ON ISOGENY GRAPHS OF SUPERSINGULAR ELLIPTIC CURVES OVER FINITE FIELDS

GORA ADJ, OMRAN AHMADI, AND ALFRED MENEZES

Abstract. We study the isogeny graphs of supersingular elliptic curves over finite fields, with an emphasis on the vertices corresponding to elliptic curves of j-invariant 0 and 1728.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q and characteristic $p > 3$, and let $\overline{\mathbb{F}}_q$ denote its algebraic closure. Let ℓ be a prime different from p. The isogeny graph $\mathcal{H}_\ell(\overline{\mathbb{F}}_q)$ is a directed graph whose vertices are the $\overline{\mathbb{F}}_q$-isomorphism classes of elliptic curves defined over $\mathbb{F}_q$, and whose directed arcs represent degree-ℓ $\overline{\mathbb{F}}_q$-isogenies (up to a certain equivalence) between elliptic curves in the isomorphism classes. See [10] and [15] for summaries of the theory behind isogeny graphs and for applications in computational number theory.

Every supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$ is isomorphic to one defined over $\mathbb{F}_{p^2}$. Pizer [12] showed that the subgraph $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ of $\mathcal{H}_\ell(\overline{\mathbb{F}}_{p^2})$ induced by the vertices corresponding to isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ is an expander graph (and consequently is connected). This property of $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ was exploited by Charles, Goren and Lauter [3] who proposed a cryptographic hash function whose security is based on the intractability of computing directed paths of a certain length between two vertices in $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. In 2011, Jao and De Feo [8] (see also [5]) presented a key agreement scheme whose security is also based on the intractability of this problem for small ℓ (typically $\ell = 2, 3$). There have also been proposals for related signature schemes [18, 7] and an undeniable signature scheme [9].

In this paper, we study the supersingular isogeny graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ whose vertices are (canonical representatives of) the $\mathbb{F}_{p^2}$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, and whose directed arcs represent degree-ℓ $\mathbb{F}_{p^2}$-isogenies between the elliptic curves. Observe that the difference between the definitions of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ is that the isomorphisms and isogenies in the former are defined over $\mathbb{F}_{p^2}$ itself. This difference necessitates a careful treatment of the vertices corresponding to supersingular elliptic curves having j-invariant equal to 0 and 1728. We note that the security of the aforementioned cryptographic schemes in fact relies on the difficulty of constructing directed paths in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ (and not in $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ as stated in [3] and [5]). Thus, it is worthwhile to study the differences between $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2})$. We also note that Delfs and Galbraith [4] studied supersingular isogeny graphs $\mathcal{G}_\ell(\mathbb{F}_p)$, and observed that they have similar 'volcano' structures as the ordinary subgraphs of $\mathcal{H}_\ell(\overline{\mathbb{F}}_p)$ [6]. The remainder of the paper is organized as follows. In §2 we provide a concise summary of the relevant

Date: February 3, 2018.

background on elliptic curves and isogenies between them. Standard references for the material in §2 are the books by Silverman [14] and Washington [17]. The supersingular isogeny graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ is defined in §3. In §4 and §5, we completely describe the three small subgraphs of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ whose vertices correspond to supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with $t = p^2 + 1 - \#E(\mathbb{F}_{p^2}) \in \{0, -p, p\}$; see Figure 1. In §6, we study the two large subgraphs of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ whose vertices correspond to supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with $t = p^2 + 1 - \#E(\mathbb{F}_{p^2}) \in \{-2p, 2p\}$, and make some observations about the number of loops at the vertices corresponding to elliptic curves with j-invariant equal to 0 or 1728.

2. Elliptic curves

Let $k = \mathbb{F}_q$ be the finite field of order q and characteristic $p \neq 2, 3$, and let $\overline{k} = \cup_{n\geq 1}\mathbb{F}_{q^n}$ denote its algebraic closure. Let $\sigma : \alpha \mapsto \alpha^q$ denote the q-power Frobenius map. An elliptic curve E over k is defined by a Weierstrass equation $E/k : Y^2 = X^3 + aX + b$ where $a, b \in k$ and $4a^3 + 27b^2 \neq 0$. The j-invariant of E is $j(E) = 1728 \cdot 4a^3/(4a^3 + 27b^2)$. One can easily check that $j(E) = 0$ if and only if $a = 0$, and $j(E) = 1728$ if and only if $b = 0$. For any extension K of k, the set of K-rational points on E is $E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\infty\}$, where ∞ is the point at infinity; we write $E = E(\overline{k})$. The chord-and-tangent addition law transforms $E(K)$ into an abelian group. For any $n \geq 2$ with $p \nmid n$, the group of n-torsion points on E is isomorphic to $\mathbb{Z}_n \oplus \mathbb{Z}_n$. In particular, if n is prime then E has exactly $n + 1$ distinct order-n subgroups.

2.1. **Isomorphisms and automorphisms.** Two elliptic curves $E/k : Y^2 = X^3 + aX + b$ and $E'/k : Y^2 = X^3 + a'X + b'$ are isomorphic over the extension field K/k if there exists $u \in K^*$ such that $a' = u^4a$ and $b' = u^6b$. If such a u exists, then the corresponding isomorphism $f : E \to E'$ is defined by $(x, y) \mapsto (u^2x, u^3y)$. If E and E' are isomorphic over K, then $j(E) = j(E')$. Conversely, if $j(E) = j(E')$, then E and E' are isomorphic over $\overline{k}$. Elliptic curves E_1/k, E_2/k that are isomorphic over $\mathbb{F}_{q^d}$ for some $d > 1$, but are not isomorphic over any smaller extension of $\mathbb{F}_q$, are said to be degree-d twists of each other. In particular, a degree-2 (quadratic) twist of $E_1/k : Y^2 = X^3 + aX + b$ is $E_2/k : Y^2 = X^3 + c^2aX + c^3b$ where $c \in k^*$ is a non-square, and $\#E_1(k) + \#E_2(k) = 2q + 2$. If $j \in \overline{k} \setminus \{0, 1728\}$, then

$$E_j : Y^2 = X^3 + \frac{3j}{1728 - j}X + \frac{2j}{1728 - j} \tag{1}$$

is an elliptic curve with $j(E) = j$. Also, $E : Y^2 = X^3 + 1$ has $j(E) = 0$ and $Y^2 = X^3 + X$ has $j(E) = 1728$.

An automorphism of E/k is an isomorphism from E to itself. The group of all automorphism of E that are defined over K is denoted by $\mathrm{Aut}_K(E)$. If $j(E) \neq 0, 1728$, then $\mathrm{Aut}_{\overline{k}}(E)$ has order 2 with generator $(x, y) \mapsto (x, -y)$. If $j(E) = 1728$, then $\mathrm{Aut}_{\overline{k}}$ is cyclic of order 4 with generator $\psi : (x, y) \mapsto (-x, yi)$ where $i \in \overline{k}$ is a primitive fourth root of unity. If $j(E) = 0$, then $\mathrm{Aut}_{\overline{k}}$ is cyclic of order 6 with generator $\rho : (x, y) \mapsto (jx, -y)$ where $j \in \overline{k}$ is a primitive third root of unity.

2.2. **Isogenies.** Let E, E' be elliptic curves defined over $k = \mathbb{F}_q$. An isogeny $\phi : E \to E'$ is a non-constant rational map defined over $\overline{k}$ with $\phi(\infty) = \infty$. An endomorphism on E is an isogeny from E to itself; the zero map $P \mapsto \infty$ is also considered to be an endomorphism on E. If the field of definition of ϕ is the extension K of k, then ϕ is called a K-isogeny. If such an isogeny exists, then E and E' are said to be K-isogenous. Tate's theorem asserts that E and E' are K-isogenous if and only if $\#E(K) = \#E'(K)$.

