23 Isogeny volcanoes

We now want to shift our focus away from elliptic curves over $\mathbb{C}$ and consider elliptic curves E/k defined over any field k; in particular, finite fields $k = \mathbb{F}_p$. In Lecture 21 we noted (but did not prove) that the moduli interpretation of the modular polynomial $X_0(N)$ as parameterizing cyclic isogenies of degree N is valid over any field. Thus we can 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 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. This motivates the following definition.

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 21.5, if $j_1 = j(E_1)$ and $j_2 = j(E_2)$ are 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 ℓ-isogenies from E_1 to E_2 that are inequivalent (with different kernels). 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, and 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, distinct from ± 1 (here we are using ρ and i both to denote elements of the endomorphism ring and roots of unity in $\bar{k}$). The automorphism -1 does not pose a problem because every elliptic curve has this automorphism, so for any ℓ-isogeny $\varphi\colon E_1 \to E_2$ the isogeny $\varphi \circ [-1] = [-1] \circ \varphi$ is isomorphic to φ (it is a separable isogeny with the same kernel, equivalently, it is obtained by post-composing φ with an isomorphism). But if E_1 has j-invariant 0 but E_2 does not then we cannot write $\varphi \circ \rho = \rho \circ \varphi$ and the isogenies φ and $\varphi \circ \rho$ are truly distinct; their kernels are two different subgroups of $E[\ell]$. However, the inequivalent isogenies $\varphi, \varphi \circ \rho, \varphi \circ \rho^2$ all have equivalent dual-isogenies: the isogeny $\hat{\varphi}\colon E_2 \to E_1$ is equivalent to $\hat{\rho} \circ \hat{\varphi}$ and $\hat{\rho}^2 \circ \varphi$ since it can be obtained by composing $\hat{\varphi}\colon E_2 \to E_1$ with an automorphism of E_1 (notice that the three dual isogenies all do 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 E_1 has j-invariant 1728 but E_2 does not is similar, except now $(j(E_1), j(E_2)$ has multiplicity 2.

Our objective in this lecture is to gain a better understanding the structure of the graph $G_\ell(k)$, at least 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). Since the endomorphism algebra is preserved by isogenies (Theorem 13.8), we know that $G_\ell(\mathbb{F}_q)$ can be partitioned into ordinary and supersingular components.[1] Since most elliptic curves are ordinary, we will focus on the ordinary components; you may explore the supersingular components on Problem Set 12.

23.1 Isogenies between elliptic curves with complex multiplication

Let E/k 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 not equal to the characteristic of k.[2] We have in mind the case where k is a finite field, but most of the theory applies more generally, so we will work in this setting. As noted above, the endomorphism algebra $\mathrm{End}^0(E) \simeq K$ is an isogeny invariant, so if $\varphi\colon E \to E'$ is an ℓ-isogeny then E' also has CM by an order $\mathcal{O}'$ in the imaginary quadratic field K. It is not necessarily the case that $\mathcal{O}'$ and $\mathcal{O}$ are the same, but the following theorem shows that they are closely related.

Theorem 23.3. *Let E/k be an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K, and suppose that there exists an isogeny $\varphi\colon E \to E'$ of prime degree ℓ. Then E' has CM by an order $\mathcal{O}'$ in K, and 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 $\hat{\phi}\colon E' \to E$ denote the dual isogeny For any $\tau \in \mathrm{End}(E)$, the composition $\varphi \circ \tau \circ \hat{\varphi}\colon E' \to E'$ is an isogeny from E' to itself, hence an element of $\mathrm{End}(E')$. Conversely, for any $\tau' \in \mathrm{End}(E')$, the composition $\hat{\varphi} \circ \tau' \circ \varphi\colon E \to E$ is an element of $\mathrm{End}(E)$. Thus the endomorphism algebras $\mathrm{End}^0(E)$ and $\mathrm{End}^0(E')$ are the same (as already noted), so E' has CM by an order $\mathcal{O}'$ in K. Furthermore, if $\mathcal{O} = [1, \tau]$ and $\mathcal{O} = [1, \tau']$, then $\varphi \circ \tau \circ \hat{\varphi}$ corresponds to $\ell\tau \in \mathcal{O}'$, since $\varphi \circ \hat{\varphi} = \ell$, and similarly, $\hat{\varphi} \circ \tau \circ \varphi$ corresponds to $\ell\tau' \in \mathcal{O}$.[3]

