THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Isogeny volcanoes

Andrew V. Sutherland

msp

THE OPEN BOOK SERIES 1 (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.507

Isogeny volcanoes

Andrew V. Sutherland

The remarkable structure and computationally explicit form of isogeny graphs of elliptic curves over a finite field have made these graphs an important tool for computational number theorists and practitioners of elliptic curve cryptography. This expository paper recounts the theory behind isogeny graphs and examines several recently developed algorithms that realize substantial (and often dramatic) performance gains by exploiting this theory.

1. Introduction

A *volcano* is a certain type of graph, one whose shape reminds us of the geological formation of the same name. A typical volcano consists of a cycle with isomorphic balanced trees rooted at each vertex.

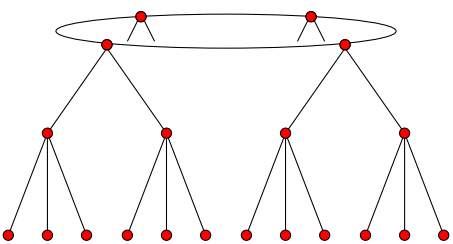

Figure 1. A volcano.

More formally, let ℓ be a prime. We define an ℓ-*volcano* as follows.

Definition 1. 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.

MSC2010: primary 11G07, 11Y16; secondary 11G15, 11G20.
Keywords: elliptic curves, isogeny graphs.

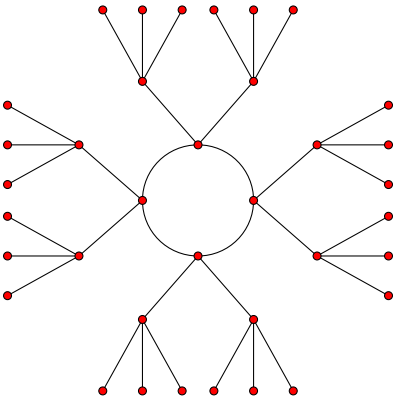

Figure 2. A 3-volcano of depth 2.

(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 $\ell + 1$.

Self-loops and multi-edges are permitted in an ℓ-volcano, but it follows from condition (2) that these can only occur on the surface. The integer d is the *depth* of the volcano (some authors use the term *height*). When $d = 0$ only condition (1) applies, and in this case V is a connected regular graph of degree at most 2. Such a graph is either a single vertex with up to two self-loops, two vertices connected by one or two edges, or a simple cycle on three or more vertices (the general case). Figure 2 gives an overhead view of the volcano depicted in Figure 1, a 3-volcano of depth 2.

We have defined volcanoes in purely graph-theoretic terms, but we are specifically interested in volcanoes that arise as components of graphs of isogenies between elliptic curves. Our first objective is to understand how and why volcanoes arise in such graphs. The definitive work in this area was done by David Kohel, whose thesis explicates the structure of isogeny graphs of elliptic curves over finite fields [30]. The term "volcano" came later, in work by Fouquet and Morain [16; 17] that popularized Kohel's work and gave one of the first examples of how isogeny volcanoes could be exploited by algorithms that work with elliptic curves.

This leads to our second objective: to show how isogeny volcanoes can be used to develop better algorithms. We illustrate this with four examples of algorithms that use isogeny volcanoes to solve some standard computational problems related to elliptic curves over finite fields. In each case, the isogeny volcano approach yields a substantial practical and asymptotic improvement over the best previous results.

2. Isogeny graphs of elliptic curves

We begin by recalling some basic facts about elliptic curves and isogenies, all of which can be found in standard references such as [31; 41; 42].

2.1. ***Elliptic curves.*** Let k be a field. An *elliptic curve* E/k is a smooth projective curve of genus 1 over k, together with a distinguished k-rational point 0. If k'/k is any field extension, the set $E(k')$ of k'-rational points of E forms an abelian group with 0 as its identity element. For convenience we assume that the characteristic of k is neither 2 nor 3, in which case every elliptic curve E/k can be written as the projective closure of a short Weierstrass equation of the form

$$Y^2 = X^3 + aX + b,$$

where the coefficients $a, b \in k$ satisfy $4a^3 + 27b^2 \neq 0$; here the distinguished point 0 is taken to be the "point at infinity" on the projective closure. Distinct Weierstrass equations may define isomorphic curves: The curves defined by $Y^2 = X^3 + a_1X + b_1$ and $Y^2 = X^3 + a_2X + b_2$ are isomorphic to one another over the algebraic closure $\bar{k}$ of k if and only if $a_2 = u^4a_1$ and $b_2 = u^6b_1$ for some $u \in \bar{k}$; the isomorphism is then defined over the field $k(u)$. It follows that the quantity

$$j(a, b) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

depends only on the $\bar{k}$-isomorphism class of E, so we may define the *j-invariant* $j(E)$ of E to be $j(a, b)$ for any model $Y^2 = X^3 + aX + b$ of E. Note that while $j(E)$ lies in k, it only determines the isomorphism class of E over the algebraic closure $\bar{k}$. Elliptic curves with the same j-invariant need not be isomorphic to one another over k; such curves are said to be *twists* of each other.

Every $j \in k$ arises as the j-invariant of an elliptic curve E/k: We have $0 = j(0, b)$ and $1728 = j(a, 0)$, while if $j \neq 0, 1728$ we can take

$$a = 3j(1728 - j) \quad \text{and} \quad b = 2j(1728 - j)^2,$$

and we find that $j = j(a, b)$. There is thus a one-to-one correspondence between the field k and the set of $\bar{k}$-isomorphism classes of elliptic curves over k. This is the vertex set of the isogeny graphs that we wish to define.

An *automorphism* of an elliptic curve E is an automorphism of E as a curve that fixes the identity element 0. Most elliptic curves have automorphism groups of order 2, with the nontrivial automorphism being the map $(X, Y) \mapsto (X, -Y)$; the only exceptions are the elliptic curves with j-invariants equal to 0 and 1728, which may have extra automorphisms. To simplify matters we will occasionally exclude these special cases from consideration.

2.2. ***Isogenies.*** Let E_1 and E_2 be elliptic curves over a field k. An *isogeny* $\varphi : E_1 \to E_2$ is a nonzero morphism of elliptic curves, that is, a nonconstant rational map that takes the identity of E_1 to the identity of E_2. (We do not require that the morphism be defined over k; we allow maps defined over the algebraic closure.) The *degree* of an isogeny is its degree as a rational map. We call an isogeny of degree n an *n-isogeny*. Elliptic curves related by an isogeny of degree n are said to be *n-isogenous*. We say that two elements j_1, j_2 of k are *n-isogenous* over k if there are n-isogenous elliptic curves E_1, E_2 over k with $j(E_1) = j_1$ and $j(E_2) = j_2$. For a given E/k, if one thinks of $j(E)$ as representing the set of twists of E, then saying that $j(E_1)$ and $j(E_2)$ are n-isogenous means that one can choose twists of E_1 and E_2 that are n-isogenous. Over an algebraically closed field, the set of twists is trivial, so the choice of twist is easy; but even over non-algebraically closed fields, it is easy in practice to find compatible twists.

Every isogeny $\varphi : E_1 \to E_2$ induces a surjective group homomorphism from $E_1(\bar{k})$ to $E_2(\bar{k})$ that has a finite kernel; in this paper, when we speak of the *kernel* of an isogeny, we will always mean the set of points in the kernel over $\bar{k}$. The kernel of an n-isogeny typically has cardinality n (in which case the isogeny is said to be *separable*), and this is always the case when n is not divisible by the characteristic of k. We are primarily interested in isogenies of prime degree $\ell \neq \operatorname{char} k$, and we shall only distinguish isogenies up to isomorphism, regarding isogenies ϕ and φ as equivalent if $\phi = \iota \circ \varphi \circ \iota'$ for some isomorphisms ι and ι'.

There are two important facts about isogenies that we need. The first is that every finite subgroup of $E_1(\bar{k})$ is the kernel of a separable isogeny over $\bar{k}$ that is uniquely determined (up to isomorphism) [41, Proposition III.4.12], and this isogeny can be explicitly computed using Vélu's algorithm [48]. The second is that every n-isogeny $\varphi : E_1 \to E_2$ has a unique *dual isogeny* $\widehat{\varphi} : E_2 \to E_1$ that satisfies

$$\varphi \circ \widehat{\varphi} = \widehat{\varphi} \circ \varphi = [n],$$

where $[n]$ is the *multiplication-by-n map* that sends $P \in E_1(\bar{k})$ to $nP = P + \cdots + P$; see [41, Theorem III.6.1]. The dual isogeny $\widehat{\varphi}$ has degree n, and $[n]$ has degree n^2.

The kernel of the multiplication-by-n map is the *n-torsion subgroup*

$$E[n] = \{P \in E(\bar{k}) : nP = 0\},$$

and for n not divisible by the characteristic of k we have

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

For primes $\ell \neq \operatorname{char} k$, there are $\ell + 1$ cyclic subgroups in $E[\ell]$ of order ℓ, each of which is the kernel of a separable ℓ-isogeny (over $\bar{k}$). Every ℓ-isogeny φ from E arises in this way, since any point in the kernel of φ also lies in the kernel of $\widehat{\varphi} \circ \varphi = [\ell]$.

Not every cyclic subgroup of $E[\ell]$ is the kernel of an isogeny defined over k; this occurs precisely when the subgroup is invariant under the action of the Galois group $G = \mathrm{Gal}(k(E[\ell])/k)$. The Galois group acts linearly on $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, which we may view as an $\mathbb{F}_\ell$-vector space of dimension two in which the order-ℓ subgroups of $E[\ell]$ are linear subspaces. If G fixes more than two linear subspaces of a two-dimensional vector space then it must fix all of them. This yields the following lemma.