The isogeny ϕ is a morphism, is surjective, is a group homomorphism, and has finite kernel. Every K-isogeny ϕ can be represented as $\phi = (r_1(X), r_2(X) \cdot Y)$ where $r_1, r_2 \in K(X)$. Let $r_1(X) = p_1(X)/q_1(X)$, where $p_1, q_1 \in K[X]$ with $\gcd(p_1, q_1) = 1$. Then the degree of ϕ is $\max(\deg p_1, \deg q_1)$. Also, ϕ is said to be separable if $r_1'(X) \neq 0$; otherwise it is inseparable. In fact, ϕ is separable if and only if $\#\mathrm{Ker}\ \phi = \deg \phi$. Note that all isogenies of prime degree $\ell \neq p$ are separable.

For every $m \geq 1$, the multiplication-by-m map $[m] : E \to E$ is a k-isogeny of degree m^2. Every degree-m isogeny $\phi : E \to E'$ has a unique dual isogeny $\hat{\phi} : E' \to E$ satisfying $\hat{\phi} \circ \phi = [m]$ and $\phi \circ \hat{\phi} = [m]$. If ϕ is a K-isogeny, then so is $\hat{\phi}$. We have $\deg \hat{\phi} = \deg \phi$ and $\hat{\hat{\phi}} = \phi$. If E'' is an elliptic curve defined over k and $\psi : E' \to E''$ is an isogeny, then $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$.

2.3. **Vélu's formula.** Let E be an elliptic curve defined over $k = \mathbb{F}_q$. Let $\ell \neq p$ be a prime, and let G be an order-ℓ subgroup of E. Then there exists an elliptic curve E' over $\overline{k}$ and a degree-ℓ isogeny $\phi : E \to E'$ with $\mathrm{Ker}\ \phi = G$. The elliptic curve E' and the isogeny ϕ are both defined over $K = \mathbb{F}_{q^t}$ where t is the smallest positive integer such that G is σ^t-invariant, i.e., $\{\sigma^t(P) : P \in G\} = G$ where $\sigma(P) = (x^q, y^q)$ if $P = (x, y)$ and $\sigma(\infty) = \infty$. Furthermore, ϕ is unique in the following sense: if E'' is an elliptic curve defined over K and $\psi : E \to E''$ is a degree-ℓ K-isogeny with $\mathrm{Ker}\ \psi = G$, then there exists an isomorphism $f : E' \to E''$ defined over K such that $\psi = f \circ \phi$.

Given the Weierstrass equation $Y^2 = X^3 + aX + b$ for E/k and an order-ℓ subgroup G of E, Vélu's formula yields an elliptic curve E' defined over K and a degree-ℓ K-isogeny $\phi : E \to E'$ with $\mathrm{Ker}\ \phi = G$.

Suppose first that $\ell = 2$ and $G = \{\infty, (\alpha, 0)\}$. Then the Weierstrass equation for E' is

$$E' \ : \ Y^2 = X^3 - (4a + 15\alpha^2)X + (8b - 14\alpha^3), \tag{2}$$

and the isogeny ϕ is given by

$$\phi = \left(X + \frac{3\alpha^2 + a}{X - \alpha},\ Y - \frac{(3\alpha^2 + a)Y}{(X - \alpha)^2} \right). \tag{3}$$

Suppose now that ℓ is an odd prime. For $Q = (x_Q, y_Q) \in G^*$, define

$$t_Q = 3x_Q^2 + a, \quad u_Q = 2y_Q^2, \quad w_Q = u_Q + t_Q x_Q.$$

Furthermore, define

$$t = \sum_{Q \in G^*} t_Q, \quad w = \sum_{Q \in G^*} w_Q,$$

and

$$r(X) = X + \sum_{Q \in G^*} \left(\frac{t_Q}{X - x_Q} + \frac{u_Q}{(X - x_Q)^2} \right). \tag{4}$$

Then the Weierstrass equation for E' is

$$E' \,:\, Y^2 = X^3 + (a-5t)X + (b-7w), \tag{5}$$

and the isogeny ϕ is given by

$$\phi = \bigl(r(X), r'(X)Y\bigr)\,. \tag{6}$$

We will henceforth denote the Vélu-generated elliptic curve E' by E/G.

2.4. **Modular polynomials.** Let ℓ be a prime. The modular polynomial $\Phi_\ell(X,Y) \in \mathbb{Z}[X,Y]$ is a symmetric polynomial of the form $\Phi_\ell(X,Y) = X^{\ell+1} + Y^{\ell+1} - X^\ell Y^\ell + \sum c_{ij}X^iY^j$, where the sum is over pairs of integers (i,j) with $0 \le i,j \le \ell$ and $i+j < 2\ell$. Modular polynomials have the following remarkable property that for any elliptic curve E characterizes the j-invariants of those elliptic curves E' for which a degree-ℓ separable isogeny $\phi : E \to E'$ exists.

Theorem 1. Suppose that the characteristic of $k = \mathbb{F}_q$ is different from ℓ. Let E/k be an elliptic curve with $j(E) = j$. Let $G_1, G_2, \ldots, G_{\ell+1}$ be the order-ℓ subgroups of E. Let $j_i = j(E/G_i)$. Then the roots of $\Phi_\ell(j,Y)$ in $\overline{k}$ are precisely $j_1, j_2, \ldots, j_{\ell+1}$.

2.5. **Supersingular elliptic curves.** Hasse's theorem states that if E is defined over $\mathbb{F}_q$, then $\#E(\mathbb{F}_q) = q+1-t$ where $|t| \le 2\sqrt{q}$. The integer t is called the trace of the q-power Frobenius map σ since the characteristic polynomial of σ acting on E is $Z^2 - tZ + q$. If $p \mid t$, then E is supersingular; otherwise it is ordinary. Every supersingular elliptic curve E over $\overline{\mathbb{F}}_q$ is isomorphic to one defined over $\mathbb{F}_{p^2}$; in particular, $j(E) \in \mathbb{F}_{p^2}$. Henceforth, we shall assume that $q = p^2$ (and $p > 3$).

Supersingularity of an elliptic curve depends only on its j-invariant. We say that $j \in \mathbb{F}_{p^2}$ is supersingular if there exists a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with $j(E) = j$; if this is the case, then all elliptic curves with j-invariant equal to j are supersingular. Note that $j = 0$ is supersingular if and only if $p \equiv 2 \pmod 3$, and $j = 1728$ is supersingular if and only if $p \equiv 3 \pmod 4$.

Schoof [13] determined the number of isomorphism classes of elliptic curves over a finite field. In particular, the number of isomorphism classes of supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with $\#E(\mathbb{F}_{p^2}) = p^2 + 1 - t$ is

$$N(t) = \begin{cases} \left(p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-4}{p}\right)\right)/12, & \text{if } t = \pm 2p, \\ 1 - \left(\frac{-3}{p}\right), & \text{if } t = \pm p, \\ 1 - \left(\frac{-4}{p}\right), & \text{if } t = 0, \end{cases} \tag{7}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. It follows that the total number of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ is $\lfloor p/12 \rfloor + \epsilon$, where $\epsilon = 0, 5, 3, 8$ if $p \equiv 1, 5, 7, 11 \pmod{12}$ respectively. Furthermore, if $t = 0$, $-p$ or p then $E(\mathbb{F}_{p^2})$ is cyclic.

3. Supersingular isogeny graphs

Let $k = \mathbb{F}_q$ where $q = p^2$, and let $\ell \ne p$ be a prime. Recall that σ is the q-th power Frobenius map. The supersingular isogeny graph $\mathcal{G}_\ell(k)$ is a directed graph whose vertex set $V_\ell(k)$ consists of canonical representatives of the k-isomorphism classes of supersingular elliptic curves defined over k. The (directed) arcs of $\mathcal{G}_\ell(k)$ are defined as follows. Let $E_1 \in V_\ell(k)$, and let G be a σ-invariant order-ℓ subgroup of E_1. Let $\phi : E_1 \to E_1/G$ be the Vélu isogeny with kernel G (recall that E_1/G and ϕ are both defined over k), and let E_2 be the canonical representative of the k-isomorphism class of elliptic curves containing E_1/G. Then (E_1, E_2) is an arc; we call E_1 the tail and E_2 the head of the arc. Note that $\mathcal{G}_\ell(k)$ can have multiple arcs (more than one arc (E_1, E_2)) and loops (arcs of the form (E_1, E_1)).

