MASARYKOVA UNIVERZITA

Přírodovědecká fakulta

Ústav matematiky a statistiky

Isogeny volcanoes in cryptography

Master's thesis

Vojtěch Suchánek

Vedoucí práce: Mgr. Marek Sýs, Ph.D. **Brno 2020**

Bibliographic Entry

Author:	Vojtěch Suchánek Faculty of Science, Masaryk University Department of Mathematics and Statistics
Title of Thesis:	Isogeny volcanoes in cryptography
Degree Programme:	Mathematics
Field of Study:	Algebra and Discrete Mathematics
Supervisor:	Mgr. Marek Sýs, Ph.D.
Academic Year:	2019/2020
Number of Pages:	x + 89
Keywords:	elliptic curve; isogeny; isogeny volcano; horizontal isogeny; vertical isogeny;endomorphism ring; key exchange; Diffie-Hellman; class group; Schoof's algorithm;

Abstrakt

V této diplomové práci se věnujeme vulkanům isogenií eliptických křivek nad konečnými tělesy. Nejprve provedeme čtenáře základy teorie isogenií a okruhu endomorfismů eliptické křivky. Poté charakterizujeme vulkány isogenií daného stupně. Následně ukážeme aplikaci vulkánů v teorii eliptických křivek a kryptografii zejména výměny klíčů. Nakonec čtenáři vysvětlíme využití isogenií při počítání bodů na křivce a navrheneme vylepšení z hlediska vulkánů. Součástí práce je implementace isogenií a vulkánů v systému počítačové algebry Sage.

Abstract

In this thesis, we study isogeny volcanoes of elliptic curves over finite fields. Firstly, we introduce the basic theory of isogenies and ring of endomorphisms of an elliptic curve. We fully describe isogeny volcanoes of a given degree. Furthermore, we illustrate the application of volcanoes in the theory of elliptic curves and cryptography, in particular, key exchange. Finally, we explain the usage of isogenies for counting points of elliptic curves a propose an improvement based on isogeny volcanoes. As a part of this thesis, implementation of isogenies and isogeny volcanoes was written in the computer algebra system Sage.

Contents

Introduction

The theory of elliptic curves is an essential topic in number theory and consequently, cryptography. Everyone one of us comes across elliptic curves on a daily basis every time we connect to the internet. At the core, the safety of these connections relies on hard problems in number theory, including the discrete logarithm problem on an elliptic curve. However, with the introduction of quantum computing, these problems do not seem to be hard enough. The solution brings the isogeny based cryptography, which is based on particular maps between elliptic curves. These maps, called isogenies, have both geometric and algebraic character. Isogenies can be factored in some sense to prime l-isogenies, so the study breaks down to these l-isogenies, similarly to factorization of integers to prime numbers. This thesis focuses on graphs based on the relation between elliptic curves given by l-isogenies. These graphs almost always take a particular shape, which is called a volcano. It turns out that volcanoes are key ingredients for understanding isogenies and elliptic curves in general.

The text is aimed at anyone with a desire to understand isogeny volcanoes and their applications. Even though the text is written for readers unfamiliar with isogenies, a basic understanding of elliptic curves is required. Good introductory reference for elliptic curves is [Was08], [ST15] or [CFA$^+$12]. The standard way to study isogeny volcanoes is through elliptic curves over complex numbers. However, this approach is quite demanding in terms of prerequisites (the reader would have to be familiar with modular functions in complex analysis). Since we are only interested in isogenies over finite fields, the text is written using only elementary methods of elliptic curves over finite fields. To the best knowledge of the author, such introductory text with complete characterization has not been available. Nonetheless, an ambitious reader looking for a deep understanding of isogenies should look into [Sil11b] or lectures in [Sut17]. A classical reference for isogeny volcanoes is the dissertation thesis of David Kohel [Koh96]. Summaries can be found in [FM02] and [Sut12]. One should not forget the wonderful habilitation thesis by Luca de Feo [DF18].

The text has seven chapters, including the appendix. In the first three chapters, we manage to, in some sense, gradually split elliptic curves into three categories based on different invariants. In the first chapter, by introducing isogenies and their basic properties, we realize that two elliptic curves are isogenous if and only if they have the same number of points. Following on this in the next chapter, we divide each class of isogenous curves into isogeny graphs. Finally, the third chapter splits each isogeny graph into so-called levels based on the endomorphism ring. This division of classes of elliptic curves allows us to prove in the fourth chapter that each isogeny graph of an ordinary elliptic curve is a volcano. With the fifth chapter, we leave the theoretical background of isogeny volcanoes and go through several applications, including determining supersingularity, finding endomorphism ring, key exchange, and Schoof's point counting algorithm. Finally, in the sixth chapter, we propose a possible improvement to [FM02] and present basic functionality of our implementation of isogenies and isogeny volcanoes in Sage. More thorough documentation is then found in the appendix.

One of the original aims of this thesis was to study the isogeny key exchange based on ordinary elliptic curves. Unfortunately, with the shift of academic community from ordinary curves to supersingular curves in the past two years, we have been forced to leave the focus on key exchange and to center our attention to more promising areas. The least we can do is to explain the reader the basic functionality of the original key exchange and the reasons why supersingular curves are more appropriate.

The contributions of this thesis can be split into three parts. Firstly, in the fourth chapter, we manage to completely characterize the volcanoes using elementary methods, avoiding complex analysis, and thus producing a more approachable text for readers less trained in this area. Secondly, we propose a solution for the $l = 2$ problem in Schoof's algorithm using isogeny volcanoes and compare our algorithm on real data. Last but not least, as a part of this thesis, we have implemented isogenies, isogeny volcanoes, endomorphisms with endomorphism ring, and horizontal walks, which are entirely missing in the official implementation or are very limited (in the case of isogenies).

List of Symbols

For easier orientation we present here the basic notation used throughout the thesis.

$\mathbb{Z}$	the set of integers
$\mathbb{N}$	the set of natural numbers (without 0)
$\mathbb{Q}$	the set of rational numbers
$\mathbb{Z}_n$	the ring of integers modulo n
$\lvert A \rvert$	the cardinality of the set A
$\ker(\phi)$	the kernel of the map ϕ
$K^\times$	the group of units of the ring K
$[A:B]$	the index of the group B in the group A
$\mathrm{Gal}(K/L)$	the Galois group of the Galois extension K/L
$\mathbb{F}_q$	finite field of size q
$\overline{K}$	the algebraic closure of field K
∞	the neutral element of elliptic curve group
$[k]_E, [k]$	multiplication-by-k isogeny on elliptic curve E
π_E, π	Frobenius endomorphism on elliptic curve E
π_p	Frobenius morphism
$E[n]$	n-torsion subgroup of elliptic curve E
$j(E)$	j-invariant of curve E
$\mathrm{End}(E)$	endomorphism ring of elliptic curve E
$A \otimes B$	tensor product of $\mathbb{Z}$-module A and B
$\mathbb{Q}(\alpha)$	simple extension field
$\mathrm{End}^0(E)$	endomorphism algebra of elliptic curve E
$R[x]$	the polynomial ring in x
$L(x, y)$	the field of rational functions in x, y
$\mathcal{O}_K$	the ring of algebraic integers of field K
$\mathrm{Cl}(\mathcal{O})$	class group of order $\mathcal{O}$
$\mathrm{lcm}(a, b)$	lowest common multiple of integers a and b
$\gcd(a, b)$	greatest common divisor of integers a and b

Chapter 1

Isogeny

This chapter introduces the notion of isogenies and their basic properties, which will be needed in the study of isogeny volcanoes. Long and complex proofs are shortened or fully omitted as we are not interested in developing a full theory of isogenies. We refer the reader to [Sil11b] or [Sut17] for more in-depth introduction. Throughout the chapter, K is a field with $\operatorname{char}(K) = p$ and $\mathbb{F}_q$ a finite field with $q = p^m$ for prime $p > 3$ and $m \in \mathbb{N}$.

Definition 1 (Isogeny)**.** Let E_1 and E_2 be elliptic curves defined over field K and L/K be an algebraic extension. We call isogeny over L any non-constant homomorphism of groups $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ for which $\alpha(\infty) = \infty$ and exist rational functions $r_1, r_2 \in L(x, y)$ satisfying for every affine point $(x, y) \in E_1(\overline{K})$:

$$\alpha((x,y)) = \begin{cases} (r_1(x,y), r_2(x,y)) & r_1(x,y) \text{ and } r_2(x,y) \text{ are defined,} \\ \infty & \text{otherwise.} \end{cases}$$

If we say that α is an isogeny, without specifying the field, we will mean $L = K$, this will usually be the case. Sometimes the term L-rational isogeny is used to specify the field L. Mind that the isogeny is defined non-constant, and some authors also call isogeny the constant map that maps every point to ∞ [Sil11b].

Immediate observation is that composition $\alpha \circ \beta$ of two isogenies α, β is also an isogeny. We will omit the symbol $\circ$ and write $\alpha\beta$. Concerning the notation, we will also often write simply $\alpha(x, y)$ instead of $\alpha((x, y))$ and $\alpha : E_1 \to E_2$ instead of $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$.

Remark 2. Isogenies are sometimes defined as morphisms of abelian varieties that preserve the identity element. In our definition, this is covered by the rational functions. It can be further shown that every such non-constant morphism induces homomorphism of groups. Our definition is therefore unnecessarily strong but underlines both important properties of isogenies. More information about abelian varieties can be found in [Sil11b].

Example 3. Trivial example of isogeny is the identity map $[1]_E : E(\overline{K}) \to E(\overline{K})$ for any elliptic curve E over K, since it is a homomorphism of groups $E_1 = E_2 = E$ and is given by rational functions $r_1(x, y) = x$, $r_2(x, y) = y$. We will denote it $[1]$ or

$[1]_E$ to underline the elliptic curve. Another obvious isogeny is $[-1] : E(\overline{K}) \to E(\overline{K})$ defined by $[-1](P) = -P$ with rational functions $r_1(x, y) = x$, $r_2(x, y) = -y$.

For better manipulation with isogenies it is appropriate to express their rational functions in the so-called standard form.

Lemma 4. Let $\alpha : E_1 \to E_2$ be an isogeny of elliptic curves over K. There exist polynomials $u, v, s, t \in K[x]$ such that the pairs u, v and s, t are coprime in $K[x]$ and satisfy for every affine point $(x, y) \in E_1(\overline{K})$:

$$\alpha(x, y) = \begin{cases} \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right) & v(x) \neq 0 \text{ and } t(x) \neq 0, \\ \infty & \text{otherwise.} \end{cases}$$

The pairs u, v and s, t are uniquely determined up to a scalar from $K^\times$.

Proof. Let $E_1 : y^2 = x^3 + a_1x + b_1$. The idea is to repeatedly substitute any y^2 in the rational functions of α by $x^3 + a_1x + b_1$. We will briefly comment the first coordinate, rest can be found in [Sil11b]. After the substitution we get $\frac{u_1(x)+u_2(x)y}{v_1(x)+v_2(x)y}$ for some $u_1, u_2, v_1, v_2 \in K[x]$. Afterwards by $\frac{u_1(x)+u_2(x)y}{v_1(x)+v_2(x)y} \cdot \frac{v_1(x)-v_2(x)y}{v_1(x)-v_2(x)y} = \frac{(u_1(x)+u_2(x)y)(v_1(x)-v_2(x)y)}{v_1^2(x)-v_2^2(x)y^2}$ and substitution of y^2 we get rid of y in the denominator. Thus we get $\frac{u_3(x)+u_4(x)y}{v_3(x)}$ for appropriate u_3, u_4, v_3. Finally, we use the argument that $-(x, y) = (x, -y)$ which implies $u_4(x) = 0$. □

We will often write $\alpha(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ and say that α is in *standard form.*

Example 5. The map $[k] : E \to E$ defined by $[k](P) = kP$ for $k \in \mathbb{Z}$ is an isogeny. It is a homomorphism of the group E to itself as in every additive group. For $[k]$ to be isogeny, it remains to find the (non-constant) rational maps. They actually arise from the addition formulas on elliptic curve. Take for example multiplication by 2 on elliptic curve $E : y^2 = x^3 + 1$ over $\mathbb{F}_5$. The addition formulas as stated in [Was08] tell us that

$$[2](x, y) = (x, y) + (x, y) = (m^2 - 2x, m(x - (m^2 - 2x)) - y), \text{ where } m = \frac{-x^2}{y},$$

which can be expressed as $[2](x, y) = \left(\frac{x^4}{y^2} - 2x, -\frac{x^2}{y}\left(-\frac{x^4}{y^2} + 3x\right) - y\right)$. The standard form can be derived in the spirit of proof of Lemma 4. For the x-coordinate: $\frac{x^4}{y^2} - 2x = \frac{x^4}{x^3+1} - 2x = \frac{-x^4-2x}{y^2}$. The y-coordinate is done in similar manner. The result is

$$[2](x, y) = \left(\frac{-x^4 - 2x}{x^3 + 1}, \frac{2x^6 - 1}{(x^3 + 1)^2}y\right).$$

Frobenius morphism

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over K. The Frobenius morphism is an isogeny $\pi_p : E(\overline{K}) \to E_p(\overline{K})$ defined by $\pi_p(x, y) = (x^p, y^p)$, where $E_p : y^2 =$

$x^3 + a^p x + b^p$. We should explain why π_p maps to E_p and is an isogeny, i.e. non-constant homomorphism of elliptic curves given by rational functions. The fact that π_p maps to E_p follows from how we exponentiate to characteristic: $(y^p)^2 = (x^3 + ax + b)^p = (x^3)^p + (ax)^p + b^p = (x^p)^3 + a^p x^p + b^p$. The rational maps of π_p are by definition (x^p, y^p) and π_p is homomorphism of groups, which can be proven using the rational functions for addition on curves.

Note that if $K = \mathbb{F}_{p^m}$ then the composition π_p^m is an isogeny with image in E. We call $\pi_p^m : E \to E$ *Frobenius endomorphism* of E and denote it π or π_E to underline the curve. We will see that Frobenius endomorphism is a key ingredient in studying elliptic curves. Here are two important properties reader should be aware of:

- For every curve E over $\mathbb{F}_q$:
$$\pi_E(x, y) = (x, y) \iff (x, y) \in E(\mathbb{F}_q).$$
This arises from the fact that $x^q = x$ for every $x \in \mathbb{F}_q$ and the polynomial $x^q - x$ has exactly q roots in $\mathbb{F}_q \subseteq \overline{\mathbb{F}}_q$.

- Frobenius endomorphism commutes with every isogeny $\phi : E_1 \to E_2$ in the sense that $\pi_{E_2}\phi = \phi\pi_{E_1}$. This can be seen again from the way we exponentiate to the field characteristic, i.e. $f(x, y)^p = f(x^p, y^p)$ for every polynomial f in $\mathbb{F}_q[x, y]$ and consequently every rational function f from $\mathbb{F}_q(x, y)$.

Kernel

In this part, we will prove that isogenies are surjective maps and have finite kernels, which can be very well described using the standard form. Further in the text, we will see that kernels are good finite representations of isogenies playing a major role in the study of isogenies and isogeny volcanoes.

Lemma 6 ([Sut17])**.** Let $\alpha(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)} y\right)$ be an isogeny of elliptic curves over K in standard form. Then $v(x)$ and $t(x)$ have the same set of roots in $\overline{K}$. Moreover, the affine points in the kernel of α are precisely the points (x, y) for which $v(x) = 0$.

Example 7. Let's compute the kernel of the isogeny [2] from Example 5. The affine points in the kernel are determined by the roots of the denominator of first coordinate: $x^3 + 1$. The roots of $x^3 + 1$ are the cube roots of -1: $\omega, \omega^2, -1 \in \mathbb{F}_{125}$. Computing the corresponding y-coordinates yields $\ker(\alpha) = \{(\omega, 0), (\omega^2, 0), (-1, 0), \infty\}$.

Example 8. Let $E_1 : y^2 = x^3 + 5x + 8$, $E_2 : y^2 = x^3 + 3x + 11$ be elliptic curves over $\mathbb{F}_{13}$. The map $\phi : E_1 \to E_2$ defined as
$$\phi(x, y) = \left(\frac{x^3 - 2x^2 + 4x + 1}{x^2 - 2x + 1}, \frac{x^3 - 3x^2 - 6}{x^3 - 3x^2 + 3x - 1} y\right)$$
is an isogeny in standard form. To find the affine points of kernel we have to find the roots of $x^2 - 2x + 1 = (x - 1)^2$, which is only $x = 1$. The corresponding points are thus $(1, 1)$ and $(1, -1)$. Thus the size of kernel is 3, including the point ∞.

Example 9. The kernel of a multiplication map $[n]$ is the set $\{P \in E(\overline{K}) \mid nP = \infty\}$. This is often denoted as $E[n]$ and called n-torsion subgroup of E. If n is a positive integer not divisible by p then $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$. This will follow from further theory. The Frobenius morphism given by $(x, y) \mapsto (x^p, y^p)$ has trivial kernel.

Corollary 10. Let $\alpha : E_1 \to E_2$ be an isogeny of elliptic curves over K and $Q \in E_2(\overline{K})$ be a point. The set $\alpha^{-1}(Q) = \{P \in E_1(\overline{K}) \mid \alpha(P) = Q\}$ is finite. In particular, the kernel of α is finite.

Proof. Let $\alpha(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ be the standard form of α. The polynomial $v(x)$ can't be constant zero, because otherwise α would be constant zero. It is therefore polynomial with finite number of roots. For each such root r, there are at most two points in E_1 with x-coordinate r. This implies that the kernel of E_1 is finite. From elementary group theory we know that $\alpha^{-1}(Q)$ is a coset in the factor group $E_1(\overline{K})/\ker(\alpha)$ and has to be therefore finite. □

Lemma 11. Every isogeny $\alpha : E_1 \to E_2$ over K is a surjective homomorphism of groups.

Proof. In the proof we will find $P = (x_P, y_P)$ in the preimage of every point $Q = (x_Q, y_Q)$. It suffices to search for x_P because then $\alpha(P) = Q$ or $\alpha(P) = -Q$. In the latter case we pick $-P$. For $\alpha(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ we wish to find x_P such that $\frac{u(x_P)}{v(x_P)} = x_Q$. So we consider the polynomial $f_Q(x) = u(x) - x_Q v(x) \in K[x]$. If f_Q is non-constant, then it has a root in $\overline{K}$, denote it x_P. The polynomials u, v are coprime so x_P can't be root of both of them and since it is root of f_Q, it is not root of v. We can therefore write $\frac{u(x_P)}{v(x_P)} = x_Q$. The case with f_Q being constant needs little bit more work. It can be shown that f_Q can be constant only for one point Q and its inverse $-Q$. We then pick a point R different from $Q, -Q, \infty$ and $2Q$. There exists a point $S \in E_1(\overline{K})$ such that $\alpha(S) = R$. Then $Q - R$ is also different from $Q, -Q$ and there exists a point T such that $\alpha(T) = Q - R$. Finally, we can see that $\alpha(T + S) = \alpha(T) + \alpha(S) = Q - R + R = Q$.

□

We have discussed the kernel and the surjectivity of isogenies. Naturally, the question about isomorphism arises. For example, the Frobenius morphism $\pi_p : E \to E_p$ is injective and surjective and so the groups $E(\overline{K})$, $E_p(\overline{K})$ are isomorphic. However, they are only isomorphic as groups, and there is no 'inverse isogeny' for π_p. We will therefore define isomorphism of elliptic curves as follows:

Definition 12 (Isomorphism)**.** We call isogeny $\alpha : E_1 \to E_2$ an isomorphism of elliptic curves if there exists an isogeny $\beta : E_2 \to E_1$ satisfying

$$\alpha\beta = [1]_{E_2} \text{ and } \beta\alpha = [1]_{E_1}.$$

Separability and degree

Definition 13 (Separability and degree)**.** Let $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ be an isogeny with the standard form $\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$. The degree of α is the positive[1] integer $\deg(\alpha) = \max\{\deg(u), \deg(v)\}$. We call α separable if the the formal derivative $\left(\frac{u(x)}{v(x)}\right)' \in K(x)$ is not constant zero. If α is not separable, we call it inseparable.

