23 Isogeny volcanoes

We now shift our focus from elliptic curves over $\mathbb{C}$ to elliptic curves other fields, and to finite fields in particular. As noted in Lecture 21, the moduli interpretation of the modular polynomial $X_0(N)$ as parameterizing cyclic isogenies of degree N is valid over any field whose characteristic does not divide N; see Theorem 21.4. We can thus use the modular equation $\Phi_N \in \mathbb{Z}[X,Y]$ to identify pairs of isogenous elliptic curves using j-invariants in any field k. When k is not algebraically closed this determines the elliptic curves involved only up to a twist, but for finite fields there are only two twists to consider (assuming $j \neq 0, 1728$), and in many applications it suffices to work with $\bar{k}$ isomorphism classes of elliptic curves defined over k, equivalently the set of j-invariants of elliptic curves E/k, which by Theorem 14.12, is just the set k itself.

We are particularly interested in the case that $N = \ell$ is a prime different from the characteristic of k. Every isogeny of degree ℓ is necessarily cyclic (since ℓ is prime), and for any fixed j-invariant $j_1 := j(E_1)$, the roots of the polynomial

$$\phi_\ell(Y) = \Phi_\ell(j_1, Y)$$

that lie in k are j-invariants of elliptic curves E_2/k that are *ℓ-isogenous* to E, meaning that there exists an isogeny $\varphi\colon E_1 \to E_2$ of degree ℓ. More precisely, there is a bijection between the roots of $\phi_\ell(Y)$ in k and the cyclic subgroups of $E[\ell]$ that are fixed $\mathrm{Gal}(\bar{k}/k)$ when the roots of $\phi_\ell(Y)$ are counted with multiplicity; over $\bar{k}$ there are $\deg \phi_\ell = \ell + 1$ (not necessarily distinct) roots of ϕ_ℓ corresponding to $\ell+1$ (necessarily distinct) cyclic subgroups of $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell$ of order ℓ. Recall from Theorem 6.10 that every finite subgroup of $E(\bar{k})$ is the kernel of a separable isogeny that is uniquely determined up to composition with isomorphisms. We are only interested in isogenies up to isomorphism, so we will consider separable isogenies to be distinct if and only if their kernels differ. We will also assume $\ell \neq \mathrm{char}(k)$ throughout, so all the isogenies we will consider in this lecture are separable.

Definition 23.1. The *ℓ-isogeny graph* $G_\ell(k)$ is the directed graph with vertex set k and edges (j_1, j_2) present with multiplicity equal to the multiplicity of j_2 as a root of $\Phi_\ell(j_1, Y)$.

As noted in Remark 21.6, if $j_1 = j(E_1)$ and $j_2 = j(E_2)$ are the j-invariants of a pair of ℓ-isogenous elliptic curves, the ordered pair (j_1, j_2) does not uniquely determine an ℓ-isogeny $\varphi\colon E_1 \to E_2$; their may be multiple inequivalent ℓ-isogenies from E_1 to E_2. This is why it is important to count edges in $G_\ell(k)$ with multiplicity. The existence of the dual isogeny guarantees that (j_1, j_2) is an edge in $G_\ell(k)$ if and only (j_2, j_1) is also an edge; provided that $j_1, j_2 \neq 0, 1728$ these edges have the same multiplicity.

Remark 23.2. The exceptions for j-invariants $0 = j(\rho)$ and $1728 = j(i)$ arise from the fact that the corresponding elliptic curves $y^2 = x^3 + B$ and $y^2 = x^3 + Ax$ have automorphisms $\rho\colon (x,y) \mapsto (\rho x, y)$ and $i\colon (x,y) \mapsto (-x, iy)$, respectively, where ρ and i denote elements of orders 3 and 4 in $\mathrm{End}(E)$ and $\bar{k}$. The automorphism -1 does not pose a problem because it fixes every cyclic subgroup of $E[\ell]$, so for any ℓ-isogeny $\varphi\colon E_1 \to E_2$ the isogeny $\varphi \circ [-1] = [-1] \circ \varphi$ has the same kernel as φ; this does not apply to ρ and i, which fix only two cyclic subgroups of $E[\ell]$. If $j(E_1) = 0$ and $j(E_2) \neq 0$ then we cannot write $\varphi \circ \rho = \rho \circ \varphi$ and the isogenies $\varphi, \varphi \circ \rho, \varphi \circ \rho^2$ will all have different kernels, but the corresponding dual-isogenies will all have the same kernel. In this situation the edge $(j(E_1), j(E_2)$ will have multiplicity 3 in $G_\ell(k)$ but the edge $(j(E_2), j(E_1))$ will have multiplicity 1. The case where $j(E_1) = 1728$ and $j(E_2) \neq 1728$ is similar, except now $(j(E_1), j(E_2)$ has multiplicity 2.