Remark 1. The definition of arcs is independent of the choice of isogeny with kernel G. This is because, as noted in §2.3, if $\phi' : E_1 \to E_2'$ is any degree-ℓ isogeny with kernel G where both E_2' and ϕ' are defined over k, then E_2' and E_1/G are isomorphic over k and consequently ϕ and ϕ' yield the same arc (E_1, E_2).

Remark 2. The definition of $\mathcal{G}_\ell(k)$ is independent of the choice of canonical representatives. Indeed, let $f : E_1' \to E_1$ be a k-isomorphism of elliptic curves, and suppose that E_1' was chosen as a canonical representative instead of E_1. Let $\psi = \phi \circ f$. Then $\operatorname{Ker} \psi = f^{-1}(G)$, and thus the σ-invariant order-ℓ subgroup $f^{-1}(G)$ of E_1' yields the arc (E_1', E_2). The claim now follows since f^{-1} yields a one-to-one correspondence between the σ-invariant order-ℓ subgroups of E_1 and E_1'.

A consequence of Tate's theorem is that the graph $\mathcal{G}_\ell(k)$ can be partitioned into five subgraphs whose vertices are the k-isomorphism classes of supersingular elliptic curves E/k with trace $t = p^2 + 1 - \#E(k) \in \{0, -p, p, -2p, 2p\}$; we denote these subgraphs by $\mathcal{G}_\ell(k, t)$. There are two such subgraphs ($t = \pm 2p$) when $p \equiv 1 \pmod{12}$, four subgraphs ($t = \pm p, \pm 2p$) when $p \equiv 5 \pmod{12}$, three subgraphs ($t = 0, \pm 2p$) when $p \equiv 7 \pmod{12}$, and five subgraphs ($t = 0, \pm p, \pm 2p$) when $p \equiv 11 \pmod{12}$. These subgraphs are further studied in §§4–6. We first fix the canonical representatives of the k-isomorphism classes of supersingular elliptic curves over k.

Suppose that $p \equiv 3 \pmod 4$, and let w be a generator of k^*. Munuera and Tena [11] showed that the representatives of the four isomorphism classes of elliptic curves E/k with $j(E) = 1728$ can be taken to be

$$E_{1728,w^i} : Y^2 = X^3 + w^i X \quad \text{for} \quad i \in [0, 3]. \tag{8}$$

Of these curves, $E_{1728,w}$ and E_{1728,w^3} have $p^2 + 1$ $\mathbb{F}_{p^2}$-rational points, and so we choose them as canonical representatives of the vertices of $\mathcal{G}_\ell(k, 0)$. Furthermore, $\#E_{1728,1}(\mathbb{F}_{p^2}) = p^2 + 1 + 2p$ and $\#E_{1728,w^2}(\mathbb{F}_{p^2}) = p^2 + 1 - 2p$; hence, we select $E_{1728,1}$ and E_{1728,w^2} as representatives of vertices in $\mathcal{G}_\ell(k, -2p)$ and $\mathcal{G}_\ell(k, 2p)$, respectively.

Suppose that $p \equiv 2 \pmod 3$, and let w be a generator of k^*. Munuera and Tena [11] also showed that the representatives of the six isomorphism classes of elliptic curves E/k with $j(E) = 0$ can be taken to be

$$E_{0,w^i} : Y^2 = X^3 + w^i \quad \text{for} \quad i \in [0, 5]. \tag{9}$$

Of these curves, $E_{0,w}$ and E_{0,w^5} have $p^2 + 1 + p$ $\mathbb{F}_{p^2}$-rational points, and so we choose them as canonical representatives of the vertices of $\mathcal{G}_\ell(k, -p)$. Similarly, E_{0,w^2} and E_{0,w^4} have $p^2 + 1 - p$ $\mathbb{F}_{p^2}$-rational points, and so we choose them as canonical representatives of the vertices of $\mathcal{G}_\ell(k, p)$. Finally, $\#E_{0,1}(\mathbb{F}_{p^2}) = p^2 + 1 + 2p$ and $\#E_{0,w^3}(\mathbb{F}_{p^2}) = p^2 + 1 - 2p$; hence, we select $E_{0,1}$ and E_{0,w^3} as representatives of vertices in $\mathcal{G}_\ell(k, -2p)$ and $\mathcal{G}_\ell(k, 2p)$, respectively.

If $j \neq 0, 1728$ is supersingular, then E_j (defined in (1)) and a quadratic twist $\tilde{E}_j$ are representatives of the two isomorphism classes of elliptic curves with j-invariant equal to

j. Furthermore, $\#E_j(\mathbb{F}_{p^2}) \in \{p^2+1-2p, p^2+1+2p\}$ and $\#E_j(\mathbb{F}_{p^2})+\#\tilde{E}_j(\mathbb{F}_{p^2}) = 2p^2+2$. We select E_j as the representative of a vertex in either $\mathcal{G}_\ell(k,-2p)$ or $\mathcal{G}_\ell(k,2p)$ depending on whether $\#E_j(\mathbb{F}_{p^2}) = p^2+1+2p$ or p^2+1-2p, and $\tilde{E}_j$ as the representative of a vertex in the other graph.

4. The subgraph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$

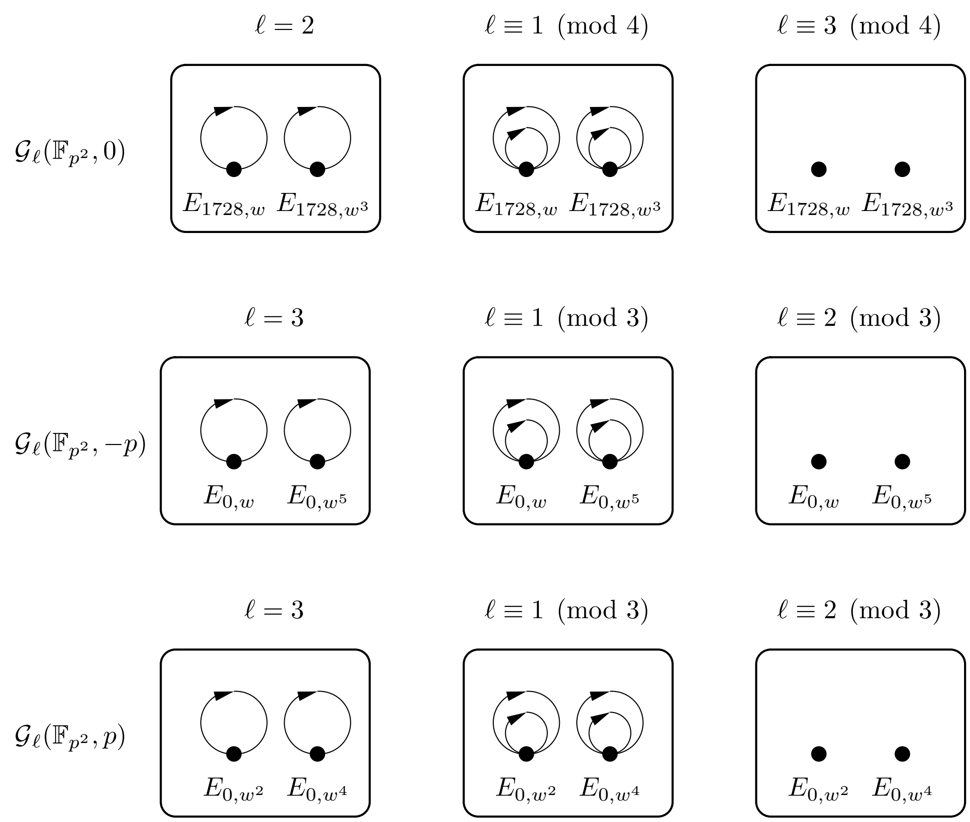

Figure 1. The small subgraphs of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$, $p \equiv 11 \pmod{12}$.