Lemma 2. *Let E/k be an elliptic curve with j-invariant not equal to* 0 *or* 1728, *and let $\ell \neq \mathrm{char}\, k$ be a prime. Up to isomorphism, the number of k-rational ℓ-isogenies from E is* $0, 1, 2,$ *or* $\ell + 1$.

2.3. ***The modular equation.*** Let $j(\tau)$ be the classical modular function defined on the upper half plane $\mathbb{H}$. For any $\tau \in \mathbb{H}$, the complex numbers $j(\tau)$ and $j(N\tau)$ are the j-invariants of elliptic curves defined over $\mathbb{C}$ that are related by an isogeny whose kernel is a cyclic group of order N. The minimal polynomial $\Phi_N(Y)$ of the function $j(Nz)$ over the field $\mathbb{C}(j(z))$ has coefficients that are integer polynomials in $j(z)$. If we replace $j(z)$ with X we obtain the *modular polynomial* $\Phi_N \in \mathbb{Z}[X, Y]$, which is symmetric in X and Y and has degree $\ell + 1$ in both variables. It parametrizes pairs of elliptic curves over $\mathbb{C}$ related by a cyclic N-isogeny. The *modular equation* $\Phi_N(X, Y) = 0$ is a canonical equation for the modular curve $Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$.

When N is a prime ℓ, every N-isogeny is cyclic, and we have

$$\Phi_\ell\big(j(E_1), j(E_2)\big) = 0 \quad \Longleftrightarrow \quad j(E_1) \text{ and } j(E_2) \text{ are } \ell\text{-isogenous.}$$

This moduli interpretation remains valid over every field, even those of positive characteristic.

2.4. ***The graph of ℓ-isogenies.*** We now use the modular equation to define the graph of ℓ-isogenies over a field k of characteristic different from ℓ.

Definition 3. 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 $\Phi_\ell(j_1, Y)$.

The vertices of $G_\ell(k)$ are j-invariants, and its edges correspond to (isomorphism classes of) ℓ-isogenies. Every edge (j_1, j_2) that is not incident to 0 or 1728 occurs with the same multiplicity as (j_2, j_1). Thus the subgraph of $G_\ell(k)$ on $k\backslash\{0, 1728\}$ is bidirected, and we may view it as an undirected graph. For any fixed k, the graphs $G_\ell(k)$ all have the same vertex set, but different edge sets, depending on ℓ. Given an elliptic curve E/k, we may view $j(E)$ as a vertex in any of these graphs, a fact that has many applications.

2.5. ***Supersingular and ordinary components.*** Over a field of positive characteristic p, an elliptic curve is *supersingular* if its p-torsion subgroup $E[p]$ is trivial; otherwise it is *ordinary*. If E is supersingular, then so is any elliptic curve isogenous to E; therefore $G_\ell(k)$ is composed of ordinary and supersingular components.

Every supersingular curve over k can be defined over a quadratic extension of the prime field of k; thus every supersingular j-invariant in $\bar{k}$ lies in $\mathbb{F}_{p^2}$ [41, Theorem V.3.1]. It follows that if E is supersingular, then the roots of $\Phi_\ell(j(E), Y)$ all lie in $\mathbb{F}_{p^2}$. Thus every vertex in a supersingular component of $G_\ell(\mathbb{F}_{p^2})$ has out-degree $\ell + 1$. (Every vertex other than those equal to or adjacent to 0 or 1728 also has in-degree $\ell + 1$.)

Remark 4. *Ramanujan graphs.* In fact, $G_\ell(\mathbb{F}_{p^2})$ has just one supersingular component [30, Corollary 78], and when $p \equiv 1 \bmod 12$ it is a *Ramanujan graph* [35], an expander graph with an essentially optimal expansion factor. This fact has cryptographic applications [10].

We are primarily interested in the ordinary components of $G_\ell(k)$, since this is where we will find isogeny volcanoes. First we need to recall some facts from the theory of complex multiplication.

2.6. ***Complex multiplication.*** A morphism from an elliptic curve E/k to itself is called an *endomorphism*; an endomorphism of E is either the zero map or an isogeny from E to itself. (We do not require that endomorphisms be defined over the base field k.) The endomorphisms of an elliptic curve E form a ring $\mathrm{End}(E)$ in which addition and multiplication are defined via the formulas

$$(\phi + \varphi)(P) = \phi(P) + \varphi(P) \quad \text{and} \quad (\phi\varphi)(P) = \phi(\varphi(P)) \quad \text{for all } P \in E(\bar{k}).$$

For every positive integer n, the multiplication-by-n map $[n]$ lies in $\mathrm{End}(E)$, and we have $[n]\phi = \phi + \cdots + \phi = n\phi$ for all $\phi \in \mathrm{End}(E)$. Since $[n]$ is never the zero endomorphism, it follows that $\mathrm{End}(E)$ contains a subring isomorphic to $\mathbb{Z}$, which we shall identify with $\mathbb{Z}$.

When $\mathrm{End}(E)$ is larger than $\mathbb{Z}$ we say that E has *complex multiplication* (CM), a term that arises from the fact that over the complex numbers, endomorphisms that do not lie in $\mathbb{Z}$ may be viewed as "multiplication-by-α" maps for some algebraic integers α. Over a finite field $\mathbb{F}_q$, every elliptic curve has complex multiplication; for ordinary elliptic curves over $\mathbb{F}_q$, the Frobenius endomorphism that sends the point (X, Y) to (X^q, Y^q) is an example of an endomorphism that does not lie in $\mathbb{Z}$.

When E has complex multiplication there are two possibilities:

$$\mathrm{End}(E) \simeq \begin{cases} \text{an order } \mathcal{O} \text{ in an imaginary quadratic field, or} \\ \text{an order } \mathcal{O} \text{ in a definite quaternion algebra,} \end{cases}$$

and in either case we say that E has CM by $\mathcal{O}$. The second case occurs if and only if E is supersingular, which is possible only in positive characteristic; we are primarily interested in the first case. It will be convenient to fix an isomorphism $\mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$ so that we may regard elements of $\mathcal{O}$ as elements of $\mathrm{End}(E)$ and vice versa.

The *endomorphism algebra* $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$ is preserved by isogenies. Thus if E has complex multiplication, then so does every elliptic curve isogenous to E, but not necessarily by the same order $\mathcal{O}$.

2.7. ***Horizontal and vertical isogenies.*** Let $\varphi : E_1 \to E_2$ be an ℓ-isogeny of elliptic curves with CM by imaginary quadratic orders $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively. Then $\mathcal{O}_1 = \mathbb{Z} + \tau_1\mathbb{Z}$ and $\mathcal{O}_2 = \mathbb{Z} + \tau_2\mathbb{Z}$, for some $\tau_1, \tau_2 \in \mathbb{H}$. The isogeny $\widehat{\varphi} \circ \tau_2 \circ \varphi$ lies in $\mathrm{End}(E_1)$, and this implies that $\ell\tau_2 \in \mathcal{O}_1$; similarly, $\ell\tau_1 \in \mathcal{O}_2$. There are thus three possibilities:

(1) $\mathcal{O}_1 = \mathcal{O}_2$, in which case we say that φ is *horizontal*.

(2) $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$, in which case we say that φ is *descending*.

(3) $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$, in which case we say that φ is *ascending*.

In the last two cases we say that φ is a *vertical* ℓ-isogeny. The orders $\mathcal{O}_1$ and $\mathcal{O}_2$ necessarily have the same fraction field $K = \mathrm{End}^0(E_1) = \mathrm{End}^0(E_2)$, and both lie in the maximal order $\mathcal{O}_K$, the ring of integers of K.

2.8. ***The CM torsor.*** Let E/k be an elliptic curve with CM by an imaginary quadratic order $\mathcal{O}$, and let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal. The $\mathfrak{a}$-*torsion subgroup*

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

is the kernel of a separable isogeny $\varphi_\mathfrak{a} : E \to E'$. Provided that $\mathfrak{a}$ has norm not divisible by the characteristic of k, we have $\deg \varphi_\mathfrak{a} = N(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$. Using the fact that $\mathfrak{a}$ is invertible, one can show that $\mathrm{End}(E) \simeq \mathrm{End}(E')$; thus $\varphi_\mathfrak{a}$ is a horizontal isogeny.

If $\mathfrak{a}$ and $\mathfrak{b}$ are two invertible $\mathcal{O}$-ideals then $\varphi_{\mathfrak{a}\mathfrak{b}} = \varphi_\mathfrak{a}\varphi_\mathfrak{b}$. Thus the group of invertible $\mathcal{O}$-ideals acts on the set of elliptic curves with endomorphism ring $\mathcal{O}$. When $\mathfrak{a}$ is a principal ideal we have $E \simeq E'$; hence there is an induced action of the ideal class group $\mathrm{Cl}(\mathcal{O})$ on the set

$$\mathrm{Ell}_\mathcal{O}(k) = \{j(E) : E/k \text{ with } \mathrm{End}(E) \simeq \mathcal{O}\}.$$

This action is faithful (only principal ideals act trivially) and transitive (see [42, Proposition II.1.2] for a proof in the case that $k = \mathbb{C}$ and $\mathcal{O} = \mathcal{O}_K$, which may be generalized via [31, Chapters 10, 13]). Provided it is nonempty, the set $\mathrm{Ell}_\mathcal{O}(k)$ is thus a principal homogeneous space, a *torsor*, for the group $\mathrm{Cl}(\mathcal{O})$. The cardinality

of $\mathrm{Ell}_{\mathcal{O}}(k)$ is either 0 or h, where $h = h(\mathcal{O}) = \#\mathrm{Cl}(\mathcal{O})$ is the *class number*. Thus either every curve $E/\bar{k}$ with CM by $\mathcal{O}$ can be defined over k, or none of them can.