It follows that $[1, \ell\tau] \subseteq \mathcal{O}'$ and $[1, \ell\tau'] \subseteq \mathcal{O}$. We thus have

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

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. We use the following terminology to distinguish the three possibilities for the ℓ-isogeny $\varphi\colon E \to E'$ of Theorem 23.3:

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

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

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

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

[1] In fact there is only one supersingular component, but we won't prove this.

[2] Note that K and k are unrelated: k is the field over which the elliptic curve is defined, while $K \simeq \mathrm{End}^0(E)$ is the endomorphism algebra of the elliptic curve, which is by definition a $\mathbb{Q}$-algebra, no matter what k is.

[3] By "correspond" we mean that they are identical as abstract elements of the field $\mathrm{End}^0(E) \simeq K$.

Horizontal ℓ-isogenies correspond to the CM action of a proper (invertible) $\mathcal{O}$-ideal of norm ℓ. For elliptic curves over $\mathbb{C}$ we proved that each proper $\mathcal{O}$-ideal $\mathfrak{a}$ induces a separable isogeny $\varphi_{\mathfrak{a}}$ of degree $\mathrm{N}\mathfrak{a}$ with kernel

$$E[\mathfrak{a}] := \{P \in E(\bar{k}) : \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

The definition of $E[\mathfrak{a}]$ makes sense over any field; the $\mathcal{O}$-ideal $\mathfrak{a}$ is a subset of $\mathrm{End}(E) \simeq \mathcal{O}$, and each endomorphism $\alpha \in \mathfrak{a}$ corresponds to a rational map with coefficients in $\bar{k}$ that we can apply to any point $P \in E(\bar{k})$. So long as $N\mathfrak{a}$ is not divisible by the characteristic k, we can define $\varphi_{\mathfrak{a}} \colon E \to E'$ to be the separable isogeny with kernel $E[\mathfrak{a}]$ given by Theorem 6.8, which is unique up to isomorphism.

Let us now consider the case where $\mathrm{N}\mathfrak{a} = \ell$. If we restrict $\varphi_{\mathfrak{a}} \colon E \to E'$ to the finite group $E[\overline{a}]$, we get a bijection whose image is the kernel of the dual isogeny $\hat{\varphi}_{\mathfrak{a}}$. The set

$$I_{\varphi_{\mathfrak{a}}(E[\overline{\mathfrak{a}}])} := \{\alpha \in \mathcal{O}' : \alpha(P) = 0 \text{ for all } P \in \varphi_{\mathfrak{a}}(E[\overline{\mathfrak{a}}])\}$$

is then a proper $\mathcal{O}'$-ideal of norm ℓ, which implies that $\mathcal{O}' = \mathcal{O}$, and in fact $I_{\ker \hat{\varphi}_{\mathfrak{a}}} = \overline{\mathfrak{a}}$, so $\hat{\varphi}_{\mathfrak{a}} \colon E' \to E$ is the same as the isogeny $\varphi_{\overline{a}} \colon E' \to E$ induced by $\overline{\mathfrak{a}}$. Thus the CM action of a proper $\mathcal{O}$-ideal of norm ℓ corresponds to a horizontal ℓ-isogeny.

Conversely, if $\varphi \colon E \to E'$ is a horizontal ℓ-isogeny then the set

$$I_{\ker \varphi} := \{\alpha \in \mathcal{O} : \alpha(P) = 0 \text{ for all } P \in \ker \varphi\}$$

is a proper $\mathcal{O}$-ideal $\mathfrak{a}$ of norm ℓ and we have $\varphi = \varphi_{\mathfrak{a}}$.