Let $q = p^2$ where $p \equiv 3 \pmod 4$, w is a generator of $\mathbb{F}_q^*$, and $\ell \neq p$ is a prime. The graph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ has two vertices, $E_{1728,w}$ and E_{1728,w^3}; to ease the notation we will call them E_w and E_{w^3} in this section. The map $\psi : (x,y) \mapsto (-x, iy)$ where $i \in \mathbb{F}_q$ satisfies $i^2 = -1$ is an automorphism of E_w and E_{w^3}.

Theorem 2. Let p and ℓ be primes with $p \equiv 3 \pmod 4$ and $\ell \neq p$.

(i) $\mathcal{G}_2(\mathbb{F}_{p^2}, 0)$ has exactly two arcs, one loop at each of its two vertices.
(ii) If $\ell \equiv 3 \pmod 4$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ has no arcs.
(iii) If $\ell \equiv 1 \pmod 4$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ has exactly four arcs, two loops at each of its two vertices.

Proof. We describe the arcs originating at E_w; the E_{w^3} case is similar.

Since $t = 0$, the characteristic polynomial of the q-power Frobenius map σ is $Z^2 + p^2$.

(i) If $\ell = 2$, then 1 is the only eigenvalue of σ acting on $E_w[2]$. Since $(0,0)$ is the only point of order 2 in $E_w(\mathbb{F}_q)$, there is only one σ-invariant order-2 subgroup of $E_w[2]$, namely $G = \{\infty, (0,0)\}$. Vélu's formula (2) yields the isogeny $\phi : E_w \to E_w/G$, where the Weierstrass equation of E_w/G is $Y^2 = X^3 - 4wX$. Now,

$$(-4)^{(q-1)/4} = ((-4)^{p-1})^{(p+1)/4} = 1.$$

Thus, E_w/G and E_w are isomorphic over $\mathbb{F}_q$ (cf. §2.1), whence G yields a loop at E_w.

(ii) If $\ell \equiv 3 \pmod 4$, then $Z^2 + p^2$ has no roots modulo ℓ, and consequently E_w has no σ-invariant order-ℓ subgroups.

(iii) If $\ell \equiv 1 \pmod 4$, then $Z^2 + p^2$ has two distinct roots modulo ℓ, namely $\pm cp \bmod \ell$ where c is a square root of -1 modulo ℓ. Let $P_0 \in E_w[\ell]^*$ with $\sigma(P_0) = [cp]P_0$, and let $G = \langle P_0 \rangle$. Then G is a σ-invariant order-ℓ subgroup of $E_w[\ell]$.

Vélu's formula (4) yields an isogeny $\phi : E_w \to E_w/G$. Since E_w and G are defined over $\mathbb{F}_q$, so is $E' = E_w/G$. Since E' is in the same isogeny class as E_w, its defining equation is of the form $Y^2 = X^3 + w'X$ for some $w' \in \mathbb{F}_q^*$. Furthermore, $\phi = (r(X), r'(X) \cdot Y)$, where

$$\begin{aligned}
r(X) &= X + \sum_{P \in G^*} \left(\frac{3x_P^2 + w}{X - x_P} + \frac{2y_P^2}{(X - x_P)^2} \right) \\
&= X + \sum_{P \in G^*} \frac{(3x_P^2 + w)(X - x_P) + 2y_P^2}{(X - x_P)^2} \\
&= X + \sum_{P \in G^*} \frac{(3x_P^2 + w)(X - x_P)(X + x_P)^2 + 2y_P^2(X + x_P)^2}{(X^2 - x_P^2)^2}.
\end{aligned}$$

Now, for all $P \in G^*$, we have

$$\sigma(\psi(P)) = \psi(\sigma(P)) = \psi([cp]P) = [cp]\psi(P)$$

and hence $\psi(P) \in G$. Let $H \subset G^*$ be such that $P \in H$ if and only if $\psi(P) \notin H$. Then

$$r(X) = X + \sum_{P \in H} \frac{w_P(X)}{(X^2 - x_P^2)^2},$$

where

$$\begin{aligned}
w_P(X) &= (3x_P^2 + w)(X - x_P)(X + x_P)^2 + 2y_P^2(X + x_P)^2 \\
&\qquad + (3x_P^2 + w)(X + x_P)(X - x_P)^2 - 2y_P^2(X - x_P)^2 \\
&= (3x_P^2 + w)(X^2 - x_P^2)(X + x_P) + 2y_P^2(X + x_P)^2 \\
&\qquad + (3x_P^2 + w)(X^2 - x_P^2)(X - x_P) - 2y_P^2(X - x_P)^2 \\
&= 2X(3x_P^2 + w)(X^2 - x_P^2) + 8y_P^2 x_P X.
\end{aligned}$$

Thus

$$r(X) = X \left(1 + 2 \sum_{P \in H} \frac{(3x_P^2 + w)(X^2 - x_P^2) + 4y_P^2 x_P}{(X^2 - x_P^2)^2} \right) \triangleq XS(X^2),$$

where $S \in \mathbb{F}_q(X)$. Also,

$$r'(X) = S(X^2) + 2X^2 S'(X^2) \triangleq T(X^2),$$

where $T \in \mathbb{F}_q(X)$.

Since $(0,0) \in E_w(\mathbb{F}_q)$ and ϕ is defined over $\mathbb{F}_q$, we have $\phi((0,0)) \in E'(\mathbb{F}_q)$. Since $E'(\mathbb{F}_q)$ is cyclic, $(0,0)$ is its only point of order 2, and hence $\phi((0,0)) = (0,0)$. Now, let $Q_0 = (x_0, y_0) \in E_w$ with $[2]Q_0 = (0,0)$; note that $x_0 \neq 0$ and $y_0 \neq 0$. From the elliptic curve point doubling formula, we deduce that $x_0 = \pm\sqrt{w}$. If $x_0 = \sqrt{w}$ then $y_0 = \pm\sqrt{2}w^{3/4}$, whereas if $x_0 = -\sqrt{w}$ then $y_0 = \pm i\sqrt{2}w^{3/4}$. Without loss of generality, suppose that $Q_0 = (\sqrt{w}, \sqrt{2}w^{3/4})$. Let $Q_0' = \phi(Q_0)$. Then

$$[2]Q_0' = [2]\phi(Q_0) = \phi([2]Q_0) = \phi((0,0)) = (0,0).$$

Therefore $Q_0' \in \{(\sqrt{w'}, \pm\sqrt{2}w'^{3/4}), (-\sqrt{w'}, \pm i\sqrt{2}w'^{3/4})\}$. Without loss of generality, suppose that $\phi(Q_0) = (\sqrt{w'}, \sqrt{2}w'^{3/4})$. Then $\sqrt{w'} = S(w)\sqrt{w}$ and so $(w'/w)^{1/2} \in \mathbb{F}_q^*$. Moreover, $\sqrt{2}w'^{3/4} = \sqrt{2}w^{3/4}T(w)$, so $(w'/w)^{3/4} \in \mathbb{F}_q^*$. Thus, $(w'/w)^{3/4}/(w'/w)^{1/2} = (w'/w)^{1/4} \in \mathbb{F}_q^*$. Hence E_w and E' are isomorphic over $\mathbb{F}_q$, so G yields a loop at E_w. Similarly, the eigenspace of $-cp \bmod \ell$ yields a second loop at E_w. $\square$

5. The subgraphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm p)$

Let $q = p^2$ where $p \equiv 2 \pmod 3$, w is a generator of $\mathbb{F}_q^*$, and $\ell \neq p$ is a prime. The graph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -p)$ has two vertices, $E_{0,w}$ and E_{0,w^5}; to ease the notation we will call them E_w and E_{w^5} in this section. The map $\rho : (x, y) \mapsto (jx, -y)$ where $j \in \mathbb{F}_q$ satisfies $j^2 + j + 1 = 0$ is an automorphism of E_w and E_{w^5}.

Theorem 3. Let p and ℓ be primes with $p \equiv 2 \pmod 3$ and $\ell \neq p$.