Remark 5. *Decomposing isogenies.* The CM action allows us to express horizontal isogenies $\varphi_{\mathfrak{a}}$ of large degree as the composition of a sequence of isogenies of smaller degree. Even if $\mathfrak{a}$ has prime norm, we may find that $[\mathfrak{a}] = [\mathfrak{p}_1 \cdots \mathfrak{p}_s]$ in $\mathrm{Cl}(\mathcal{O})$, where the $\mathfrak{p}_i$ are prime ideals with norms smaller than $\mathfrak{a}$. Under the generalized Riemann hypothesis (GRH), we can find, in probabilistic subexponential time, an equivalence $[\mathfrak{a}] = [\mathfrak{p}_1 \cdots \mathfrak{p}_s]$ in which the $\mathfrak{p}_i$ have norms that are polylogarithmic in the class number h and $s = O(\log h)$; see [11, Theorem 2.1]. This makes horizontal isogenies asymptotically easier to compute than vertical isogenies (this holds even without the GRH), which has implications for cryptography; see [6; 18; 19; 20; 27; 28].

2.9. ***Horizontal isogenies.*** Every horizontal ℓ-isogeny φ arises from the action of an invertible $\mathcal{O}$-ideal $\mathfrak{l}$ of norm ℓ, namely, the ideal of endomorphisms $\alpha \in \mathcal{O}$ whose kernels contain the kernel of φ. If ℓ divides the index of $\mathcal{O}$ in the maximal order $\mathcal{O}_K$ of its fraction field K, then no such ideals exist. Otherwise we say that $\mathcal{O}$ is *maximal at* ℓ, and in this case the number of invertible $\mathcal{O}$-ideals of norm ℓ is equal to

$$1 + \left(\frac{\mathrm{disc}(K)}{\ell}\right) = \begin{cases} 0 & \text{if } \ell \text{ is inert in } K, \\ 1 & \text{if } \ell \text{ is ramified in } K, \\ 2 & \text{if } \ell \text{ splits in } K. \end{cases}$$

Each such $\mathcal{O}$-ideal gives rise to a horizontal ℓ-isogeny. In the split case we have $(\ell) = \mathfrak{l} \cdot \bar{\mathfrak{l}}$, and the $\mathfrak{l}$-orbits partition $\mathrm{Ell}_{\mathcal{O}}(k)$ into cycles corresponding to the cosets of $\langle [\mathfrak{l}] \rangle$ in $\mathrm{Cl}(\mathcal{O})$. When $\mathfrak{l}$ is principal the ideal class $[\mathfrak{l}]$ is trivial, which leads to self-loops in $G_\ell(k)$. We can also have $[\mathfrak{l}] = [\bar{\mathfrak{l}}]$ even though $\mathfrak{l} \neq \bar{\mathfrak{l}}$, which gives rise to double edges in $G_\ell(k)$.

2.10. ***Vertical isogenies.*** Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D, and let $\mathcal{O}' = \mathbb{Z} + \ell\mathcal{O}$ be the order of index ℓ in $\mathcal{O}$. To simplify matters, let us assume that $\mathcal{O}$ and $\mathcal{O}'$ have the same group of units $\{\pm 1\}$; this holds whenever $D < -4$, and excludes only the cases $\mathcal{O} = \mathbb{Z}[i]$ and $\mathcal{O} = \mathbb{Z}[\zeta_3]$, which correspond to the special j-invariants 1728 and 0, respectively.

The map that sends each invertible $\mathcal{O}'$-ideal $\mathfrak{a}$ to the invertible $\mathcal{O}$-ideal $\mathfrak{a}\mathcal{O}$ preserves norms and induces a surjective homomorphism

$$\rho : \mathrm{Cl}(\mathcal{O}') \to \mathrm{Cl}(\mathcal{O}).$$

See [12, Proposition 7.20] for a proof in the case that $\mathcal{O}$ is the maximal order; the general case is proved similarly (see [4, Lemma 3] and [7, §3]). Under a suitable identification of the class groups $\mathrm{Cl}(\mathcal{O}')$ and $\mathrm{Cl}(\mathcal{O})$ with their torsors $\mathrm{Ell}_{\mathcal{O}'}(k)$ and

$\mathrm{Ell}_{\mathcal{O}}(k)$, the vertical isogenies from $\mathrm{Ell}_{\mathcal{O}'}(k)$ to $\mathrm{Ell}_{\mathcal{O}}(k)$ correspond to the map from $\mathrm{Cl}(\mathcal{O}')$ to $\mathrm{Cl}(\mathcal{O})$ given by ρ. To show this, let us prove the following lemma.

Lemma 6. *Let E'/k be an elliptic curve with CM by $\mathcal{O}'$. Then there is a unique ascending ℓ-isogeny from E' to an elliptic curve E/k with CM by $\mathcal{O}$.*

Proof. The existence of E'/k implies that $\mathrm{Ell}_{\mathcal{O}'}(k)$ is nonempty, and since $\mathcal{O}$ contains $\mathcal{O}'$, it follows that $\mathrm{Ell}_{\mathcal{O}}(k)$ is also nonempty.[1]

Let us suppose that there exists an ascending ℓ-isogeny $\phi_1 : E_1' \to E_1$, for some elliptic curve E_1' with CM by $\mathcal{O}'$. Twisting E_1 if necessary, we may choose an invertible $\mathcal{O}'$-ideal $\mathfrak{a}'$ so that the horizontal isogeny $\varphi_{\mathfrak{a}'}$ maps E_1' to E'. If we now set $\mathfrak{a} = \rho(\mathfrak{a}')$ and let E be the image of $\varphi_{\mathfrak{a}} \circ \phi_1$, then E has CM by $\mathcal{O}$, and there is a unique isogeny $\phi : E' \to E$ such that $\phi \circ \varphi_{\mathfrak{a}'} = \varphi_{\mathfrak{a}} \circ \phi_1$, by [41, Corollary 4.11]. We have $\deg \phi = \deg \varphi_{\mathfrak{a}} \deg \phi_1 / \deg \varphi_{\mathfrak{a}'} = \ell$, thus ϕ is an ascending ℓ-isogeny. It follows that if any elliptic curve E_1'/k with CM by $\mathcal{O}'$ admits an ascending ℓ-isogeny, then so does every such elliptic curve.

We now proceed by induction on $d = v_\ell([\mathcal{O}_K : \mathcal{O}])$. Let $D_K = \mathrm{disc}(K)$. For $d = 0$, every elliptic curve E/k with CM by $\mathcal{O}$ admits $\ell + 1$ k-rational ℓ-isogenies, of which $1 + \left(\frac{D_K}{\ell}\right)$ are horizontal. The remaining $\ell - \left(\frac{D_K}{\ell}\right) > 0$ must be descending, and their duals are ascending ℓ-isogenies from elliptic curves with CM by $\mathcal{O}'$. It follows that there are a total of $\left(\ell - \left(\frac{D_K}{\ell}\right)\right) h(\mathcal{O})$ ascending ℓ-isogenies from $\mathrm{Ell}_{\mathcal{O}'}(k)$ to $\mathrm{Ell}_{\mathcal{O}}(k)$. By [12, Theorem 7.24], this is equal to the cardinality $h(\mathcal{O}')$ of $\mathrm{Ell}_{\mathcal{O}'}(k)$. Since there is at least one ascending ℓ-isogeny from each elliptic curve E'/k with CM by $\mathcal{O}'$, there must be exactly one in each case.

The argument for $d > 0$ is similar. By the inductive hypothesis, every elliptic curve E/k with CM by $\mathcal{O}$ admits exactly one ascending ℓ-isogeny, and since ℓ now divides $[\mathcal{O}_K : \mathcal{O}]$, there are no horizontal isogenies from E, and all ℓ of the remaining ℓ-isogenies from E must by descending. There are thus a total of $\ell h(\mathcal{O})$ ascending ℓ-isogenies from $\mathrm{Ell}_{\mathcal{O}'}(k)$, which equals the cardinality $h(\mathcal{O}')$ of $\mathrm{Ell}_{\mathcal{O}'}(k)$. □

It follows from the proof of Lemma 5 that there is a one-to-one correspondence between the graph of the function ρ and the edges of $G_\ell(k)$ that lead from $\mathrm{Ell}_{\mathcal{O}'}(k)$ to $\mathrm{Ell}_{\mathcal{O}}(k)$. Indeed, let us pick a vertex $j_1' \in \mathrm{Ell}_{\mathcal{O}'}(k)$ and let j_1 be its unique neighbor in $\mathrm{Ell}_{\mathcal{O}}(k)$ given by Lemma 6. If we identify the edge (j_1', j_1) in $G_\ell(k)$ with the edge $(1_{\mathrm{Cl}(\mathcal{O}')}, 1_{\mathrm{Cl}(\mathcal{O})})$ in the graph of ρ, then every other edge in the correspondence is determined in a way that is compatible with the actions of $\mathrm{Cl}(O')$ and $\mathrm{Cl}(O)$ on the torsors $\mathrm{Ell}_{\mathcal{O}'}(k)$ and $\mathrm{Ell}_{\mathcal{O}}(k)$. Under this correspondence, the vertices in $\mathrm{Ell}_{\mathcal{O}'}(k)$ that are connected to a given vertex v in $\mathrm{Ell}_{\mathcal{O}}(k)$ (the *children* of v) correspond to

[1] One way to see this is to note that k contains all the roots of the Hilbert class polynomial for $\mathcal{O}'$, hence it must contain all the roots of the Hilbert class polynomial for $\mathcal{O}$, since the ring class field of $\mathcal{O}'$ contains the ring class field of $\mathcal{O}$; see Section 3.4.

a coset of the kernel of ρ, a cyclic group of order $\ell - \left(\frac{D_K}{\ell}\right)$ generated by the class of an invertible $\mathbb{O}'$-ideal of norm ℓ^2; see [7, Lemma 3.2].