The uniqueness of standard form ensures that the degree and separability are well defined. We will often call *n-isogeny* any isogeny of degree n.

Remark 14. There are other definitions of degree and separability ([Sil11b]), which are more general but require further knowledge about function fields. Function field $K(E_1)$ of elliptic curve E_1 over K consists, roughly speaking, of rational functions $\frac{g}{h}$ where g, h are homogenous polynomials from $K[x,y,z]$ of the same degree and h is not divisible by the projective form of $E_1 : y^2z - x^3 - axz^2 - bz^3$. Arbitrary isogeny $\alpha : E_1 \to E_2$ then induces injection of function fields $\alpha^* : K(E_2) \to K(E_1)$ by composition from the right. The degree of α is then defined as the degree of extension of field $K(E_1)$ over $\alpha^*(K(E_2))$ and α is separable if the extension is separable. This definition of degree allows us, for example, to quickly prove the multiplicativity of degree, which we will show in another way.

Lemma 15. ([Sut17]) Let $\alpha : E_1 \to E_2$ be an isogeny $\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ of elliptic curves over K. The following are equivalent:

(i) α is inseparable,

(ii) $v' = u' = 0$,

(iii) There exists an isogeny $\beta : E_p \to E_2$ such that $\alpha = \beta\pi_p$ where $\pi_p : E_1 \to E_p$.

Example 16. The degree of Frobenius morphism π_p is p. The degrees of $[1]$ and $[-1]$ are both 1. In Example 5 we can see that $\deg([2]) = 4$. It might seem that $\deg([k]) = k^2$. This is true but we will prove it later using the dual isogeny. Frobenius morphism is inseparable since $(x^p)' = px^{p-1} = 0$ and $1' = 0$ by Lemma 15 (ii) or directly from (iii). On the other hand, the isogeny $[2]$ from Example 5 is separable which we can verify from definition or use Lemma 15 and differentiate the denominator $(x^3+1)' = 3x^2 \neq 0$ and similarly numerator.

Example 17. In Example 8 we had an isogeny $\phi : E_1 \to E_2$ with the x-coordinate map $\frac{x^3-2x^2+4x+1}{x^2-2x+1}$. Clearly $(x^2-2x+1)'$ is not zero and the map is therefore separable. The degree of the isogeny is 3. Previously, we have computed the size of $\ker(\phi)$ to also be 3. We will see that this is not coincidence and there is a connection between degree and size of kernel.

[1] The degree can't be zero, otherwise both polynomials are constant and the isogeny is not surjective.

Corollary 18. For every isogeny $\alpha : E_1 \to E_2$ of elliptic curves over K there exists a separable isogeny α_s and a integer $n \geq 0$ such that

$$\alpha = \alpha_s \pi_p^n, \quad \deg(\alpha) = \deg(\alpha_s) p^n.$$

If K is finite field then there exists a separable isogeny α'_s such that $\alpha = \pi_p^n \alpha'_s$.

Proof. It's trivial for separable α. The proof for general K comes from applying Lemma 15 (iii): If α is inseparable then $\alpha = \beta\pi_p$ and $\deg(\beta) < \deg(\alpha)$. Either β is separable or we repeat the step for β. The case $K = \mathbb{F}_q$ uses the fact that every element of $\mathbb{F}_q$ has a unique p-th root. We then conclude that $\alpha\pi_p(x, y) = \alpha(x^p, y^p) = \pi_p\overline{\alpha}$ where $\overline{\alpha}$ is a map that comes from α by replacing its coefficients by their p-th root. It remains to show that $\overline{\alpha}$ is an isogeny from E_1 to E'_1 where if E_1 is given by $y^2 = x^3 + a_1x + b_1$ then $E'_1 : y^2 = x^3 + a_1^p x + b_1^p$. We leave out the details and refer the reader to [Sut17]. □

The degree of α_s is called the *separable degree* of α and we will denote it $\deg_s(\alpha)$. The immediate consequence of the previous corollary is the fact that if $p \nmid \deg(\alpha)$, then α is separable. The converse is not true but for an example we will have to wait for the dual isogeny $\widehat{\pi}$ (see footnote for Corollary 34).

Theorem 19. If $\alpha : E_1 \to E_2$ is an isogeny for E_1, E_2 over K then $\deg_s(\alpha) = |\ker(\alpha)|$ and in particular, if α is separable then $\deg(\alpha) = |\ker(\alpha)|$.

Proof. From Corollary 18 and the injectivity of Frobenius morphism, it suffices to assume that α is separable. The kernel of α has the same size as preimage of $\alpha^{-1}(Q)$ of any point $Q \in E_2(\overline{K})$, since α is homomorphism. To prove the theorem we will fix a point Q and construct a separable polynomial $f \in \overline{K}[x]$ such that $\deg(f) = \deg(\alpha)$ and each root x_0 of f defines a unique point $(x_0, y_0) \in \alpha^{-1}(Q)$. Since the degree of separable polynomial is exactly the number of its roots, the theorem indeed follows.

Let $\alpha(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ be the standard form. Consider a point $Q = (x_Q, y_Q) \in E_2(\overline{K})$ such that:

(i) $y_Q \neq 0$

(ii) $x_Q \neq a_u/a_v$ where a_u, a_v are the leading coefficients of u and v

(iii) For any point $(x_0, y_0) \in \alpha^{-1}(Q)$, x_0 is not a root of $u'v - v'u$

We can find such Q as $E_2(\overline{K})$ is infinite and there are only a finite number of points satisfying each of the properties (in (ii) we use the fact that α is separable and Lemma 15, i.e. $u'v - v'u \neq 0$). Let $f = u(x) - x_Q v(x)$. Clearly, $\deg(f) = \deg(\alpha)$ from definition of degree and (ii). The polynomial f is not separable if there exists root r of f which is also root of f'. In another words $u(r) - x_Q v(r) = u'(r) - x_Q v'(r) = 0$, which doesn't happen because of (iii), and so f is separable. Finally, each root r of f corresponds to two points P,$-P$ with $x_P = r$. Exactly one of them map to Q since $\alpha(P) = \alpha(-P)$ implies $P = -P$ and $y_Q = 0$ which is in contradiction with (i). So the number of roots of f is equal to $\alpha^{-1}(Q)$. □

Corollary 20. If $\alpha : E_1 \to E_2$ is an isogeny then $\ker(\alpha) \subseteq E[\deg(\alpha)]$.

Proof. The size of $\ker(\alpha)$ is $\deg_s(\alpha)$ and $\deg_s(\alpha) \mid \deg(\alpha)$. This means $\deg(\alpha)P = \infty$ for every point $P \in \ker(\alpha)$. □

Corollary 21. If $\alpha : E_1 \to E_2$ is an isogeny of elliptic curves over $\mathbb{F}_q$ and α has prime degree l where $l \nmid q$, then $\ker(\alpha)$ is a cyclic group of order l.

Another consequence of the Theorem 19 is the multiplicative property of degree.

Corollary 22. If $\alpha : E_1 \to E_2$ and $\beta : E_2 \to E_3$ are isogenies and $\gamma : E_1 \to E_3$ is the composition $\gamma = \beta\alpha$ then $\deg(\gamma) = \deg(\beta) \cdot \deg(\alpha)$ and $\deg_s(\gamma) = \deg_s(\beta) \cdot \deg_s(\alpha)$.

Proof. All three of the isogenies are surjective so $|\ker(\gamma)| = |\ker(\beta)||\ker(\alpha)|$. Theorem 19 then implies $\deg(\gamma_s) = \deg(\beta_s) \cdot \deg(\alpha_s)$. The proof for inseparable isogenies can be found in [Sil11b]. □

Notice that composition of isogenies is separable if and only if each of them is separable.

Isogenies from kernels

The kernel of every isogeny $\alpha : E_1 \to E_2$ is a finite subgroup of $E_1(\overline{K})$. It is natural to ask if every finite subgroup of $E_1(\overline{K})$ is a kernel of a suitable isogeny from E_1. In the context of abelian groups, every subgroup G of the group E_1 defines a surjective homomorphism uniquely up to isomorphism of the image. The image is then isomorphic to quotient group E_1/G. But it is not clear why this homomorphism is given by rational functions or why there exists an elliptic curve with the group structure E_1/G.

Before we move on to the theorem that answers these questions, we need to introduce stable subgroup. Stable subgroups will help us describe for curves E_1, E_2 over K and any isogeny $\phi : E_1 \to E_2$ over L, the relation of the field K and L.

Definition 23 (Stable subgroup)**.** Let E be an elliptic curve over K and L/K algebraic extension. Subgroup $G \subseteq E(\overline{K})$ is stable over L if $(\sigma(x), \sigma(y)) \in G$ for every affine $(x, y) \in G$ and $\sigma \in \mathrm{Gal}(\overline{K}/L)$.

If the reader is not familiar with Galois theory then the following lemma gives us an equivalent definition for finite fields.

Lemma 24. Let E be an elliptic curve over $\mathbb{F}_q$. Finite subgroup $G \subseteq E(\overline{\mathbb{F}}_q)$ is stable over $\mathbb{F}_{q^m}$ if $\pi_E^m(x, y) \in G$ for every affine $(x, y) \in G$.

Proof. One of the results of Galois theory is the fact that for any extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^m})$ is cyclic and generated by the automorphism $x \mapsto x^{q^m}$. □

Example 25. Any n-torsion $E[n] \subseteq E(\overline{\mathbb{F}}_q)$ is stable over $\mathbb{F}_q$ as $\pi_E(nP) = n\pi_E(P) = \infty \in E[n]$ for any $P \in E[n]$. Consider the curve $E : y^2 = x^3 + 1$ over $\mathbb{F}_5$ with the extension $\mathbb{F}_{25} = \mathbb{F}_5[z]/(z^2 - z + 2)$ and the subgroup $G = \{((3z + 3, z + 2), (3z + 3, 4z+3)), \infty\} \subseteq E(\mathbb{F}_{25})$ generated by $(3z+3, z+2)$. We can see that G is not stable over $\mathbb{F}_5$ since $\pi(3z + 3, z + 2) = (2z + 1, 4z + 3) \notin G$. However, G is stable over $\mathbb{F}_{25}$ as $\pi^2(3z + 3, z + 2) = \pi(3z^{25} + 3, z^{25} + 2) = (3z + 3, z + 2) \in G$.

As mentioned, we will be interested in stable subgroups in the context of kernels of isogenies. If $\phi : E_1 \to E_2$ is an isogeny of elliptic curves over the field $\mathbb{F}_q$, the kernel of ϕ is then stable over $\mathbb{F}_q$ because if $P \in \ker(\phi)$ then $\phi(\pi_{E_1}(P)) = \pi_{E_2}(\phi(P)) = \pi_{E_2}(\infty) = \infty$ where we used the fact that Frobenius endomorphism commutes with every isogeny. But this means $\pi_{E_1}(P) \in \ker(\phi)$. Every kernel of isogeny over $\mathbb{F}_q$ is therefore finite subgroup of $E_1(\overline{\mathbb{F}}_q)$, which is stable over $\mathbb{F}_q$. This can be generalized for any isogeny over L [Sil11b].

Surprisingly, the opposite is true: every finite subgroup stable over L is a kernel of appropriate isogeny over L as the next theorem shows. The proof is beyond the scope of this text [Sil11b].

Theorem 26. Let E_1 be an elliptic curve over K and G be a finite subgroup of $E_1(\overline{K})$. There exists an algebraic extension L/K, an elliptic curve E_2 over L and a separable isogeny $\alpha : E_1 \to E_2$ over L with $\ker(\alpha) = G$. The curve E_1 is unique up to isomorphism over L, i.e. if there is another such isogeny $\alpha_2 : E_1 \to E_3$ then there exists an isomorphism $\rho : E_3 \to E_2$ over L such that $\alpha = \rho\alpha_2$.

$$\begin{tikzcd}
G \subseteq E_1 \arrow[r, "\alpha"'] \arrow[d, "\alpha_2"'] & E_2 \\
E_3 \arrow[ur, "\rho"'] &
\end{tikzcd}$$

The field extension L/K is the minimal extension such that G is stable over L.

Corollary 27. Let E_1 be an elliptic curve over $\mathbb{F}_q$ and G be a finite subgroup of $E_1(\overline{K})$ such that $\pi_{E_1}(P) \in G$ for all $P \in G$. Then there exists an elliptic curve E_2 over $\mathbb{F}_q$ and a separable isogeny $\alpha : E_1 \to E_2$ with $\ker(\alpha) = G$. The curve E_2 and isogeny α are unique up to isomorphism over $\mathbb{F}_q$.

Theorem 26 together with Corollary 18 tell us that we can identify every isogeny, up to an isormophism, by its kernel and degree. If $\alpha = \alpha_s \pi_p^n$ is the decomposition of an isogeny α, where α_s is separable, then kernel of α defines α_s, up to an isomorphism, and degree of α determines the integer n.

Corollary 28. Any separable isogeny $\alpha : E_1 \to E_2$ with $\deg(\alpha) \neq 1$ can be expressed as a composition of prime degree isogenies.

Proof. The kernel G of α is non-trivial, it therefore contains prime order subgroup H. Theorem 26 implies that there is an isogeny $\alpha_2 : E_1 \to E_3$ with $\ker(\alpha_2) = H$. Now consider the subgroup $\alpha_2(G) \subseteq E_2$. The order of this subgroup is $|G|/|H|$ and $\alpha_2(G)$ is a kernel of some separable isogeny $\beta : E_3 \to E_4$. What is kernel of $\beta\alpha_2$? Every point $P \in E$ such that $\alpha_2(P) \in \ker(\beta)$ which is equivalent to $P \in G$. We therefore have two separable isogenies α and $\beta\alpha_2$ with the same kernel which means that there is an isomorphism $\rho : E_4 \to E_3$. If we denote $\gamma = \rho\beta$ then $\alpha = \gamma\alpha_2$ where γ has degree $|G|/|H|$ and α_2 has prime degree $|H|$. We can apply the same argument to γ and proceed by induction. □

Dual isogeny

We close this chapter with the notion of dual isogeny, which shows us that isogenies are not 'one-way', and it is better to think of isogenies as symmetric relations. Moreover, dual isogenies will help us describe the torsion subgroup $E[n]$ as well as introduce the term ordinary elliptic curve, which is the focus of this thesis.

Lemma 29. If $\alpha : E_1 \to E_2$, $\beta : E_1 \to E_3$ are isogenies of elliptic curves over K where α is separable and satisfying $\ker(\alpha) \subseteq \ker(\beta)$ then there exists a unique isogeny $\gamma : E_2 \to E_3$ such that $\beta = \gamma\alpha$.

Proof. We will prove it for $K = \mathbb{F}_q$, see [Sil11b] for complete proof. Denote the composition $\beta = \pi_p^b \beta_s$ from Corollary 18 and consider the subgroup $\alpha(\ker(\beta)) \subseteq E_2$. It is stable over $\mathbb{F}_q$ because $\ker(\beta)$ is stable over $\mathbb{F}_q$ and $\pi_{E_2}\alpha = \alpha\pi_{E_1}$. It therefore generates an isogeny $\gamma' : E_2 \to E_2'$. Seeing that $\gamma'\alpha$, β_s have the same kernel, they must differ only by isomorphism $\rho : E_2' \to E_3'$, i.e. $\rho\gamma'\alpha = \beta_s$. Finally, $\gamma = \pi_p^b \rho\gamma'\alpha$ is the desired isogeny.

$$\begin{tikzcd}
E_1 \arrow[r, "\beta_s"'] \arrow[d, "\alpha"'] & E_3' \arrow[r, "\pi_p^b"'] & E_3 \\
E_2 \arrow[r, "\gamma'"'] & E_2' \arrow[u, "\rho"] &
\end{tikzcd}$$

□

Lemma 30. For any n-isogeny $\alpha : E_1 \to E_2$ there exists a unique isogeny $\widehat{\alpha} : E_2 \to E_1$ for which $\widehat{\alpha}\alpha = [n]$.

Proof. For separable isogeny α the statement is a corollary of Lemma 29 if we recall that $\ker(\alpha) \subseteq E[\deg(\alpha)]$. The difficulty comes from the inseparable part. Notice that the uniqueness is trivial: If $\beta\alpha = \gamma\alpha$, then $\beta = \gamma$ by the surjectivity of α. We refer the reader to [Sil11b] for complete proof. □

Definition 31 (Dual isogeny)**.** We call the isogeny $\widehat{\alpha}$ from Lemma 30 the dual isogeny of α.

We have already met a special type of dual isogeny in the context of isomorphism. Every isomorphism α satisfies $\widehat{\alpha}\alpha = [1]$. Isomorphisms are therefore exactly the 1-isogenies. We can now say that two elliptic curves are *isogenous*(*n-isogenous*) whenever there is an isogeny (n-isogeny) between them.

Lemma 32. Let $\alpha : E_1 \to E_2$, $\beta : E_2 \to E_3$, $\gamma : E_1 \to E_2$ be any isogenies[2] and $n = \deg(\alpha)$ then

(i) $\alpha\widehat{\alpha} = [n]$

(ii) $\widehat{\beta\alpha} = \widehat{\alpha}\widehat{\beta}$, $\quad \widehat{\alpha + \gamma} = \widehat{\alpha} + \widehat{\gamma}$

[2] We have not defined what is a sum of isogenies, but it can be easily proved that the map $(\alpha + \gamma)(P) = \alpha(P) + \gamma(P)$ is an isogeny.

(iii) $\widehat{[m]} = [m]$ and $\deg([m]) = m^2$ for all $m \in \mathbb{Z}$

(iv) $\deg(\widehat{\alpha}) = n, \quad \widehat{\widehat{\alpha}} = \alpha.$

Proof. (i) Consider $(\alpha\widehat{\alpha})\alpha = \alpha(\widehat{\alpha}\alpha) = \alpha[n] = [n]\alpha$. Recall that if α is non-constant and $\beta\alpha = \gamma\alpha$ then $\gamma = \delta$ for isogenies β, γ. So $\alpha\widehat{\alpha} = [n]$.

(ii) Let $\deg(\beta) = m$. Then $(\widehat{\alpha}\widehat{\beta})(\beta\alpha) = \widehat{\alpha}(\widehat{\beta}\beta)\alpha = \widehat{\alpha}[m]\alpha = [m][n] = [mn]$, where we know that $\deg(\beta\alpha) = \deg(\beta)\deg(\alpha) = mn$. The second part assumes some knowledge on Weil's pairing so we refer the reader to [Sil11b].

(iii) We will prove the first part by two inductions, for the non-positive and non-negative part. The statement is trivial for isogenies $[-1], [1]$. Let $\widehat{[m]} = [m]$ for some $m \in \mathbb{Z}$. Using (iii) we get that $\widehat{[m \pm 1]} = \widehat{[m] \pm [1]} = \widehat{[m]} \pm \widehat{[1]} = [m] \pm [1] = [m \pm 1]$, which provides the two needed induction steps. The second part follows from $[\deg(m)] = \widehat{[m]}[m] = [m][m] = [m^2]$.

(iv) Using (iii): $n^2 = \deg([n]) = \deg(\widehat{\alpha}\alpha) = \deg(\widehat{\alpha})\deg(\alpha) = \deg(\widehat{\alpha})n$. The second part is a consequence of (i).

□

Corollary 33. If E is an elliptic curve over $\mathbb{F}_q$ and $n \in \mathbb{Z}$ then $[n]$ is inseparable if and only if $p \mid n$.

Proof. If $[n]$ is inseparable then $[n] = \pi_p\alpha$ for some α and $p \mid \deg([n]) = n^2$ which means $p \mid n$. Suppose $n = pm$ for $m \in \mathbb{Z}$. Clearly $[p][m] = [n]$, so it suffices to show that $[p]$ is inseparable because composition of inseparable isogeny with any isogeny is inseparable. By definition of dual $\pi_p\widehat{\pi_p} = [\deg(\pi_p)] = [p]$. Hence $[p]$ is inseparable. □

Corollary 34. If E is an elliptic curve over $\mathbb{F}_q$ and n integer satisfying $p \nmid n$ then $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. Moreover $E[p] \cong \mathbb{Z}_p$ or $E[p] = \{\infty\}$.