Our objective in this lecture is to elucidate the structure of the graph $G_\ell(k)$ in the case that $k = \mathbb{F}_q$ is a finite field. Recall from Lecture 14 that elliptic curves over finite fields may be classified according to their endomorphism algebras and are either ordinary (meaning $\mathrm{End}^0(E)$ is an imaginary quadratic field) or supersingular (meaning $\mathrm{End}^0(E)$ is a quaternion algebra). Whether E is ordinary or supersingular is an isogeny invariant (by Theorem 14.1), so the graph $G_\ell(\mathbb{F}_q)$ can always be partitioned into ordinary and supersingular components. Since most elliptic curves are ordinary, we will focus on the ordinary components; you will have an opportunity to investigate the supersingular components on Problem Set 12.

23.1 Isogenies between elliptic curves with complex multiplication

Theorem 23.3. *Let $\varphi\colon E \to E'$ be an ℓ-isogeny of elliptic curves defined over a field k. Then $\mathrm{End}^0(E') \simeq \mathrm{End}^0(E)$, and if $\mathrm{End}^0(E) = K$ is an imaginary quadratic field then $\mathrm{End}(E) = \mathcal{O}$ and $\mathrm{End}(E') = \mathcal{O}'$ are orders in K such that one of the following holds:*

$$\text{(i) } \mathcal{O} = \mathcal{O}', \qquad \text{(ii) } [\mathcal{O} : \mathcal{O}'] = \ell, \qquad \text{(iii) } [\mathcal{O}' : \mathcal{O}] = \ell.$$

Proof. Let $\hat\varphi\colon E' \to E$ be the dual isogeny. If $\phi \in \mathrm{End}(E)$, the isogeny $\varphi \circ \phi \circ \hat\varphi\colon E' \to E'$ is an endomorphism $\phi' \in \mathrm{End}(E')$ with

$$\begin{aligned}
\mathrm{T}\phi' &= \phi + \phi' = \varphi \circ \phi \circ \hat\varphi + \varphi \circ \hat\phi \circ \hat\varphi = \varphi \circ [\mathrm{T}\phi] \circ \hat\varphi = \varphi \circ \hat\varphi \circ [\mathrm{T}\phi] = \ell\,\mathrm{T}\phi,\\
\mathrm{N}\phi' &= \phi \circ \phi' = \varphi \circ \phi \circ \hat\varphi \circ \varphi \circ \hat\phi \circ \hat\varphi = \varphi \circ \phi \circ [\ell] \circ \hat\phi \circ \hat\varphi = \varphi \circ [\ell\,\mathrm{N}\phi] \circ \hat\varphi = \ell^2 \mathrm{N}\phi,
\end{aligned}$$

and ϕ' is a root of $x^2 - (\mathrm{T}\phi')x + \mathrm{N}\phi' = x^2 - (\mathrm{T}\phi)(\ell x) + \ell^2\mathrm{N}\phi = 0$. Thus $\phi'/\ell \in \mathrm{End}^0(E')$ is a root of $x^2 - (\mathrm{T}\phi)x + \mathrm{N}\phi$, and it follows that the characteristic polynomial of every $\phi \in \mathrm{End}(E)$ has a root in $\mathrm{End}^0(E')$ and therefore $\mathrm{End}(E) \subseteq \mathrm{End}^0(E')$. Applying the same argument in the reverse direction shows that $\mathrm{End}(E') \subseteq \mathrm{End}^0(E)$, so we must have $\mathrm{End}^0(E') = \mathrm{End}^0(E)$.

If $\mathrm{End}^0(E') \simeq \mathrm{End}(E)$ is an imaginary quadratic field with $\mathcal{O} = [1, \tau]$ and $\mathcal{O} = [1, \tau']$, then $\varphi \circ \tau \circ \hat\varphi = \ell\tau \in \mathcal{O}'$ and $\hat\varphi \circ \tau \circ \varphi = \ell\tau' \in \mathcal{O}$. Thus $[1, \ell\tau] \subseteq [1, \tau']$ and $[1, \ell\tau'] \subseteq [1, \tau]$, and therefore

$$[1, \ell^2\tau] \subseteq [1, \ell\tau'] \subseteq [1, \tau].$$

The index of $[1, \ell^2\tau]$ in $[t, \tau]$ is ℓ^2, so the index of $[1, \ell\tau']$ in $[1, \tau]$ must be $1, \ell$, or ℓ^2. These correspond to cases (iii), (i), and (ii) of the theorem, respectively. □

Definition 23.4. Theorem 23.3 allows us to distinguish ℓ-isogenies $\varphi\colon E \to E'$ of elliptic curves with CM by an imaginary quadratic field as follows:

(i) when $\mathcal{O} = \mathcal{O}'$ we say that φ is *horizontal*,

(ii) when $[\mathcal{O} : \mathcal{O}'] = \ell$ we say that φ is *descending*,

(iii) when $[\mathcal{O}' : \mathcal{O}] = \ell$ we say that φ is *ascending*.