2.11. ***Ordinary elliptic curves over finite fields.*** We now assume that k is a finite field $\mathbb{F}_q$. Let $E/\mathbb{F}_q$ be an ordinary elliptic curve and let π_E denote the Frobenius endomorphism $(X, Y) \mapsto (X^q, Y^q)$. The *trace of Frobenius* is given by

$$t = \operatorname{Tr} \pi_E = q + 1 - \#E(\mathbb{F}_q),$$

and π_E satisfies the characteristic equation $\pi_E^2 - t\pi_E + q = 0$. As an element of the imaginary quadratic order $\mathbb{O} \simeq \operatorname{End}(E)$, the Frobenius endomorphism corresponds to an algebraic integer with trace t and norm q. Thus we have the *norm equation*

$$4q = t^2 - v^2 D_K,$$

in which D_K is the discriminant of the field $K = \mathbb{Q}(\sqrt{t^2 - 4q})$ containing $\mathbb{O}$, and $v = [\mathbb{O}_K : \mathbb{Z}[\pi_E]]$. We have

$$\mathbb{Z}[\pi_E] \subseteq \mathbb{O} \subseteq \mathbb{O}_K,$$

thus $[\mathbb{O}_K : \mathbb{O}]$ divides v, and the same is true for any elliptic curve $E/\mathbb{F}_q$ with Frobenius trace t.

Let us now define

$$\operatorname{Ell}_t(\mathbb{F}_q) = \{j(E) : E/\mathbb{F}_q \text{ satisfies } \operatorname{Tr} \pi_E = t\},$$

the set of $\overline{\mathbb{F}}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ with a given Frobenius trace t. By a theorem of Tate [47], $\operatorname{Ell}_t(\mathbb{F}_q)$ corresponds to an isogeny class, but note that $\operatorname{Ell}_t(\mathbb{F}_q) = \operatorname{Ell}_{-t}(\mathbb{F}_q)$. For any ordinary elliptic curve $E/\mathbb{F}_q$ with Frobenius trace $t = \operatorname{Tr} \pi_E$, we may write $\operatorname{Ell}_t(\mathbb{F}_q)$ as the disjoint union

$$\operatorname{Ell}_t(\mathbb{F}_q) = \bigsqcup_{\mathbb{Z}[\pi_E] \subseteq \mathbb{O} \subseteq \mathbb{O}_K} \operatorname{Ell}_{\mathbb{O}}(\mathbb{F}_q),$$

of cardinality equal to the Kronecker class number $H(t^2 - 4q)$; see [40, Definition 2.1].

2.12. ***The main theorem.*** We now arrive at our main theorem, which states that the ordinary components of $G_\ell(\mathbb{F}_q)$ (other than the components of 0 and 1728) are ℓ-volcanoes, and characterizes the structure of these components. The proof follows easily from the material we have presented, as the reader may wish to verify.

Theorem 7 (Kohel). *Let V be an ordinary component of $G_\ell(\mathbb{F}_q)$ that does not contain* 0 *or* 1728. *Then V is an ℓ-volcano for which the following hold*:

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

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

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

(4) *The depth of* V *is* $d = v_\ell\big((t^2 - 4q)/D_0\big)/2$, *where* $t^2 = (\operatorname{Tr}\pi_E)^2$ *for any* E *with* $j(E) \in V$.

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

Remark 8. *Special cases.* Theorem 7 is easily extended to the case where V contains 0 or 1728. Parts (1)–(5) still hold; the only necessary modification is the claim that V is an ℓ-volcano. When V contains 0, if V_1 is nonempty 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 nonempty 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 (respectively, 2-to-1) discrepancy arises from the action of $\operatorname{Aut}(E)$ on the cyclic subgroups of $E[\ell]$ when $j(E) = 0$ (respectively, $j(E) = 1728$). Otherwise, V satisfies all the requirements of an ℓ-volcano, and most of the algorithms we present in the next section are equally applicable to V.

Example 9. Let $p = 411751$ and $\ell = 3$. The graph $G_3(\mathbb{F}_p)$ has a total of 206254 components, of which 205911 are ordinary and 343 are supersingular. The supersingular components all lie in the same isogeny class (which is connected in $G_3(\mathbb{F}_{p^2})$), while the ordinary components lie in 1283 distinct isogeny classes.

Let us consider the isogeny class $\operatorname{Ell}_t(\mathbb{F}_p)$ for $t = 52$. We then have $4p = t^2 - v^2 D$ with $v = 2 \cdot 3^2 \cdot 5$ and $D = -203$. The subgraph $G_{\ell,t}(\mathbb{F}_p)$ of $G_\ell(\mathbb{F}_p)$ on $\operatorname{Ell}_t(\mathbb{F}_p)$ (known as a *cordillera* [33]) consists of ten 3-volcanoes, all of which have depth $d = v_\ell(v) = 2$. It contains a total of 1008 vertices distributed as follows:

- 648 vertices lie in six 3-volcanoes with $[\mathbb{O}_K : \mathbb{O}_0] = 10$ and $|V_0| = 12$.
- 216 vertices lie in two 3-volcanoes with $[\mathbb{O}_K : \mathbb{O}_0] = 5$ and $|V_0| = 12$.
- 108 vertices lie in a 3-volcano with $[\mathbb{O}_K : \mathbb{O}_0] = 2$ and $|V_0| = 12$.
- 36 vertices lie in a 3-volcano with $[\mathbb{O}_K : \mathbb{O}_0] = 1$ and $|V_0| = 4$.

For comparison:

- $G_{2,52}(\mathbb{F}_p)$ consists of 252 2-volcanoes of depth 1 with $|V_0| = 1$.
- $G_{5,52}(\mathbb{F}_p)$ consists of 144 5-volcanoes of depth 1 with $|V_0| = 1$.
- $G_{7,52}(\mathbb{F}_p)$ consists of 504 7-volcanoes with two vertices and one edge.
- $G_{11,52}(\mathbb{F}_p)$ consists of 1008 11-volcanoes that are all isolated vertices.

3. Applications

We now consider several applications of isogeny volcanoes, starting with one that is very simple, but nevertheless instructive.

3.1. ***Finding the floor.*** Let $E/\mathbb{F}_q$ be an ordinary elliptic curve. Then $j(E)$ lies in an ordinary component V of $G_\ell(\mathbb{F}_q)$. We wish to find a vertex on the *floor* of V, that is, a vertex v in level V_d, where d is the depth of V. Such vertices v are easily distinguished by their (out-)degree, which is the number of roots of $\Phi_\ell(v, Y)$ that lie in $\mathbb{F}_q$ (counted with multiplicity).

Proposition 10. *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 $\ell + 1$. □

We note that if $j(E)$ is on the floor then $E[\ell](\mathbb{F}_q)$ is necessarily cyclic (otherwise there would be another level below the floor). This is useful, for example, when using the CM method to construct Edwards curves [34], and shows that every ordinary elliptic curve $E/\mathbb{F}_q$ is isogenous to some $E'/\mathbb{F}_q$ with $E'(\mathbb{F}_q)$ cyclic.

Our strategy for finding the floor is 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 $v_i \ne v_{i-2}$ (so backtracking is prohibited).

Algorithm (FINDFLOOR).

Input: An ordinary vertex $v_0 \in G_\ell(\mathbb{F}_q)$.

Output: A vertex on the floor of the component of v_0.

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.

The complexity of FINDFLOOR is given by the following proposition, in which $\mathsf{M}(n)$ denotes the time to multiply two n-bit integers. It is worth noting that for large ℓ the complexity is dominated by the time to substitute v into $\Phi_\ell(X, Y)$, not by root-finding (a fact that is occasionally overlooked).

Proposition 11. *Given $\Phi_\ell \in \mathbb{F}_q[X, Y]$, each step of* FINDFLOOR *can be accomplished in $O(\ell^2 \mathsf{M}(n) + \mathsf{M}(\ell n) n)$ expected time, where $n = \log q$. The expected number of steps s is $\delta + O(1)$, where δ is the distance from v_0 to the floor.*

Proof. Computing $\phi(Y) = \Phi_\ell(v, Y)$ involves $O(\ell^2)$ $\mathbb{F}_q$-operations, or $O(\ell^2 \mathsf{M}(n))$ bit operations. The neighbors of v are the distinct roots of $\phi(Y)$ that lie in $\mathbb{F}_q$, which are precisely the roots of $f(Y) = \gcd(Y^q - Y, \phi(Y))$. Computing $Y^q \bmod \phi$ involves $O(n)$ multiplications in the ring $\mathbb{F}_q[Y]/(\phi)$, each of which can be accomplished using $O(\mathsf{M}(\ell n))$ bit operations, via Kronecker substitution [22], yielding an $O(\mathsf{M}(\ell n)n)$ bound. With the fast Euclidean algorithm the gcd of two polynomials of degree $O(\ell)$ can be computed using $O(\mathsf{M}(\ell n) \log \ell)$ bit operations. If $\log \ell < n$ then this is bounded by $O(\mathsf{M}(\ell n)n)$, and otherwise it is bounded by $O(\ell^2 \mathsf{M}(n))$. Thus the total time to compute $f(Y)$ for any particular v is $O(\ell^2 \mathsf{M}(n) + \mathsf{M}(\ell n)n)$.