Proof. We will prove this for n prime. Rest can be found in [Sut17]. If $p \nmid n$ then $[n]$ is separable and Lemma 32 (iii) implies $|E[n]| = n^2$. Since n is prime then every affine point in $E[n]$ has order n and the result follows. Now the second statement: Since $[p] = \pi_p\widehat{\pi_p}$, then $E[p] = \ker(\widehat{\pi_p})$. The degree of $\widehat{\pi_p}$ is p so its separable degree and consequently the size of kernel is either[3] 1 or p. □

The elliptic curves for which $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ are called *ordinary* and other curves are called *supersingular*. We will see that ordinary and supersingular curves often behave in very different ways. We will be mainly interested in the ordinary curves.

We close this chapter with theorem due to Sato, which underlines the fact that being isogenous is an equivalence on the set of elliptic curves. Moreover, it gives us invariant that uniquely determines each class of isogenous curves - the cardinality $|E(\mathbb{F}_q)|$. The proof can be found in [Sil11b].

Theorem 35. Elliptic curves E_1, E_2 defined over $\mathbb{F}_q$ are isogenous if and only if $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$.

[3] Notice that when E is ordinary then $\widehat{\pi_p}$ is separable and has degree divisible by p

Chapter 2

Isogeny graphs

The theorem of Sato and dual isogeny has established that being isogenous is a symmetric relation on the set of all elliptic curves over $\mathbb{F}_q$. Any symmetric relation on a finite set invokes an undirected graph. The aim of this chapter is to introduce such graphs, in particular isogeny volcanoes, which bring a new approach for studying isogenies in the context of cryptography. Throughout the chapter, $\mathbb{F}_q$ is a finite field with $q = p^m$, $p > 2$ and l is a prime distinct from p.

In the light of Theorem 26 and Lemma 24 which characterize isogenies using finite subgroups of elliptic curves only up to isomorphism, we will define the oriented graph $g_l(\mathbb{F}_q)$ (more precisely oriented multigraph) as follows:

- Vertices are classes of elliptic curves over $\mathbb{F}_q$ which are isomorphic over $\mathbb{F}_q$, denoted by $[E]$ for class containing all elliptic curves isomorphic to E.
- Edges are classes of l-isogenies defined as: Two l-isogenies $\phi : E_1 \to E_2$, $\phi' : E_1' \to E_2'$ are in the same class if and only if $\rho'\phi\rho = \phi'$ for some isomorphisms $\rho : E_1' \to E_1$ and $\rho' : E_2 \to E_2'$. Each such class $[\phi]$, where $\phi : E_1 \to E_2$, is an edge from $[E_1]$ to $[E_2]$.

$$\begin{tikzcd}
E_1 \arrow[r, "\phi"'] \arrow[d, phantom] & E_2 \arrow[d, "\rho'"'] \\
E_1' \arrow[u, "\rho"] \arrow[r, "\phi'"'] & E_2'
\end{tikzcd}$$

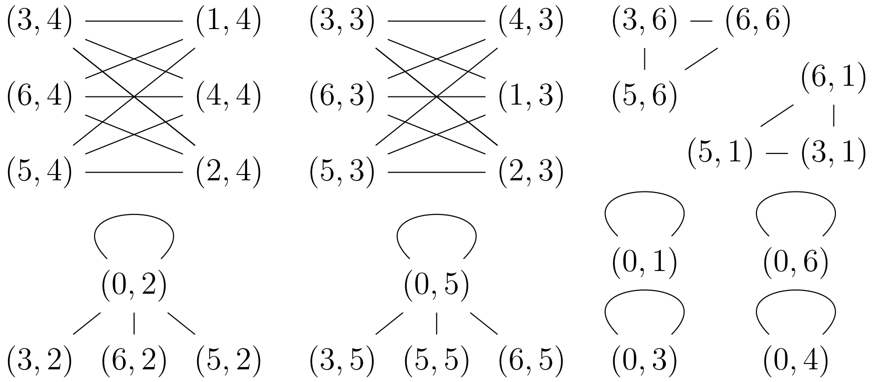
Besides multiple edges between two vertices, loops are also permitted in $g_l(\mathbb{F}_q)$.

Lemma 36. For every two vertices $[E_1]$, $[E_2] \in g_l(\mathbb{F}_q)$ there is a bijection between edges from $[E_1]$ to $[E_2]$ and edges from $[E_2]$ to $[E_1]$ given by $[\phi] \mapsto [\widehat{\phi}]$

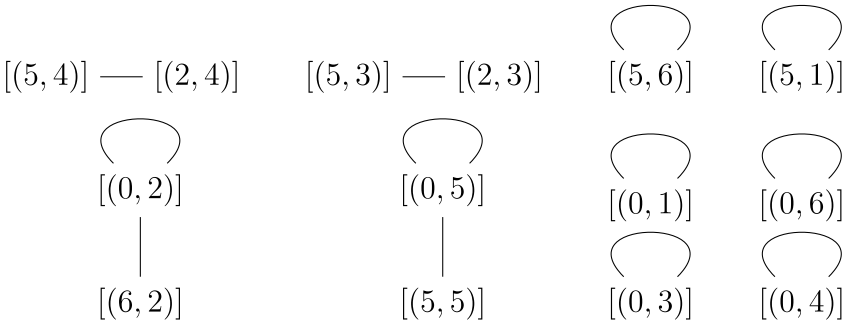
Proof. If $[\widehat{\phi_1}] = [\widehat{\phi_2}]$ then $\rho_1\widehat{\phi_1}\rho_2 = \widehat{\phi_2}$. By Lemma 32 $\phi_2 = \widehat{\widehat{\phi_2}} = \widehat{\rho_1\widehat{\phi_1}\rho_2} = \widehat{\rho_2}\phi_1\widehat{\rho_1}$, which means $[\phi_1] = [\phi_2]$. So the map is injective and clearly surjective. □

Because of the Lemma 36, we will often treat $g_l(\mathbb{F}_q)$ as undirected, uniting the opposite edges $[\phi]$ and $[\widehat{\phi}]$.

Example 37. Consider elliptic curves over $\mathbb{F}_7$ and all 3-isogenies between them. In the picture, every tuple (a, b) represents elliptic curve given by $y^2 = x^3 + ax + b$, every isogeny and its dual is represented by one edge and elliptic curves with no 3-isogenies are omitted.



It can be shown that the isomorphism classes are
$[(3,4),(6,4),(5,4)]$, $[(1,4),(4,4),(2,4)]$, $[(3,3),(6,3),(5,3)]$, $[(0,3)]$,
$[(4,3),(1,3),(2,3)]$, $[(3,6),(6,6),(5,6)]$, $[(6,1),(5,1),(3,1)]$, $[(0,1)]$
$[(3,2),(6,2),(5,2)]$, $[(3,5),(5,5),(6,5)]$, $[(0,2)]$, $[(0,5)]$, $[(0,4)]$.
The graph $g_3(\mathbb{F}_7)$ then looks like:



Looking at the graph $g_3(\mathbb{F}_7)$, we can see some duplicity of each components. This is in fact not a coincidence and is a result of underlying isomorphisms. These isomorphisms are not defined over $\mathbb{F}_7$ but over some extension of $\mathbb{F}_7$. Fortunately, all isomorphisms can be described very well:

Lemma 38. Elliptic curves $E : y^2 = x^3 + ax + b$, $E' : y^2 = x^3 + a'x + b'$ over $\mathbb{F}_q$ are isomorphic over $\overline{\mathbb{F}}_q$ if and only if $a' = u^4 a$, $b' = u^6 b$ for some $u \in \overline{\mathbb{F}}_q^{\times}$ and the isomorphism is $(x, y) \mapsto (u^2 x, u^3 y)$.

Proof. Any isomorphism over $\overline{\mathbb{F}}_q$ is by definition isogeny over $\overline{\mathbb{F}}_q$ of degree 1. Such isogeny has standard form $(u(x), s(x)y)$ where $u, s \in \overline{\mathbb{F}}_q[x]$ are polynomials of degree 1. If we express u, s as general linear polynomials and substitute in the curve equation of E' we should arrive at the result. □

Definition 39 (j-invariant)**.** Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_q$. The j-invariant of E is defined as

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \in \mathbb{F}_q.$$

The denominator is non-zero since E is not a singular curve. It can be shown that for every element $j \in \mathbb{F}_q$ there is an elliptic curve over $\mathbb{F}_q$ with j as a j-invariant. The proof follows from the fact that every $E : y^2 = x^3 + ax + b$ satisfies $a = 3j(E)(1728 - j(E))$ and $b = 2j(E)(1728 - j(E))^2$ (See [Was08]). The motivation for the name j-invariant is the invariance over isomorphisms over $\overline{\mathbb{F}}_q$.

Theorem 40. ([Sut17]) Let E and E' be elliptic curves over $\mathbb{F}_q$. Then E and E' are isomorphic over $\overline{\mathbb{F}}_q$ if and only if $j(E) = j(E')$. If $j(E) = j(E') \neq 0, 1728$ then E and E' are isomorphic over $\mathbb{F}_{q^2}$, where the isomorphism is (u^2x, u^3y) for $u^2 \in \mathbb{F}_q$.

Elliptic curves isomorphic over $\overline{\mathbb{F}}_q$ but not over $\mathbb{F}_q$ are called *twists*. In particular, if $j(E) = j(E') \neq 0, 1728$ then E is called *quadratic twist* of E'.

Lemma 41. Let E be an elliptic curve over $\mathbb{F}_q$ with $j(E) \neq 0, 1728$. If E_1' and E_2' are quadratic twists of E then E_1' and E_2' are isomorphic (over $\mathbb{F}_q$).

Proof. From Lemma 38 we know that $E_1' : y^2 = x^3 + u_1^4ax + u_1^6b$ and $E_2' : y^2 = x^3 + u_2^4ax + u_2^6b$ for some $u_1, u_2 \in \overline{\mathbb{F}}_q$. By Theorem 40 $u_1^2, u_2^2 \in \mathbb{F}_q$. Also $u_1, u_2 \notin \mathbb{F}_q$, and so u_1^2, u_2^2 are not quadratic residues. Hence $\frac{u_1^2}{u_2^2}$ is a quadratic residue and $\frac{u_1}{u_2} = u \in \mathbb{F}_q$. Finally, $u_1^4a = u^4u_2^4a$ and $u_1^6b = u^6u_2^6b$, which means that E_1' and E_2' are isomorphic over $\mathbb{F}_q$ by Lemma 38. □

Elliptic curves with j-invariant 0 or 1728 correspond to the cases $a = 0$, $b = 0$. These often behave in different and more complicated manner than curves with other j-invariants. The reason behind these complications is the fact that they have too many automorphisms (isomorphisms with the same domain and codomain).

Lemma 42. Let E be an elliptic curve over $\mathbb{F}_q$:

(i) If $j(E) \neq 0, 1728$ then there are only 2 automorphisms of E defined over $\overline{\mathbb{F}}_q$: $[1]$ and $[-1]$.

(ii) If $j(E) = 0$ or 1728 then the number of automorphisms of E over $\overline{\mathbb{F}}_q$ is d where $2 < d$ and $d \mid 24$.

Proof. Let $\rho, \sigma : E \to E$ be two automorphisms given by $u_\rho, u_\sigma \in \overline{\mathbb{F}}_q$ respectively, in the sense of Lemma 38. If E is given by $y^2 = x^3 + ax + b$ then $au_\rho^4 = au_\sigma^4$ and $u_\rho^6b = u_\sigma^6b$. Assuming $j(E_1) \neq 0, 1728$ we get $a, b \neq 0$ and consequently $u_\rho^2 = u_\sigma^2$. Last equation can be expressed as $(u_\rho - u_\sigma)(u_\rho + u_\sigma) = 0$ and thus $u_\rho = \pm u_\sigma$. There are therefore at most two automorphisms and they differ by $[-1]$. The case for (ii) can be found in [Sil11b]. □

We will almost always omit the cases of j-invariant equal to 0 or 1728 and only briefly comment their situation. Equipped with this knowledge about isomorphisms we can gain further information about $g_l(\mathbb{F}_q)$ - the degree of each vertex. Firstly, we will look at the number of l-isogenies from a given elliptic curve.

Lemma 43. *Let E be an elliptic curve over $\mathbb{F}_q$. Up to an isomorphism, there are exactly $l+1$ isogenies over $\overline{\mathbb{F}}_q$ of degree l. The number of them defined over $\mathbb{F}_q$ is either $0, 1, 2$ or $l+1$.*

Proof. Every l-isogeny is separable as $l \neq p$. Every separable isogeny is uniquely determined by the kernel, up to an isomorphism. The kernels of l-isogenies over $\overline{\mathbb{F}}_q$ are precisely the subgroups of $E[l]$ or order l. We know that $E[l] \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ and it can be easily shown that the group $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ has the following $l+1$ subgroups of order l: $\langle(0,1)\rangle, \langle(1,0)\rangle, \langle(1,1)\rangle, \ldots, \langle(1,l-1)\rangle$[1].

It remains to count the isogenies defined over $\mathbb{F}_q$. Counting isogenies over $\mathbb{F}_q$ is equivalent to count the subgroups of $E[l]$ of order l, which are stable over $\mathbb{F}_q$. Let G be such subgroup generated by P. Then $\pi(P) = \lambda P$ for some $\lambda \in \mathbb{Z}/l\mathbb{Z}$. In another words, if we consider the restriction π_l of π to the vector space $E[l]$ over $\mathbb{Z}/l\mathbb{Z}$ then λ is its eigenvalue and G subspace of eigenspace associated to λ. Since $E[l] \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ is a vector space of dimension 2, π_l can either have 0 eigenvalues, 2 distinct eigenvalues or 1 eigenvalue with geometric multiplicity 1 or 2.

If there are 0 eigenvalues, then we have no l-isogenies. If there are two distinct eigenvalues λ, μ, then both eigenspaces G_λ, G_μ have size l and are therefore the only subgroups of $E[l]$ of size l stable over $\mathbb{F}_q$, hence two l-isogenies.

If π_l has one eigenvalue of geometric multiplicity 1, which means that the size of associated eigenspace is l, we have exactly one isogeny.

Finally, if π_l has one eigenvalue of geometric multiplicity 2, i.e. $\pi(P) = \lambda P$ for all $P \in E[l]$, then each subgroup of $E[l]$ of size l is a kernel of l-isogeny, hence $l+1$ l-isogenies.

□

Remark 44. We can also express the restriction π_l of π to $E[l]$ using two-by-two matrices over $\mathbb{Z}/l\mathbb{Z}$. If π_l has any eigenvalues, we can use the Jordan normal form to obtain one of the following matrices (corresponding to 1 eigenvalue λ with multiplicity 1 or 2 and 2 eigenvalues λ, μ).

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \quad \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

Corollary 45. *Let E be an elliptic curve over $\mathbb{F}_q$ with $j(E) \neq 0, 1728$. If $\phi_1, \ldots, \phi_k$ are all isogenies from E with pairwise different kernel then edges from $[E]$ are precisely the classes $[\phi_1], \ldots, [\phi_k]$. In particular, the number of outgoing edges from $[E]$ is $0, 1, 2$ or $l+1$.*

Proof. Suppose there is another edge $[\psi]$ from $[E]$ for $\psi : E_1 \to E_2$. Then there exists an isomorphism $\rho : E \to E_1$ and $\psi\rho$ is an l-isogeny and must be equal to one

[1] $\langle x \rangle$ denotes the subgroup generated by element x

of $\phi_1, \dots, \phi_k$, up to isomorphism. Hence $[\phi] = [\phi_i]$ for some $i \in \{1, \dots, k\}$. Now we will prove that if $[\phi_i] = [\phi_j]$ then $i = j$. If $[\phi_i] = [\phi_j]$ then $\rho_1 \phi_i \rho_2 = \phi_j$ where ρ_1 is an isomorphism and ρ_2 must be automorphism of E and so $\rho_2 = [\pm 1]$ by Lemma 42. This implies $\phi_j = \rho_1 \phi_i [\pm 1] = \pm \rho_1 \phi_i$. Thus ϕ_i and ϕ_j have the same kernel and $i = j$. The second statement is a consequence of Lemma 43. □

Example 46. Consider elliptic curves $E_1 : y^2 = x^3 + x$, $E_2 : y^2 = x^3 + x + 3$, over $\mathbb{F}_5$ and an 2-isogeny $\phi : E_1 \to E_2$, defined as

$$\phi(x, y) = \left(\frac{x^2 - 2x - 2}{x - 2}, \frac{x^2 y + xy + y}{x^2 + x - 1} \right),$$

The j-invariant of E_1 is $1728 \frac{4 \cdot 1^3}{4 \cdot 1^3 + 27 \cdot 0^2} = 1728$. The affine points (x, y) in kernel are those for which $x = 2$, which is only $(2, 0)$. There is an automorphism which sends $(2, 0)$ to $(3, 0)$ which doesn't lie in $\ker(\phi)$ and generates another 2-isogeny. We have therefore two isogenies with different kernel but in the same class $[\phi]$ as they differ only by isomorphism ρ.

Quadratic twists are uniquely determined up to an isomorphism. We can therefore call a vertex $[E]$ a (quadratic) twist of vertex $[E']$ if E is quadratic twist of E'. We will denote $[E']$ as $[E]^t$. Similarly we can assign to each edge $[\phi]$ its quadratic twist $[\phi]^t$. Furthermore, if V is a component of $g_l(\mathbb{F}_q)$ without vertices $[E]$, for which $j(E) = 0$ or 1728, we can consider the *twisted component* of V: the induced subgraph of $g_l(\mathbb{F}_q)$ on the set of vertices $V^t = \{[E]^t \mid [E] \in V\}$.

Lemma 47. Let V be a component of $g_l(\mathbb{F}_q)$ without vertices $[E]$, for which $j(E) = 0$ or 1728. The map $f : V \to V^t$ defined by $f([E]) = [E]^t$ is an isomorphism of graphs, i.e. a bijection on the set of vertices which satisfies for all $[E_1], [E_2] \in V$: There is a bijection between the set of edges from $[E_1]$ to $[E_2]$ and the set of edges from $[E_1]^t$ to $[E_2]^t$.

Proof. We know that the map f is a bijection on the set of vertices of V. It remains to count the number of edges between $[E_1]$, $[E_2]$ and between $[E_1]^t$, $[E_2]^t$.

At first we will count the number of edges adjacent to $[E_1]$ and number of edges adjacent to $[E_1]^t$. By Corollary 45, it suffices to count number of isogenies from E_1 and E_1^t with pairwise different kernel up to an isomorphism. In another words we will count the number of subgroups of order l stable over $\mathbb{F}_q$ of both elliptic curves. Let $\rho : E_1 \to E_1^t$, $\rho(x, y) = (u^2 x, u^3 y)$ be any isomorphism over $\overline{\mathbb{F}}_q$. If $G \subseteq E_1(\overline{\mathbb{F}}_q)$ is a subgroup of order l stable over $\mathbb{F}_q$, then $\rho(G)$ also has order l. Whether it is also stable over $\mathbb{F}_q$ depends on the Frobenius endomorphism, i.e $\pi_E(x, y) \in \rho(G)$ for all $(x, y) \in \rho(G)$. This is equivalent to $((u^2 x)^q, (u^3 y)^q) \in \rho(G)$ for all $(x, y) \in G$. We know that $u^2 \in \mathbb{F}_q$ so $((u^2 x)^q, (u^3 y)^q) = (u^2 x^q, (u^3 y)^q)$. Since G is stable over $\mathbb{F}_q$ then $(x^q, y^q) \in G$ and $\rho(x^q, y^q) \in \rho(G)$ as well as $-\rho(x^q, y^q) \in \rho(G)$. However, $\pm\rho(x^q, y^q) = \pm(u^2 x^q, u^3 y^q) = (u^2 x^q, \pm u^3 y^q)$ and these are the only points in $E_1^t(\overline{\mathbb{F}}_q)$ with x-coordinate $u^2 x^q$. It must be therefore that $((u^2 x)^q, (u^3 y)^q)$ is one of them and in particular $((u^2 x)^q, (u^3 y)^q) \in \rho(G)$.