Lemma 23.5. *Let E/k be an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K and let $\ell \neq \mathrm{char}(k)$ be prime. If ℓ divides $[\mathcal{O}_K : \mathcal{O}]$ then there are no horizontal ℓ-isogenies from E, and otherwise the number of horizontal ℓ-isogenies is $1 + \left(\frac{D}{\ell}\right) \in \{0, 1, 2\}$, where $D = \mathrm{disc}(\mathcal{O})$.*

Proof. Let $\mathcal{O}_K = [1, \tau]$. If ℓ divides $[\mathcal{O}_K : \mathcal{O}]$ then $\mathcal{O} = [1, \ell n\tau]$ for some $n \in \mathbb{Z}_{>0}$. By Lemma 21.2, the index-ℓ sublattices of $\mathcal{O}$ are $[1, \ell^2 n\tau]$, which is not an ideal, and those of the form $L_i = [\ell, \ell n\tau + i]$ for some $0 \leq i < \ell$. If L_i is an ideal then it must be closed under multiplication by $\ell n\tau$, which implies $i = 0$, but then L_i is also closed under multiplication by $n\tau \notin \mathcal{O}$ and cannot possibly be a proper $\mathcal{O}$-ideal, by Definition 17.6.

We now assume ℓ does not divide $[\mathcal{O}_K : \mathcal{O}]$. Each $\mathcal{O}_K$-ideal $\mathfrak{a}$ of norm ℓ corresponds to an $\mathcal{O}$-ideal $\mathfrak{a} \cap \mathcal{O}$ of norm ℓ (since $[\mathcal{O}_K : \mathfrak{a}] = \ell$ is prime to $[\mathcal{O}_K : \mathcal{O}]$), and this is $\mathcal{O}$-ideal is invertible, hence proper, since the fractional $\mathcal{O}$-ideal $\frac{1}{\ell}(\overline{\mathfrak{a}} \cap \mathcal{O})$ is its inverse (the key point is that $\ell\mathcal{O}_K \cap \mathcal{O} = \ell\mathcal{O}$ because $[\mathcal{O}_K : \mathcal{O}]$ is prime to ℓ). Conversely, if $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal of norm ℓ , then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal of norm ℓ. Thus in the number of proper $\mathcal{O}$-ideals of norm ℓ is simply the number of $\mathcal{O}_K$-ideals of norm ℓ, which is $1 + \left(\frac{D}{\ell}\right)$, by Lemma 22.5. □

In the previous lecture we proved that if $k = \mathbb{F}_p$ is a finite field with $4p = t^2 - v^2 D$ and $t \not\equiv 0 \bmod p$ then the polynomial $H_D(X)$ then splits into distinct linear factors in $\mathbb{F}_p[X]$, and its roots are the reductions of j-invariants of elliptic curves $\hat{E}$ defined over the ring class field $L = K_{\mathcal{O}}$, where $\mathcal{O}$ is the imaginary quadratic order with discriminant D (recall that $j(\hat{E})$ is an algebraic integer, hence an element of $\mathcal{O}_L$, and the reduction map sends elements of $\mathcal{O}_L$ to their image in $\mathcal{O}_L/\mathfrak{q} \simeq \mathbb{F}_p$, where $\mathfrak{q}$ is a prime $\mathcal{O}_L$-ideal or norm p dividing $p\mathcal{O}_L$).