The degree of $f(Y)$ is the number of distinct roots of $\Phi_\ell(Y, v)$ in $\mathbb{F}_q$. For $\ell > 3$, this is less than or equal to 2 if and only if v is on the floor. For $\ell \le 3$ we can count roots with multiplicity by taking gcds with derivatives of ϕ, within the same time bound. To find a random root of $f(Y)$ we use the probabilistic splitting algorithm of [37]; since we need only one root, this takes $O(\mathsf{M}(\ell n)n)$ expected time.

For every vertex v in a level V_i above the floor, at least 1/3 of v's neighbors lie in level V_{i+1}, thus within $O(1)$ expected steps the path will be extended along a descending edge. Once this occurs, every subsequent edge in the path must be descending, since we are not allowed to backtrack along the single ascending edge, and we will reach the floor within $\delta + O(1)$ steps. □

Remark 12. *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 $v_{s+1} \ne v_{s-1}$.

The FINDFLOOR algorithm finds a path of expected length $\delta + O(1)$ from v_0 to the floor. With a bit more effort we can find a path of exactly length δ, using a simplified version of an algorithm from [17].

Algorithm (FINDSHORTESTPATHTOFLOOR).

Input: An ordinary $v_0 \in G_\ell(\mathbb{F}_q)$.

Output: A shortest path to the floor of the component of v_0.

1. Let $v_0 = j(E)$. If $\deg v_0 \le 2$ 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. (If v_0 does not have three distinct neighbors then just pick all of them.)
3. Output a path that reached the floor.

The correctness of the algorithm follows from the fact that at most two of v_0's neighbors do not lie along descending edges, so one of the three paths must begin with a descending edge. This path must then consist entirely of descending edges,

yielding a shortest path to the floor. The algorithm takes at most 3δ steps, each of which has complexity bounded as in Proposition 11.

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 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; see [43, §4.1] for algorithms and further details. We should also mention that an alternative approach based on pairings has recently been developed by Ionica and Joux [25; 26], which is more efficient when d is large.

3.2. ***Identifying supersingular curves.*** Both algorithms in the previous section assume that their input is the j-invariant of an ordinary elliptic curve. But what if this is not the case? If we attempt to "find the floor" on the supersingular component of $G_\ell(\mathbb{F}_{p^2})$ we will never succeed, since every vertex has out-degree $\ell + 1$. On the other hand, from part (4) of Theorem 7 (and Remark 8), we know that every ordinary component of $G_\ell(\mathbb{F}_{p^2})$ has depth less than $\log_\ell 2p$, so we can bound the length of the shortest path to the floor from any ordinary vertex.

This suggests that, with minor modifications, the algorithm FINDSHORTESTPATHTOFLOOR can be used to determine whether a given elliptic curve $E/\mathbb{F}_q$ is ordinary or supersingular. If $j(E) \notin \mathbb{F}_{p^2}$ then E must be ordinary, so we may assume $v_0 = j(E) \in \mathbb{F}_{p^2}$ (even if E is defined over $\mathbb{F}_p$, we want to work in $\mathbb{F}_{p^2}$). We modify step 2 of the algorithm so that if none of the three paths reaches the floor within $\log_\ell 2p$ steps, it reports that its input is supersingular and terminates. Otherwise, the algorithm succeeds and can report that its input is ordinary. This works for any prime ℓ, but using $\ell = 2$ gives the best running time.

This yields a Las Vegas algorithm to determine whether a given elliptic curve is ordinary or supersingular in $\widetilde{O}(n^3)$ expected time, where $n = \log q$. For comparison, the best previously known Las Vegas algorithm has an expected running time of $\widetilde{O}(n^4)$, and the best known deterministic algorithm runs in $\widetilde{O}(n^5)$ time. Remarkably, the average time for a random input is only $\widetilde{O}(n^2)$. This matches the complexity of the best known Monte Carlo algorithm for this problem, with better constant factors; see [45] for further details.

3.3. ***Computing endomorphism rings.*** We now turn to a more difficult problem: determining the endomorphism ring of an ordinary elliptic curve $E/\mathbb{F}_q$. We assume that the trace of Frobenius $t = \operatorname{Tr} \pi_E$ is known; this can be computed in polynomial time using Schoof's algorithm [39]. By factoring $4q - t^2$, we can compute the positive integer v and fundamental discriminant D satisfying the norm equation $4q = t^2 - v^2 D$. We then know that $\mathbb{Z}[\pi_E]$ has index v in the maximal order $\mathbb{O}_K$,

where $K = \mathbb{Q}(\sqrt{D})$. The order $\mathcal{O} \simeq \mathrm{End}(E)$ is uniquely determined by its index u in $\mathcal{O}_K$, and u must be a divisor of v. Let us assume $D < -4$.

We can determine u by determining the level of $j(E)$ in its component of $G_\ell(\mathbb{F}_q)$ for each of the primes ℓ dividing v. If $v = \ell_1^{e_1} \cdots \ell_w^{e_w}$ is the prime factorization of v, then $u = \ell_1^{d_1} \cdots \ell_w^{d_w}$, where $\delta_i = e_i - d_i$ is the distance from $j(E)$ to the floor of its ℓ_i-volcano. But it may not be practical to compute δ_i using FINDSHORTESTPATHTOFLOOR when ℓ_i is large: Its complexity is quasiquadratic in ℓ_i, which may be exponential in $\log q$ (and computing Φ_{ℓ_i} is even harder). More generally, we do not know any algorithm for computing a vertical ℓ-isogeny whose complexity is not at least linear in ℓ (in general, quadratic in ℓ). This would seem to imply that we cannot avoid a running time that is exponential in $\log q$.

However, as noted in Remark 5, computing horizontal isogenies is easier than computing vertical isogenies. We now sketch an approach to computing $\mathrm{End}(E)$ that uses horizontal isogenies to handle large primes dividing v, based on the algorithm in [4]. To simplify the presentation, we assume that v is squarefree; the generalization to arbitrary v is straightforward.

Let $\mathcal{L}$ be the lattice of orders in $\mathcal{O}_K$ that contain $\mathbb{Z}[\pi_E]$. Our strategy is to determine whether u is divisible by a given prime divisor ℓ of v using a smooth relation that holds in an order $\mathcal{O} \in \mathcal{L}$ if and only if $\mathcal{O}$ is maximal at ℓ. This relation will hold in $\mathrm{End}(E)$ if and only if u is not divisible by ℓ.

A *smooth relation* R is a multiset $\{\mathfrak{p}_1^{r_1}, \ldots, \mathfrak{p}_s^{r_s}\}$ in which the $\mathfrak{p}_i$ are invertible $\mathbb{Z}[\pi_E]$-ideals with prime norms p_i occurring with multiplicity r_i, such that p_i and r_i satisfy bounds that are subexponential in $\log q$. We say that R *holds* in $\mathcal{O} \in \mathcal{L}$ if the $\mathcal{O}$-ideal $R_\mathcal{O} = (\mathfrak{p}_1\mathcal{O})^{r_1} \cdots (\mathfrak{p}_s\mathcal{O})^{r_s}$ is principal. If $\mathcal{O}' \subset \mathcal{O}$, the existence of the norm-preserving homomorphism $\rho : \mathrm{Cl}(\mathcal{O}') \to \mathrm{Cl}(\mathcal{O})$ defined as in Section 2.10 implies that if R holds in $\mathcal{O}'$, then it holds in $\mathcal{O}$. It thus suffices to find a relation that holds in the order of index v/ℓ in $\mathcal{O}_K$, but not in the order of index ℓ in $\mathcal{O}_K$. Under the GRH, for $\ell > 3$ we can find such an R in probabilistic subexponential time [3].

To determine whether R holds in $\mathcal{O} \simeq \mathrm{End}(E)$, we compute the CM action of $[R_\mathcal{O}] \in \mathrm{Cl}(\mathcal{O})$ on $j(E) \in \mathrm{Ell}_\mathcal{O}(\mathbb{F}_q)$. This involves walking r_i steps along the surface of a p_i-volcano for each of the $\mathfrak{p}_i$ appearing in R and then checking whether we wind up back at our starting point $j(E)$. None of the p_i divide v, so these p_i-volcanoes all have depth 0 and consist of either a single edge or a cycle. We must choose a direction to walk along each cycle (one corresponds to the action of $\mathfrak{p}_i$, the other to $\bar{\mathfrak{p}}_i$). There are methods to determine the correct choice, but in practice we can make s small enough so that it is easy to simply try every combination of choices and count how many work; see [4] for details.

Under the GRH, this algorithm has a subexponential expected running time of $L[1/2, \sqrt{3}/2]$ plus the cost of factoring $4q - t^2$ (the latter is heuristically negligible, using the number field sieve, and provably bounded by $L[1/2, 1]$ in [32]). Bisson [3] has recently improved this to $L[1/2, \sqrt{2}/2]$ plus the cost of factoring $4q - t^2$.