We have proved that there is a bijection between the set e_1 of edges adjacent to $[E_1]$ and the set e_1^t of edges adjacent to $[E_1]^t$. We now have to show that the there is the same number of edges in e_1 adjacent to $[E_2]$ as is the number of edges in e_1^t adjacent to $[E_2]^t$. We will again use the bijection ρ between stable subgroups of E_1 and E_1^t. Let $\phi : E_1 \to E_2$ and $\psi : E_1^t \to E_3$ be l-isogenies generated by G and $\rho(G)$ and consider the isogeny $\alpha = \psi\rho\widehat{\phi} : E_2 \to E_3$ defined over $\mathbb{F}_{q^2}$. If we prove that $E_2[l] \subseteq \ker(\alpha)$ then there exists an isogeny $\beta : E_2 \to E_3$ over $\mathbb{F}_{q^2}$ such that $l\beta = \alpha$ by Lemma 29 and comparing degree $\deg(\alpha) = \deg(\psi\rho\widehat{\phi}) = l \cdot 1 \cdot l = l^2$ with degree $\deg(l\beta) = l^2 \deg(\beta)$ tells us that $\deg(\beta) = 1$ and β is isomorphism over $\mathbb{F}_{q^2}$ between E_2 and E_3. Hence $[E_2]^t = [E_3]$ and we have a bijection between edges from $[E_1]$ to $[E_2]$ and $[E_1]^t$ to $[E_2]^t$ as desired.

$$\begin{tikzcd}
E_1 \arrow[r, "\rho"] \arrow[d, "\phi"'] & E_1^t \arrow[d, "\psi"] \\
E_2 \arrow[r, "\alpha"'] & E_3
\end{tikzcd}$$

It remains to show that $E_2[l] \subseteq \ker(\alpha)$. Let P, Q be generators of $E_1[l]$ such that $\langle P \rangle = \ker(\phi)$. Then $\phi(Q) \in E_2[l]$ and we can complete the point to basis $\phi(Q), R$ of $E_2[l]$. We will prove that $\alpha(\phi(Q)) = \infty$ and $\alpha(R) = \infty$, the rest will follow from Lemma 29. Trivially, $\alpha(\phi(Q)) = \psi\rho\widehat{\phi}\phi(Q) = \infty$. By definition of dual $\phi\widehat{\phi}(R) = \infty$ hence $\widehat{\phi}(R) \in \ker(\phi)$ and consequently $\rho\widehat{\phi}(R) \in \ker(\psi)$, which yields $\alpha(R) = \infty$.

□

The proof of the next lemma will have to wait for the next chapter, but is the last important piece of information about twisted components in $g_l(\mathbb{F}_q)$.

Lemma 48. If E and E^t are quadratic twists and E is ordinary, then E and E^t are not isogenous. In particular, for any component V of $g_l(\mathbb{F}_q)$, V^t and V are disjoint.

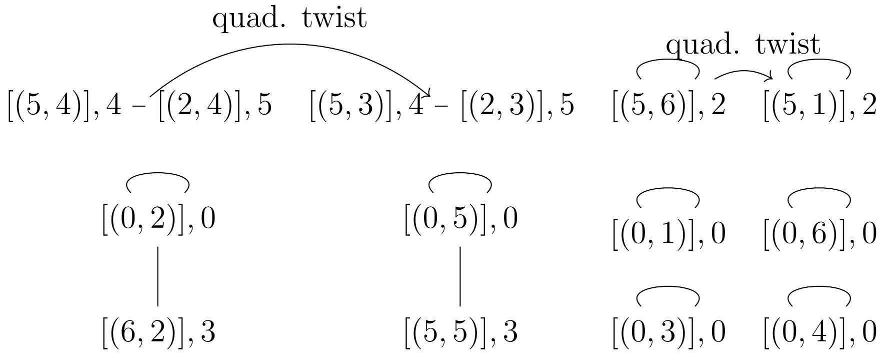
We can now define the l-isogeny graph $G_l(\mathbb{F}_q)$. The idea is to simply unite every component with its twisted component.

Definition 49 (Isogeny graph)**.** The l-isogeny graph $G_l(\mathbb{F}_q)$ is an undirected multigraph with vertices $\mathbb{F}_q$ and edges defined as follows. For each $j, j' \in \mathbb{F}_q$:

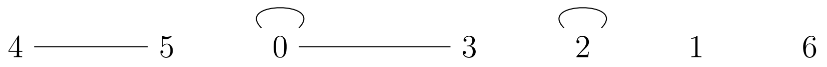
- If neither j or j' is equal to 0 or 1728 then there is edge between j and j' for each edge in $g_l(\mathbb{F}_q)$ between $[E]$ and $[E']$ where E and E' are elliptic curves such that $j(E) = j$ and $j(E') = j'$.
- Otherwise there is an edge between j and j' if and only if there exist l-isogenous elliptic curves E and E' such that $j(E) = j$ and $j(E') = j'$.

We will represent edges of $G_l(\mathbb{F}_q)$ as a tuple $([\phi], [\phi]^t)$.

Example 50. Continuing on the example of $g_3(\mathbb{F}_5)$ we can compute j-invariant of each vertex and thus identify the twists (j-invariant is written next to each vertex).



The graph $G_3(\mathbb{F}_7)$ then looks like (including the vertices with no edges):



We have so far not talked about ordinary and supersingular curves in the context of isogeny graphs. As it turns out, all components will be composed of j-invariants of only supersingular curves or of only ordinary curves. Recall that an elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if the separable degree $\deg_s[p] = 1$.

Lemma 51. Let $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ be an isogeny. Then E_1 is supersingular if and only if E_2 is supersingular.

Proof. For every $P \in E_1(\overline{K})$ we have $[p]_{E_2}\alpha(P) = \alpha(P) + \cdots + \alpha(P) = \alpha(pP) = \alpha[p]_{E_1}(P)$. So $[p]_{E_2}\alpha = \alpha[p]_{E_1}$ and

$$\deg_s([p]_{E_2}\alpha) = \deg_s(\alpha[p]_{E_1})$$

$$\deg_s([p]_{E_2})\deg_s(\alpha) = \deg_s(\alpha)\deg_s([p]_{E_1})$$
$$\deg_s([p]_{E_2}) = \deg_s([p]_{E_1})$$

In particular $\deg_s[p]_{E_2} = 1$ if and only if $\deg_s[p]_{E_1} = 1$. □

Every isomorphism is an isogeny (and supersingularity doesn't depend on the field of definition) so it makes sense to call j-invariant supersingular or ordinary dependent on the curves they represent and consequently call components of $G_l(\mathbb{F}_q)$. The focus of this thesis are the ordinary components but here we provide a brief summary about the supersingular ones.

Supersingular isogeny graphs

Lemma 52. If E is a supersingular curve over $\mathbb{F}_q$ then $j(E) \in \mathbb{F}_{p^2} \subseteq \overline{\mathbb{F}}_q$.

Proof. Consider the map $[p]$ which can be expressed as $\alpha\pi^r$ for some non-negative integer r and separable isogeny α. The kernel of $[p]$ is trivial, and so is the kernel of α and α is therefore isomorphism, which means $\deg(\alpha) = 1$. Using the fact that $\deg[p] = p^2$ implies $\deg(\pi^r) = p^r = p^2$ and $[p] = \alpha\pi^2$. Recall that the codomain E'

of the Frobenius p^2-morphism is given by $y^2 = x^3 + a^{p^2}x + b^{p^2}$ assuming the domain E is $y^2 = x^3 + ax + b$. This yields that $E' \cong E$ by isomorphim α and thus

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

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

$$j(E) = j(E)^{p^2}.$$

Elements of $\mathbb{F}_q$ which are fixed by $x \mapsto x^{p^2}$ are precisely those which lie in $\mathbb{F}_{p^2}$. □

It can be further shown that every l-isogeny from a given supersingular curve is defined over $\mathbb{F}_{p^2}$. Since there is always $l + 1$ such isogenies, then the supersingular components, not including 0 or 1728, are regular graphs of degree $l + 1$. One can prove that there is always only one supersingular component (see [Koh96]).

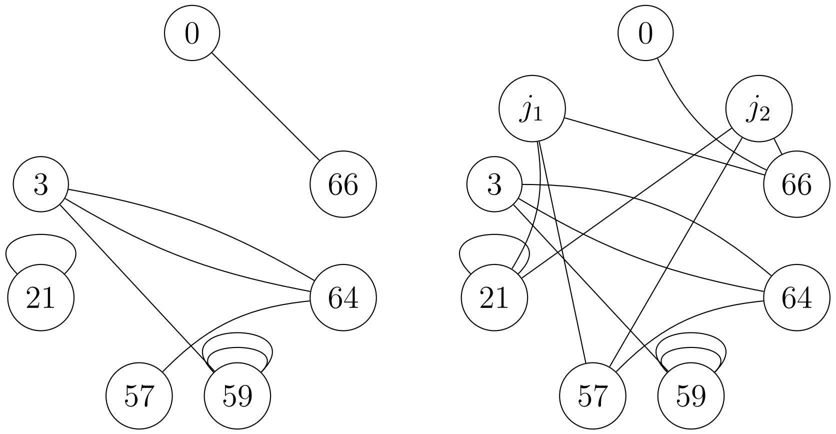


Figure 2.1: Supersingular components of $G_2(\mathbb{F}_{101^2})$ and $G_2(\mathbb{F}_{101})$ where $\mathbb{F}_{101^2} \cong \mathbb{F}_{101}[z]/(z^2 + 97z + 2)$ and $j_1 = z + 35$, $j_2 = 100z + 39$

Volcanoes

The behaviour of ordinary components of $G_l(\mathbb{F}_q)$ is rather different. They are the so called l-volcanoes or sometimes just volcanoes. We will at first introduce the volcanoes in pure graph theoretic terms and in the following chapters show that they actually form the ordinary components of $G_l(\mathbb{F}_q)$. Hopefully, reader will find it easier to follow the theory this way. The definition we use here is a bit different as the original definition from [Sut12]. The reason is that our definition describes precisely the possible graphs of ordinary elliptic curves.

Definition 53 (Volcano)**.** An l-volcano V is a connected undirected multigraph whose vertices are partitioned into one or more levels $V_0, \ldots, V_d$ such that the following hold:

(i) The subgraph on V_0 is a regular graph of degree at most 2 which has no loops if $|V_0| > 1$.

(ii) For $i < d$, each vertex in V_i has degree $l + 1$.

(iii) 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.

The integer d is called a depth of volcano, the level V_0 crater (or surface) and the level V_d floor of the volcano. For any $j(E) \in V_i$ we will say the $j(E)$ (or simply E) has depth i.

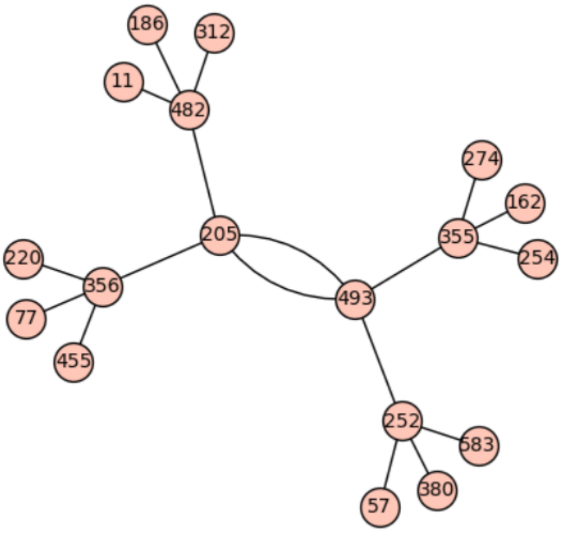


Figure 2.2: A 3-volcano with depth 2. One of ordinary components of $G_3(409)$ rendered by Sage functions implemented for this thesis.

More informally, a l-volcano is a graph with a cycle on the surface and isomorphic balanced trees rooted at each vertex of the cycle. We have defined volcanoes as multigraphs, but it is clear from (iii) that multi-edges and loops can occur only on the surface.

It can happen that the volcano has zero depth, meaning there is only surface. In that case, V is a connected regular graph of degree at most 2. This is either a single cycle on at least 3 vertices or one of the 5 following: single vertex with 0, 1 or 2 loops, two vertices connected with 0 or 2 edges.

Looking at the definition of volcano, the j-invariants of ordinary components of $G_l(\mathbb{F}_q)$ should be divided into some sort of levels, depending on what depth they lie. This suggests that all of the j-invariants on the same level share some property. This property, as we will present in the next chapter, is the endomorphism ring.

Modular polynomials

The standard way [Sut12] of defining $G_l(\mathbb{F}_q)$ is actually quite different and utilizes something called modular polynomial:

For each prime l, there is a polynomial $\Phi_l(X, Y) \in \mathbb{Z}[X, Y]$ satisfying for every prime power $q \neq 2, 3$ and $j, j' \in \mathbb{F}_q$ the following: There exist l-isogenous elliptic curves E and E' over $\overline{\mathbb{F}}_q$ such that $j(E) = j, j(E') = j'$ if and only if

$$\Phi_{l,q}(j_1, j_2) = 0,$$

where $\Phi_{l,q}(X, Y) \in \mathbb{F}_q[X, Y]$ is the polynomial Φ_l with every coefficient taken as element of $\mathbb{F}_q$. Moreover, $\Phi_l(X, Y)$ is symmetric in X and Y (i.e. $\Phi_l(X, Y) = \Phi_l(Y, X)$) and has degree $l + 1$ in each variable. The polynomial $\Phi_l(X, Y)$ is called modular polynomial. We will often write Φ_l instead of $\Phi_{l,q}$ if the finite field will be clear.

Remark 54. Unfortunately, the theory behind modular polynomials requires a background in complex analytic number theory and elliptic curves over the complex field. Even explaining the proper definition, let alone any proof of its properties would take several other chapters for the reader not familiar with this topic. We will therefore avoid them in the theory and meet them again in practical applications where we will be handling them as black boxes. Readers not satisfied with this can see for example [Sut17].

The l-th modular polynomial characterizes l-isogenous elliptic curves over $\overline{\mathbb{F}}_q$. The classical definition ([Sut12]) of $G_l(\mathbb{F}_q)$ is then: The l-isogeny graph $G_l(\mathbb{F}_q)$ has vertex set $\mathbb{F}_q$ and directed edges (j_1, j_2) present with multiplicity equal to the multiplicity of j_2 as a root of $\Phi_l(j_1, X)$.

This doesn't seem to correspond with our definition. First of all, this definition defines $G_l(\mathbb{F}_q)$ as directed graph. This isn't an issue as the multiplicity of edges from j_1 to j_2 is the same as from j_2 to j_1, except for cases $0, 1728$, so usually the graph is treated as undirected. Secondly, and more importantly, we have defined edges by l-isogenies of elliptic curves over $\mathbb{F}_q$. On the other hand, edge in the classical definition is conditioned by the existence of l-isogenous curves in some extension. It would seem that we have fewer edges in our $G_l(\mathbb{F}_q)$. The opposite is true, except for the case of supersingular elliptic curves:

Lemma 55 ([Sil11b])**.** If E_1, E_2 are ordinary elliptic curves over $\overline{\mathbb{F}}_q$ such that $j(E_1)$, $j(E_2) \in \mathbb{F}_q \setminus \{0, 1728\}$ and E_1, E_2 are l-isogenous (over $\overline{\mathbb{F}}_q$) then there exist elliptic curves E_1', E_2' over $\mathbb{F}_q$ such that $j(E_1') = j(E_1)$, $j(E_2) = j(E_2')$ and E_1, E_2' are l-isogenous over $\mathbb{F}_q$.

The only difference is indeed in supersingular curves. For example, in the discussed $G_3(\mathbb{F}_7)$ the vertex 6 is a supersingular vertex and has no edges. Nonetheless, the polynomial $\Phi_3(6, x)$ can be shown to have 4 roots, all equal to 6. Thus the vertex would have 4 loops even though there is no elliptic curve over $\mathbb{F}_7$ with j-invariant 6 that is a domain of any 3-isogeny. The isogenies are defined over higher extension. This slight discrepancy won't affect us as we will focus on the ordinary elliptic curves. We will get back to modular polynomials in further chapters, as they provide a good computational tool for isogenies and volcanoes.

Chapter 3

Endomorphism ring

An important type of isogeny is an endomorphism - an isogeny from curve to itself. As it turns out, endomorphisms on a given elliptic curve E form a ring $\mathrm{End}(E)$. These endomorphism rings distinguish isogenous elliptic curves and splits them to levels of volcanoes. We will focus only on ordinary elliptic curves as the endomorphism ring of supersingular curves have a different (and more complex) structure. The aim of this chapter is to characterize the ring $\mathrm{End}(E)$ and prove that it is isomorphic to order in an imaginary quadratic field. Throughout the chapter, K is a field with $\mathrm{char}(K) = p$ and $\mathbb{F}_q$ a finite field with $q = p^n$ for prime $p > 3$.

Definition 56 (Endomorphism)**.** Let E be an elliptic curve over the field K. Every isogeny $\alpha : E(\overline{K}) \mapsto E(\overline{K})$ is called endomorphism of E. In addition, we will call endomorphism also the zero map $[0] : E(\overline{K}) \mapsto E(\overline{K})$, defined as $[0](P) = \infty$ for all $P \in E(\overline{K})$.

Example 57. The multiplication isogeny $[m]$ for $m \in \mathbb{Z}$ as well as the Frobenius endomorphism π_E of elliptic curve E over $\mathbb{F}_q$ are examples of endomorphisms.

There are two natural operations $+$ and $\circ$ on the set of endomorphisms of given curve. The addition: $(\alpha + \beta)(P) = \alpha(P) + \beta(P)$ for all $P \in E(\overline{K})$ inherits commutativity and associativity from E. The set of endomorphisms of E therefore form an abelian group $\mathrm{End}(E)$ with $[0]$ as neutral element. The composition $\alpha \circ \beta$ is asociative and has $[1]$ as multiplicative identity. It can be proven that these two operations satisfy the distributive property and therefore form a ring [Sil11b]. We call this ring endomorphism ring $\mathrm{End}(E)$.

Remark 58. Some authors define $\mathrm{End}(E)$ as a ring of all endomorphisms defined over $\overline{K}$. We will see that in our case of ordinary curves over finite fields it actually doesn't make any difference. In another words, we will see that every endomorphism over $\overline{\mathbb{F}}_q$ of such curve is defined over $\mathbb{F}_q$.

The addition and multiplication of endomorphisms $[m]$ behaves exactly like the corresponding operations in $\mathbb{Z}$, i.e. $[m] + [n] = [m + n]$, $[m][n] = [mn]$. This gives us an inclusion of rings $\mathbb{Z} \subseteq \mathrm{End}(E)$. We will therefore identify $[m]$ with $m \in \mathbb{Z}$ and often omit the brackets. The inclusion also tells us that the characteristic of $\mathrm{End}(E)$ is the characteristic of $\mathbb{Z}$, which is 0.

We will prove that there is an inclusion of $\mathrm{End}(E)$ into a imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ and under this inclusion every endomorphism can be expressed as:

$$a + b\pi_E \quad a, b \in \mathbb{Q}.$$

This illustrates the importance of Frobenius endomorphism. Here we show three typical examples of endomorphism ring:

- The elliptic curve $E : y^2 = x^3 + 5x + 6$ defined over $\mathbb{F}_{17}$ has endomorphism ring isomorphic to $\mathbb{Z}[2\sqrt{2}i] \subset \mathbb{Q}(\sqrt{2}i)$ where the Frobenius endomorphism corresponds to $3 + 2\sqrt{2}i$ so we can write $\mathrm{End}(E) \cong \mathbb{Z}[\pi_E]$.