We collectively refer to ascending and descending isogenies as *vertical* isogenies.

Theorem 23.5. *Let $E/\mathbb{C}$ be an elliptic curve with CM by an order $\mathcal{O}$ of discriminant D in an imaginary quadratic field K, and let ℓ be prime. If $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ then E admits $1 - \left(\frac{D}{\ell}\right)$ horizontal, $\ell + \left(\frac{D}{\ell}\right)$ descending, and no ascending ℓ-isogenies. Otherwise E admits no ascending, ℓ descending, and one ascending ℓ-isogenies.*

Proof. We first consider the special case in which E corresponds to a torus $\mathbb{C}/L$ with $L := \ell\mathcal{O}$ homothetic to $\mathcal{O}$. As explained in Lecture 18 (see §18.5), every ℓ-isogeny $\varphi\colon E \to E'$ arises from a lattice inclusion $L \subseteq L'$ of index ℓ. The lattices L' containing $L = \ell\mathcal{O}$ with index ℓ are precisely the index-ℓ sublattices of $\mathcal{O}$. By Lemma 21.2, these are the lattices $L_i := [\ell, \tau + i]$ for $0 \le i < \ell$ and the lattice $L_\ell := [1, \ell\tau]$. We then have

$$\mathcal{O}' := \mathrm{End}(E') \simeq \mathrm{End}(\mathbb{C}/L') = \mathcal{O}(L') := \{\alpha \in \mathcal{O} : \alpha L' \subseteq L'\},$$

so it suffices to compute $\mathcal{O}(L')$ for the lattices $L' \in \{L_0, L_1, \dots, L_\ell\}$. By definition, we have $\mathcal{O}(L') = \mathcal{O}$ precisely when L' is a proper $\mathcal{O}$-ideal. By Corollary 22.7,if $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ there are $1 - \left(\frac{D}{\ell}\right)$, each corresponding to a horizontal ℓ-isogeny, and otherwise there are no proper $\mathcal{O}$-ideals of norm ℓ and no horizontal ℓ-isogenies.

If $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ we cannot have $[\mathcal{O}' : \mathcal{O}] = \ell$, in which case we must have $1 - \left(\frac{D}{\ell}\right)$ horizontal, no ascending, and $\ell + \left(\frac{D}{\ell}\right)$ descending ℓ-isogenies. Otherwise $\mathcal{O}$ is an index-ℓ suborder of some order $\mathcal{O}'' := [1, \omega]$ in $\mathcal{O}_K$, where $\tau = \ell\omega$ and $\omega^2 - a\omega + b = 0$, with $a = \mathrm{T}\omega, b = \mathrm{N}\omega \in \mathbb{Z}$. By Theorem 23.3, either $\mathcal{O}' = \mathcal{O}''$ and φ is an ascending isogeny, or $\mathcal{O}' \ne \mathcal{O}''$ and φ is a descending isogeny (since φ cannot be horizontal). The lattice $L_0 = [\ell, \tau]$ is fixed by $\mathcal{O}''$, since $\omega\ell = \tau \in L_0$ and $\omega\tau = \ell\omega^2 = \ell(a\omega - b) = a\tau - b\ell \in L_0$. On the other hand, none of the lattices L_i with $0 < i < \ell$ are fixed by $\mathcal{O}''$, since $\omega(\tau + i) = \ell\omega^2 + i\omega = (\ell a + i)\omega - b\ell$ is not an element of $\mathcal{O} \supseteq L_i$ for $0 < i < \ell$, and $L_\ell = [1, \ell\tau]$ is not fixed by $\mathcal{O}''$ because $\omega \cdot 1 = \omega$ is not an element of $\mathcal{O}$. It follows that φ is an ascending ℓ-isogeny if and only if $L' = L_0$, so there are one ascending and ℓ descending ℓ-isogenies.