Example 13. Let $q = 2^{320} + 261$ and suppose that $E/\mathbb{F}_q$ has Frobenius trace

$$t = 230641434457621363389123643439267139273704045955 8.$$

Then $4q = t^2 - v^2 D$, where $D = -147759$ and $v = 2^2 p_1 p_2$, with

$$p_1 = 16447689059735824784039,$$
$$p_2 = 71003976975490059472571.$$

We can easily determine the level of $j(E)$ in its 2-volcano by finding a shortest path to the floor. For p_1 and p_2 we instead use smooth relations R_1 and R_2.

Let $\mathbb{O}_1$ be the order of index p_1 in $\mathbb{O}_K$, and $\mathbb{O}_1'$ the order of index v/p_1 in $\mathbb{O}_K$. The relation

$$R_1 = \{\mathfrak{p}_5, \mathfrak{p}_{19}^2, \bar{\mathfrak{p}}_{23}^{210}, \mathfrak{p}_{29}, \mathfrak{p}_{31}, \bar{\mathfrak{p}}_{41}^{145}, \mathfrak{p}_{139}, \bar{\mathfrak{p}}_{149}, \mathfrak{p}_{167}, \bar{\mathfrak{p}}_{191}, \bar{\mathfrak{p}}_{251}^{6}, \mathfrak{p}_{269}, \bar{\mathfrak{p}}_{587}^{7}, \bar{\mathfrak{p}}_{643}\}$$

holds in $\mathbb{O}_1$ but not in $\mathbb{O}_1'$ (here $\mathfrak{p}_\ell$ denotes the ideal of norm ℓ corresponding to the reduced binary quadratic form $\ell x^2 + bxy + cy^2$ with $b \geq 0$). If we now let $\mathbb{O}_2$ be the order of index p_2 in $\mathbb{O}_K$ and $\mathbb{O}_2'$ the order of index v/p_2 in $\mathbb{O}_K$, then

$$R_2 = \{\mathfrak{p}_{11}, \bar{\mathfrak{p}}_{13}^{576}, \mathfrak{p}_{23}^2, \bar{\mathfrak{p}}_{41}, \bar{\mathfrak{p}}_{47}, \mathfrak{p}_{83}, \mathfrak{p}_{101}, \bar{\mathfrak{p}}_{197}^{28}, \bar{\mathfrak{p}}_{307}^{3}, \mathfrak{p}_{317}, \bar{\mathfrak{p}}_{419}, \mathfrak{p}_{911}\}$$

holds in $\mathbb{O}_2$ but not in $\mathbb{O}_2'$.

Including the time to compute the required modular polynomials and the time to find the relations R_1 and R_2, the total time to compute $\mathrm{End}(E)$ in this example is less than half an hour. In contrast, it would be completely infeasible to directly compute a vertical isogeny of degree p_1 or p_2; writing down even a single element of the kernel of such an isogeny would require more than 2^{80} bits.

3.4. ***Computing Hilbert class polynomials.*** Let $\mathbb{O}$ be an imaginary quadratic order with discriminant D. The *Hilbert class polynomial* H_D is defined by

$$H_D(X) = \prod_{j \in \mathrm{Ell}_{\mathbb{O}}(\mathbb{C})} (X - j).$$

Equivalently, $H_D(X)$ is the minimal polynomial of the j-invariant of the lattice $\mathbb{O}$ over the field $K = \mathbb{Q}(\sqrt{D})$. Remarkably, its coefficients lie in $\mathbb{Z}$.

The field $K_{\mathbb{O}} = K(j(\mathbb{O}))$ is the *ring class field* of $\mathbb{O}$. If a prime q splits completely in $K_{\mathbb{O}}$, then $H_D(X)$ splits completely in $\mathbb{F}_q[X]$ and its roots form the set $\mathrm{Ell}_{\mathbb{O}}(\mathbb{F}_q)$. Each root is then the j-invariant of an elliptic curve $E/\mathbb{F}_q$ with $\mathrm{End}(E) \simeq \mathbb{O}$. We

must have $\#E(\mathbb{F}_q) = q + 1 - t$, where the norm equation $4q = t^2 - v^2 D$ uniquely determines the integers t and v up to sign, for $D < -4$. We can thus use a root of $H_D(X)$ in $\mathbb{F}_q$ to construct an elliptic curve $E/\mathbb{F}_q$ with exactly $q + 1 - t$ rational points; under some reasonable heuristic assumptions about the distribution of prime numbers, we can achieve any desired cardinality for $E(\mathbb{F}_q)$ by choosing q and D appropriately [8]. This is known as the *CM method*, which is commonly used in elliptic curve cryptography and elliptic curve primality proving.

We now outline an algorithm to compute $H_D(X)$ using the CRT approach described in [1; 43]. Under the GRH it runs in $O(|D|(\log|D|)^{5+o(1)})$ expected time, which is quasilinear in the $O(|D|\log|D|)$ size of $H_D(X)$. The same approach can be used to compute many other types of class polynomials; see [14].

Algorithm (COMPUTEHILBERTCLASSPOLYNOMIAL).

Input: An imaginary quadratic discriminant D.

Output: The Hilbert class polynomial $H_D(X)$.

1. Select a sufficiently large set of primes p that satisfy $4p = t^2 - v^2 D$.
2. For each prime p, compute $H_D(X) \bmod p$ as follows:
   (a) Generate random elliptic curves $E/\mathbb{F}_p$ until $\#E(\mathbb{F}_p) = p + 1 - t$.
   (b) Use volcano climbing to find E' isogenous to E with $\mathrm{End}(E') \simeq \mathbb{O}$.
   (c) Enumerate $\mathrm{Ell}_{\mathbb{O}}(\mathbb{F}_p)$ by applying the $\mathrm{Cl}(\mathbb{O})$-action to $j(E')$.
   (d) Compute $H_D(X) = \prod_{j \in \mathrm{Ell}_{\mathbb{O}}(\mathbb{F}_p)} (X - j) \bmod p$.
3. Use the CRT to recover $H_D(X)$ over $\mathbb{Z}$ (or over $\mathbb{F}_q$ via the explicit CRT).

Isogeny volcanoes play a key role in the efficient implementation of this algorithm, not only in step 2(b), but also in step 2(c), which is the most critical step and merits further discussion. Given any sequence of generators $\alpha_1, \ldots, \alpha_k$ for a finite abelian group G, if we let $G_i = \langle \alpha_1, \ldots, \alpha_i \rangle$ and define $r_i = [G_i : G_{i-1}]$, then every element β of G can be uniquely represented in the form $\beta = \alpha_1^{e_1} \cdots \alpha_k^{e_k}$, with $0 \le e_i < r_i$. This is a special case of a *polycyclic presentation*. We can use a polycyclic presentation of $\mathrm{Cl}(\mathbb{O})$ to enumerate the torsor $\mathrm{Ell}_{\mathbb{O}}(\mathbb{F}_p)$ by enumerating the list of exponent vectors $(e_1, \ldots, e_k)$ in reverse lexicographic order. At each step we apply the action of the generator α_i that transforms the current exponent vector to the next in the list (usually $i = 1$, since e_1 varies most frequently).

Using generators of the form $\alpha_i = [\mathfrak{l}_i]$, where $\mathfrak{l}_i$ is an invertible $\mathbb{O}$-ideal of prime norm ℓ_i, this amounts to walking along the surfaces of various ℓ-volcanoes. To make this process as efficient as possible, it is crucial to minimize the size of the primes ℓ_i. This is achieved by choosing $\mathfrak{l}_1$ to minimize ℓ_1 and then minimizing each ℓ_i subject to $[\mathfrak{l}_i] \notin \langle [\mathfrak{l}_1], \ldots, [\mathfrak{l}_{i-1}] \rangle$; this is called an *optimal presentation* [43, §5.1]. This will often cause us to use a set of generators that is larger than strictly needed.

As an example, for $D = -79947$ the class group $\mathrm{Cl}(\mathcal{O})$ is cyclic of order 100, generated by the class of an ideal with norm 19. But the optimal presentation for $\mathrm{Cl}(\mathcal{O})$ uses ideals $\mathfrak{l}_1$ and $\mathfrak{l}_2$ with norms 2 and 13, respectively. The classes of these ideals are not independent, we have $[\mathfrak{l}_2]^5 = [\mathfrak{l}_1]^{18}$, but they do form a polycyclic presentation with $r_1 = 20$ and $r_2 = 5$. Using this presentation to enumerate $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ is more than 100 times faster than using any single generator of $\mathrm{Cl}(\mathcal{O})$. One can construct examples where the optimal presentation is exponentially faster than any presentation that minimizes the number of generators; see [43, §5.3].

Enumerating $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ using a polycyclic presentation involves walking along the surfaces of various ℓ-volcanoes, as in the previous section when testing relations. But using an optimal presentation will often mean that some of the primes ℓ_i divide v. This always happens, for example, when $D \equiv 1 \bmod 8$, since in this case $\ell_1 = 2$ divides v. Thus we must be prepared to walk along the surface of an ℓ-volcano of nonzero depth. We now give a simple algorithm to do this.

Algorithm (WALKSURFACEPATH).

Input: A vertex v_0 on the surface V_0 of an ℓ-volcano of depth d and a positive integer $n < \#V_0$.

Output: A path $v_0, \ldots, v_n$ in V_0.

1. If v_0 has a single neighbor v_1, then return the path v_0, v_1. Otherwise, walk a path $v_0, \ldots, v_d$ and set $i \leftarrow 0$.
2. While $\deg v_{i+d} = 1$: Replace $v_{i+1}, \ldots, v_{i+d}$ by extending the path $v_0, \ldots, v_i$ by d steps, starting from an unvisited neighbor v'_{i+1} of v_i.
3. Extend the path $v_0, \ldots, v_{i+d}$ to $v_0, \ldots, v_{i+d+1}$ and increment i.
4. If $i = n$ then return $v_0, \ldots, v_n$; otherwise, go to step 2.