- The curve $E : y^2 = x^3 + (2z + 4)x + 2z$ over $\mathbb{F}_{25} = \mathbb{F}_5[z]/(z^2 + 4z + 2)$ has an endomorphism ring isomorphic to $\mathbb{Z}[\sqrt{6}i] = \mathbb{Z}[\frac{\pi_E+1}{2}]$ where the Frobenius endomorphism corresponds to $-1 + 2\sqrt{6}i$.

- On the other hand, the elliptic curve $E : y^2 = x^3+1$ over $\mathbb{F}_{25}$ has endomorphism ring $\mathrm{End}(E) \cong \mathbb{Z}$ and the Frobenius morphism corresponds to 5. The curve E is in fact supersingular. We will see that for ordinary curves over finite fields is the endomorphism ring always strictly bigger[1] than $\mathbb{Z}$.

We now begin our journey of fully characterizing the structure of endomorphims ring $\mathrm{End}(E)$ of ordinary elliptic curves defined over finite field. The strategy will be the following:

1. Introduce modules and their basic properties.

2. Define tensor product $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$ of $\mathbb{Z}$-modules and show inclusion $\mathrm{End}(E) \subseteq \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$.

3. Prove that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$ is a field isomorphic to imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ for appropriate $D < 0$.

Modules and algebras

We start with the definition of module. Strictly speaking, we define what is usually called (unital) left-module.

Definition 59 (R-Module)**.** Let R be a ring. A R-module is an abelian group $(G, +)$ with a map $\cdot : R \times G \to G$ (we will denote the image of tuple (r, g) as $r \cdot g$ or simply rg) that satisfies for all $r, s \in R$, $g, h \in G$:

- $(r + s)g = rg + sg$,

- $(rs)g = r(sg)$,

- $r(g + h) = rg + rh$,

[1] Whenever $\mathrm{End}(E) \neq \mathbb{Z}$ it is often said that E has *complex multiplication.*

- $1g = g$.

We call the map an *action* of the ring R on the group G.

Example 60. Any abelian group is a $\mathbb{Z}$-module with the action of $\mathbb{Z}$ defined as $rg = g + \cdots + g$ (r summands). The terms abelian group and $\mathbb{Z}$-module are therefore interchangeable. In particular the additive group of $\mathrm{End}(E)$ is a $\mathbb{Z}$-module.

Example 61. Besides the group $E(\overline{K})$ being $\mathbb{Z}$-module, it is also $\mathrm{End}(E)$-module. The action of the ring $\mathrm{End}(E)$ is defined in the obvious way: $\alpha \cdot P = \alpha(P)$ for every $P \in E(\overline{K})$ and $\alpha \in \mathrm{End}(E)$.

The notion of free abelian group also transfers to $\mathbb{Z}$-modules. Recall that a finitely generated free abelian group is a group isomorphic to $\mathbb{Z}^r$ for $r \in \mathbb{N}$.

Definition 62 (Free module)**.** If the abelian group of $\mathbb{Z}$-module G is free then we call G a *free $\mathbb{Z}$-module.* If $G \cong \mathbb{Z}^r$, we say that G has *rank* r. Any r-tuple of generators of the group G is called the basis of this $\mathbb{Z}$-module.

Example 63. If R is a field then every R-module is actually a vector space over the field R. The axioms in the definition of R-module are the axioms for scalar multiplication in the vector space. It is hence appropriate to view modules as generalized vector spaces over rings. In particular every imaginary quadratic field is a vector space over $\mathbb{Q}$ and hence a $\mathbb{Q}$-module.

There is a way to enlarge a $\mathbb{Z}$-module (endomorphism ring) into a $\mathbb{Q}$-module (our imaginary quadratic field), by extending the action $\mathbb{Z} \times G \to G$ into $\mathbb{Q} \times G \to G$, which is in some sense universal. The idea is to define $r \cdot g$, for $r \in \mathbb{Q}$, $g \in G$ as a formal symbol in such a way that these symbols form a group with an action of $\mathbb{Q}$.

Definition 64 (Tensor product)**.** Let R be a commutative ring and A,B be two R-modules. The tensor product $A \otimes_R B$ of A and B is the free R-module generated by the formal expressions $a \otimes b$ where $a \in A$ and $b \in B$, satisfying the relations

$$(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b, \quad a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2,$$

$$(ra) \otimes b = a \otimes (rb) = r(a \otimes b),$$

for all $a_1, a_2, a \in A$, $b_1, b_2, b \in B$ and $r \in R$.

The elements of $A \otimes_R B$, which are called *tensors*, are of the form $\sum_i r_i a_i \otimes b_i$ for $r_i \in R$, $a_i \in A$ and $b_i \in B$. This can be simplified for our case of $A = \mathbb{Q}$:

Lemma 65. Let B be a $\mathbb{Z}$-module. Then every element of $\mathbb{Q} \otimes_{\mathbb{Z}} B$ can be written in the form $r \otimes b$ with $r \in \mathbb{Q}$ and $b \in B$.

Proof. It suffices to prove the lemma for every element of the form $r_1 \otimes b_1 + r_2 \otimes b_2$. Let $r_1 = \frac{s_1}{t_1}$ and $r_2 = \frac{s_2}{t_2}$ with $s_1, t_1, s_2, t_2 \in \mathbb{Z}$, $t_1, t_2 \neq 0$. Then

$$\frac{s_1}{t_1} \otimes b_1 + \frac{s_2}{t_2} \otimes b_2 = \frac{s_1 t_2}{t_1 t_2} \otimes b_1 + \frac{s_2 t_1}{t_1 t_2} \otimes b_2 = \frac{1}{t_1 t_2} \otimes (s_1 t_2 b_1 + s_2 t_1 b_2),$$

where $\frac{1}{t_1 t_2} \in \mathbb{Q}$ and $(s_1 t_2 b_1 + s_2 t_1 b_2) \in B$

□

This simple form from Lemma 65 is by no means unique. After all, the zero element can be expressed as $0 \otimes b = a \otimes 0$ for all a, b of given modules. We can express the equality of two tensors if we slightly modify the proof of the previous lemma:

$$\frac{s_1}{t_1} \otimes a_1 = \frac{s_2}{t_2} \otimes a_2 \iff s_1 t_2 a_1 = s_2 t_1 a_2.$$

We can now introduce the tensor product $\mathrm{End}^0(E) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$. So far we know that it is a $\mathbb{Z}$-module since we have focused only on the additive group of $\mathrm{End}(E)$. We know that it is also a ring, and we would like to extend the multiplication from $\mathrm{End}(E)$ to $\mathrm{End}^0(E)$ and have an inclusion $\mathrm{End}(E) \subset \mathrm{End}^0(E)$ as rings.

Let $\alpha, \beta \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$ and $\alpha = (a_1 \otimes b_1)$, $\beta = (a_2 \otimes b_2)$ for some $a_1, a_2 \in \mathbb{Q}$ and $b_1, b_2 \in \mathrm{End}(E)$. We then define $\alpha\beta$ as

$$\alpha\beta = (a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2),$$

which can be shown to be well-defined (use the discussed condition on two equal tensors below Lemma 65). The asociativity of this multiplication comes from the asociativity of multiplication on $\mathrm{End}(E)$. The addition and multiplication can be shown to satisfy the distributive property. This gives the tensor product $\mathrm{End}^0(E) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$ a structure of ring with the multiplicative identity $1 \otimes 1$. The ring $\mathrm{End}^0(E)$ is often called *endomorphism algebra*. The reason for the introduction of the tensor product are the inclusions of rings

$$\mathrm{End}(E) \subset \mathrm{End}^0(E), \quad \alpha \mapsto 1 \otimes \alpha,$$

$$\mathbb{Q} \subset \mathrm{End}^0(E), \quad r \mapsto r \otimes 1$$

For every $q \otimes \alpha \in \mathrm{End}^0(E)$ there exists $n \in \mathbb{Z}$ such that $nq \in \mathbb{Z}$ and $n(q \otimes \alpha) = 1 \otimes nq\alpha \in \mathrm{End}(E)$. Thus we can view elements of $\mathrm{End}^0(E)$ as rational multiples of endomorphisms. We will omit the symbol $\otimes$ in all of the elements $r \otimes \alpha \in \mathrm{End}^0(E)$ and write $r\alpha$. Reader must keep in mind that this element $r\alpha$ is a formal symbol and generally not an endomorphism. Furthemore, it can be shown that the elements of $\mathbb{Q}$ commute with every element[2] of $\mathrm{End}^0(E)$, in other words: $r\alpha = \alpha r$ for every $r \in \mathbb{Q}$ and $\alpha \in \mathrm{End}^0(E)$.

Norm and trace of endomorphism

We now have to prove that the endomorphism algebra $\mathrm{End}^0(E)$ is a field. Firstly, we need to find inverse element α^{-1} for every nonzero $\alpha \in \mathrm{End}^0(E)$. Recall that we have defined for every isogeny α the dual isogeny $\widehat{\alpha}$ satisfying $\alpha\widehat{\alpha} = [\deg \alpha]$. This applies in particular for endomorphisms. Obviously, dual endomorphism is also endomorphism. So the idea would be to put $\alpha^{-1} = \frac{1}{\deg \alpha}\widehat{\alpha}$. This is the right approach but it only applies to elements of $\mathrm{End}(E)$ as we have not defined $\widehat{\alpha}$ for every $\alpha \in \mathrm{End}^0(E)$. We have to first generalize the notion of degree and dual endomorphism to $\mathrm{End}^0(E)$.

[2] If a ring has such property, we call it $\mathbb{Q}$-algebra. This is the reason for the name endomorphism algebra.

Definition 66 (Dual)**.** Let $\alpha \in \operatorname{End}^0(E)$. There is an endomorphism $\beta \in \operatorname{End}(E)$ and $r \in \mathbb{Q}$ such that $r\beta = \alpha$. The dual of α is then defined as

$$\widehat{\alpha} = r\widehat{\beta},$$

where $\widehat{\beta}$ is the usual dual of endomorphism. The dual of 0 is defined as 0.

The definition of dual doesn't depend on the choice of β as tell us the next lemma.

Lemma 67. Let $\alpha, \beta \in \operatorname{End}(E)$ and $u, v \in \mathbb{Q}$. If $u\alpha = v\beta$ in $\operatorname{End}^0(E)$ then $u\widehat{\alpha} = v\widehat{\beta}$.

Proof. Let $u = \frac{r_1}{s_1}$, $v = \frac{r_2}{s_2}$. Then $r_1 s_2 \alpha = r_2 s_1 \beta$. Taking the dual:

$$\widehat{r_1 s_2 \alpha} = \widehat{r_2 s_1 \beta} \Rightarrow r_1 s_2 \widehat{\alpha} = r_2 s_1 \widehat{\beta} \Rightarrow \frac{r_1}{s_1}\widehat{\alpha} = \frac{r_2}{s_2}\widehat{\beta}.$$

□

Clearly, $\widehat{r} = r$ for all $r \in \mathbb{Q}$ and it is easy to prove that the dual in $\operatorname{End}^0(E)$ satisfies the properties of the dual isogeny:

$$\widehat{\alpha\beta} = \widehat{\beta}\widehat{\alpha}, \quad \widehat{\alpha + \beta} = \widehat{\alpha} + \widehat{\beta} \text{ and } \widehat{\widehat{\alpha}} = \alpha.$$

Definition 68 (Norm)**.** The norm of $\alpha \in \operatorname{End}^0(E)$ is defined as $N(\alpha) = \alpha\widehat{\alpha}$.

Every element α of $\operatorname{End}^0(E)$ is of the form $r\phi$, where $r \in \mathbb{Q}$, $\phi \in \operatorname{End}(E)$. Plugging it in the definition of norm, we get $N(0) = 0$ and for $\alpha \neq 0$:

$$N(\alpha) = (r\phi)\widehat{(r\phi)} = (r\phi)(r\widehat{\phi}) = r^2 \deg \phi.$$

Realizing this, it is easy to prove the following properties.

Lemma 69. For all $\alpha, \beta \in \operatorname{End}^0(E)$:

(i) $N(\alpha) \in \mathbb{Q}_0^+$,

(ii) $N(\alpha) = \deg(\alpha) \in \mathbb{N}$ if $\alpha \in \operatorname{End}(E)$,

(iii) $N(\alpha) = 0$ if and only if $\alpha = 0$,

(iv) $N(\widehat{\alpha}) = N(\alpha)$,

(v) $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof. (i) , (ii), (iii). Let $\alpha = r\phi$. Then $N(\alpha) = \alpha\widehat{\alpha} = r^2 \deg(\phi) \geq 0$. Moreover $r^2 \deg(\phi) = 0$ if and only if $r = 0$ or $\phi = 0$, either way $\phi = 0$ and $\alpha = 0$. This proves (iii). Also $\alpha \in \operatorname{End}(E)$ implies $\phi = \alpha$ and therefore $N(\alpha) = \deg(\alpha) \in \mathbb{N}$ which is (ii).

(iv)
$$\alpha N(\widehat{\alpha}) = \alpha\widehat{\alpha}\widehat{\widehat{\alpha}} = \alpha\widehat{\alpha}\alpha = \alpha N(\alpha) = N(\alpha)\alpha,$$
where we used the fact that norm is rational and every element of $\mathbb{Q}$ commutes with every element of $\operatorname{End}^0(E)$. Hence $\alpha(N(\widehat{\alpha}) - N(\alpha)) = 0$ and since the ring $\operatorname{End}^0(E)$ has no zero divisors, either $\alpha = 0$ or $N(\widehat{\alpha}) = N(\alpha)$ in which case we are done. If $\alpha = 0$ then clearly $N(\widehat{0}) = 0 = N(0)$.

□

Now we can construct the inverse elements.

Lemma 70. Every nonzero $\alpha \in \operatorname{End}^0(E)$ has a multiplicative inverse α^{-1}.

Proof. If $\alpha \neq 0$ then $N(\alpha) \neq 0$. Putting $\alpha^{-1} = \frac{1}{N(\alpha)}\widehat{\alpha}$, it follows that α^{-1} is left inverse
$$\frac{1}{N(\alpha)}\widehat{\alpha}\alpha = \frac{1}{N(\alpha)}\widehat{\alpha}\widehat{\widehat{\alpha}} = \frac{1}{N(\alpha)}N(\widehat{\alpha}) = \frac{1}{N(\alpha)}N(\alpha) = 1$$
and right inverse
$$\alpha\frac{1}{N(\alpha)}\widehat{\alpha} = \frac{1}{N(\alpha)}\alpha\widehat{\alpha} = \frac{1}{N(\alpha)}N(\alpha) = 1.$$

□

We are heading towards an isomorphism between $\operatorname{End}^0(E)$ and quadratic number field so let us stop here and try to look at elements of $\operatorname{End}^0(E)$ as complex numbers[3]. For $\alpha \in \mathbb{C}$ we know that $\alpha^{-1} = \frac{1}{|\alpha|}\overline{\alpha}$. Comparing it with just computed inverse element of $\operatorname{End}^0(E)$, it should hint us that the dual endomorphism is in fact the complex conjugate and the norm is the usual norm in $\mathbb{C}$, i.e. the absolute value.

Following on this, every element of imaginary quadratic number field $\mathbb{Q}(\sqrt{D})$ has a quadratic minimal polynomial over $\mathbb{Q}$ and we can express its coefficients using the complex conjugate. The minimal polynomial of $\alpha \in \mathbb{Q}(\sqrt{D})$ is $(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha}$. If we carry this to $\operatorname{End}^0(E)$ we get the polynomial
$$x^2 - (\alpha+\widehat{\alpha})x + \alpha\widehat{\alpha} = x^2 - (\alpha+\widehat{\alpha})x + N(\alpha) \in \operatorname{End}^0(E)[x].$$
The norm is rational as we have proved. So it remains to show that the coefficient $\alpha + \widehat{\alpha}$ is also rational.

Definition 71 (Trace)**.** We define the trace of $\alpha \in \operatorname{End}^0(E)$ as $T(\alpha) = \alpha + \widehat{\alpha}$.

Lemma 72. For all $\alpha, \beta \in \operatorname{End}^0(E)$:

(i) $T(\alpha) = 1 + N(\alpha) - N(1-\alpha) \in \mathbb{Q}$,

(ii) $T(\alpha) \in \mathbb{Z}$ if $\alpha \in \operatorname{End}(E)$,

(iii) $T(\alpha+\beta) = T(\alpha) + T(\beta)$,

[3] All elements of $\operatorname{End}(E)$ can be then seen as multiplication by a complex number, hence the term *complex multiplication.*

(iv) $T(r\alpha) = rT(\alpha)$ for all $r \in \mathbb{Q}$,

(v) $T(\alpha) = T(\widehat{\alpha})$.

Proof. (i) $T(\alpha) = \alpha + \widehat{\alpha} = 1 + \alpha\widehat{\alpha} - (1-\alpha)(1-\widehat{\alpha}) = 1 + N(\alpha) - N(1-\alpha)$.

(ii) If $\alpha \in \operatorname{End}(E)$ then $1 - \alpha \in \operatorname{End}(E)$. The rest follows from (i) and the fact that $N(\beta) \in \mathbb{Z}$ for all $\beta \in \operatorname{End}(E)$.

(iii) $T(\alpha+\beta) = \alpha + \beta + \widehat{\alpha+\beta} = \alpha + \beta + \widehat{\alpha} + \widehat{\beta} = T(\alpha) + T(\beta)$.

(iv) $T(r\alpha) = r\alpha + \widehat{r\alpha} = r\alpha + \widehat{\alpha}\widehat{r} = r\alpha + \widehat{\alpha}r = r\alpha + r\widehat{\alpha} = rT(\alpha)$.

(v) $T(\widehat{\alpha}) = \widehat{\alpha} + \widehat{\widehat{\alpha}} = \widehat{\alpha} + \alpha = T(\alpha)$.

□

Trace is a useful computational tool for determining whether curve is ordinary. This test is used in practice as we will see in the following chapters.

Corollary 73. An elliptic curve E over $\mathbb{F}_{p^n}$ is ordinary if and only if $p \nmid T(\pi_E)$.

Proof. We will prove the equivalent statement that E is supersingular if and only if $p \mid T(\pi_E)$. If $p \mid T(\pi_E)$ then $T(\pi_E) = pk$ for some $k \in \mathbb{Z}$. Since $[p]$ is inseparable then so is $T(\pi_E)$ and consequently $T(\pi_E) - \pi_E = \widehat{\pi_E}$. It follows that $\widehat{\pi}$ is inseparable and since $\deg \widehat{\pi} = p$ then its separable degree is 1 and so $\ker[\widehat{\pi}]$ is trivial. Finally, π is injective so $\ker \widehat{\pi}\pi = \ker[p] = E[p]$ is trivial which means that E is supersingular. The opposite direction is similar. □

Equipped with the properties of the trace we can prove that every endomorphism is a root of monic quadratic polynomial from $\mathbb{Z}[x]$.

Lemma 74. Every $\alpha \in \operatorname{End}^0(E)$ is a root of $f(x) = x^2 - T(\alpha)x + N(\alpha) \in \mathbb{Q}[x]$. Moreover if $\alpha \in \operatorname{End}(E)$ then $f \in \mathbb{Z}[x]$.

Proof. We verify this by simply plugging in:

$$\alpha^2 - \alpha T(\alpha) + N(\alpha) = \alpha^2 - \alpha(\alpha + \widehat{\alpha}) + \alpha\widehat{\alpha} = 0.$$

The second statement follows from Lemma 72 and Lemma 69.