We now consider the general case, in which L is homothetic to a proper $\mathcal{O}$-ideal $\mathfrak{a}$, which we can assume has prime norm $p \ne \ell$ (by Theorem 21.11, every ideal class in $\mathrm{cl}(\mathcal{O})$ contains infinitely ideals of prime norm). The CM action of $\mathfrak{a}$ is then a horizontal p-isogeny $\varphi_\mathfrak{a}\colon E \to E_0$, with $E_0 \simeq \mathbb{C}/\mathcal{O}$. Let $\varphi\colon E \to E'$ be an ℓ-isogeny, let $\mathcal{O}' = \mathrm{End}(E')$, and let $\mathfrak{a}'$ be the $\mathcal{O}'$-ideal $\mathfrak{a}$, $\mathfrak{a}\mathcal{O}'$, or $\mathfrak{a} \cap \mathcal{O}'$, depending on whether φ is horizontal, descending, or ascending. We must have $[\mathcal{O}' : \mathfrak{a}'] = [\mathcal{O}_K : \mathfrak{a}'\mathcal{O}_K] = [\mathcal{O}_K : \mathfrak{a}] = [\mathcal{O} : \mathfrak{a}] = p$, since p does divide $[\mathcal{O}_K : \mathcal{O}]$ or $[\mathcal{O}_K : \mathcal{O}']$ because $\mathfrak{a}$ is proper and $p \ne \ell$; it follows that $\mathfrak{a}'$ is a proper $\mathcal{O}'$-ideal of norm p, and we have a horizontal p-isogeny $\varphi_{\mathfrak{a}'}\colon E' \to E'_0$ with $E'_0 \simeq \mathbb{C}/\mathcal{O}'$. Up to isomorphism, there is a unique ℓ-isogeny $\varphi_0\colon E_0 \to E'_0$ such that the diagram

$$\begin{array}{ccc} E & \xrightarrow{\varphi_\mathfrak{a}} & E_0 \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi_0} \\ E' & \xrightarrow{\varphi_{\mathfrak{a}'}} & E'_0 \end{array}$$

commutes, namely the isogeny with kernel $\varphi_\mathfrak{a}(\ker(\varphi_{\mathfrak{a}'} \circ \varphi))$ given by Theorem 6.10. Since $\varphi_\mathfrak{a}$ and $\varphi_{\mathfrak{a}'}$ are both horizontal, the ℓ-isogeny φ_0 must be of the same type (horizontal, descending, or ascending) as φ. The theorem then follows from the special case proved above. □

Theorem 23.5 extends to any field whose characteristic is not ℓ (provided that one takes into rationality into account: ℓ-isogenies admitted by E over $\bar{k}$ need not be defined over k). We won't prove this in full generality, but we can use Deuring's lifting theorem to address the case where k is a finite field $\mathbb{F}_q$.

For an imaginary quadratic order $\mathcal{O}$ with discriminant D and any field k we define

$$\mathrm{Ell}_\mathcal{O}(k) := \{j(E) \in k : \mathrm{End}(E) = \mathcal{O}\},$$

the set of j-invariants of elliptic curves over k with CM by $\mathcal{O}$; for $k = \mathbb{C}$ this is the same as the set of roots of the Hilbert class polynomial $H_D(X)$, whose cardinality is the class number $h(D) := \#\mathrm{Cl}(\mathcal{O})$, and a result of Deuring noted in the previous lecture (see Theorem 22.12 yields a similar statement for finite fields.

Lemma 23.6. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D and let $\mathbb{F}_q$ be a finite field with $q \perp D$. The set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is either empty or has cardinality $h(D)$. If $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is nonempty, so is $\mathrm{Ell}'_{\mathcal{O}}(\mathbb{F}_q)$ for every imaginary quadratic order $\mathcal{O}'$ containing $\mathcal{O}$.*

Proof. If $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is nonempty then there is an elliptic curve $E/\mathbb{F}_q$ with CM by $\mathcal{O}$. Its Frobenius endomorphism π_E is an element of $\mathrm{End}(E) = \mathcal{O}$ with trace $t = \mathrm{tr}\,\pi_E$ and norm q, and we must have $t \perp q$, since E is ordinary, by Corollary 14.19. The discriminant of the characteristic polynomial $x^2 - tx + q$ has a root $\pi_E \in \mathcal{O}$ that is not in $\mathbb{Z}$ (because $t \neq \pm 2\sqrt{q}$), so its discriminant $t^2 - 4q$ is a square in $\mathcal{O} - \mathbb{Z}$, hence of the form $v^2 D$ for some $v \in \mathbb{Z}$. We then have $4q = t^2 - v^2 D$ with $t \perp q$, so $p \nmid D$, and it follows from Theorem 22.5 and Remark 22.11 that q is the norm of a prime ideal in $\mathcal{O}_L$, where L is the ring class field of $\mathcal{O}$. By Theorem 22.12, the Hilbert class polynomial $H_D(X)$ of degree $h(D)$ splits into distinct linear factors in $\mathbb{F}_q[X]$ and its roots form the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ of cardinality $h(D)$.