It is not difficult to show that the corresponding elliptic curve $E/\mathbb{F}_p$ obtained by reducing an integral Weierstrass equation for $\hat{E}$ modulo $\mathfrak{q}$ must have $\mathcal{O} \subseteq \mathrm{End}(E)$; each

endomorphism of $\hat{E}$ can be written as a rational map with coefficients in $\mathcal{O}_L$ that we can reduce modulo $\mathfrak{q}$. It takes a bit more work to show $\mathcal{O} = \mathrm{End}(E)$, but this can be done. Moreover, this accounts for all the elliptic curves over $\mathbb{F}_p$ that have CM by $\mathcal{O}$. This is a consequence of the *Deuring lifting theorem* and related results (see Theorems 12, 13, and 14 in [6, §13]), which we will not take the time to prove.

We should note that this does not apply when p is not of the form $4p = t^2 - v^2 D$; in this case there cannot be any elliptic curves defined over $\mathbb{F}_p$ with CM by $\mathcal{O}$. To see this, note that if $E/\mathbb{F}_p$ has CM by $\mathcal{O}$ then the Frobenius endomorphism has the form

$$\pi = \frac{t \pm v\sqrt{D}}{2} \in \mathcal{O} \simeq \mathrm{End}(E),$$

for some integer v, with $t = \operatorname{tr}\pi \not\equiv 0 \bmod p$. We have $p = \mathrm{N}\pi = \pi\overline{\pi}$, so

$$4p = 4\pi\overline{\pi} = t^2 - v^2 D.$$

Moreover, we must have $t \not\equiv 0 \bmod p$ because E is not supersingular.

Remark 23.6. It can happen that $H_D(X)$ has roots in $\mathbb{F}_p$ even when p is not of the form $4p = t^2 - v^2 D$, but by the argument above, these roots cannot be j-invariants of elliptic curves with CM by $\mathcal{O}$. This cannot happen $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits in K (which occurs exactly when $\left(\frac{D}{p}\right) = 1$), because L/K is Galois and the residue field extensions $\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}$ all have the same degree (so $H_D \bmod p$ either has no roots at all or splits completely). But $L/\mathbb{Q}$ is typically not Galois and if p is inert in K then we can easily have H_D with roots modulo p; this is one way to construct supersingular curves; see [1].

It follows from our discussion that for any prime p the set

$$\mathrm{Ell}_\mathcal{O}(\mathbb{F}_p) := \{E/\mathbb{F}_p : \mathrm{End}(E) \simeq \mathcal{O}\}$$

is either empty or has cardinality equal to the class number $h(\mathcal{O})$.

Having determined the number of horizontal ℓ-isogenies that an elliptic curve E/k with CM by $\mathcal{O}$ can have in Lemma 23.5, we would now like to determine the number of ascending and descending ℓ-isogenies E can have, at least in the case that $k = \mathbb{F}_p$ is a finite field. In the proof of Lemma 23.5 we used the fact that the map that sends a proper $\mathcal{O}$-ideal $\mathfrak{a}$ to the $\mathcal{O}_K$-ideal $\mathfrak{a}\mathcal{O}$ is norm-preserving and surjective in the sense that every $\mathcal{O}_K$-ideal $\mathfrak{a}$ with norm prime to $[\mathcal{O}_K : \mathcal{O}]$ is in its image. It also commutes with multiplication of invertible ideals and induces a surjective group homomorphism of ideal class groups. This holds more generally if we replace $\mathcal{O}_K$ by any order $\mathcal{O}'$ containing $\mathcal{O}$. If $\mathcal{O} \subseteq \mathcal{O}'$ then we always have a surjective group homomorphism

$$\psi\colon \mathrm{cl}(\mathcal{O}) \twoheadrightarrow \mathrm{cl}(\mathcal{O}')$$

that is induced by the norm-preserving map $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}'$ defined on invertible ideals. If we are working in a finite field $\mathbb{F}_p$ with $4p = t^2 - v^2 D$, where $D = \mathrm{disc}(\mathcal{O})$, then the sets $\mathrm{Ell}_\mathcal{O}(\mathbb{F}_p)$ and $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$ are both nonempty, since we can also write $4p = t^2 - v^2 f^2 D'$, where $f = [\mathcal{O}' : \mathcal{O}]$. These sets are torsors for the corresponding class groups $\mathrm{cl}(\mathcal{O})$ and $\mathrm{cl}(\mathcal{O}')$, and it is natural to ask if there is a surjective map of sets $\mathrm{Ell}_\mathcal{O}(\mathbb{F}_p) \twoheadrightarrow Ell_{\mathcal{O}'}(\mathbb{F}_p)$ corresponding to ψ that can be realized via isogenies. In terms of the case $[\mathcal{O}' : \mathcal{O}] = \ell$ that we are interested in, these will be ascending isogenies.