(i) $\mathcal{G}_3(\mathbb{F}_{p^2}, -p)$ has exactly two arcs, one loop at each of its two vertices.
(ii) If $\ell \equiv 2 \pmod 3$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -p)$ has no arcs.
(iii) If $\ell \equiv 1 \pmod 3$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -p)$ has exactly four arcs, two loops at each of its two vertices.

Proof. We describe the arcs originating at E_w; the E_{w^5} case is similar.

Since $t = -p$, the characteristic polynomial of the q-power Frobenius map σ is $Z^2 + pZ + p^2$.

(i) If $\ell = 3$, then -1 is the only eigenvalue of σ acting on $E_w[3]$ with eigenvectors $(0, \pm\sqrt{w})$. Indeed, the x-coordinate of any point in $E_w[3]^*$ is a root of the 3-division polynomial $3X(X^3 + 4w)$, and if $x^3 + 4w = 0$ then $x^{p^2} \neq x$ since $(-4w)^{1/3} \notin \mathbb{F}_{p^2}$. Thus, $G = \langle(0, \sqrt{w})\rangle$ is the unique σ-invariant order-3 subgroup of E_w. Vélu's formula (4) yields the isogeny $\phi : E_w \to E_w/G$, where the Weierstrass equation of E_w/G is $Y^2 = X^3 - 27w$. Now,

$$(-27)^{(q-1)/6} = ((-27)^{p-1})^{(p+1)/6} = 1.$$

Thus, E_w/G and E_w are isomorphic over $\mathbb{F}_q$ (cf. §2.1), whence G yields a loop at E_w.

(ii) If $\ell \equiv 2 \pmod 3$, then $Z^2 + pZ + p^2$ has no roots modulo ℓ, and consequently E_w has no σ-invariant order-ℓ subgroups.

(iii) If $\ell \equiv 1 \pmod 3$, then $Z^2 + pZ + p^2$ has two distinct roots modulo ℓ, namely $\lambda_1 = (-1 + \sqrt{-3})p/2 \bmod \ell$ and $\lambda_2 = (-1 - \sqrt{-3})p/2 \bmod \ell$. The corresponding eigenspaces, $\langle P_0\rangle$ and $\langle Q_0\rangle$, are the only two σ-invariant order-ℓ subgroups of E_w.

Let $G = \langle P_0 \rangle$, and let $\phi : E_w \to E_w/G$ be the Vélu isogeny. Since E_w and G are defined over $\mathbb{F}_q$, so is $E' = E_w/G$. Since E' is in the same isogeny class as E_w, its defining equation is of the form $Y^2 = X^3 + w'$ for some $w' \in \mathbb{F}_q^*$. Furthermore, $\phi = (r(X), r'(X) \cdot Y)$, where

$$\begin{aligned} r(X) &= X + \sum_{P \in G^*} \left(\frac{3x_P^2}{X - x_P} + \frac{2y_P^2}{(X - x_P)^2} \right) \\ &= X + \sum_{P \in G^*} \frac{3x_P^2(X^3 - x_P^3)(X^2 + x_P X + x_P^2) + 2y_P^2(X^2 + x_P X + x_P^2)^2}{(X^3 - x_P^3)^2} \\ &= X + \sum_{P \in G^*} \frac{3x_P^2(X^3 - x_P^3)(X - jx_P)(X - j^2 x_P) + 2y_P^2(X - jx_P)^2(X - j^2 x_P)^2}{(X^3 - x_P^3)^2}. \end{aligned}$$

Now, for all $P \in G^*$, we have

$$\sigma(\rho(P)) = \rho(\sigma(P)) = \rho([\lambda_1]P) = [\lambda_1]\rho(P)$$

and hence $\rho(P), \rho^2(P) \in G$. Let $H \subset G^*$ be such that $P \in H$ if and only if $\rho(P) \notin H$ and $\rho^2(P) \notin H$. Then

$$r(X) = X + \sum_{P \in H} \frac{w_1(X) + 2y_P^2 w_2(X)}{(X^3 - x_P^3)^2},$$

where

$$\begin{aligned} w_1(X) &= 3x_P^2(X^3 - x_P^3)(X - jx_P)(X - j^2 x_P) + 3j^2 x_P^2 (X^3 - x_P^3)(X - x_P)(X - j^2 x_P) \\ &\quad + 3j x_P^2 (X^3 - x_P^3)(X - x_P)(X - jx_P) \\ &= 9x_P^3 X(X^3 - x_P^3) \end{aligned}$$

and

$$\begin{aligned} w_2(X) &= (X - jx_P)^2(X - j^2 x_P)^2 + (X - x_P)^2(X - j^2 x_P)^2 + (X - x_P)^2(X - jx_P)^2 \\ &= 3X(X^3 + 2x_P^3). \end{aligned}$$

Thus we can write $r(X) = XS(X^3)$ where $S \in \mathbb{F}_q(X)$.

The order-2 points in E_w and E' are $(-j^u w^{1/3}, 0)$ $(u = 0, 1, 2)$ and $(-j^u w'^{1/3}, 0)$ $(u = 0, 1, 2)$, respectively. Thus $\phi((w^{1/3}, 0)) = (j^u w'^{1/3}, 0)$ for some $u \in \{0, 1, 2\}$. Since $r(X) = XS(X^3)$, we have $j^u w'^{1/3} = w^{1/3} S(w)$, from which we deduce that

$$(w'/w)^{1/3} \in \mathbb{F}_q^*. \tag{10}$$

Now consider the q-power Frobenius map σ' acting on E'. As with the case of E_w, the only order-3 points $P' \in E'$ satisfying $\sigma'(P') = -P'$ are $(0, \pm\sqrt{w'})$. On the other hand

$$\sigma'(\phi((0, \sqrt{w}))) = \phi(\sigma((0, \sqrt{w}))) = \phi((0, -\sqrt{w})) = -\phi((0, \sqrt{w})),$$

and hence $\phi((0, \sqrt{w})) = (0, \pm\sqrt{w'})$. Thus, $\pm\sqrt{w'} = \sqrt{w} r'(0)$, implying that

$$(w'/w)^{1/2} \in \mathbb{F}_q^*. \tag{11}$$

Finally, (10) and (11) give $(w'/w)^{1/6} \in \mathbb{F}_q^*$, and thus E_w and E' are isomorphic over $\mathbb{F}_q$. Hence G yields a loop at E_w. Similarly, $\langle Q_0 \rangle$ yields a second loop at E_w. $\square$

The proof of Theorem 4 is similar to that of Theorem 3.

Theorem 4. Let p and ℓ be primes with $p \equiv 2 \pmod 3$ and $\ell \neq p$.

(i) $\mathcal{G}_3(\mathbb{F}_{p^2}, p)$ has exactly two arcs, one loop at each of its two vertices.
(ii) If $\ell \equiv 2 \pmod 3$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, p)$ has no arcs.
(iii) If $\ell \equiv 1 \pmod 3$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, p)$ has exactly four arcs, two loops at each of its two vertices.

6. The subgraphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$

As noted in §3, the vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ have distinct j-invariants. Moreover, there is a one-to-one correspondence between the vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and the vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$; namely, if E is a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ then the chosen quadratic twist $\tilde{E}$ is a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$. Now, the characteristic polynomial of the q-power Frobenius map σ acting on any vertex E in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ is $Z^2 + 2pZ + p^2 = (Z + p)^2$, so $(\sigma + [p])^2 = 0$. Since nonzero endomorphisms are surjective, we must have $\sigma + [p] = 0$. Hence $\sigma = [-p]$ and all order-ℓ subgroups of E are σ-invariant. It follows that every vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ has outdegree $\ell+1$. Similarly, every vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$ has outdegree $\ell + 1$.

By Theorem 1, the j-invariants of the heads of arcs with tail E in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ are precisely the roots of $\Phi_\ell(j(E), Y)$ (all $\ell + 1$ of which lie in $\mathbb{F}_{p^2}$). These roots are also the j-invariants of the heads of arcs with tail $\tilde{E}$ in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$. Hence the directed graphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$ are isomorphic.