If $\mathcal{O}'$ is an order of discriminant D' that contains $\mathcal{O}$ with index u, then $D = u^2 D'$ and $4q = t^2 - u^2 v^2 D'$, so q is also the norm of a prime ideal in $\mathcal{O}_{L'}$, where L' is the ring class field of $\mathcal{O}'$, and we have $q \perp \mathcal{O}'$, since $D' | D$. This implies that $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_q)$ is nonempty and has cardinality $h(D')$, by the same argument used above for $\mathcal{O}$. □

Corollary 23.7. *Let $E/\mathbb{F}_q$ be an elliptic curve with CM by an order $\mathcal{O}$ of discriminant $D \perp q$ in an imaginary quadratic field K, and let $\ell \nmid q$ be prime. Then E admits $1 - \left(\frac{D}{\ell}\right)$ horizontal ℓ-isogenies and one or zero ascending ℓ-isogenies, depending on whether $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ or not. The number of descending ℓ-isogenies admitted by E over $\mathbb{F}_q$ is either zero or $\ell + \left(\frac{D}{\ell}\right)$, depending on whether $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_q)$ is empty or not, where $\mathcal{O}'$ is the order of index ℓ in $\mathcal{O}$.*

Proof. This follows from Theorem 23.5, Lemma 23.6, and the Deuring lifting theorem (see Theorem 22.13). If $\varphi\colon E \to E'$ is an ℓ-isogeny of CM elliptic curves over $\mathbb{C}$ with $\mathrm{End}(E) = \mathcal{O}$ and $\mathrm{End}(E') = \mathcal{O}'$ and $\mathbb{F}_q$ is a finite field for which the sets $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ and $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_q)$ are both nonempty, then we can view $\varphi\colon E \to E'$ as an isogeny of elliptic curves L, where L the larger of the two ring class fields for $\mathcal{O}$ and $\mathcal{O}'$ (one must contain the other since either $\mathcal{O} \subseteq \mathcal{O}'$ or $\mathcal{O}' \subseteq \mathcal{O}$), and q the norm of a prime ideal $\mathfrak{q}$ in $\mathcal{O}_L$. We can use the reduction map $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{q} = \mathbb{F}_q$ to reduce integral equations for E, E', and φ modulo $\mathfrak{q}$ to obtain a corresponding ℓ-isogeny $\overline{\varphi}\colon \overline{E} \to \overline{E}'$ of elliptic curves over $\mathbb{F}_q$ with $\mathrm{End}(\overline{E}) = \mathrm{End}(E) = \mathcal{O}$, $\mathrm{End}(\overline{E}') = \mathrm{End}(E') = \mathcal{O}'$, and $\deg \overline{\varphi} = \deg \varphi = \ell$ (the degree of φ cannot change because $\ell \nmid q$, so $E[\ell] \simeq \overline{E}[\ell]$, which implies $\ker \varphi \simeq \ker \overline{\varphi}$, and $\overline{\varphi}$ must be separable).

Conversely, if $\overline{\varphi}\colon \overline{E} \to \overline{E}'$ is an ℓ-isogeny of elliptic curves over $\mathbb{F}_q$, we can lift $\overline{E}$ and $\overline{E}'$ to elliptic curves over L with $\mathrm{End}(E) = \mathrm{End}(\overline{E}) = \mathcal{O}$ and $\mathrm{End}(E') = \mathrm{End}(\overline{E}') = \mathcal{O}'$. There is then a corresponding ℓ-isogeny $\varphi\colon E \to E'$ whose kernel reduces to the kernel of $\overline{\varphi}$ (as above, the reduction map gives a bijection $E[\ell] \simeq \overline{E}[\ell]$ for $\ell \nmid q$). □

If $E/\mathbb{F}_q$ is an elliptic curve with CM by an imaginary quadratic order $\mathcal{O}$ and $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal, then as in Definition 18.12 we have an $\mathfrak{a}$-torsion subgroup

$$E[\mathfrak{a}] := \{P \in E(\overline{\mathbb{F}}_q) : \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

Provided the norm of $\mathfrak{a}$ is prime to q, there is a corresponding separable isogeny $\varphi_{\mathfrak{a}}\colon E \to E'$ with $\ker \varphi_{\mathfrak{a}} = E[\mathfrak{a}]$ and $\deg \varphi_{\mathfrak{a}} = \mathrm{N}\mathfrak{a}$ uniquely determined up to isomorphism, by Theorem 6.10. As in the proof above we can lift the isogeny $\varphi_{\mathfrak{a}}\colon E \to E'$ to a number field $L \subseteq \mathbb{C}$ where it corresponds to the CM action of $\mathrm{cl}(\mathcal{O})$, which implies that we must have $\mathrm{End}(E') = \mathrm{End}(E) = \mathcal{O}$; if $\mathrm{N}\mathfrak{a}$ is a prime ℓ this means that $\varphi_{\mathfrak{a}}$ is a horizontal ℓ-isogeny. By Theorem 21.11, every ideal class in $\mathrm{cl}(\mathcal{O})$ contains infinitely many ideals of prime norm, and in particular, an ideal whose norm is prime to q. This allows us to define the CM action of $\mathrm{cl}(\mathcal{O})$ on the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ in terms of horizontal ℓ-isogenies for various primes $\ell \nmid q$. As with the CM action on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$, the action of the inverse of an ideal $\mathfrak{a}$ is given by the dual isogeny $\hat{\varphi}_{\mathfrak{a}}$. We thus have the following corollary.