Given an elliptic curve E with CM by $\mathcal{O}$ with index ℓ in $\mathcal{O}'$ there is a natural candidate for an ascending isogeny to a curve E' with CM by $\mathcal{O}'$. If we put $\mathcal{O}' = [1, \tau]$ and $\mathcal{O} = [1, \ell\tau]$ then $\mathfrak{a} = [\ell, \ell\tau]$ is an $\mathcal{O}$-ideal of norm ℓ (it is the intersection of $\ell\mathcal{O}$ with $\mathcal{O}'$), but as noted in the proof of Lemma 23.5, it is not a proper $\mathcal{O}$-ideal so it does not correspond to the CM action of a class in $\mathrm{cl}(\mathcal{O})$. Nevertheless, the $\mathfrak{a}$-torsion subgroup $E[\mathfrak{a}]$ is an order-ℓ subgroup of $E[\ell]$ and there is a corresponding separable isogeny $\varphi_{\mathfrak{a}}$ with kernel $E[\mathfrak{a}]$ whose image is an elliptic curve E' with CM by $\mathcal{O}'$. Rather than prove this directly, we are going to use a simpler combinatorial argument to show that every elliptic curve E with CM by $\mathcal{O}$ admits a unique ascending isogeny to an elliptic curve E' with CM by $\mathcal{O}'$, which will tell us everything we need to know. In order to apply our combinatorial argument we need to know the cardinality of $\ker \psi$, which is just the ratio of the class numbers $h(\mathcal{O})/h(\mathcal{O}')$. This ratio is given by the following lemma.

Lemma 23.7. *Let ℓ be a prime, let $\mathcal{O}$ be an index-ℓ suborder of an imaginary quadratic order $\mathcal{O}'$ of discriminant $D' < -4$. Then*

$$\frac{h(\mathcal{O})}{h(\mathcal{O}')} = \ell - \left(\frac{D'}{\ell}\right) \tag{1}$$

Proof. This follows directly from [3, Thm. 7.24]. □

Remark 23.8. To handle $D' = -3, -4$ one needs to include a correction factor to account for the fact that in these cases $\mathcal{O}'$ has a larger unit group than $\mathcal{O}$; this corresponds to the difference in the multiplicities of the edges of the ℓ-isogeny graph incident to j-invariants 0 and 1728 (with CM by the orders of discriminant -3 and -4, respectively). Divide the RHS of (1) by 3 when $D' = 3$ and by 2 when $D' = -4$.

Theorem 23.9. *Let $E/\mathbb{F}_p$ be an elliptic curve with CM by an imaginary quadratic order $\mathcal{O}$ that is an index-ℓ suborder of $\mathcal{O}'$, with $D' = \mathrm{disc}(\mathcal{O}') < -4$ and $\ell \neq \mathrm{char}(k)$ prime. Up to isomorphism, there is a unique ℓ-isogeny from E to an elliptic curve $E'/\mathbb{F}_p$ with CM by $\mathcal{O}$.*