Algorithm WALKSURFACEPATH requires us to know the depth d of the ℓ-volcano, which we may determine from the norm equation. It works by walking an arbitrary path to the floor and then backing up d steps to a vertex that must be on the surface (whenever we leave the surface we must descend to the floor in exactly d steps). When d or ℓ is large, this algorithm is not very inefficient and the pairing-based approach of [25] may be faster. But in the context of computing Hilbert class polynomials, both d and ℓ are typically quite small.

Remark 14. *Walking the surface with gcds.* An alternative approach to walking the surface using gcds is given in [14]. Suppose we have already enumerated $v_0, \ldots, v_n$ along the surface of an ℓ-volcano, and have also taken a single step from v_0 to an adjacent vertex v'_0 on the surface of an ℓ'-volcano. We can then compute a path $v'_0, \ldots, v'_n$ along the surface of the ℓ-volcano containing v'_0 by computing each v'_{i+1} as the unique root of $f(Y) = \gcd(\Phi_\ell(v'_i, Y), \Phi_{\ell'}(v_{i+1}, Y))$.

The vertex v'_{i+1} is guaranteed to be on the surface, and the root-finding operation is trivial, since $f(Y)$ has degree 1. This approach is generally much faster than using either WALKSURFACEPATH or the algorithm in [25], and in practice most of the vertices in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ can be enumerated this way; see [14] for further details.

Remark 15. *Space complexity.* A key virtue of the CRT approach is that by using the *explicit CRT* [2, Theorem 3.2], it is possible to directly compute the coefficients of $H_D(X)$ modulo an integer m (the characteristic of $\mathbb{F}_q$, for example), without first computing the coefficients over $\mathbb{Z}$. This means we can compute $H_D(X)$ over $\mathbb{F}_q$ with a space complexity that is quasilinear in $h(D)\log q$, which may be much smaller than $|D|\log|D|$. When $h(D)$ is sufficiently composite (often the case), we can use a decomposition of the ring class field to find a root of $H_D(X)$ in $\mathbb{F}_q$ with a space complexity quasilinear in $h(D)^{1/2}\log q$; see [44]. The low space complexity of the CRT approach has greatly increased the range of feasible discriminants for the CM method: Examples with $|D| \approx 10^{16}$ can now be handled [44], whereas $|D| \approx 10^{10}$ was previously regarded as a practical upper limit [13].

3.5. ***Computing modular polynomials.*** All of the algorithms we have discussed depend on modular polynomials $\Phi_\ell(X, Y)$; we even used them to define the graph of ℓ-isogenies. We now outline an algorithm to compute Φ_ℓ, using the CRT approach described in [7]. Under the GRH, it runs in $O(\ell^3(\log \ell)^{3+o(1)})$ expected time, which makes it the fastest method known for computing $\Phi_\ell(X, Y)$.

Algorithm (COMPUTEMODULARPOLYNOMIAL).

Input: An odd prime ℓ.

Output: The modular polynomial $\Phi_\ell(X, Y)$.

1. Pick an order $\mathcal{O}$ with $h(\mathcal{O}) > \ell + 1$ and let $D = \mathrm{disc}(\mathcal{O})$.
2. Select a sufficiently large set of primes p that satisfy $4p = t^2 - \ell^2 v^2 D$, with $\ell \nmid v$ and $p \equiv 1 \bmod \ell$.
3. For each prime p, compute $\Phi_\ell(X, Y) \bmod p$ as follows:
   (a) Enumerate $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ starting from a root v_0 of $H_D(X) \bmod p$.
   (b) Use Vélu's algorithm to compute a descending ℓ-isogeny from v_0 to v'_0.
   (c) Enumerate $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$ using v'_0 as a starting point, where $[\mathcal{O} : \mathcal{O}'] = \ell$.
   (d) Map the ℓ-volcanoes that make up $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p) \cup \mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$.
   (e) Interpolate $\Phi_\ell(X, Y) \bmod p$.
4. Use the CRT to recover $\Phi_\ell(X, Y)$ over $\mathbb{Z}$ (or over $\mathbb{F}_q$ via the explicit CRT).

The restrictions on p ensure that each element of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ lies on the surface of an ℓ-volcano of depth 1 whose floor consists of elements of $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$. An example with $\ell = 5$ and $D = -151$ is shown in Figure 3.

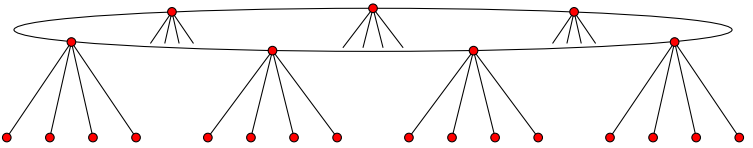

Figure 3. A volcano with $\ell = 5$ and $D = -151$.

When we enumerate $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ in step 3(a), we use a polycyclic presentation $\boldsymbol{\alpha}$ for $\mathrm{Cl}(\mathcal{O})$ derived from prime ideals whose norms are all less than ℓ (for $\ell > 2$ this is always possible). By expressing the class γ of an invertible $\mathcal{O}$-ideal of norm ℓ in terms of $\boldsymbol{\alpha}$, we can then determine all of the horizontal ℓ-isogenies between elements of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ without knowing Φ_ℓ. In our example with $D = -151$, the presentation $\boldsymbol{\alpha}$ consists of a single generator α corresponding to an ideal of norm 2, with $\gamma = \alpha^3$. Thus our enumeration of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ yields a cycle of 2-isogenies that we can convert to a cycle of 5-isogenies by simply picking out every third element.

The application of Vélu's algorithm in step 3(b) involves picking a random point P of order ℓ and computing the ℓ-isogeny φ with $\langle P \rangle$ as its kernel. This process is greatly facilitated by our choice of p, which ensures that P has coordinates in $\mathbb{F}_p$, rather than an extension field. We may find that φ is a horizontal ℓ-isogeny, but we can easily detect this and try again with a different P.

As in step 3(a), when we enumerate $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$ in step 3(c) we use a polycyclic presentation $\boldsymbol{\beta}$ for $\mathrm{Cl}(\mathcal{O}')$ derived from prime ideals whose norms are all less than ℓ. There are no horizontal ℓ-isogenies between elements of $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$, but we need to connect each element of $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$ to its ℓ-isogenous parent in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$. This is done by identifying one child v' of each parent and then identifying that child's siblings, which are precisely the elements of $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$ related to v' by a cyclic isogeny of degree ℓ^2. By expressing the class γ' of an invertible $\mathcal{O}'$ ideal of norm ℓ^2 in terms of $\boldsymbol{\beta}$, we can identify the ℓ^2-isogeny cycles of siblings in $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$; these are precisely the cosets of the homomorphism $\rho : \mathrm{Cl}(\mathcal{O}') \to \mathrm{Cl}(\mathcal{O})$ in Section 2.10.

After identifying the horizontal isogenies among the vertices v in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ and the children of each v, we can completely determine the subgraph of $G_\ell(\mathbb{F}_p)$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p) \cup \mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_p)$; this is what it means to "map" the ℓ-volcanoes in step 3(d). In our example with $D = -151$ there is just one ℓ-volcano; Figure 4 depicts the result of mapping this ℓ-volcano when $p = 4451$.

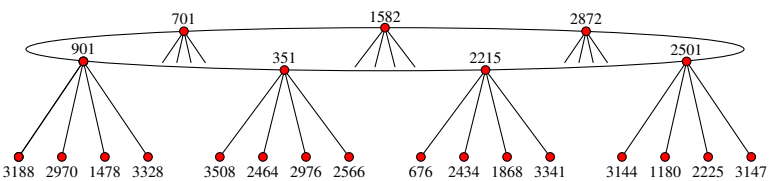

Figure 4. The fully labeled example.

In step 3(e) we compute, for each of $\ell+2$ vertices $v_i \in \mathrm{Ell}_{\mathbb{O}}(\mathbb{F}_p)$, the polynomial $\phi_i(Y) = \Phi_\ell(v_i, Y) = \prod_j (Y - v_{ij})$, where v_{ij} ranges over the $\ell+1$ neighbors of v_i in $G_\ell(\mathbb{F}_p)$. We can then interpolate the coefficients of $\Phi_\ell(X,Y) = \sum_{i,j} c_{ij} X^i Y^j$ as follows: If $\psi_j(X)$ is the unique polynomial of degree at most $\ell+1$ for which $\psi_j(v_i)$ is the coefficient of Y^j in $\phi_i(Y)$, then c_{ij} is the coefficient of X^i in $\psi_j(X)$.

Remark 16. *Weber modular polynomials.* This algorithm can compute modular polynomials for many modular functions besides the j-function; see [7, §7]. This includes the Weber f-function that satisfies $(f(z)^{24} - 16)^3 = f(z)^{24} j(z)$. The modular polynomials $\Phi_\ell^f(X,Y)$ for $f(z)$ are sparser than $\Phi_\ell(X,Y)$ by a factor of 24, and have coefficients whose binary representation is smaller by a factor of approximately 72. Thus the total size of Φ_ℓ^f is roughly 1728 times smaller than Φ_ℓ, and it can be computed nearly 1728 times faster.

Remark 17. *Modular polynomials of composite level.* A generalization of this approach that efficiently computes modular polynomials $\Phi_N(X,Y)$ for composite values of N can be found in [9].