Corollary 23.8. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D and let $\mathbb{F}_q$ be a finite field with $q \perp D$. If the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is nonempty then it is a $\mathrm{cl}(\mathcal{O})$-torsor in which the action of the ideal class of any proper $\mathcal{O}$-ideal of prime norm $\ell \nmid q$ is given by a horizontal ℓ-isogeny, and the inverse of this action is given by the dual isogeny.*

Remark 23.9. As noted above, every ideal class in $\mathrm{cl}(\mathcal{O})$ contains infinitely many proper $\mathcal{O}$-ideals of prime norm ℓ. This means that if we want to compute the action of a given proper $\mathcal{O}$-ideal $\mathfrak{l}_1$ of prime norm ℓ_1, we can compute this action using any other proper $\mathcal{O}$-ideal $\mathfrak{l}_2$ of prime norm ℓ_2 that lies is in the same ideal class. This has many practical applications: when ℓ_1 is large it allows us to use a much smaller ℓ_2. Indeed, under the Generalized Riemann Hypothesis, we can always find a prime ℓ_2 bounded by $O(\log^2 |D|)$.

23.2 Isogeny volcanoes

Having determined the exact number of horizontal, ascending, and descending ℓ-isogenies that arise for an ordinary elliptic curve over a finite field, we can now completely determine the structure of the ordinary components of $G_\ell(\mathbb{F}_p)$. Figure 1 depicts a typical example.

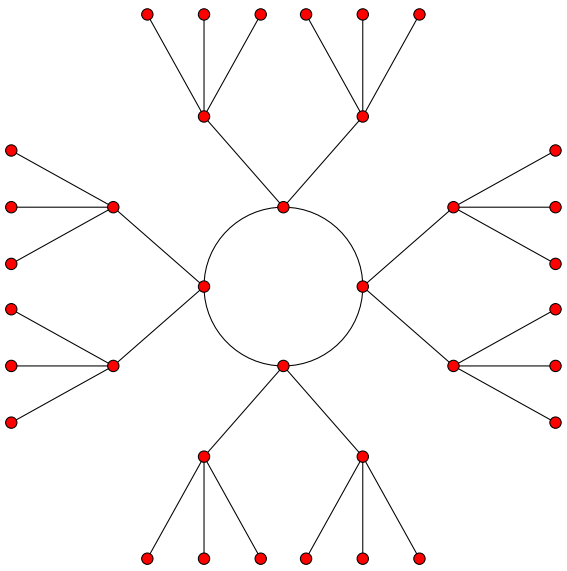

Figure 1: An ordinary component of $G_3(\mathbb{F}_p)$.

Figure 2 shows the same graph from a different perspective. With a bit of imagination, one can see the profile of a volcano: there is a crater formed by the cycle at the top, and the trees handing down from each edge form the sides of the volcano.

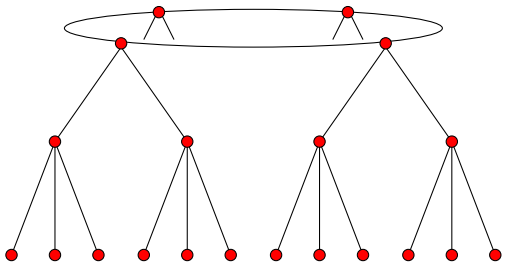

Figure 2: A 3-volcano of depth 2.

Definition 23.10. An *ℓ-volcano* V is a connected undirected graph whose vertices are partitioned into one or more *levels* $V_0, \dots, V_d$ such that the following hold:

1. The subgraph on V_0 (the *surface*) is a regular graph of degree at most 2.
2. For $i > 0$, each vertex in V_i has exactly one neighbor in level V_{i-1}, and this accounts for every edge not on the surface.
3. For $i < d$, each vertex in V_i has degree $\ell + 1$.

Level V_d is called the *floor* of the volcano; the floor and surface coincide when $d = 0$.

As with $G_\ell(k)$, an ℓ-volcano may have multiple edges and self-loops, but it is an undirected graph. If the surface of an ℓ-volcano has more than two vertices, it must be a simple cycle. Two vertices may be connected by 1 or 2 edges, and a single vertex may have 0, 1, or 2 self-loops. As an abstract graph, an ℓ-volcano is determined by the integers ℓ, d, $|V_0|$.

If we ignore components that contain the two exceptional j-invariants 0 and 1728, the ordinary components of $G_\ell(\mathbb{F}_p)$ are all ℓ-volcanoes. This was proved by David Kohel in his Ph.D. thesis [6], although the term "volcano" was coined later by Fouquet and Morain in [3].