□

We call the polynomial from the Lemma 74 the *characteristic polynomial* of endomorphism α. The characteristic polynomial of Frobenius endomorphism $f(x) = x^2 - tx + q$, where $T(\pi) = t$, $N(\pi) = q$, will be the key to prove that $\operatorname{End}^0(E)$ is a quadratic number field. Firstly, we will prove that f doesn't have real roots thus making

$$\mathbb{Q}(\pi) \cong \mathbb{Q}[x]/(x^2 - tx + q) \cong \mathbb{Q}(\sqrt{D})$$

imaginary quadratic number field where $D = t^2 - 4q$. Secondly, we will show that

$$\operatorname{End}^0(E) = \mathbb{Q}(\pi).$$

Lemma 75. If E is ordinary curve then the characteristic polynomial $x^2 - tx + q$ of π_E does not have real roots. In particular, $\pi_E \notin \mathbb{Z}$.

Proof. It suffices to prove that $qx^2 - tx + 1 > 0$ for all $x \in \mathbb{R}$ as this polynomial has the same discriminant. Since $\mathbb{Q}$ is dense in $\mathbb{R}$ we can just prove that for all $\frac{r}{s} \in \mathbb{Q}$:

$$q\left(\frac{r}{s}\right)^2 - t\frac{r}{s} + 1 > 0,$$

This is equivalent to $qr^2 - trs + s^2 > 0$ as $s^2 > 0$. Furthermore, $qr^2 - trs + s^2 = N(r\pi - s) \geq 0$ since:

$$N(r\pi - s) = (r\pi - s)(\widehat{r\pi - s}) =$$
$$= (r\pi - s)(r\hat{\pi} - s) = qr^2 - trs + s^2.$$

If $N(r\pi - s) = 0$ then $r\pi = s$. Hence $\pi \in \mathbb{Q}$ and since it is a root of monic polynomial over $\mathbb{Z}$ then $\pi \in \mathbb{Z}$. If $\pi \in \mathbb{Z}$ it follows $\deg(\pi) = \pi^2$ but the degree of π is $q = p^m$, so $p \mid \pi$ which is in contradiction with Corollary 73. □

Lemma 76. If E is an ordinary elliptic curve over $\mathbb{F}_q$ then $\mathrm{End}^0(E) = \mathbb{Q}(\pi_E)$.

Proof. The inclusion $\mathbb{Q}(\pi) \subseteq \mathrm{End}^0(E)$ is clear. Let $\alpha \in \mathrm{End}^0(E)$ then

$$T(\alpha\pi) = \alpha\pi + \widehat{\alpha\pi} = \alpha\pi + \hat{\pi}\hat{\alpha} = \alpha\pi + (t - \pi)(T(\alpha) - \alpha) =$$

$$= \alpha\pi + tT(\alpha) - \pi T(\alpha) - t\alpha + \pi\alpha = tT(\alpha) - \pi T(\alpha) + (-t + 2\pi)\alpha$$

where we used the fact that $\alpha\pi = \pi\alpha$. Since $\pi \notin \mathbb{Q}$ then $2\pi - t \neq 0$ and it follows that

$$\alpha = \frac{T(\alpha\pi) - tT(\alpha) + \pi T(\alpha)}{2\pi - t} \in \mathbb{Q}(\pi).$$

□

We can now summarize the main theorem of this chapter following from the ideas discussed.

Theorem 77. If E is an ordinary elliptic curve over $\mathbb{F}_q$ then $\mathrm{End}^0(E) \cong \mathbb{Q}(\sqrt{D})$, where $D = (T(\pi_E))^2 - 4q < 0$.

The following corollary is often called Hasse's theorem, which is an important result as it bounds the cardinality $|E(\mathbb{F}_q)|$.

Corollary 78. For every elliptic curve E over $\mathbb{F}_q$: $|E(\mathbb{F}_q)| = q + 1 - T(\pi_E)$. Moreover, if E is ordinary then $|q + 1 - |E(\mathbb{F}_q)|| < 2\sqrt{q}$.

Proof. Recall that $P \in E(\mathbb{F}_q)$ if and only if $\pi_E(P) = P$. This is equivalent to $\ker(\pi_E - 1) = E(\mathbb{F}_q)$. There exists a separable isogeny α such that $1 - \pi_E = \pi^s\alpha$ or equivalently $1 = \pi_E - \pi^s\alpha$. If $s > 0$ then left side is inseparable while right side is separable. So it must be $s = 0$, which means that $1 - \pi_E$ is separable and consequently $N(1 - \pi_E) = |\ker(\pi_E - 1)| = |E(\mathbb{F}_q)|$. The rest follows from Lemma 72 (i). The second statement is a corollary of Theorem 77. □

Example 79. Consider the elliptic curve $y^2 = x^3 + x + 2$ over $\mathbb{F}_5$. One can compute that $|E(\mathbb{F}_5)| = 4$. The trace of π_E is then $5 + 1 - 4 = 2$ and the characteristic polynomial is $x^2 - 2x + 5 = (x-1)^2 + 4$ so $(\pi_E - 1)^2 = -4$ and $\mathrm{End}^0(E) \cong \mathbb{Q}(i)$. We now have two options. We can identify π_E with $1 + 2i$ or $1 - 2i$, this depends on the choice of isomorphism. Either way we choose, the other root will then correspond to the dual endomorphism $\widehat{\pi_E}$.

This ends our characterization of $\mathrm{End}^0(E)$. Now we would like to describe the ring $\mathrm{End}(E)$ in relation to the field $\mathrm{End}^0(E)$.

Orders

We start with the definition of order, which is the structure that precisely describes endomorphism rings of ordinary elliptic curves over finite field.

Definition 80 (Order)**.** Let K be a number field. We call a subring $\mathcal{O}$ of K an order if it is a finitely generated free $\mathbb{Z}$-module of rank equal to the degree of a field extension $[K : \mathbb{Q}]$.

Remark 81. It can be shown that orders are precisely the subrings of K which are finitely generated free $\mathbb{Z}$-modules satisfying $K = \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}$.

Example 82. There is only one order in the field $\mathbb{Q}$, that is $\mathbb{Z}$. But for example in the field $K = \mathbb{Q}(i)$ the ring $\mathbb{Z}$ is not an order as it has rank 1. Example of order in this field is $\mathbb{Z}[i]$. More relevant example for us is $\mathbb{Z}[\pi]$, which is an order in $\mathrm{End}^0(E)$.

For $\mathrm{End}(E)$ to be an order in $\mathrm{End}^0(E)$, it remains to show that it is a free $\mathbb{Z}$-module of rank 2. The proof is rather technical and reader can skip but it introduces an interesting object called dual $\mathbb{Z}$-module.

Lemma 83. Let E be an ordinary elliptic curve over $\mathbb{F}_q$. The endomorphism ring $\mathrm{End}(E)$ is a free $\mathbb{Z}$-module of rank 2.

Proof. The idea is to grip $\mathrm{End}(E)$ between two free $\mathbb{Z}$-modules

$$A \subseteq \mathrm{End}(E) \subseteq A^*$$

of rank 2 in $\mathrm{End}^0(E)$. It follows from this that $\mathrm{End}(E)$ is also a free $\mathbb{Z}$-module of rank 2 (subgroup of $\mathbb{Z}^2$ containing $\mathbb{Z}^2$ is $\mathbb{Z}^2$).

Let $1, \pi_E$ be the basis of $\mathrm{End}^0(E)$ as a vector space over $\mathbb{Q}$. We replace π_E with $\pi_E - \frac{1}{2}T(\pi_E)$ to get an element with zero trace and multiply it with an integer to get $\tau \in \mathrm{End}(E)$. It is clear that $1, \tau$ is still basis since τ and π_E differ only by adding and multiplying by rational number. Let A be the free $\mathbb{Z}$-module generated by $1, \tau$. Then $A \subseteq \mathrm{End}(E)$ and we have a lower bound on $\mathrm{End}(E)$. We find the upper bound by constructing the so-called *dual* $\mathbb{Z}$-module of A:

$$A^* = \{\alpha \in \mathrm{End}^0(E) \mid T(\alpha), T(\alpha\tau) \in \mathbb{Z}\}.$$

The fact that this is a $\mathbb{Z}$-module arises from the linearity of T. The inclusion $\mathrm{End}(E) \subseteq A^*$ holds because $T(\phi) \in \mathbb{Z}$ for all $\phi \in \mathrm{End}(E)$. It remains to find the generators of A^*. Let's try to take $1, \tau$. Every element of A^* can be expressed as $\alpha = a + b\tau$ for $a, b \in \mathbb{Q}$ since $1, \tau$ is a basis of the whole vector space. We would like to have $a, b \in \mathbb{Z}$. We know that $T(\alpha)$, $T(\alpha\tau) \in \mathbb{Z}$ from the definition of A^*. Hence

$$T(\alpha) = T(a) + T(b)T(\tau) = a \in \mathbb{Z},$$

$$T(\alpha\tau) = T(a\tau + b\tau^2) = aT(\tau) + bT(\tau^2) = bT(\tau^2) \in \mathbb{Z}.$$

This doesn't necessarily imply that $b \in \mathbb{Z}$. So we have to replace τ. If we take instead $e = \frac{1}{T(\tau^2)}\tau$, then $1, e$ is still basis of $\mathrm{End}^0(E)$, $T(e) = 0$ and $e \in A^*$. On top of that, if $\alpha \in A^*$ and $\alpha = a + be$, where $a, b \in \mathbb{Q}$, then

$$T(\alpha) = T(a) + T(b)T(e) = a \in \mathbb{Z},$$

$$T(\alpha\tau) = T(a\tau + be\tau) = aT(\tau) + bT(e\tau) = \frac{b}{T(\tau^2)}T(\tau^2) = b \in \mathbb{Z}.$$

So $1, e \in A^*$ and every element of A^* can be expressed as $\mathbb{Z}$-linear combination of 1 and e. This means that A^* is a free $\mathbb{Z}$-module of rank 2. □

It can be shown that in every number field K exists an order. Moreover, if we assume the ordering of orders by inclusion, then every order lies in a maximal order (assuming Zorn's lemma). In addition, it can be proved that there is only one maximal order $\mathcal{O}_K$ in K. We will summarize some important properties of $\mathcal{O}_K$ for imaginary quadratic field K:

- $\mathcal{O}_K$ is also called *ring of algebraic integers* of K. An algebraic integer is an element of K that is a root of a monic polynomial from $\mathbb{Z}[x]$, so $\mathcal{O}_K$ contains precisely the elements of K which are roots of such polynomials. In our case of quadratic fields, we're talking about quadratic polynomials (recall the characteristic polynomial from Lemma 74). It follows that for every $\alpha \in K$: $\alpha \in \mathcal{O}_K$ if and only if $N(\alpha), T(\alpha) \in \mathbb{Z}$. Reader can found more information about algebraic integers in [Cox13].

- $\mathcal{O}_K$ is a $\mathbb{Z}$-module of rank 2 and one can show that if $K = \mathbb{Q}(\sqrt{N})$ where N is square-free integer then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{N}] & N \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{N}}{2}] & N \equiv 1 \pmod 4 \end{cases}$$

  In our case we have $K = \mathbb{Q}(\sqrt{D})$, so N is the square-free part of D. This can be expressed in more compact form if define the discriminant d_K of K as $d_K = N$ if $N \equiv 1 \pmod 4$ and $d_K = 4N$ otherwise. We can then write $\mathcal{O}_K = \mathbb{Z}[\frac{d_K+\sqrt{d_K}}{2}]$. Also notice the connection of d_K and π as $\pi = \frac{-t+v\sqrt{d_K}}{2}$ for appropriate $v \in \mathbb{Z}$.

- K is the field of fractions of $\mathcal{O}_K$, in another words every element of K can be expressed as a fraction $\frac{a}{b}$ where $a, b \in \mathcal{O}_K$

- Every order $\mathcal{O}$ in a quadratic field K has finite index in $\mathcal{O}_K$, and if we set $c = [\mathcal{O}_K : \mathcal{O}]$, then $\mathcal{O} = \mathbb{Z}[c\tau_K]$ where $\mathcal{O}_K = \mathbb{Z}[\tau_K]$. The c is called *conductor* of order $\mathcal{O}$.

Lemma 84. The conductor of $\mathbb{Z}[\pi]$ is v where $D = v^2 d_K$. In particular, $\mathcal{O}_K = \mathbb{Z}[\frac{\pi-a}{v}]$ for appropriate $a \in \mathbb{Z}$.

Proof. If $D = d_K v^2$ and $\tau_K = \frac{d_K+\sqrt{d_K}}{2}$ then

$$\pi_E = \frac{t+\sqrt{D}}{2} = \frac{t+\sqrt{d_K}v}{2} = \frac{t+(2\tau_K - d_K)v}{2} = v\tau_K + \frac{t-d_K v}{2}.$$

Since $t^2 - 4q = d_K v^2$, then $t^2 \equiv d_K v^2 \pmod 4$ and $t \equiv d_K v \pmod 2$. Thus $a = \frac{t-d_K v}{2} \in \mathbb{Z}$ which yields $\tau_K = \frac{\pi-a}{v}$ and $\mathbb{Z}[\pi_E] = \mathbb{Z}[v\tau_K]$. □

We can summarize the structure of endomorphism ring as follows.

Corollary 85. Let E be an ordinary elliptic curve over the finite field $\mathbb{F}_q$ and π_E its Frobenius endomorphism. The endomorphism ring End(E) is isomorphic to an order $\mathcal{O}$ in imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ where $D = T(\pi_E)^2 - 4q$. Moreover, for the order $\mathcal{O}$:

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

where $\mathcal{O}_K$ is the ring of algebraic integers of K. The conductor of $\mathcal{O}$ divides the integer $v = \sqrt{\frac{t^2-4q}{d_K}}$ where d_K is the discriminant of K.

Remark 86. It will be beneficial to identify End$^0(E)$ with $\mathbb{Q}(\sqrt{D})$ and End(E) with $\mathcal{O}$. However, the reader should keep in mind that these objects are only isomorphic and in our case there is no canonical isomorphism. There are two isomorphisms between End$^0(E)$ and $\mathbb{Q}(\sqrt{D})$ depending on whether we put $\pi_E = \frac{-t+\sqrt{D}}{2}$ or $\pi_E = \frac{-t-\sqrt{D}}{2}$. Thus we will be always silently making an arbitrary choice.

Lemma 87. If E_1, E_2 are elliptic curves with $\mathcal{O}_1 = $ End(E_1), $\mathcal{O}_2 = $ End(E_2) and $\phi : E_1 \to E_2$ an isogeny then any endomorphism $\alpha \in \mathcal{O}_1 \cap \mathcal{O}_2$ commutes with ϕ, i.e. $\alpha\phi = \phi\alpha$.

Proof. Since E is ordinary then $\alpha \in \mathbb{Q}(\pi)$ and $\alpha = \frac{u+v\pi}{w}$ for $u, v, w \in \mathbb{Z}$. For any point $P \in E$ there exists Q such that $P = wQ$. Hence

$$\phi(\alpha(P)) = \phi\left(\left(\frac{u+v\pi}{w}\right)(P)\right) = \phi\left(\left(\frac{u+v\pi}{w}\right)(wQ)\right) =$$

$$= \phi\left((u+v\pi)(Q)\right) = (u+v\pi)(\phi(Q)) = \frac{u+v\pi}{w}(\phi(wQ)) = \alpha(\phi(P)),$$

where we used the fact that π and any integer commute with isogenies. □

We should address the case of j-invariant 0 or 1728 in the context of endomorphism ring. We know that elliptic curves corresponding to these special cases have nontrivial automorphisms. These correspond to units of $\mathcal{O}_K$. It can be shown ([Cox13]) that in general the units of $\mathcal{O}_K$, for K imaginary quadratic field, are always ± 1 except for the case when $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}\left(\frac{1+\sqrt{-3}}{2}\right)$. These special cases are exactly our special cases of j-invariants.

Lemma 88 ([Sch95])**.** If E is ordinary elliptic curve with $j(E) = 0$ then $\text{End}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ and if $j(E) = 1728$ then $\text{End}(E) \cong \mathbb{Z}[i]$.

Example 89. Consider an elliptic curve $E : y^2 = x^3 - 4x - 3$ defined over $\mathbb{F}_{17}$. Using point counting algorithm, one can find the order $|E(\mathbb{F}_{17})| = 12$. By Hasse's theorem the trace of π_E is then $17+1-12 = 6$. It follows that the characteristic polynomial of π_E is $x^2 - 6x + 17$ with the discriminant -32 and $\text{End}^0(E) \cong \mathbb{Q}(\sqrt{2}i)$. The maximal order in $\mathbb{Q}(\sqrt{2}i)$ is $\mathbb{Z}[\sqrt{2}i]$ and the Frobenius endomorphism corresponds to $3 \pm 2\sqrt{2}i$.

$$\mathbb{Z}[2\sqrt{2}i] \subseteq \text{End}(E) \subseteq \mathbb{Z}[\sqrt{2}i].$$

The index $[\mathbb{Z}[\sqrt{2}i] : \mathbb{Z}[2\sqrt{2}i]]$ is 2 and there are therefore two possibilities: Either $\text{End}(E) \cong \mathbb{Z}[2\sqrt{2}i]$ or $\text{End}(E) \cong \mathbb{Z}[\sqrt{2}i]$. Solving this, in general, can be quite difficult. Naive way is to start looking for the rational maps representing $\sqrt{2}i$ in $\text{End}(E)$. Much more sophisticated solution comes from the isogeny volcanoes.

At the beginning of this chapter we have made a claim that for ordinary E holds $\text{End}(E) = \text{End}_{\overline{\mathbb{F}}_q}(E)$, i.e. every endomorphism over $\overline{\mathbb{F}}_q$ can be defined over $\mathbb{F}_q$. So we should clarify this. We will prove something stronger:

Lemma 90. If E and E' are ordinary isogenous curves over $\mathbb{F}_q$ then any isogeny $\psi : E \to E'$ over $\overline{\mathbb{F}}_q$ is defined over $\mathbb{F}_q$. In particular, $\text{End}(E) = \text{End}_{\overline{\mathbb{F}}_q}(E)$.

Proof. If E and E' are isogenous then there exists an isogeny $\phi : E' \to E$. We can assume that ϕ is separable otherwise we would have chosen $1 - \phi$. Consider the endomorphism $\phi\psi \in \text{End}_{\mathbb{F}_{q^m}}(E)$ and let $\mathbb{Z}[\pi_E]$ have index m in $\text{End}_{\mathbb{F}_{q^m}}(E)$. It follows that $m\phi\psi \in \mathbb{Z}[\pi_E]$ and $m\phi\psi$ is defined over $\mathbb{F}_q$. Finally, we use the Lemma 29 which tells us that ψ is uniquely determined and must be defined over $\mathbb{F}_q$. □

Chapter 4

Horizontal isogenies

Previous three chapters focused on isogenies and endomorphism ring of elliptic curves. Now is the time to discuss how are these two concepts related. In particular, what can we say about endomorphism rings of isogenous elliptic curves and how does it relate to ordinary components of $G_l(\mathbb{F}_q)$. The goal of this chapter is to prove that any such ordinary component V is a volcano. For the whole chapter $\mathbb{F}_q$ is a finite field with $q = p^m$, $p > 3$, l a prime distinct from p and V doesn't contain vertices 0 or 1728.

Firstly, we will prove that isogenous curves share an endomorphism algebra, and isomorphic curves share an endomorphism ring. This will allow us to assign to V an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ and to every vertex an order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{D})$. Through this classification by orders, we will partition vertices into classes, we will call levels, as in the Definition 53 of a volcano.

Lemma 91. If E_1 and E_2 are isogenous ordinary elliptic curves, then

$$\mathrm{End}^0(E_1) \cong \mathrm{End}^0(E_2).$$

Proof. If E_1 and E_2 are isogenous, then $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$ by Theorem 35. This is equivalent, by Hasse's theorem, to $T(\pi_{E_1}) = T(\pi_{E_2})$, which implies $D_1 = T(\pi_{E_1})^2 - 4q = T(\pi_{E_2})^2 - 4q = D_2$. □

Lemma 92. If E_1 and E_2 are ordinary elliptic curves such that $j(E_1) = j(E_2) \in V$ and $\mathrm{End}(E_1) = \mathcal{O}_1$, $\mathrm{End}(E_2) = \mathcal{O}_2$ are orders in fields K_1, K_2 respectively, then

(i) $T(\pi_{E_1}) = -T(\pi_{E_2})$ if E_1 is a twist of E_2,

(ii) $K_1 = K_2$

(iii) $\mathcal{O}_1 = \mathcal{O}_2$.

Proof. (i) If E_1 is given by $y^2 = x^3 + ax + b$, then by Theorem 40 and Lemma 38 there exists $u \in \mathbb{F}_{q^2}$ such that $y^2 = x^3 + u^4ax + u^6b$ defines E_2. If we make a substitution $y = y/u^2$, $x = x/u^2$, $d = 1/u^2 \in \mathbb{F}_q$, then clearly $y^2 = d(x^3+ax+b)$ also defines E_2. Any element $x \in \mathbb{F}_q$ determines a point $(x, y) \in E_1(\mathbb{F}_q)$ if and only if $x^3 + ax + b$ is a quadratic residue in $\mathbb{F}_q$ which is true if and only if

$d(x^3+ax+b)$ is zero or a quadratic nonresidue as d is quadratic nonresidue. Hence x defines a point (x,y) in $E_1(\mathbb{F}_q)$ with $y \neq 0$ if and only if it doesn't define a point in $E_2(\mathbb{F}_q)$. Furthemore, for each $x \in \mathbb{F}_q$ either $x^3+ax+b=0$, or there are exactly two points (x,y), $(x,-y)$ with x-coordinate equal to x. Putting this all together gets us $|E_1(\mathbb{F}_q)|+|E_2(\mathbb{F}_q)| = 2q+2$. Finally, $T(\pi_{E_1})+T(\pi_{E_2}) = q+1-|E_1|+q+1-|E_2| = 0$.

(ii) If $j(E_1)=j(E_2)$, then either E_1, E_2 are isomorphic over $\mathbb{F}_q$, so isogenous (which is solved in Lemma 91), or one is twist of the other. In the latter case $T(\pi_{E_1}) = -T(\pi_{E_2})$ by (i) so $T(\pi_{E_1})^2 = T(\pi_{E_2})^2$ and $\mathbb{Q}(\sqrt{T(\pi_{E_1})^2-4q}) = \mathbb{Q}(\sqrt{T(\pi_{E_2})^2-4q})$.

(iii) Let $\mathcal{O}_1 = \mathbb{Z}[\tau_1]$ and $\mathcal{O}_2 = \mathbb{Z}[\tau_2]$ for appropriate τ_1, τ_2. If $\rho : E_1 \to E_2$ is any isomorphism over $\overline{\mathbb{F}}_q$, then $\rho\tau_1\widehat{\rho}$ is an endomorphism in $\mathcal{O}_2$ with dual $\rho\widehat{\tau}_1\widehat{\rho}$. Let's look at its trace and norm:

$$T(\rho\tau_1\widehat{\rho}) = \rho\tau_1\widehat{\rho} + \rho\widehat{\rho}_1\widehat{\rho} = \rho(\tau_1+\widehat{\tau}_1)\widehat{\rho} = \rho T(\tau_1)\widehat{\rho} = \phi\widehat{\rho}T(\tau_1) = T(\tau_1).$$

$$N(\rho\tau_1\widehat{\rho}) = \rho\tau_1\widehat{\rho}\rho\widehat{\tau}_1\widehat{\rho} = \rho\tau_1\widehat{\tau}_1\rho = \rho N(\tau_1)\widehat{\rho} = \rho\widehat{\rho}N(\tau_1) = N(\tau_1).$$

If the elements $\rho\tau_1\widehat{\rho} \in \mathcal{O}_2 \subseteq K_2 = K_1$ and $\tau_1 \in \mathcal{O}_1 \subseteq K_1$ have the same trace and norm, they have the same characteristic equation. It follows that they are either equal or one is the dual of the other. Either way $\tau_1 \in \mathbb{Z}[\tau_2]$ and consequently $\mathbb{Z}[\tau_1] \subseteq \mathbb{Z}[\tau_2]$. Symmetrically $\mathbb{Z}[\tau_2] \subseteq \mathbb{Z}[\tau_1]$ and $\mathbb{Z}[\tau_2] = \mathbb{Z}[\tau_1]$

□

By Lemma 91 we can assign to V an imaginary quadratic field K and to each vertex $j(E) \in V$ an order $\mathcal{O} \subseteq K$ by Lemma 92.

Lemma 93. Let E_1, E_2 be ordinary elliptic curves over $\mathbb{F}_q$, $\phi : E_1 \to E_2$ an l-isogeny and $\mathrm{End}(E_1) = \mathcal{O}_1$, $\mathrm{End}(E_2) = \mathcal{O}_2$ orders in imaginary quadratic field K. Then one of the following holds:

(i) $\mathcal{O}_1 \subseteq \mathcal{O}_2$ and $[\mathcal{O}_2 : \mathcal{O}_1] = l$

(ii) $\mathcal{O}_2 \subseteq \mathcal{O}_1$ and $[\mathcal{O}_1 : \mathcal{O}_2] = l$

(iii) $\mathcal{O}_1 = \mathcal{O}_2$

Proof. The proof is similar to proof of Lemma 92 (iii). Again for $\mathcal{O}_1 = \mathbb{Z}[\tau_1]$, $\mathcal{O}_2 = \mathbb{Z}[\tau_2]$ we consider the endomorphism $\phi\tau_1\widehat{\phi}$ in $\mathcal{O}_2$ with dual $\phi\widehat{\tau}_1\widehat{\phi}$. Looking at its trace and norm:

$$T(\phi\tau_1\widehat{\phi}) = \phi\tau_1\widehat{\phi} + \phi\widehat{\tau}_1\widehat{\phi} = \phi(\tau_1+\widehat{\tau}_1)\widehat{\phi} = \phi T(\tau_1)\widehat{\phi} = lT(\tau_1) = T(l\tau_1),$$

$$N(\phi\tau_1\widehat{\phi}) = \phi\tau_1\widehat{\phi}\phi\widehat{\tau}_1\widehat{\phi} = \phi\tau_1 l\widehat{\tau}_1\phi = \phi l N(\tau_1)\widehat{\phi} = l^2N(\tau_1) = N(l\tau_1),$$

we see that the elements $\phi\tau_1\widehat{\phi}$, $l\tau_1$ are either equal or one is the dual of the other. Either way $l\tau_1 \in \mathbb{Z}[\tau_2]$ and symmetrically $l\tau_2 \in \mathbb{Z}[\tau_1]$. We can then write for $a_1, a_2, b_1, b_2 \in \mathbb{Z}$:

$$l\tau_1 = a_2 + b_2\tau_2,\ l\tau_2 = a_1 + b_1\tau_1.$$

$$l^2\tau_1 = la_2 + b_2 l\tau_2 = la_2 + b_2 a_1 + b_2 b_1 \tau_1.$$

Comparing the basis elements we get $l^2 = b_1 b_2$. The three cases $b_1 = l^2$, $b_2 = l^2$ and $b_1 = b_2 = l$ correspond to the three cases from the statement. For example, if $l \mid b_1$ in $\mathcal{O}_2$, then $l \mid a_1$ and $\tau_2 \in \mathbb{Z}[\tau_1]$. Consequently $\mathbb{Z}[\tau_2] \subseteq \mathbb{Z}[\tau_1]$ and $[\mathbb{Z}[\tau_1] : \mathbb{Z}[\tau_2]] = \frac{b_2}{l}$. □

The previous lemma allows us to distinguish l-isogenies into three categories:

Definition 94. Let $\phi : E_1 \to E_2$ be an l-isogeny between ordinary elliptic curves over $\mathbb{F}_q$ and $\mathcal{O}_1, \mathcal{O}_2$ be the corresponding endomorphism rings. We call ϕ

(i) horizontal if $\mathcal{O}_1 = \mathcal{O}_2$,

(ii) ascending if $\mathcal{O}_1 \subsetneq \mathcal{O}_2$,

(iii) descending if $\mathcal{O}_2 \subsetneq \mathcal{O}_1$.

We will also use the term vertical isogeny for the last two cases.

We can label any isomorphism class of l-isogenies $[\phi]$ as horizontal, ascending or descending based on the type of ϕ. This clearly doesn't depend on the choice of ϕ as isomorphisms preserve endomorphism rings. Following on this, each edge of V is represented by classes $([\phi], [\psi])$ where $[\phi]$ is a twist of $[\psi]$. The class $[\phi]$ is horizontal (vertical) if and only if $[\psi]$ is horizontal (vertical), thus we can label each such edge of V correspondingly.

Lemma 95. Vertices of V can be uniquely partitioned into classes V_0, V_1, …, V_d, such that all vertices of V_i have the same order $\mathcal{O}_i$ and $[\mathcal{O}_i : \mathcal{O}_{i+1}] = l$ for all $i = 0, \dots, d-1$.

Proof. Since V is finite we can pick a vertex $v_0 \in V$ which has order $\mathcal{O}_0$ with the smallest conductor. Let V_0 be all vertices with order $\mathcal{O}_0$. Consequence of Lemma 93 is that $\mathcal{O} \subseteq \mathcal{O}_0$ for order $\mathcal{O}$ of any vertex $v \in V$. Furthermore the index $[\mathcal{O}_0 : \mathcal{O}]$ is a power of l. Define $\mathcal{O}_i \subseteq \mathcal{O}_0$ as the order with index l^i and V_i as the vertices with order $\mathcal{O}_i$.

□

We will call the subsets V_i of V *levels* of V. Horizontal edges can be by definition only across individual levels. However, looking at the Definition 53 of a volcano as a graph, it tells us that we should be finding horizontal edges only at the most upper level. For proving that, we have to develop a bit more theory about orders in quadratic number fields. In particular, we will focus on ideals in these orders.

Reader unfamiliar with ideals can look in [DF04] for introduction. Here are some basic facts about ideals in orders $\mathcal{O}$ of imaginary quadratic number fields reader should be aware of:

- Any ideal in $\mathcal{O}$ is a $\mathbb{Z}$-module of rank at most 2 as well as $\mathcal{O}$-module of rank at most 2. We can write $\mathfrak{a} = (\alpha, \beta)$ for α, β being the generators of $\mathfrak{a}$ as $\mathcal{O}$-module. Ideals of rank 1 are also called principal. They are denoted as $a\mathcal{O}$ or (a) where a is the generator.

- We can add and multiply any two ideals in $\mathcal{O}$ by

  $$(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma, \beta\gamma, \alpha\delta, \beta\delta), \quad (\alpha, \beta) + (\gamma, \delta) = (\alpha, \beta, \gamma, \delta)$$

  Both of these operations are associative and commutative.

- Prime ideals are those ideals $\mathfrak{a}$ that satisfy the following implication for all $\alpha, \beta \in \mathcal{O}$:

  $$\alpha\beta \in \mathfrak{a} \Rightarrow \alpha \in \mathfrak{a} \text{ or } \beta \in \mathfrak{a}.$$

  Every nonzero prime ideal is maximal ideal. The opposite is not generally true but it is in our case of imaginary quadratic number field.

- Norm of an ideal is defined as $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$ which can be shown to be finite number. This definition of ideal agrees with our norm, i.e. $N(\alpha) = |\mathcal{O}/(\alpha)|$. One can see that $N(\mathfrak{a}) \in \mathfrak{a}$ as $N(\mathfrak{a}) \cdot (1 + \mathfrak{a}) = 0$ which means $N(\mathfrak{a}) \in \mathfrak{a}$.

What use to us will be ideals? For an isogeny $\phi : E_1 \to E_2$, define

$$\mathfrak{a}_\phi = \{\alpha \in \mathrm{End}(E_1) \mid \ker(\phi) \subseteq \ker(\alpha)\}.$$

It is easy to verify that it is an ideal of $\mathrm{End}(E_1)$. Also notice that since $[\deg \phi](P) = \infty$ for $P \in \ker \phi$ then $(\deg \phi) \subseteq \mathfrak{a}_\phi$. We will show that there is a correspondence between ideals of $\mathrm{End}(E_1)$ and isogenies, allowing us to characterize types of isogenies, and consequently types of edges in V, by these ideals.

$$\begin{array}{l} \text{Ideals in } \mathcal{O} \text{ of} \\ \text{norm } l \end{array} \longleftrightarrow \begin{array}{l} \text{Classes of} \\ l\text{-isogenies} \end{array}$$

Our goal is to formalize this correspondence step by step for descending, ascending and horizontal isogenies. Since the majority of the proofs will be rather technical, reader not interested in the deep understanding can skip this part and continue after Lemma 103. We start with the descending isogenies.

Lemma 96. If $\phi : E_1 \to E_2$ is an l-isogeny over $\mathbb{F}_q$, then $\mathfrak{a}_\phi = (l)$ if and only if ϕ is descending.

Proof. Denote the orders $\mathrm{End}(E) = \mathbb{Z}[\tau]$, $\mathrm{End}(E_2) = \mathbb{Z}[l\tau]$. Firstly, let $E_1[l] = \langle P, Q \rangle$ such that $\ker(\phi) = \langle P \rangle$. Furthermore since $\phi(Q) \in E_2[l] \setminus \{\infty\}$, let $E_2[l] = \langle \phi(Q), R \rangle$ for appropriate $R \in E_2[l]$.

Assume that ϕ is descending. The inclusion $(l) \subseteq \mathfrak{a}_\phi$ was already discussed, the opposite inclusion remains. We will prove that $l \mid \alpha$ for any $\alpha \in \mathfrak{a}_\phi$. Let $\alpha \in \mathfrak{a}_\phi$. By definition of $\mathfrak{a}_\phi$: $\alpha P = \infty$. Clearly $l\alpha \in \mathbb{Z}[l\tau] \subseteq \mathbb{Z}[\tau]$. If we prove that also $\alpha \in \mathbb{Z}[l\tau]$, then $\alpha = a + bl\tau$ for some $a, b \in \mathbb{Z}$, where $l \mid a$, because $aP = \infty$. Hence $l \mid \alpha$. So it remains to show that $\alpha \in \mathbb{Z}[l\tau]$. It suffice to prove that $E_2[l] \subseteq \ker(l\alpha)$ and $l \mid l\alpha$ by Lemma 29 which yields $\alpha \in \mathbb{Z}[l\tau]$. To prove $E_2[l] = \langle \phi(Q), R \rangle \subseteq \ker(l\alpha)$ we apply $l\alpha$ on the generators with the help of Lemma 87:

$$l\alpha\phi(Q) = \phi(l\alpha Q) = \phi(\alpha(lQ)) = \infty.$$

For the second generator R, let $S \in E_1(\overline{\mathbb{F}}_q)$ such that $\phi(S) = R$. We can see that $lS \in \langle P \rangle$ as $\phi(lS) = l\phi(S) = lR = \infty$. Hence

$$l\alpha R = l\alpha\phi(S) = \phi(l\alpha S) = \phi(\alpha(lS)) = \infty.$$

Assume now that $\mathfrak{a}_\phi = (l)$ and ϕ is not descending for contradiction. Let $\tau(P) = aP + bQ$ for some $a, b \in \mathbb{Z}$. Then

$$\infty = \tau(\infty) = \tau(\phi(P)) = \phi(\tau(P)) = \phi(aP + bQ) = b\phi(Q),$$

which implies $b = 0$ as $\phi(Q) \neq \infty$. So we can write $(\tau - a)(P) = \infty$ and consequently $\tau - a \in \mathfrak{a}_\phi = (l)$. Thus $\tau - a = l\beta$ for $\beta \in \mathbb{Z}[\tau]$ and $\beta = c + d\tau$ for some $c, d \in \mathbb{Z}$. This is a contradiction since $\tau - a = lc + ld\tau$ yields $ld = 1$. □

Lemma 97. If $\phi : E_1 \to E_2$ is an l-isogeny, which is not descending, then $\mathfrak{a}_\phi$ is a prime ideal of norm l.

Proof. If ϕ is not descending, then $\mathfrak{a}_\phi \neq (l)$ by Lemma 96. Remembering that $(l) \subseteq \mathfrak{a}_\phi$ and taking the norm

$$N(\mathfrak{a}_\phi) = |\operatorname{End}(E_1)/\mathfrak{a}_\phi| = \frac{|\operatorname{End}(E_1)/(l)|}{|\mathfrak{a}_\phi/(l)|} = \frac{l^2}{|\mathfrak{a}_\phi/(l)|},$$

we arrive at three options for norm of $\mathfrak{a}_\phi$: $1, l$ or l^2. If $N(\mathfrak{a}_\phi) = 1$, then $\mathfrak{a}_\phi = \operatorname{End}(E_1)$ and $1 \in \mathfrak{a}_\phi$, which implies $1 \cdot P = \infty$ for all $P \in \ker(\phi)$, contradiction. The case $N(\mathfrak{a}_\phi) = l^2$ means $\mathfrak{a}_\phi = (l)$. This yields that ϕ is descending by Lemma 96. So the only option is that $N(\mathfrak{a}_\phi) = l$. Any ideal of prime norm is prime ideal. □

Lemma 98. Let $\phi : E_1 \to E_2$ be an l-isogeny over $\mathbb{F}_q$. If $\operatorname{End}(E_1) = \mathbb{Z}[\tau]$ has conductor c and ϕ is horizontal, then $l \nmid c$.

Before we will prove this lemma, we will show how prime ideals containing l look like in an order with conductor divisible by l. This will be useful in the proof.

Lemma 99. If $\mathbb{Z}[\tau]$ is an order in imaginary quadratic number field with conductor c divisible by l, then (l, τ) is the only prime ideal containing l.

Proof. The ring $\mathbb{Z}[\tau]/(l, \tau)$ contains elements $a + b\tau + (l, \tau) = a_0 + (l, \tau)$ where $0 \leq a_0 < l$, $a_0 \equiv a \pmod{l}$. So it has size l and must be isomorphic to $\mathbb{Z}/l\mathbb{Z}$ which is a domain, thus (l, τ) is a prime ideal.

It remains to show uniqueness. Assume $\mathfrak{a}$ is any prime ideal in $\mathbb{Z}[\tau]$ containing l, hence $(l) \subseteq \mathfrak{a}$. We will show that $(l, \tau)^2 \subseteq \mathfrak{a}$ which will imply $(l, \tau) \subseteq \mathfrak{a}$ (as $\mathfrak{a}$ is prime ideal) and consequently $(l, \tau) = \mathfrak{a}$ (as prime ideals are maximal).

We know that $\tau = c\tau_K$ where $\mathcal{O}_K = \mathbb{Z}[\tau_K]$ so $\tau^2 = c^2\tau_K^2$. Since $c\tau_K^2 \in \mathbb{Z}[\tau]$ and $l \mid c$ then $c(c\tau_K^2) = \tau^2 \in (l)$. Using this we get

$$(l, \tau)(l, \tau) = (l^2, l\tau, \tau^2) \subseteq (l) \subseteq \mathfrak{a}.$$

□

We can proceed to proof of Lemma 98.

Proof. Suppose for contradiction that l divides the conductor. In that case by Lemma 97 and Lemma 99 we conclude that $\mathfrak{a}_\phi = (l, \tau)$. Since ϕ is horizontal, we get the same equality for the dual isogeny: $\mathfrak{a}_{\widehat{\phi}} = (l, \tau)$. Denote $\mathcal{O}_K = \mathbb{Z}[\tau_K]$ and $\tau = c\tau_K$. Lemma 29 tells us that there is an isogeny $\psi : E_2 \to E_1$ such that $\tau = \psi\phi$. We will show that $\psi = \omega\widehat{\phi}$, for appropriate $\tau \in \mathrm{End}(E_1)$, thus $\tau = \omega l$ and $l \mid \tau$, contradiction. For $\psi = \omega\widehat{\phi}$ it suffices to show that $\ker(\widehat{\phi}) \subseteq \ker(\psi)$.

Firstly, we will prove that $E_2[l] \cap \ker(\psi) \neq \{\infty\}$ by considering the norm: $N(\tau) = N(c)N(\tau_K)$. Since $l \mid c$ then $l^2 \mid N(\tau)$. This implies $\deg\tau = l \deg\psi$ and $l \mid \deg\psi$. Thus there exists an affine point $S \in \ker(\psi) \cap E_2[l]$.