Remark 18. *Evaluating modular polynomials.* Most applications that use $\Phi_\ell(X,Y)$, including all the algorithms we have considered here, only require the instantiated polynomial $\phi(Y) = \Phi_\ell(j(E), Y)$. A space-efficient algorithm for directly computing $\phi(Y)$ without using $\Phi_\ell(X,Y)$ appears elsewhere in this volume [46].

The isogeny volcano algorithm for computing $\Phi_\ell(X,Y)$ has substantially increased the feasible range of ℓ: It is now possible to compute Φ_ℓ with $\ell \approx 10{,}000$, and for Φ_ℓ^f we can handle $\ell \approx 60{,}000$. It has also greatly reduced the time required for these computations, as may be seen in the tables of [7, §8].

Acknowledgements

I am grateful to Gaetan Bisson for his feedback on an early draft of this article, and to the editors for their careful review.

The author was supported by NSF grant DMS-1115455.

References

[1] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter, *Computing Hilbert class polynomials*, in van der Poorten and Stein [36], 2008, pp. 282–295. MR 2009j:11200

[2] Daniel J. Bernstein and Jonathan P. Sorenson, *Modular exponentiation via the explicit Chinese remainder theorem*, Math. Comp. **76** (2007), no. 257, 443–454. MR 2007f:11142

[3] Gaetan Bisson, *Computing endomorphism rings of elliptic curves under the GRH*, J. Math. Cryptol. **5** (2011), no. 2, 101–113. MR 2012k:11201

[4] Gaetan Bisson and Andrew V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, J. Number Theory **131** (2011), no. 5, 815–831. MR 2012a:11080

[5] Ljiljana Brankovic, Paul D. Coddington, John F. Roddick, Chris Steketee, James R. Warren, and Andrew L. Wendelborn (eds.), *ACSW Frontiers* 2007: *Proceedings of the Fifth Australasian Symposium on Grid Computing and e-Research* (*AusGrid* 2007), *the Fifth Australasian Information Security Workshop* (*Privacy Enhancing Technologies*) (*AISW* 2007), *and the Australasian Workshop on Health Knowledge Management and Discovery* (*HKMD* 2007), *Ballarat*, *Australia*, *January* 2007, Conferences in Research and Practice in Information Technology, no. 68, Sydney, Australian Computer Society, 2007.

[6] Reinier Bröker, Denis Charles, and Kristin Lauter, *Evaluating large degree isogenies and applications to pairing based cryptography*, in Galbraith and Paterson [21], 2008, pp. 100–112. MR 2012i:94143

[7] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), no. 278, 1201–1231. MR 2012m:11180

[8] Reinier Bröker and Peter Stevenhagen, *Efficient CM-constructions of elliptic curves over finite fields*, Math. Comp. **76** (2007), no. 260, 2161–2179. MR 2008i:11077

[9] Jan Hendrik Bruinier, Ken Ono, and Andrew V. Sutherland, *Class polynomials for nonholomorphic modular functions*, 2013. arXiv 1301.5672 [math.NT]

[10] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren, *Cryptographic hash functions from expander graphs*, J. Cryptology **22** (2009), no. 1, 93–113. MR 2010d:94074

[11] Andrew M. Childs, David Jao, and Vladimir Soukharev, *Constructing elliptic curve isogenies in quantum subexponential time*, 2012. arXiv 1012.4019v2 [quant-ph]

[12] David A. Cox, *Primes of the form* $x^2 + ny^2$: *Fermat*, *class field theory and complex multiplication*, John Wiley & Sons, New York, 1989. MR 90m:11016

[13] Andreas Enge, *The complexity of class polynomial computation via floating point approximations*, Math. Comp. **78** (2009), no. 266, 1089–1107. MR 2010h:11097

[14] Andreas Enge and Andrew V. Sutherland, *Class invariants by the CRT method*, in Hanrot et al. [23], 2010, pp. 142–156. MR 2012d:11246

[15] Claus Fieker and David R. Kohel (eds.), *Algorithmic number theory*: *Proceedings of the 5th International Symposium* (*ANTS-V*) *held at the University of Sydney*, *July* 7–12, 2002, Lecture Notes in Computer Science, no. 2369, Berlin, Springer, 2002. MR 2004j:11002

[16] Mireille Fouquet, *Anneau d'endomorphismes et cardinalité des courbes elliptiques*: *aspects algorithmiques*, Ph.D. thesis, École polytechnique, 2001. http://www.math.jussieu.fr/~fouquet/Manuscrit.ps.gz

[17] Mireille Fouquet and François Morain, *Isogeny volcanoes and the SEA algorithm*, in Fieker and Kohel [15], 2002, pp. 276–291. MR 2005c:11077

[18] Steven Galbraith and Anton Stolbunov, *Improved algorithm for the isogeny problem for ordinary elliptic curves*, Appl. Algebra Engrg. Comm. Comput. **24** (2013), no. 2, 107–131. MR 3063894

[19] Steven D. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, LMS J. Comput. Math. **2** (1999), 118–138. MR 2001k:11113

[20] Steven D. Galbraith, Florian Hess, and Nigel P. Smart, *Extending the GHS Weil descent attack*, in Knudsen [29], 2002, pp. 29–44. MR 2004f:94060

[21] Steven D. Galbraith and Kenneth G. Paterson (eds.), *Pairing-based cryptography—Pairing* 2008: *Proceedings of the 2nd International Conference held at Royal Holloway*, *University of London*, *Egham*, *September* 1–3, 2008, Lecture Notes in Computer Science, no. 5209, Berlin, Springer, 2008. MR 2011j:94001

[22] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, 2nd ed., Cambridge University Press, 2003. MR 2004g:68202

[23] Guillaume Hanrot, François Morain, and Emmanuel Thomé (eds.), *Algorithmic number theory: Proceedings of the 9th Biennial International Symposium (ANTS-IX) held in Nancy, July 19–23, 2010*, Lecture Notes in Computer Science, no. 6197, Berlin, Springer, 2010. MR 2011g:11002

[24] Everett W. Howe and Kiran S. Kedlaya (eds.), *Algorithmic number theory: Proceedings of the 10th Biennial International Symposium (ANTS-X) held in San Diego, July 9–13, 2012*, The Open Book Series, no. 1, Berkeley, Mathematical Sciences Publishers, 2013, THIS VOLUME.

[25] Sorina Ionica and Antoine Joux, *Pairing the volcano*, in Hanrot et al. [23], 2010, pp. 201–208. MR 2011m:11127

[26] ———, *Pairing the volcano*, Math. Comp. **82** (2013), no. 281, 581–603. MR 2983037

[27] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan, *Do all elliptic curves of the same order have the same difficulty of discrete log?*, in Roy [38], 2005, pp. 21–40. MR 2007e:94060

[28] David Jao and Vladimir Soukharev, *A subexponential algorithm for evaluating large degree isogenies*, in Hanrot et al. [23], 2010, pp. 219–233. MR 2011h:11144

[29] Lars Knudsen (ed.), *Advances in cryptology—EUROCRYPT 2002: Proceedings of the 21st International Annual Conference on the Theory and Applications of Cryptographic Techniques held in Amsterdam, April 28–May 2, 2002*, Lecture Notes in Computer Science, no. 2332, Berlin, Springer, 2002. MR 2003m:94074

[30] David Russell Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California, Berkeley, 1996, p. 117. http://search.proquest.com/docview/304241260 MR 2695524

[31] Serge Lang, *Elliptic functions*, 2nd ed., Graduate Texts in Mathematics, no. 112, Springer, New York, 1987. MR 88c:11028

[32] H. W. Lenstra, Jr. and Carl Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), no. 3, 483–516. MR 92m:11145

[33] J. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls, *Isogeny cordillera algorithm to obtain cryptographically good elliptic curves*, in Brankovic et al. [5], 2007, pp. 127–131.

[34] François Morain, *Edwards curves and CM curves*, 2009. arXiv 0904.2243 [math.NT]

[35] Arnold K. Pizer, *Ramanujan graphs and Hecke operators*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 1, 127–137. MR 90m:11063

[36] Alfred J. van der Poorten and Andreas Stein (eds.), *Algorithmic number theory: Proceedings of the 8th International Symposium (ANTS-VIII) held in Banff, AB, May 17–22, 2008*, Lecture Notes in Computer Science, no. 5011, Berlin, Springer, 2008. MR 2009h:11002

[37] Michael O. Rabin, *Probabilistic algorithms in finite fields*, SIAM J. Comput. **9** (1980), no. 2, 273–280. MR 81g:12002

[38] Bimal Roy (ed.), *Advances in cryptology—ASIACRYPT 2005: Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security held in Chennai, December 4–8, 2005*, Lecture Notes in Computer Science, no. 3788, Berlin, Springer, 2005. MR 2007a:94218

[39] René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494. MR 86e:11122

[40] ———, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, 183–211. MR 88k:14013

[41] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 106, Springer, New York, 1986. MR 87g:11070

[42] _____, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 151, Springer, New York, 1999. MR 96b:11074

[43] Andrew V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), no. 273, 501–538. MR 2011k:11177

[44] _____, *Accelerating the CM method*, LMS J. Comput. Math. **15** (2012), 172–204. MR 2970725

[45] _____, *Identifying supersingular elliptic curves*, LMS J. Comput. Math. **15** (2012), 317–325. MR 2988819

[46] _____, *On the evaluation of modular polynomials*, in Howe and Kedlaya [24], 2013, pp. 531–535.

[47] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR 34 #5829

[48] Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. http://gallica.bnf.fr/ark:/12148/bpt6k56191248/f52.image MR 45 #3414

ANDREW V. SUTHERLAND: drew@math.mit.edu
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, United States

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS