Then*

$$\#S(\mathbb{F}_q, \ell) = \sum_{\substack{t^2<4q,\, p\nmid t,\\ \ell^2|(t^2-4q)}} H\left(\frac{t^2-4q}{\ell^2}\right); \tag{5.1}$$

$$\#S_*(\mathbb{F}_q, \ell) = \sum_{\substack{t^2<4p,\, p\nmid t,\\ \ell^4|(t^2-4q)}} H\left(\frac{t^2-4q}{\ell^4}\right); \tag{5.2}$$

$$\#S_0(\mathbb{F}_q, \ell) = \sum_{\substack{t^2<4q,\, p\nmid t,\\ \ell^2||(t^2-4q),\\ (\frac{(t^2-4q)/\ell^2}{\ell})=-1}} H\left(\frac{t^2-4q}{\ell^2}\right). \tag{5.3}$$

Proof. The hypothesis on q and ℓ implies that each $E \in S(\mathbb{F}_q, \ell)$ is ordinary [9, Lem. 4.8]. Consequently,

$$S(\mathbb{F}_q, \ell) = \bigcup_{t^2<4q, p\nmid t} S(\mathbb{F}_q, \ell, t).$$

Moreover, $S(\mathbb{F}_q, \ell, t)$ is nonempty only if $\ell^2 | (1 - t + q)$.

So, suppose t is an integer such that $t^2 < 4q$, $p \nmid t$, and $\ell^2 | (1 - t + q)$. Let $m = \operatorname{ord}_\ell(f_{t,q})$, and write $f_{t,q} = \ell^m f_{t,q}^{(\ell')}$. By Theorem 2.1, the endomorphism rings of members of $I(\mathbb{F}_q, t)$ are precisely those orders of the form $\mathcal{O}(f\Delta_{t,q})$, where f is a divisor of $f_{t,q}$. Using this description, Lemma 5.2 and Theorem 2.1(b), we have

$$\begin{aligned}\#S(\mathbb{F}_q, \ell, t) &= \sum_{0\le\nu\le m-1} \sum_{f'|f_{t,q}^{(\ell')}} h((\ell^\nu f')^2 \Delta_{K_{t,q}}) \\ &= H\left(\frac{\Delta_{T,q}}{\ell^2}\right).\end{aligned}$$

This justifies equation (5.1); equations (5.2) and (5.3) are derived in analogous fashion. □

Remark 5.4. Fix an odd prime ℓ. The moduli scheme $Y(\ell)$ is actually a fine moduli scheme. Let $\mathcal{Y}(1)$ be the moduli *stack* of elliptic curves. The moduli point in $\mathcal{Y}(1)(\mathbb{F}_q)$ of an elliptic curve $E/\mathbb{F}_q$ is counted with multiplicity $\frac{1}{\#\operatorname{Aut}(E)}$; with this understanding we have, for example, the formula

$$\#\mathcal{Y}(1)(\mathbb{F}_p) = \sum_{E/\mathbb{F}_p} \frac{1}{\#\operatorname{Aut}(E)} = p.$$

The forgetful functor $Y(\ell) \to \mathcal{Y}(1)$ is a covering map of stacks, with automorphism group $\mathrm{SL}_2(\mathbb{Z}/\ell)$.

For a quadratic imaginary order $\mathcal{O}$, let $\widetilde{h}(\mathcal{O}) = h(\mathcal{O})/\#\mathcal{O}_K^\times$; define $\widetilde{H}$ analogously. In the context of Theorem 2.1(b), $\widetilde{h}(\mathcal{O})$ counts the number of isomorphism classes of elliptic curves, *weighted by automorphisms*, with endomorphism ring $\mathcal{O}$.

Let $\widetilde{S}(\mathbb{F}_q, \ell)$ be the set of moduli points, in $\mathcal{Y}(1)(\mathbb{F}_q)$, corresponding to isomorphism classes of elliptic curves with full split ℓ-torsion. The stacky version of Theorem 5.3 then states that

$$\#\widetilde{S}(\mathbb{F}_q, \ell) = \sum_{\substack{t^2<4q,\, p\nmid t,\\ \ell^2 \mid (t^2-4q)}} \widetilde{H}\left(\frac{t^2-4q}{\ell^2}\right)$$

and thus

$$\#Y(\ell)(\mathbb{F}_q) = \#\,\mathrm{SL}_2(\mathbb{Z}/\ell) \cdot \sum_{\substack{t^2<4q,\, p\nmid t,\\ \ell^2 \mid (t^2-4q)}} \widetilde{H}\left(\frac{t^2-4q}{\ell^2}\right).$$

Note that, unless the fundamental discriminant of $t^2 - 4q$ is -3 or -4, $\widetilde{H}((t^2-4q)/\ell^2) = \frac{1}{2}H((t^2-4q)/\ell^2)$; in the language of [10, p.165], $\widetilde{H}$ is twice the weighted Kronecker class number there. Consequently, $0 \le \#S(\mathbb{F}_q, \ell) - \frac{1}{2}\#\widetilde{S}(\mathbb{F}_q, \ell) \le \frac{7}{12}$.

Now consider the special case of $\ell = 3$. We have seen (Section 3.2) that $X(3)$ has genus zero, and $Y(3)$ has Euler characteristic -2; $Y(3)$ is isomorphic to the complement of four points in $\mathbb{P}^1$. Our result implies – and machine calculation in examples confirms – that

$$48 \sum_{\substack{t^2<4p, p\nmid t,\\ t^2\equiv 4p \bmod 9}} \widetilde{H}\left(\frac{t^2-4p}{9}\right) = p - 3.$$

While the formulae in Theorem 5.3 do not lead to a proof of Theorem 1.1, they have the (modest) virtue of being well-suited to computer experimentation. Following the suggestion of the referee, in Table 1 we tabulate ratios $R_0(p, \ell)$ and $R_*(p, \ell)$ for some small values of p and ℓ.

Remark 5.5. For any integer $m > 1$, denote by $\Phi_m(x, y) \in \mathbb{Z}[x, y]$ the classical modular equation [7, §5.2]; it satisfies the relation $\Phi_m(j(\tau), j(m\tau)) = 0$, where τ is in the upper-half plane and $j(\tau)$ is the (complex analytic) j-function. If m is not a square then $\Phi_m(x, x)$ is a monic polynomial of degree > 1 [7, p. 55]. If m is prime to the characteristic of $\mathbb{F}_q$ and if $j_1, j_2 \in \mathbb{F}_q$, then $\Phi_m(j_1, j_2) = 0$ if and only if there exist elliptic curves $E_i/\mathbb{F}_q$ with j-invariant j_i which are related by an $\mathbb{F}_q$-cyclic m-isogeny (cf. [8, §1]). Combine these remarks and we see that for any prime ℓ there exists a constant $C(\ell) > 0$ such that if $\ell \nmid q$, then there are at most $C(\ell)$ elliptic curves over $\mathbb{F}_q$ with an $\mathbb{F}_q$-rational point P of order ℓ such that $E/\langle P\rangle$ is $\overline{\mathbb{F}}_q$-isomorphic to E. In particular, the example mentioned in the introduction, where we have a curve $E/\mathbb{F}_5$ which is $\mathbb{F}_5$-isomorphic to $E/\langle(0,0)\rangle$, is an exception and not a norm.

p	$R_0(\mathbb{F}_p, 3)$	$R_*(\mathbb{F}_p, 3)$	$R_0(\mathbb{F}_p, 5)$	$R_*(\mathbb{F}_p, 5)$	$R_0(\mathbb{F}_p, 7)$	$R_*(\mathbb{F}_p, 7)$
1051	0.193182	0.045455	0.388889	0.000000	0.500000	0.000000
4201	0.205128	0.039886	0.380282	0.000000	0.230769	0.000000
17011	0.226375	0.041608	0.334507	0.003521	0.179245	0.000000
65731	0.225995	0.036327	0.333942	0.012774	0.393229	0.000000
131251	0.223807	0.037393	0.323126	0.006856	0.418726	0.000000
525001	0.223561	0.036959	0.326134	0.007656	0.397068	0.005099
1049791	0.221357	0.037093	0.326056	0.008173	0.359345	0.001927
4194961	0.222175	0.036770	0.317863	0.007824	0.364326	0.003293
16777531	0.222351	0.037182	0.318880	0.007982	0.364186	0.003298
67109071	0.222262	0.037117	0.320049	0.007892	0.367168	0.002938
134217931	0.222194	0.037073	0.319479	0.007960	0.365801	0.003075
536871091	0.222223	0.037044	0.320204	0.008040	0.367686	0.002823
1073741971	0.222272	0.037044	0.319993	0.007991	0.367260	0.002915
4294969141	0.222238	0.037038	0.319990	0.008014	0.367115	0.002934
17179869631	0.222220	0.037035	0.319979	0.008001	0.367251	0.002909
68719483351	0.222219	0.037038	0.320016	0.007995	0.367464	0.002913
137438957041	0.222222	0.037036	0.319987	0.008002	0.367296	0.002922
549755814301	0.222221	0.037038	0.319995	0.008000	0.367356	0.002916
Predicted	0.222222	0.037037	0.320000	0.008000	0.367347	0.002915

Table 1. Ratios $R_0(\mathbb{F}_p, \ell) = \#S_0(\mathbb{F}_p, \ell)/\#S(\mathbb{F}_p, \ell)$ and $R_*(\mathbb{F}_p, \ell) = \#S_*(\mathbb{F}_p, \ell)/\#S(\mathbb{F}_p, \ell)$

6. Abelian varieties

Many of the results of Section 3 generalize readily to abelian varieties of arbitrary dimension, although it seems difficult to be as precise about the quantities which arise. In this section we give a quick summary of the analogous statements for abelian varieties. The first three lemmas presented here are direct generalizations of the results of Section 3.1, and their proofs are straight-forward.

Let ℓ be a rational prime and let K be a field which contains a primitive ℓ^{th} root of unity. In particular, ℓ is invertible in K.

Lemma 6.1. *Let X/K be an abelian variety of dimension g. Suppose that $X[\ell](K) \cong (\mathbb{Z}/\ell)^{\oplus 2g}$; let $\{P, Q_2, \cdots, Q_{2g}\}$ be a basis for the ℓ-torsion. Let $X' = X/\langle P\rangle$, and suppose $R \in X(K)$ satisfies $[\ell]R = P$. Let R' be the image of R in $X'(K)$, and define Q'_i analogously. Then $\{P', Q'_2, \cdots, Q'_{2g}\}$ is a basis for $X'[\ell](K) \cong (\mathbb{Z}/\ell)^{\oplus 2g}$.*

Lemma 6.2. *Suppose X/K is an abelian variety of dimension g with $X[\ell](K) \cong (\mathbb{Z}/\ell)^{\oplus 2g}$. Let $\{P, Q_2, \cdots, Q_{2g}\}$ be a basis for $X[\ell]$, and suppose $R \in X(\overline{K})$ satisfies $[\ell]R = P$. Let $X' = X/\langle P\rangle$. Then $X'[\ell](K) \cong (\mathbb{Z}/\ell)^{\oplus 2g}$ if and only if the set $R + \langle P\rangle$ is stable under* $\mathrm{Gal}(K)$.

Lemma 6.3. *Let $X/\mathbb{F}_q$ be a principally polarized abelian variety over a finite field such that $q \equiv 1 \bmod \ell$. Suppose that $X[\ell](\mathbb{F}_q) \cong (\mathbb{Z}/\ell)^{\oplus 2g}$.*

(a) *After a choice of (symplectic) basis for $X[\ell^2](\overline{\mathbb{F}}_q)$, the action of $\mathrm{Fr}_{X/\mathbb{F}_q}$ is given by a matrix $\alpha = 1 + \ell\beta \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^2)$, where $\beta \in \mathfrak{gsp}_{2g}(\mathbb{Z}/\ell)$.*

(b) *The following are equivalent:*
  (i) *For each $P \in X[\ell](\mathbb{F}_q)$ of order ℓ, $(X/\langle P\rangle)[\ell](\mathbb{F}_q) \not\cong (\mathbb{Z}/\ell)^{\oplus 2g}$;*
  (ii) *The matrix β has no $\mathbb{F}_\ell$-rational eigenspace.*

(c) *The following are equivalent:*
  (i) *For each $P \in X[\ell](\mathbb{F}_q)$ of order ℓ, $(X/\langle P\rangle)[\ell](\mathbb{F}_q) \cong (\mathbb{Z}/\ell)^{\oplus 2g}$;*
  (ii) *The matrix β is scalar.*

Now let S be a scheme on which there exists a primitive ℓ^{th} root of unity, and suppose that $X \to S$ is a principally polarized abelian scheme. Attached to this data and a choice of geometric point $s \in S$ is a representation $\rho_{X/S,\ell^2} : \pi_1(S,s) \to \mathrm{Aut}(X_s[\ell^2])$. The image of this representation is constrained to live in $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^2)$. We make the further assumption that the image of $\pi_1(S,s)^{(\mathrm{geom})}$ is in fact $G^{(1)}_{g,\ell}$, where

$$G_{g,\ell} = \{\alpha \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^2) : \alpha \equiv \mathrm{id} \bmod \ell\}$$

and

$$G^{(q)}_{g,\ell} = m^{-1}(q)$$

where $m : \mathrm{GSp}_{2g} \to \mathbb{G}_m$ is the usual "multiplier" map, whose kernel is the symplectic group.

Such an example is provided by the universal abelian scheme over $\mathcal{A}_{g,1,\ell}$, the moduli space of principally polarized abelian varieties of dimension g equipped with a trivialization of the ℓ-torsion. Alternatively, one can start with any family of abelian varieties with maximal ℓ-adic monodromy – for instance, a sufficiently general family of hyperelliptic curves – and then pass to an étale cover of the base which trivializes the ℓ-torsion of the abelian scheme. As in, e.g., [1, Prop. 3.4], an appeal to [5, Thm. 9.7.13] yields:

Lemma 6.4. *There exists a constant $C = C(X/S,\ell)$ such that for each $W \subset G_\ell$ stable under conjugation and for $q \gg 0$ with $q \equiv 1 \bmod \ell$,*

$$\left| \frac{\#\{s \in S(\mathbb{F}_q) : \rho_{X/S,\ell^2}(\mathrm{Fr}_{X_s}) \in W\}}{\#S(\mathbb{F}_q)} - \frac{\#W^{(q)}}{\#G^{(q)}_\ell} \right| < \frac{C}{\sqrt{q}}.$$

Taken together with the calculations above, this gives a way to (asymptotically) compute ratios such as the proportion of abelian varieties with full ℓ-torsion such that no ℓ-isogeny yields an abelian variety with split ℓ-torsion

Acknowledgment. We thank Professor Silverman and the referee for useful comments. In particular, much of Section 5 was written in response to a suggestion of the referee.

References

[1] J. D. Achter and D. Sadornil, On the probability of having rational ℓ-isogenies. *Arch. Math.* **90** (2008) 511-519.

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg* **14** (1941) 197-272.

[3] M. Fouquet and F. Morain, Isogeny volcanoes and the SEA algorithm, in: Algorithmic Number Theory SymposiumANTS V (C. Fieker and D. R. Kohel, eds.), *Lecture Notes in Computer Science* vol. 2369, Springer, 2002, p. 276291.

[4] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves.* Princeton Univ. Press, 1985.

[5] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy.* Amer. Math. Soc., 1999.

[6] D. Kohel, *Endomorphism rings of elliptic curves over finite fields.* Ph.D. thesis, University of California at Berkeley, 1996.

[7] S. Lang, *Elliptic functions.* Springer-Verlag, 1983.

[8] A. Ogg, Diophantine equations and modular forms. *Bull. AMS* **81** (1975) 14-27.

[9] R. Schoof, Nonsingular plane cubic curves over finite fields. *J. Comb. Theory, Ser. A* **46** (1987) 183-211.

[10] R. Schoof and M. van der Vlugt, Hecke operators and the weight distributions of certain codes. *J. Comb. Theory, Ser. A* **57** (1991) 163-186.

[11] G. Shimura, *Introduction to the arithmetic theory of automorphic forms.* Princeton Univ. Press, 1971.

[12] A. V. Sutherland, Isogeny volcanoes. *Algorithmic Number Theory Symposium (ANTS X)*, 2012. http://arxiv.org/abs/1208.5370

[13] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed. Springer-Verlag, 2009.

[14] J. Tate, Endomorphisms of Abelian varieties over finite fields. *Invent. Math.* **2** (1966) 134-144.

[15] J. Vélu, Isogénies entre courbes elliptiques. *C. R. Acad. Sc. Paris* **273** (1971) 238-241.

Department of Mathematics, Colorado State University. Fort Collins, CO 80523-1874
E-mail address: j.achter@colostate.edu

Department of Mathematics & Statistics, University of Massachusetts. Amherst, MA 01003-9305 USA
E-mail address: siman@math.umass.edu