Sutherland [15] defines the isogeny graph $\mathcal{H}_\ell(\overline{\mathbb{F}}_{p^2})$ to have vertex set $\overline{\mathbb{F}}_{p^2}$ and arcs (j_1, j_2) present with multiplicity equal to the multiplicity of j_2 as a root of $\Phi_\ell(j_1, Y)$ in $\overline{\mathbb{F}}_{p^2}$. The following shows that $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$, the supersingular component of $\mathcal{H}_\ell(\overline{\mathbb{F}}_{p^2})$, is isomorphic to $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$.

Theorem 5. $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ are isomorphic.

Proof. Recall that all supersingular elliptic curves over $\overline{\mathbb{F}}_{p^2}$ are defined over $\mathbb{F}_{p^2}$. Hence the map $\beta : E \mapsto j(E)$ is a bijection between the vertex sets of $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. Now, let (E_1, E_2) be an arc of multiplicity $c \geq 0$ in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. By Theorem 1, $j(E_2)$ is a root of multiplicity c of $\Phi_\ell(j(E_1), Y)$. Hence $(j(E_1), j(E_2))$ is an arc of multiplicity c in $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. Thus, β preserves arcs and $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p) \cong \mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. □

6.1. **Indegree.** Suppose that p is prime and let E be a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Then all automorphisms of E are defined over $\mathbb{F}_{p^2}$; we denote the group of all automorphisms of E by $\mathrm{Aut}(E)$. Recall from §2.1 that $\#\mathrm{Aut}(E) = 4, 6$ or 2 depending on whether $j(E) = 1728$, $j(E) = 0$ or $j(E) \neq 0, 1728$.

Let $\ell \neq p$ be a prime. Let E_1, E_2 be two vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, and let $\phi_1, \phi_2 : E_1 \to E_2$ be two degree-ℓ $\mathbb{F}_{p^2}$-isogenies. We say that ϕ_1 and ϕ_2 are *equivalent* if they have the same kernel, or, equivalently, if there exists $\rho_2 \in \mathrm{Aut}(E_2)$ such that $\phi_2 = \rho_2 \circ \phi_1$. Thus, the arcs (E_1, E_2) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ can be seen as the classes of equivalent degree-ℓ $\mathbb{F}_{p^2}$-isogenies from E_1 to E_2. We define ϕ_1 and ϕ_2 to be *automorphic* if there exists $\rho_1 \in \mathrm{Aut}(E_1)$ such that ϕ_2 and $\phi_1 \circ \rho_1$ are equivalent. Hence, if ϕ_1 and ϕ_2 are automorphic then there exist $\rho_1 \in \mathrm{Aut}(E_1)$ and $\rho_2 \in \mathrm{Aut}(E_2)$ such that $\phi_2 = \rho_2 \circ \phi_1 \circ \rho_1$. Since $\hat{\phi}_2 = \rho_1^{-1} \circ \hat{\phi}_1 \circ \rho_2^{-1}$, it follows that the duals of automorphic isogenies are automorphic.

Theorem 6. Let E be a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and let $n = \#\mathrm{Aut}(E)/2$. Let a and b denote the number of arcs (E, E_{1728}) and arcs (E, E_0) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, respectively. Then the indegree of E is $(\ell + a + 2b + 1)/n$.

Proof. Let E_1, E_2 be two vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, and let $\mathrm{Aut}(E_i) = \langle \rho_i \rangle$ and $n_i = \#\mathrm{Aut}(E_i)/2$ for $i = 1, 2$. Let $\phi : E_1 \to E_2$ be a degree-ℓ $\mathbb{F}_{p^2}$-isogeny.

Suppose first that the kernel of ϕ is not an eigenspace of ρ_1. Consider the set

$$\mathcal{A} = \{\rho_2^j \circ \phi \circ \rho_1^i \;:\; 0 \le i < 2n_1,\; 0 \le j < 2n_2\}$$

of isogenies automorphic to ϕ. Since $\rho_i^{n_i} = -1$ for $i \in \{1, 2\}$, we have

$$\mathcal{A} = \{\rho_2^j \circ \phi \circ \rho_1^i \;:\; 0 \le i < n_1,\; 0 \le j < 2n_2\}.$$

One can check that if $(i, j) \ne (i', j')$ where $0 \le i, i' < n_1$ and $0 \le j, j' < 2n_2$, then $\rho_2^j \circ \phi \circ \rho_1^i = \rho_2^{j'} \circ \phi \circ \rho_1^{i'}$ implies that the kernel of ϕ is an eigenspace of ρ_1. Hence the set $\mathcal{A}$ has size exactly $2n_1n_2$ and the isogenies in $\mathcal{A}$ can be partitioned into n_1 classes of equivalent isogenies, each class comprised of $2n_2$ isogenies. Similarly, the set

$$\hat{\mathcal{A}} = \{\rho_1^i \circ \hat{\phi} \circ \rho_2^j \;:\; 0 \le i < 2n_1,\; 0 \le j < 2n_2\}$$

of dual isogenies can be partitioned into n_2 classes of equivalent isogenies, each class comprised of $2n_1$ isogenies. Consequently, ϕ generates n_1 different arcs (E_1, E_2) and $\hat{\phi}$ generates n_2 different arcs (E_2, E_1). Because duals of automorphic isogenies are automorphic, if there is another degree-ℓ $\mathbb{F}_{p^2}$-isogeny ψ from E_1 to E_2 not automorphic to ϕ, then ψ (resp. $\hat{\psi}$) generates a set of n_1 (resp. n_2) arcs (E_1, E_2) (resp. (E_2, E_1)) disjoint from those generated by ϕ (resp. $\hat{\phi}$). Therefore, the number r_{out} of arcs (E_1, E_2) generated by isogenies whose kernels are not eigenspaces of ρ_1 and the number r_{in} of arcs (E_2, E_1) generated by their duals are multiples of n_1 and n_2, respectively. Moreover, we have

$$r_{\text{in}} = \frac{n_2 \cdot r_{\text{out}}}{n_1}. \tag{12}$$

Suppose now that the kernel of ϕ is an eigenspace of ρ_1. This scenario occurs only if E_1 has j-invariant 1728 or 0. Suppose E_1 has j-invariant 1728, and let ρ_1 be the automorphism $(x, y) \mapsto (-x, iy)$ where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. Denote by G the kernel of ϕ, and let $\phi' : E_1 \to E_1/G$ denote the Vélu isogeny. By (5), E_1/G has equation $Y^2 = X^3 + aX - 7w$ for some $a \in \mathbb{F}_{p^2}$ and $w = \sum_{Q \in G^*}(5x_Q^3 + 3x_Q)$. Since $\rho_1(G) = G$, if $(x, y) \in G$ then $(-x, iy) \in G$. Hence $w = 0$ and we conclude that E_1/G is isomorphic to E_1 over $\mathbb{F}_{p^2}$, i.e., $E_2 = E_1$. A similar argument using the automorphism $(x, y) \mapsto (jx, -y)$ with $j \in \mathbb{F}_{p^2}$ satisfying $j^2 + j + 1 = 0$ shows that we also have $E_2 = E_1$ when the j-invariant of E_1 is 0. Thus, if the kernel of ϕ is an eigenspace of ρ_1, the arcs generated by ϕ are loops at E_1. Therefore, we can generalize (12) to the total number t_{out} of arcs (E_1, E_2) and the total number t_{in} of arcs (E_2, E_1) and obtain

$$t_{\text{in}} = \frac{n_2 \cdot t_{\text{out}}}{n_1}. \tag{13}$$

Now, let E be a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and $n = \#\mathrm{Aut}(E)/2$. Denote by E_j the vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ having j-invariant $j \in \mathbb{F}_{p^2}$. Let a be the number of arcs (E, E_{1728}) and b the number of arcs (E, E_0). Note that the number of arcs (E, E_j), $j \notin \{0, 1728\}$, is $c = \ell - a - b + 1$. From (13) we have

$$\mathrm{indegree}(E) = \frac{c}{n} + \frac{2a}{n} + \frac{3b}{n},$$

whence

$$\text{indegree}(E) = \frac{\ell + a + 2b + 1}{n}.$$

□

6.2. **Loops.** Let E_{1728} and E_0 denote the vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ with j-invariants 1728 and 0. In §6.2.1 and §6.2.2 we investigate the number of loops at E_{1728} and E_0 in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$.