Theorem 23.11 (Kohel)**.** *Let $\mathbb{F}_q$ be a finite field, let $\ell \nmid q$ be a prime, and let V be an ordinary component of $G_\ell(\mathbb{F}_q)$ that does not contain the j-invariants 0 or 1728. Then V is an ℓ-volcano for which the following hold:*

(i) *The vertices in level V_i all have the same endomorphism ring $\mathcal{O}_i$.*

(ii) *The subgraph on V_0 has degree $1 + \left(\frac{D_0}{\ell}\right)$, where $D_0 = \operatorname{disc}(\mathcal{O}_0)$.*

(iii) *If $\left(\frac{D_0}{\ell}\right) \geq 0$, then $|V_0|$ is the order of $[\mathfrak{l}]$ in $\operatorname{cl}(\mathcal{O}_0)$; otherwise $|V_0| = 1$.*

(iv) *The depth of V is d, where $4q = t^2 - \ell^{2d} v^2 D_0$ with $\ell \nmid v$, $t^2 = (\operatorname{tr} \pi_E)^2$, for $j(E) \in V$.*

(v) *$\ell \nmid [\mathcal{O}_K : \mathcal{O}_0]$ and $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$ for $0 \leq i < d$.*

Proof. Let V be an ordinary component of $G_\ell(\mathbb{F}_q)$ that does not contain 0 or 1728. The only automorphisms admitted by elliptic curves E with $j(E) \neq 0, 1728$ are $\pm 1 \in \operatorname{End}(E)$, thus as explained in Remark 23.2, every edge (j_1, j_2) in V occurs with the same multiplicity as the edge (j_2, j_1), allowing us to view V as an undirected graph.

Since V is an ordinary component, every vertex is the j-invariant of an ordinary elliptic curves whose endomorphism ring is an order $\mathcal{O}$ in an imaginary quadratic field, by Corollary 14.19. It follows from Theorem 23.3 that the order $\mathcal{O}$ arising for elliptic curves with $j(E) \in V$ all lie in the same quadratic field K and differ only in the ℓ-adic valuation ν_ℓ of the conductor of $[\mathcal{O}_K : \mathcal{O}]$. By Corollary 23.7, every $j(E) \in V$ for which $\mathrm{End}(E) = \mathcal{O}$ has conductor divisible by ℓ admits an ascending ℓ-isogeny, and it follows that we can partition V into levels $V_0, \dots, V_d$ with $j(E) \in V_i$ if and only if $v_\ell([\mathcal{O}_K : \mathcal{O}]) = i$; the set V is finite so d is bounded; this proves (i) and (v), and Corollary 23.7 also implies (ii) and that V is an ℓ-volcano as claimed.

If $\left(\frac{D_0}{\ell}\right) = -1$ then V_0 has degree 0 and we must have $|V_0| = 1$. Otherwise there exists a proper $\mathcal{O}_0$-ideal $\mathfrak{l}$ of norm ℓ, and its ideal class $[\mathfrak{l}] \in \mathrm{cl}(\mathcal{O})$ acts on V_0 via horizontal ℓ-isogenies, by Corollary 23.8. This proves (iii).

Part (iv) follows from Theorem 22.5 and Remark 22.11. If $4q = t^2 - v^2\ell^{2d}D_0$ with $\ell \nmid v$, then the sets $\mathrm{Ell}_{\mathcal{O}_i}(k)$ must be non-empty for $0 \le i \le d$, but the set $\mathrm{Ell}_{\mathcal{O}_{d+1}}(k)$ must be empty since ℓ^{d+1} does not divide v. □

Remark 23.12. Theorem 23.11 can be extended to the case where V contains 0 or 1728 following Remark 23.2. Parts (i)-(v) still hold, the only necessary modification is the claim that V is an ℓ-volcano. When V contains 0, if V_1 is non-empty then it contains $\frac{1}{3}(\ell - \left(\frac{-3}{\ell}\right))$ vertices, and each vertex in V_1 has three incoming edges from 0 but only one outgoing edge to 0. When V contains 1728, if V_1 is non-empty then it contains $\frac{1}{2}(\ell - \left(\frac{-1}{\ell}\right))$ vertices, and each vertex in V_1 has two incoming edges from 1728 but only one outgoing edge to 1728. This 3-to-1 (resp. 2-to-1) discrepancy arises from the action of $\mathrm{Aut}(E)$ on the cyclic subgroups of $E[\ell]$ when $j(E) = 0$ (resp. 1728). Otherwise, V satisfies all the requirements of an ℓ-volcano, and most of the algorithms designed for ℓ-volcanoes work just as well on ordinary components of $G_\ell(\mathbb{F}_q)$ that contain 0 or 1728.