Proof. The existence of $E/\mathbb{F}_p$ implies that $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ is non-empty, hence has cardinality $h(\mathcal{O})$, and we must have

$$4p = t^2 - v^2 D = t^2 - v^2\ell^2 D',$$

where $t = \mathrm{tr}\,\pi_E$ is the trace of the Frobenius endomorphism of E. Thus $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$ is also non-empty and has cardinality $h(\mathcal{O}')$, and the same argument applies to any order that contains $\mathcal{O}$. For each $j(E') \in \mathrm{Ell}_{\mathcal{O}'}$ every ℓ-isogeny $E' \to E''$ leads to an elliptic curve that has CM by $\mathcal{O}$, $\mathcal{O}'$ or an order that contains $\mathcal{O}'$ with index ℓ, and every such curve is defined over $\mathbb{F}_p$. It follows that the polynomial $\Phi_\ell(j(E'), Y) \in \mathbb{F}_p[Y]$ has $\ell + 1$ roots corresponding to $\ell + 1$ distinct ℓ-isogenies.

We proceed by induction on the power of ℓ dividing $[\mathcal{O}_K : \mathcal{O}']$. In the base case ℓ does not divide $[\mathcal{O}_K : \mathcal{O}']$ and none of the elliptic curves E' with CM by $\mathcal{O}'$ have any ascending ℓ-isogenies, and each has exactly $1 + \left(\frac{D'}{\ell}\right)$ horizontal ℓ-isogenies. This implies that there are $\ell - \left(\frac{D'}{\ell}\right) > 0$ descending ℓ-isogenies for each E', a total of

$$\left(\ell - \left(\frac{D'}{\ell}\right)\right) h(\mathcal{O}') \tag{2}$$

descending ℓ-isogenies in all.

So let $E_1' \to E_1$ be one of these descending ℓ-isogenies, with E_1' and E_1 twisted so that $\operatorname{tr}\pi_{E_1} = \operatorname{tr}\pi_{E_1'} = t$ (as opposed to $-t$), and let $\phi_1 \colon E_1 \to E_1'$ be the dual isogeny, which we note is an ascending ℓ-iosgeny. Now choose a proper $\mathcal{O}$-ideal $\mathfrak{a}$ of prime norm distinct from ℓ and p for which $\varphi_{\mathfrak{a}} \colon E_1 \to E$ is a horizontal isogeny corresponding to the CM action of $\mathfrak{a}$ on E_1; this is possible because $j(E_1)$ and $j(E)$ are elements of the $\operatorname{cl}(\mathcal{O})$-torsor $\operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_p)$. Let $\mathfrak{a}' = \mathfrak{a}\mathcal{O}'$ be the corresponding proper $\mathcal{O}'$-ideal and let $\varphi_{\mathfrak{a}'} \colon E_1' \to E'$ be the horizontal isogeny corresponding to the CM action of $\mathfrak{a}'$ on E_1'. We then have a commutative diagram of isogenies

$$\begin{array}{ccc} E_1' & \xrightarrow{\varphi_{\mathfrak{a}'}} & E' \\ \uparrow{\scriptstyle \phi_1} & & \uparrow{\scriptstyle \phi} \\ E_1 & \xrightarrow{\varphi_{\mathfrak{a}}} & E \end{array}$$

in which ϕ is the separable isogeny defined (up to isomorphism) by

$$\ker \phi := \varphi_{\mathfrak{a}}(\ker(\varphi_{\mathfrak{a}'}(\phi_1)).$$

We then have

$$\deg \varphi_{\mathfrak{a}} \deg \phi = \deg \phi_1 \deg \varphi_{\mathfrak{a}}$$

and

$$\deg \varphi_{\mathfrak{a}} = \mathrm{N}\mathfrak{a} = \mathrm{N}\mathfrak{a}' = \deg_{\varphi_{\mathfrak{a}}},$$

so $\deg \phi = \deg \phi_1 = \ell$. Thus ϕ is an ascending ℓ-isogeny. This argument did not depend on any property of E other than that it has CM by $\mathcal{O}$. It follows that every elliptic curve $E/\mathbb{F}_p$ with CM by $\mathcal{O}$ admits an ascending ℓ-isogeny, and by Lemma 23.7 there are

$$h(\mathcal{O}) = \left(\ell - \left(\frac{D'}{\ell}\right)\right) h(\mathcal{O}')$$

such $E/\mathbb{F}_p$ with distinct j-invariants $j(E) \in \operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_p)$. But the RHS above is exactly the total number of descending ℓ-isogenies from elliptic curves $E'/\mathbb{F}_p$ with CM by $\mathcal{O}'$ given by (2). It follows that each elliptic curve $E/\mathbb{F}_p$ with CM by $\mathcal{O}$ has exactly one ascending ℓ-isogeny to a curve $E'/\mathbb{F}_p$ with CM by $\mathcal{O}'$.