6.2.1. E_{1728} *loops.* We begin by noting that

$$\Phi_2(X, 1728) = (X - 1728)(X - 287496)^2.$$

Since $287496 - 1728 = 2^3 \cdot 3^6 \cdot 7^2$, we see that 1728 is a triple root of $\Phi_2(X, 1728)$ in $\mathbb{Z}_p[X]$ if $p = 7$ and a single root if $p > 7$. Hence the number of loops at E_{1728} in $\mathcal{G}_2(\mathbb{F}_{p^2}, -2p)$ is three if $p = 7$ and one if $p > 7$ (and $p \equiv 3 \pmod 4$).

Lemma 7. Let $p \equiv 3 \pmod 4$ be a prime, and let $\ell \neq p$ be an odd prime. Then the number of loops at E_{1728} is even. Moreover, if $\ell \equiv 1 \pmod 4$ then there are at least two loops at E_{1728}.

Proof. Let ρ denote the automorphism $(x, y) \mapsto (-x, iy)$ of E_{1728} where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. Since $\#\text{Aut}(E_{1728})/2 = 2$ we have from the first part of the proof of Theorem 6 that the number of loops at E_{1728} generated by isogenies whose kernels are not eigenspaces of ρ is even.

The characteristic polynomial $Z^2 + 1$ of ρ splits modulo ℓ if and only if $\ell \equiv 1 \pmod 4$. Hence, if $\ell \equiv 3 \pmod 4$ then all the loops at E_{1728} are generated by isogenies whose kernels are not eigenspaces of ρ and thus the number of loops is even. Now suppose that $\ell \equiv 1 \pmod 4$. The eigenspaces of ρ modulo ℓ are two different order-ℓ subgroups of E_{1728}. The second part of the proof of Theorem 6 shows that the edges generated by these subgroups are loops at E_{1728}. □

Theorem 8. Let $\ell \equiv 3 \pmod 4$ be a fixed prime. Let $p \equiv 3 \pmod 4$, $p \neq \ell$, be a prime for which E_{1728} has at least one loop in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Then $p \leq \Phi_\ell(1728, 1728)$.

Proof. Let $r \equiv 1 \pmod 4$ be a prime. The elliptic curve $E/\mathbb{F}_r : Y^2 = X^3 + X$ is ordinary, has j-invariant 1728, and has endomorphism ring $\mathbb{Z}[i] \subseteq \mathbb{Q}(i)$ with discriminant $D = -1$. Proposition 23 of [10] tells us that there are exactly $1 + \left(\frac{D}{\ell}\right) = 0$ degree-ℓ isogenies over $\overline{\mathbb{F}}_r$ to E. Hence by Theorem 1, we must have $\Phi_\ell(1728, 1728) \not\equiv 0 \pmod r$ and so $\Phi_\ell(1728, 1728) \neq 0$.

Now, since E_{1728} has a loop in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, we have $\Phi_\ell(1728, 1728) \equiv 0 \pmod p$ and hence $p \leq \Phi_\ell(1728, 1728)$. □

Theorem 9. Let $\ell \equiv 1 \pmod 4$ be a fixed prime. Then $\Phi_\ell(1728, Y) = (Y - 1728)^2 G_\ell(Y)$ where $G_\ell \in \mathbb{Z}[Y]$. Moreover, if $p \equiv 3 \pmod 4$ is a prime for which E_{1728} has at least three loops in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, then $p \leq G_\ell(1728)$.

Proof. Write $\Phi_\ell(1728, Y) = (Y - 1728)^2 G_\ell(Y) + H(Y)$, where $G_\ell, H \in \mathbb{Z}[Y]$ and $\deg H \leq 1$. For any prime $p \equiv 3 \pmod 4$, since there are at least two loops at E_{1728} in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, we have $H(Y) = 0 \pmod p$. Hence $H(Y) = 0$.

Let $r \equiv 1 \pmod 4$ be a prime $\neq \ell$. Proposition 23 of [10] tells us that there are exactly $1 + \left(\frac{-1}{\ell}\right) = 2$ degree-ℓ isogenies over $\overline{\mathbb{F}}_r$ to $E/\mathbb{F}_r : Y^2 = X^3 + X$. Hence there can be at most two loops at E in $\mathcal{H}_\ell(\overline{\mathbb{F}}_r)$, and so by Theorem 1 we must have $G_\ell(1728) \neq 0$. Now, there are more than two loops at E_{1728} in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ if and only if $G_\ell(1728) \equiv 0 \pmod p$. It follows that $p \leq G_\ell(1728)$. □

6.2.2. E_0 *loops.* We have

$$\Phi_2(X, 0) = (X - 2^4 \cdot 3^3 \cdot 5^3)^3,$$

whence 0 is a triple root of $\Phi_2(X, 0)$ in $\mathbb{Z}_p[X]$ if $p = 5$ and not a root if $p > 5$. Hence the number of loops at E_0 in $\mathcal{G}_2(\mathbb{F}_{p^2}, -2p)$ is three if $p = 5$ and zero if $p > 5$ (and $p \equiv 2 \pmod 3$). Similarly, since

$$\Phi_3(X, 0) = X(X - 2^{15} \cdot 3 \cdot 5^3)^3,$$

we conclude that the number of loops at E_0 in $\mathcal{G}_3(\mathbb{F}_{p^2}, -2p)$ is four if $p = 5$ and one if $p > 5$ (and $p \equiv 2 \pmod 3$).

Lemma 10. Let $p \equiv 2 \pmod 3$ be a prime, and let $\ell \neq 3, p$ be an odd prime. If $\ell \equiv 2 \pmod 3$, then the number of loops at E_0 is $\equiv 0 \pmod 3$. If $\ell \equiv 1 \pmod 3$, then the number of loops at E_0 is $\equiv 2 \pmod 3$.

Proof. Similar to the proof of Lemma 7. □

Theorem 11. Let $\ell \equiv 2 \pmod 3$ be a fixed odd prime. Let $p \equiv 2 \pmod 3$, $p \neq \ell$, be a prime for which E_0 has at least one loop in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Then $p \leq \Phi_\ell(0, 0)$.

Proof. Let $r \equiv 1 \pmod 3$ be a prime. The elliptic curve $E/\mathbb{F}_r : Y^2 = X^3 + 1$ is ordinary, has j-invariant 0, and has endomorphism ring $\mathbb{Z}[(1+\sqrt{-3})/2] \subseteq \mathbb{Q}(\sqrt{-3})$ with discriminant $D = -3$. Proposition 23 of [10] tells us that there are exactly $1 + \left(\frac{D}{\ell}\right) = 0$ degree-ℓ isogenies over $\overline{\mathbb{F}}_r$ to E. Hence by Theorem 1, we must have $\Phi_\ell(0, 0) \not\equiv 0 \pmod r$ and so $\Phi_\ell(0, 0) \neq 0$.

Now, since E_0 has a loop in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ we have $\Phi_\ell(0, 0) \equiv 0 \pmod p$ and hence $p \leq \Phi_\ell(0, 0)$. □

Theorem 12. Let $\ell \equiv 1 \pmod 3$ be a fixed prime. Let $p \equiv 2 \pmod 3$ be a prime for which E_0 has at least three loops in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Write $\Phi_\ell(0, Y) = Y^2 G_\ell(Y) + H(Y)$, where $G_\ell, H \in \mathbb{Z}[Y]$ and $\deg H \leq 1$. Then $p \leq G_\ell(0)$.