23.3 Finding the floor

The vertices that lie on the floor of an ℓ-volcano V are distinguished by their degree.

Lemma 23.13. *Let v be a vertex in an ordinary component V of depth d in $G_\ell(\mathbb{F}_q)$. Either $\deg v \le 2$ and $v \in V_d$, or $\deg v = \ell + 1$ and $v \notin V_d$.*

Proof. If $d = 0$ then $V = V_0 = V_d$ is a regular graph of degree at most 2 and $v \in V_d$. Otherwise, either $v \in V_d$ and v has degree 1, or $v \notin V_d$ and v has degree $\ell + 1$. □

Given an arbitrary vertex $v \in V$, we would like to find a vertex on the floor of V. Our strategy is very simple: if $v_0 = j(E)$ is not already on the floor then we will construct a random path from v_0 to a vertex v_s on the floor. By a *path*, we mean a sequence of vertices $v_0, v_1, \dots, v_s$ such that each pair (v_{i-1}, v_i) is an edge and $v_i \ne v_{i-2}$ (no backtracking).

Algorithm FindFloor
Given an ordinary vertex $v_0 \in G_\ell(\mathbb{F}_q)$, find a vertex on the floor of its component.

1. If $\deg v_0 \le 2$ then output v_0 and terminate.
2. Pick a random neighbor v_1 of v_0 and set $s \leftarrow 1$.
3. While $\deg v_s > 1$: pick a random neighbor $v_{s+1} \ne v_{s-1}$ of v_s and increment s.
4. Output v_s.

Remark 23.14 (**Removing known roots**). As a minor optimization, rather than picking v_{s+1} as a root of $\phi(Y) = \Phi_\ell(v_s, Y)$ in step 3 of the FindFloor algorithm, we may use $\phi(Y)/(Y - v_{s-1})^e$, where e is the multiplicity of v_{s-1} as a root of $\phi(Y)$. This is slightly faster and eliminates the need to check that $v_{s+1} \neq v_{s-1}$.

Notice that once FindFloor picks a descending edge (one leading closer to the floor), every subsequent edge must also be descending, because it is not allowed to backtrack along the single ascending edge and there are no horizontal edges below the surface. It follows that the expected length of the path chosen by FindFloor is $\delta + O(1)$, where δ is the distance from v_0 to the floor along a shortest path. With a bit more effort we can find a path of exactly length δ, a shortest path to the floor. The key to doing so is observe that all but at most two of the $\ell + 1$ edges incident to any vertex above the floor must be descending edges. Thus if we construct *three* random paths from v_0 that all start with a different initial edge, then one of the initial edges must be a descending edge, which necessarily leads to a shortest path to the floor.

Algorithm FindShortestPathToFloor
Given an ordinary $v_0 \in G_\ell(\mathbb{F}_q)$, find a shortest path to the floor of its component.

1. Let $v_0 = j(E)$. If $\deg v_0 \leq 2$ then output v_0 and terminate.
2. Pick three neighbors of v_0 and extend paths from each of these neighbors in parallel, stopping as soon as any of them reaches the floor.[1]
3. Output a path that reached the floor.

The main virtue of FindShortestPathToFloor is that it allows us to compute δ, which tells us the level $V_{d-\delta}$ of $j(E)$ relative to the floor V_d. It effectively gives us an "altimeter" $\delta(v)$ that we may be used to navigate V. We can determine whether a given edge (v_1, v_2) is horizontal, ascending, or descending, by comparing $\delta(v_1)$ to $\delta(v_2)$, and we can determine the exact level of any vertex.[2]

There are many practical applications of isogeny volcanoes, some of which you will explore on Problem Set 12. See the survey paper [8] for further details and references.

References

[1] R. Bröker, K. Lauter, and A.V. Sutherland, *Modular polynomials via isogeny volcanoes*, Mathematics of Computation **81**, 2012, 1201–1231.

[2] D.A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Wiley, 1989.

[3] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, Algorithmic Number Theory Fifth International Symposium (ANTS V), LNCS **2369**, Spring 2002, 276–291.

[4] S. Ionica and A. Joux, *Pairing the volcano*, Mathematics of Computation **82** (2013), 581–603.

[1] If v_0 does not have three distinct neighbors then just pick all of them.

[2] A more sophisticated approach that uses the Weil pairing (to be discussed in Lecture 24) can be found in [4]; the pairing based approach is more efficient when d is large, but in practice d is usually small.

[5] S. Lang, *Elliptic functions*, second edition, Springer, 1987.

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

[7] J. H. Silverman, *The arithmetic of elliptic curves*, second edition, Springer, 2009.

[8] A.V. Sutherland, *Isogeny volcanoes*, Algorithmic Number Theory 10th International Symposium (ANTS X), Open Book Series **1**, MSP 2013, 507–530.

18.783 Elliptic Curves
Spring 2017