This completes the proof of the base case, and the inductive step is essentially the same. Now $[\mathcal{O}_K : \mathcal{O}']$ is divisible by ℓ so there are no horizontal ℓ-isogenies between elliptic curves $E'/\mathbb{F}_p$ with CM by $\mathcal{O}'$, and each admits exactly one ascending ℓ-isogeny (by the inductive hypothesis), and therefore admits exactly $\ell = \ell - \left(\frac{D'}{\ell}\right)$ descending ℓ-isogenies (note that ℓ now divides D'). Thus there are again a total of $(\ell - \left(\frac{D'}{\ell}\right))h(\mathcal{O}')$ descending ℓ-isogenies and this matches the cardinality of $\operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_p)$, so each elliptic curve $E/\mathbb{F}_p$ with CM by $\mathcal{O}$ admits exactly one ascending ℓ-iosogeny. □

Remark 23.10. The theorem above holds for any finite field $\mathbb{F}_q$ and the proof is the same.

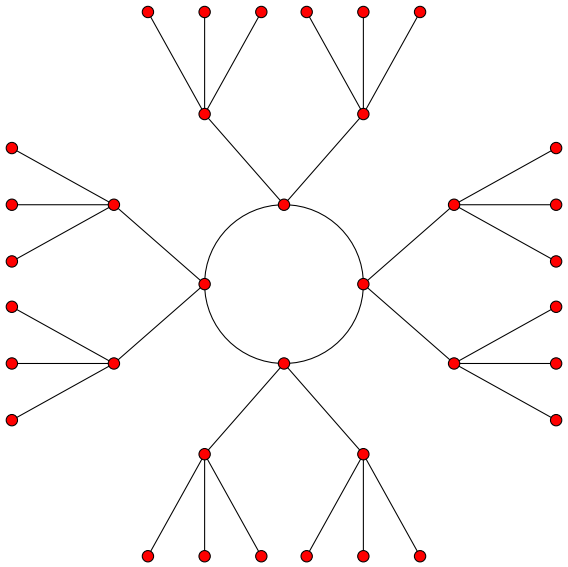

Figure 1: An ordinary component of $G_3(\mathbb{F}_p)$.

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 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.

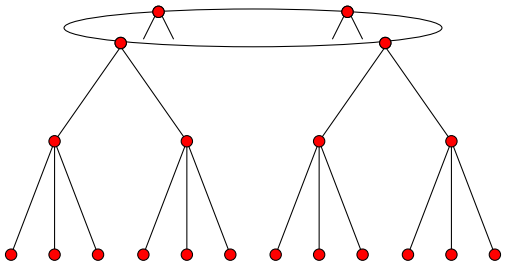

Figure 2: A 3-volcano of depth 2.

Definition 23.11. An *ℓ-volcano* V is a connected undirected graph whose vertices are partitioned into one or more *levels* $V_0, \ldots, V_d$ 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 $G_\ell(K)$, we allow multiple edges and self-loops, but now we work with an undirected graph. Note that if the surface of an ℓ-volcano has more than two vertices, it must be a simple cycle. Two vertices may be connected by one or two edges, and a single vertex may have 0, 1, or 2 self-loops. Note that, as an abstract graph, an ℓ-volcano is completely determined by the integers ℓ, d, and $|V_0|$.

Remarkably, if we ignore the 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 PhD thesis.[4]

Theorem 23.12 (**Kohel**). *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 $4p = t^2 - \ell^{2d} v^2 D_0$ with $\ell \perp v D_0$, $t^2 = (\operatorname{tr} \pi_E)^2$ 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. The theorem follows easily from the results we have already proved. Let V be an ordinary component of $G_\ell(\mathbb{F}_q)$ that does not contain 0 or 1728. Then, as previously noted, V is bi-directed and can be viewed as an undirected graph. It follows from Theorem 23.3 that every vertex of V corresponds to an elliptic curve with CM by an order $\mathcal{O}$ in the same imaginary quadratic field K and that the orders $\mathcal{O}$ that occur differ only the power of ℓ that divides their conductor. Furthermore, if ℓ^d is the largest power of ℓ that divides the conductor of any of the orders $\mathcal{O}$, then we may partition V into levels $V_0, \ldots, V_d$ corresponding to orders $\mathcal{O}_0, \ldots, \mathcal{O}_d$ for which $\nu_\ell([\mathcal{O}_K : \mathcal{O}_i]) = \ell$, This addresses (i) and (v).

Parts (ii) and (iii) follow from Lemma 23.5 and the CM action of $\operatorname{cl}(\mathcal{O}_0)$, and part (iv) follows from Theorem 22.10 (which can be generalized to prime powers q): if we have $4q = t^2 - v^2 D_0$ then the sets $\operatorname{Ell}_{\mathcal{O}_i}(k)$ are all non-empty but the set $\operatorname{Ell}_{\mathcal{O}_{d+1}}(k)$ must be empty since ℓ^{d+1} does not divide v.

Finally, for $i > d$ every $v \in V_i$ must have degree $\ell + 1$, because the roots of $\Phi_\ell(v, Y)$ (which has degree $\ell + 1$) all lie in $\operatorname{Ell}_{O_i}(\mathbb{F}_q)$, $\operatorname{Ell}_{O_{i+1}}(\mathbb{F}_q)$, or, for $i > 0$, $\operatorname{Ell}_{O_{i-1}}(\mathbb{F}_q)$. This, together with (ii) and Theorem 23.3, proves that V is indeed an ℓ-volcano. □

Remark 23.13. Theorem 23.12 is easily extended to the case where V contains 0 or 1728, via 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 $\frac{1}{3}\left(\ell - \left(\frac{-3}{\ell}\right)\right)$ 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 $\frac{1}{2}\left(\ell - \left(\frac{-1}{\ell}\right)\right)$ 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 $\operatorname{Aut}(E)$ 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 ordinarycomponents of $G_\ell(\mathbb{F}_q)$ that contain 0 or 1728.

[4]The term "volcano" was not used by Kohel, it was introduced by Fouquet and Morain in [4].

23.3 Finding the floor

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

Lemma 23.14. *Let v be a vertex in an ordinary component V of depth d in $G_\ell(\mathbb{F}_q)$. Either $\deg v \leq 2$ 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 $v_0, v_1, \ldots, v_s$ such that each pair (v_{i-1}, v_i) is an edge and $v_i \neq v_{i-2}$ (no backtracking is allowed).

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 $\deg v_0 \leq 2$ 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 $v_{s+1} \neq v_{s-1}$ of v_s and increment s.
4. Output v_s.

Remark 23.15 (**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.[5]
3. Output a path that reached the floor.

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

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.[6]

There are many practical applications of isogeny volcanoes, some of which you will explore on Problem Set 12. See the survey paper [9] for further details and references.

References

[1] R. Bröker, *Constructing supersingular elliptic curves*, Journal of Combinatorics and Number Theory **1** (2009), 269–273.

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

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

[4] 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.

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

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

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

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

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

[6] An alternative approach based on the Weil pairing (to be discussed in Lecture 24) has recently been developed by Ionica and Joux [5], which is more efficient when d is large.

18.783 Elliptic Curves

Spring 2015