Proof. Similar to the proof of Theorem 9. □

Remark 3. It is worth mentioning that portions of Lemmas 7 and 10 can be obtained using standards properties of modular polynomials and the j modular function. Indeed, these properties lets one prove that when $p \equiv 3 \pmod 4$ and $\ell \equiv 1 \pmod 3$ then there are at least two loops at E_{1728}; also, when $p \equiv 2 \pmod 3$ and $\ell \equiv 1 \pmod 3$ then there are at least two loops at E_0. The proofs we have given are elementary and self contained.

For primes $\ell \equiv 1 \pmod 4$ (resp. $\ell \equiv 3 \pmod 4$), let $p^1_{1728}(\ell)$ (resp. $p^3_{1728}(\ell)$) denote the largest prime $p \equiv 3 \pmod 4$, $p \neq \ell$, for which E_{1728} has at least three loops (resp. at least one loop) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Similarly, for odd primes $\ell \equiv 1 \pmod 3$ (resp. $\ell \equiv 2 \pmod 3$), let $p^1_0(\ell)$ (resp. $p^2_0(\ell)$) denote the largest prime $p \equiv 2 \pmod 3$, $p \neq \ell$, for which E_0 has at least three loops (resp. at least one loop) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Table 1 lists $p^1_{1728}(\ell)$, $p^3_{1728}(\ell)$, $p^1_0(\ell)$, $p^2_0(\ell)$ for all primes $\ell \leq 283$. These values were obtained by factoring the relevant values of the modular polynomial Φ_ℓ; the modular polynomials were obtained from Sutherland's database [1, 16]. For example, $p^3_{1728}(\ell)$ is the largest prime factor of $\Phi_\ell(1728, 1728)$ that is congruent to 3 modulo 4.

Bröker and Sutherland [2] proved that $h(\Phi_\ell) \leq 6\ell \log \ell + 18\ell$ for all primes ℓ and conjectured that $\lim \inf_{\ell\to\infty}(h(\Phi_\ell) - 6\ell \log \ell)/\ell > 11.8$; here $h(\Phi_\ell)$ denotes the natural logarithm of the largest coefficient (up to sign) of $\Phi_\ell(X, Y)$. Thus the coefficients of $\Phi_\ell(X, Y)$ are very large. So, for example, one expects that $\Phi_\ell(1728, 1728)$ is a very large integer with at least one relatively large prime factor. In light of this, the size of the numbers in Table 1 are surprisingly small. For example, $\Phi_{19}(1728, 1728)$ is a 822-decimal digit number with prime factorization

$$\Phi_{19}(1728, 1728) = 2^{180} \cdot 3^{124} \cdot 7^{40} \cdot 11^{24} \cdot 19^2 \cdot 23^8 \cdot 31^8 \cdot 47^8 \cdot 59^8 \cdot 67^4 \cdot 71^8,$$

whereby $\Phi_{19}(1728, 1728)$ is 71-smooth and $p^3_{1728}(19) = 71$.

ℓ	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
$p^1_{1728}(\ell)$	–	19	–	–	47	67	–	–	107	–	139	163	–	–	211
$p^3_{1728}(\ell)$	11	–	23	–	–	–	71	83	–	107	–	–	167	179	–
$p^1_0(\ell)$	–	–	17	–	23	–	53	–	–	89	107	–	113	–	–
$p^2_0(\ell)$	–	11	–	–	–	47	–	53	83	–	–	107	–	137	131
ℓ	59	61	67	71	73	79	83	89	97	101	103	107	109	113	127
$p^1_{1728}(\ell)$	–	239	–	–	283	–	–	347	383	379	–	–	431	443	–
$p^3_{1728}(\ell)$	227	–	263	239	–	311	331	–	–	–	383	419	–	–	503
$p^1_0(\ell)$	–	179	197	–	191	233	–	–	263	–	293	–	311	–	353
$p^2_0(\ell)$	173	–	–	197	–	–	233	263	–	251	–	317	–	311	–
ℓ	131	137	139	149	151	157	163	167	173	179	181	191	193	197	199
$p^1_{1728}(\ell)$	–	547	–	587	–	619	–	–	691	–	719	–	743	787	–
$p^3_{1728}(\ell)$	523	–	547	–	599	–	647	659	–	691	–	751	–	–	787
$p^1_0(\ell)$	–	–	401	–	449	467	461	–	–	–	491	–	563	–	593
$p^2_0(\ell)$	389	383	–	443	–	–	–	449	503	521	–	569	–	587	–
ℓ	211	223	227	229	233	239	241	251	257	263	269	271	277	281	283
$p^1_{1728}(\ell)$	–	–	–	911	919	–	947	–	1019	–	1063	–	1103	1123	–
$p^3_{1728}(\ell)$	839	887	907	–	–	947	–	991	–	1051	–	1039	–	–	1123
$p^1_0(\ell)$	617	653	–	683	–	–	719	–	–	–	–	809	827	–	821
$p^2_0(\ell)$	–	–	677	–	683	701	–	701	743	773	743	–	–	839	–

TABLE 1. The values $p^1_{1728}(\ell)$, $p^3_{1728}(\ell)$, $p^1_0(\ell)$, $p^2_0(\ell)$ for all odd primes $\ell \leq 283$.

References

[1] R. Bröker, K. Lauter and A. Sutherland, "Modular polynomials via isogeny volcanoes", *Mathematics of Computation*, 278 (2012), 1201–1231.

[2] R. Bröker and A. Sutherland, "An explicit height bound for the classical modular polynomial", *The Ramanujan Journal*, 22 (2010), 293–313.

[3] D. Charles, E. Goren and K. Lauter, "Cryptographic hash functions from expander graphs", *Journal of Cryptology*, 22 (2009), 93–113.

[4] C. Delfs and S. Galbraith, "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$", *Designs, Codes and Cryptography*, 78 (2016), 425–440.

[5] L. De Feo, D. Jao and J. Plût, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", *Journal of Mathematical Cryptology*, 8 (2014), 209–247.

[6] M. Fouquet and F. Morain, "Isogeny volcanoes and the SEA algorithm", *Algorithmic Number Theory — ANTS 2002*, LNCS 2369 (2002), 276–291.

[7] S. Galbraith, C. Petit and J. Silva, "Identification protocols and signature schemes based on supersingular isogeny problems", *Advances in Cryptology — ASIACRYPT 2017*, LNCS 10624 (2017), 3–33.

[8] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", *Post-Quantum Cryptography — PQCrypto 2011*, LNCS 7071 (2011), 19–34.

[9] D. Jao and V. Soukharev, "Isogeny-based quantum-resistant undeniable signatures", *Post-Quantum Cryptography — PQCrypto 2014*, LNCS 8772 (2014), 160–179.

[10] D. Kohel, "Endomorphism rings of elliptic curves over finite fields", Ph.D. thesis, UC Berkeley, 1996.

[11] C. Munuera and J. Tena, "An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite fields", *Rendiconti Del Circolo Matematico Di Palermo, Serie II*, XLII (1993), 106–116.

[12] A. Pizer, "Ramanujan graphs and Hecke operators", *Bulletin of the American Mathematical Society*, 23 (1990), 127–137.

[13] R. Schoof, "Nonsingular plane cubic curves over finite fields", *Journal of Combinatorial Theory, Series A*, 46 (1987), 183–211.

[14] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, second edition, 2009.

[15] A. Sutherland, "Isogeny volcanoes", *Algorithmic Number Theory — ANTS 2013*, MSP Open Book Series, 1 (2013), 507–530.

[16] A. Sutherland, "Modular polynomials", math.mit.edu/~drew/ClassicalModPolys.html.

[17] L. Washington, *Elliptic Curves: Number Theory and Cryptography.* Chapman & Hall/CRC, second edition, 2008.

[18] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao and V. Soukharev, "A post-quantum digital signature scheme based on supersingular isogenies", *Financial Cryptography and Data Security — FC 2017*, to appear.

Department of Combinatorics & Optimization, University of Waterloo, Canada
E-mail address: `gora.adj@gmail.com`

Institute for Research in Fundamental Sciences, Iran
E-mail address: `oahmadid@gmail.com`

Department of Combinatorics & Optimization, University of Waterloo, Canada
E-mail address: `ajmeneze@uwaterloo.ca`