As before denote $E_1[l] = \langle P, Q\rangle$ and $E_2[l] = \langle \phi(Q), R\rangle$ where $\ker(\phi) = \langle P\rangle$ and $\ker(\widehat{\phi}) = \langle\phi(Q)\rangle$. We can write $S = a\phi(Q) + bR$ for appropriate $a, b \in \mathbb{Z}$. We will prove that $\phi(Q) \in \ker(\psi)$ which will finish the proof. Since $\psi(S) = \infty$ then

$$\infty = \phi(\psi(S)) = \tau(S) = \tau(a\phi(Q) + bR) = b\tau(R),$$

where we used $\tau \in \mathfrak{a}_{\widehat{\phi}}$. Either $\tau(R) = \infty$ and $l \mid \tau$, contradiction, or $b = 0$. The latter case implies $S = a\phi(Q) \in \ker(\psi)$ and $\phi(Q) \in \ker(\psi)$ which we wanted to prove. □

Lemma 100. Let $\phi : E_1 \to E_2$ be an l-isogeny over $\mathbb{F}_q$. If $\mathrm{End}(E_1)$ has conductor c, then ϕ is ascending if and only if $l \mid c$ and $\mathfrak{a}_\phi = (l, \tau)$.

Proof. If ϕ is ascending, then $l \mid c$ and by Lemma 99, we get that $\mathfrak{a}_\phi = (l, \tau)$.

On the other hand if $\mathfrak{a}_\phi = (l, \tau)$, then ϕ is not descending and is therefore ascending or horizontal and it can't be horizontal because of Lemma 98 and the condition $l \mid c$.

□

We have managed to assign to every l-isogeny ϕ an ideal $\mathfrak{a}_\phi$, we should transfer this to V. Each edge of V is a tuple $([\phi], [\psi])$. We will show in the following that we can assign to each $[\phi]$ and ideal and this doesn't depend on the choice of ϕ.

Corollary 101. If $\phi : E_1 \to E_2$, $\psi : E_1' \to E_2'$ are l-isogenies such that $[\phi] = [\psi]$, then $\mathfrak{a}_\phi = \mathfrak{a}_\psi$.

Proof. By definition $\phi = \rho_2\psi\rho_1$ for some isomorphisms $\rho_1 : E_1 \to E_1'$ and $\rho_2 : E_2' \to E_2$. Let $\alpha \in \mathfrak{a}_\phi$ and $\ker(\psi) = \langle Q\rangle$. If we prove that $\alpha(Q) = \infty$, then $\mathfrak{a}_\phi \subseteq \mathfrak{a}_\psi$. The other inclusion is symmetrical.

If $Q \in \ker(\psi)$, then for each $P \in \rho_1^{-1}(Q)$: $P \in \ker(\phi)$. Hence $\alpha(P) = \infty$ and $\rho_1\alpha(P) = \infty$. Finally, $\alpha\rho_1(P) = \alpha(Q) = \infty$ by Lemma 87. □

We thus get a map that assigns to every class of l-isogenies $[\phi]$ from vertex $j(E)$ an ideal in $\mathrm{End}(E)$. Let's look at the situation the opposite way now. Assume we have an ideal $\mathfrak{a} \subseteq \mathrm{End}(E)$ and define

$$E[\mathfrak{a}] = \{P \in E(\overline{\mathbb{F}}_q) \mid \alpha(P) = \infty, \text{ for all } \alpha \in \mathfrak{a}\} = \bigcap_{\alpha \in \mathcal{A}} \ker(\alpha),$$

where $\mathcal{A} = \{\alpha \in \text{End}(E) \mid \ker(\phi) \subseteq \ker(\alpha)\}$. The set $E[\mathfrak{a}]$ is a finite subgroup of $E(\overline{\mathbb{F}}_q)$ since it is an intersection of finite subgroups. Hence, it is a kernel of an isogeny $\phi_{\mathfrak{a}} : E \to E'$. We will at first focus on prime ideals $\mathfrak{a}$ of norm l in which case $l \in \mathfrak{a}$ and therefore $E[\mathfrak{a}] \subseteq E[l]$. Be aware that $\phi_{\mathfrak{a}}$ and E' are not uniquely determined and both are a priori defined over some extension of $\mathbb{F}_q$.

Lemma 102. If $\mathfrak{a}$ is a prime ideal of norm l in an order $\text{End}(E_1) = \mathbb{Z}[\tau]$ with conductor c, then there exists an l-isogeny $\phi_{\mathfrak{a}} : E_1 \to E_2$ where $\ker(\phi_{\mathfrak{a}}) = E_1[\mathfrak{a}]$, E_2 is defined over $\mathbb{F}_q$ and:

(i) $\phi_{\mathfrak{a}}$ is an ascending isogeny if $l \mid c$.

(ii) $\phi_{\mathfrak{a}}$ is a horizontal isogeny if $l \nmid c$.

Proof. Firstly we have to realize that $|E_1[\mathfrak{a}]| = l$: There are three possibilities for $|E_1[\mathfrak{a}]| = 1, l, l^2$ as a subgroup of $E_1[l]$. If $E_1[\mathfrak{a}] = l^2$, then $E_1[\mathfrak{a}] = E_1[l]$ and $l \mid \alpha$ for all $\alpha \in \mathfrak{a}$, hence $\mathfrak{a} = (l)$ which doesn't have norm l. It remains the case $E[\mathfrak{a}] = \{\infty\}$. If we denote $\mathfrak{a} = (\alpha, \beta)$, then $\ker(\alpha) \cap \ker(\beta) = E[\mathfrak{a}] = \{\infty\}$. Since $l \mid N(\alpha)$ and $l \mid N(\beta)$ it follows that there exist $P \in \ker(\alpha) \cap E_1[l]$, $Q \in \ker(\beta) \cap E_1[l]$ satisfying $\alpha(Q) \neq \infty$, $\beta(P) \neq \infty$. Considering $l \in \mathfrak{a}$, there exist $a, b \in \mathbb{Z}$ such that $l = a\alpha + b\beta$. Thus $\infty = lP = (a\alpha + b\beta)P = b\beta P$, which implies $l \mid b$ and similarly $l \mid a$ which is contradiction since $1 = \frac{a}{l}\alpha + \frac{b}{l}\beta \in \mathfrak{a}$.

By discussion above there exists an l-isogeny $\phi_{\mathfrak{a}}$ defined over some extension of $\mathbb{F}_q$. At first we will prove (i) and (ii) for the extension. The fact that we can choose $\phi_{\mathfrak{a}}$ defined over $\mathbb{F}_q$ will follow from the next Lemma 103.

(i) If $l \mid c$, then $\phi_{\mathfrak{a}}$ is not horizontal from Lemma 98, so it must be either ascending or descending. Assume the latter for contradiction. We will consider the ideal

$$\mathfrak{a}_{\phi_{\mathfrak{a}}} = \{\alpha \in \mathcal{O} \mid \ker(\phi_{\mathfrak{a}}) \subseteq \ker(\alpha)\},$$

which must be equal to (l) as $\phi_{\mathfrak{a}}$ is descending (Lemma 96). By definition $\mathfrak{a} \subseteq \mathfrak{a}_{\phi_{\mathfrak{a}}}$ as every element of $\mathfrak{a}$ satisfies $\ker \phi_{\mathfrak{a}} \subseteq \ker \alpha$ and $\mathfrak{a}_{\phi_{\mathfrak{a}}}$ is an ideal of all such elements. This means that $\mathfrak{a} \subseteq (l)$ and doesn't have norm l, contradiction.

(ii) Since $l \nmid c$ and $\mathfrak{a} \neq (l)$, then $\phi_{\mathfrak{a}}$ can't be ascending or descending.

□

Lemma 103. Let $\phi : E_1 \to E_2$ be any l-isogeny of ordinary elliptic curves over $\mathbb{F}_{q^n}$:

(i) If ϕ is not descending and $j(E_1) \in \mathbb{F}_q$, then $j(E_2) \in \mathbb{F}_q$.

(ii) If E_1 and E_2 are defined over $\mathbb{F}_q$, then there exists an isomorphism $\rho : E_2 \to E_2'$ such that $\rho\psi : E_1 \to E_2'$ is an l-isogeny over $\mathbb{F}_q$.

Proof. (i) If $j(E_1) \in \mathbb{F}_q$, then there is an elliptic curve E_1' over $\mathbb{F}_q$ and isomorphism $\rho_1 : E_1' \to E_1$. Hence $\phi\rho_1 : E_1' \to E_2$ is an l-isogeny over $\mathbb{F}_{q^n}$ which is not ascending so $\text{End}(E_1) \subseteq \text{End}(E_2)$ and $\pi : (x, y) \mapsto (x^q, y^q)$ is in $\text{End}(E_2)$. Thus E_2 is defined over $\mathbb{F}_q$ and $j(E_2) \in \mathbb{F}_q$.

(ii) If $\pi(\ker(\psi)) = \ker(\psi)$, there is an isogeny $\phi : E_1 \to E_2'$ over $\mathbb{F}_q$ with $\ker(\phi) = \ker(\psi)$, and isomorphism $\rho : E_2' \to E_2$ satisfying $\rho\psi = \phi$ by Theorem 26.

Suppose that $\pi(\ker\psi) \neq \ker(\psi)$ and consider the isogeny $\psi\pi : E_1 \to E_2$ over $\mathbb{F}_{q^n}$ which has kernel distinct from $\ker(\psi)$. By Corollary 18, there is an isogeny $\psi' : E \to E'$ defined over $\mathbb{F}_{q^n}$ such that $\psi\pi = \pi\psi'$. Moreover, $\ker(\psi') = \ker(\psi') = \ker(\psi\pi) \neq \ker(\psi)$. We have therefore two l-isogenies ψ, ψ' defined over $\mathbb{F}_{q^n}$. However, the endomorphism $\alpha = \widehat{\psi'}\psi : E_1 \to E_1$ must by defined over $\mathbb{F}_q$. Both $\ker(\psi)$ and $\ker(\psi')$ are subgroups of $E_1[l]$ of order l generated by P, Q respectively and since they are different subgroups then $\langle P, Q\rangle = E_1[l]$. Clearly, $P \in \ker(\alpha)$. If also $Q \in \ker(\alpha)$ then $E_1[l] = \ker(\alpha)$ and $\alpha = l$ as $\deg(\alpha) = l^2$. Furthermore, $\widehat{\psi'} = \widehat{\psi}$ and $\psi = \psi'$ which is contradiction as they have different kernels.

So it must be that $Q \notin \ker(\alpha)$. Since α is defined over $\mathbb{F}_q$, $\pi(P) \in E[l] \cap \ker(\alpha) = \langle P\rangle$. Hence $\ker\phi$ is $\mathbb{F}_q$-stable and there exists an l-isogeny $\phi : E_1 \to E_2'$ and isomorphism $\rho : E_2 \to E_2'$ such that $\rho\psi = \phi$.

□

Let us stop here and recapitulate what we have learned. We have encountered two maps. One is assigning to every class $[\phi]$ of non-descending[1] l-isogeny a prime ideal of norm l, i.e.

$$\text{class of non-descending isogenies } [\phi] \ \mapsto \text{prime } \mathfrak{a}_\phi \text{ ideal of norm } l.$$

This is well defined by Corollary 101. The other map assigns to any prime ideal $\mathfrak{a}$ of norm l a non-descending isogeny, i.e. $\mathfrak{a} \mapsto \phi_{\mathfrak{a}}$. This isogeny $\phi_{\mathfrak{a}}$ is uniquely determined only up to isomorphism hence

$$\text{prime ideal } \mathfrak{a} \text{ of norm } l \ \mapsto \text{class of non-descending isogenies } [\phi_{\mathfrak{a}}].$$

Natural question arises: Are these inverses? Or more precisely, is it true that $\mathfrak{a}_{\phi_{\mathfrak{a}}} = \mathfrak{a}$ and $[\phi_{\mathfrak{a}_\phi}] = [\phi]$? By definition, every element of $\mathfrak{a}$ satisfies $\ker\phi_{\mathfrak{a}} \subseteq \ker\alpha$ and $\mathfrak{a}_{\phi_{\mathfrak{a}}}$ is an ideal of all such elements, so $\mathfrak{a} \subseteq \mathfrak{a}_{\phi_{\mathfrak{a}}}$. The equality then holds from the fact that they have the same norm. Similarly, we can prove that $\ker\phi_{\mathfrak{a}_\phi} = \ker\phi$, by proving one inclusion since they have the same order: By definition $\ker\phi \subseteq \bigcap_{\alpha\in\mathfrak{a}_\phi}\ker\alpha = E[\mathfrak{a}_\phi] = \ker\phi_{\mathfrak{a}_\phi}$. We indeed have bijection between ideals in $\mathrm{End}(E)$ of norm l and non-descending l-isogenies.

If l divides the conductor of $\mathrm{End}(E)$, there is no horizontal isogeny from E, and there is exactly one prime ideal of norm l in $\mathrm{End}(E)$ which corresponds to exactly one ascending isogeny.

Corollary 104. Let E be an ordinary elliptic curve such that $j(E) \in V$. If $l \mid c$ where c is the conductor of $\mathrm{End}(E)$, then there is, up to isomorphism, exactly one ascending l-isogeny from E. In particular, if $\mathcal{O}_0$ is the order corresponding to V_0 with conductor c_0, then $l \mid c_0$.

[1] Non-descending isogeny is an isogeny which is not descending.

On the other hand, if l doesn't divide c, then there is no ascending isogeny and every non-descending l-isogeny is horizontal, hence we get the following bijection

$$\begin{tikzcd}
\text{Ideals in } \mathcal{O} \text{ of norm } l & \mathfrak{a} \arrow[r] & {[\phi_{\mathfrak{a}}]} & \text{Classes of horizontal } l\text{-isogenies} \\
& \mathfrak{a}_\phi & {[\phi]} \arrow[l] &
\end{tikzcd}$$

We can see that the study of horizontal l-isogenies reduces to studying prime ideals of norm l in $\mathcal{O}$. So the next goal is to understand how such ideals behave.

Prime ideals

We are in a situation of ordinary elliptic curve with endomorphism ring isomorphic to an order $\mathcal{O}$ of imaginary quadratic number field. At first, assume that $\mathcal{O}$ is the maximal order $\mathcal{O}_K$. The maximal order has many nice properties, which general orders don't share. One of the most important for us is the following theorem:

Theorem 105 ([Cox13])**.** If K is a number field, then any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be written as a product

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n$$

of prime ideals, and the decomposition is unique up to order. Furthermore, the $\mathfrak{p}_i$'s are exactly the prime ideals of $\mathcal{O}_K$ containing $\mathfrak{a}$.

The proof is beyond the scope and point of this text. What this means for us? The factorization of (l) in $\mathcal{O}_K$ tells us how many horizontal edges are there from $j(E)$. Moreover, every such prime ideal will correspond to one of those edges. However, how can we determine such factorization? To help us with this comes another proposition, again without proof:

Proposition 106 ([Cox13])**.** Let K be a quadratic field of discriminant d_K. Let l be prime[2] in $\mathbb{Z}$.

(i) If $\left(\frac{d_K}{l}\right) = 0$ then $(l) = \mathfrak{l}^2$ for some prime ideal $\mathfrak{l}$ of $\mathcal{O}_K$.

(ii) If $\left(\frac{d_K}{l}\right) = 1$, then $(l) = \mathfrak{l}\mathfrak{l}'$, where $\mathfrak{l}, \mathfrak{l}'$ are prime ideals in $\mathcal{O}_K$.

(iii) If $\left(\frac{d_K}{l}\right) = -1$, then (l) is a prime ideal in $\mathcal{O}_K$.

Furthermore, the prime ideals in (i)-(iii) above give all nonzero prime ideals of $\mathcal{O}_K$.

[2] For $l \neq 2$, $\left(\frac{n}{l}\right)$ is the Legendre symbol and for $l = 2$ we use the Kronecker symbol:
$$\left(\frac{n}{l}\right) = \begin{cases} 0 & n \equiv 0 \pmod 4 \\ 1 & n \equiv 1 \pmod 8 \\ -1 & n \equiv 5 \pmod 8 \end{cases}$$

So the situation is quite clear in $\mathcal{O}_K$ but what about in general order $\mathcal{O} \subseteq \mathcal{O}_K$ with conductor c, $l \nmid c$? We will see that we can transfer the knowledge of prime ideals in $\mathcal{O}_K$ to $\mathcal{O}$. We are going to construct a bijection between prime ideals of $\mathcal{O}$ and of $\mathcal{O}_K$. More precisely, we will construct two maps which are inverses of each other:

$$\begin{tikzcd}
\text{Ideals in } \mathcal{O}_K & \mathfrak{a} \arrow[r] & \mathfrak{a} \cap \mathcal{O} & \text{Ideals in } \mathcal{O} \text{ of} \\
\text{of norm } l & \mathfrak{a}\mathcal{O}_K & \mathfrak{a} \arrow[l] & \text{norm } l
\end{tikzcd}$$

The main focus of this section are prime ideals of norm l, but for easier study of these ideals we will have to consider more general concept:

Definition 107. Let $\mathcal{O}$ be an order of imaginary quadratic field and $f \in \mathbb{Z}$. An ideal $\mathfrak{a} \subseteq \mathcal{O}$ is prime to f if $\gcd(N(\mathfrak{a}), f) = 1$.

We will be in particular interested in ideals prime to conductor of $\mathcal{O}$. These encompass any ideal of norm l as we are dealing with orders with conductor not divisible by l.

Lemma 108. Let $\mathcal{O}$ be an order in imaginary quadratic field K with conductor c.

(i) If $\mathfrak{b} \subseteq \mathcal{O}_K$ is an $\mathcal{O}_K$ ideal prime to c, then $\mathfrak{b} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal of the same norm and there exists a ring isomorphism $\mathcal{O}/(\mathcal{O} \cap \mathfrak{b}) \to \mathcal{O}_K/\mathfrak{b}$.

(ii) If $\mathfrak{a} \subseteq \mathcal{O}$ is an $\mathcal{O}$ ideal prime to c, then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal of the same norm and there exists a ring isomorphism $\mathcal{O}/\mathfrak{a} \to \mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$.

(iii) For any $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{a}'$ and $\mathcal{O}_K$-ideals $\mathfrak{b}, \mathfrak{b}'$, the following relations hold:

$$\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{a},\ (\mathfrak{b} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{b},$$

$$(\mathfrak{b} \cap \mathcal{O})(\mathfrak{b}' \cap \mathcal{O}) = \mathfrak{b}\mathfrak{b}' \cap \mathcal{O},\ (\mathfrak{a}\mathcal{O}_K)(\mathfrak{a}'\mathcal{O}_K) = (\mathfrak{a}\mathfrak{a}')\mathcal{O}_K.$$

Proof. We will refer the reader to [Cox13]. The important fact for the proof in the reference is that $\mathfrak{b} + (l) = \mathcal{O}_K$ and $\mathfrak{a} + (l) = \mathcal{O}$. This can be seen if we recall the Bezout's identity: If $\gcd(N(\mathfrak{b}), c) = 1$, there exist $a, b \in \mathbb{Z}$ such that $aN(\mathfrak{b}) + bc = 1$, which implies $1 \in \mathfrak{b} + (l)$ and similarly for $\mathfrak{a}$.

□

Corollary 109. The map $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ is a bijection between $\mathcal{O}_K$-ideals prime to the conductor c of $\mathcal{O}$ and $\mathcal{O}$-ideals prime to c. For any prime l coprime with c, this bijection can be restricted between the set of prime ideals of $\mathcal{O}_K$ of norm l and prime ideals of $\mathcal{O}$ of norm l. Furthermore, each ideal in $\mathcal{O}$ prime to the conductor can be uniquely factorized into a product of prime ideals.

Proof. The first claim follows immediately from the previous Lemma 108. The lemma also tells us that $\mathcal{O}_K/\mathfrak{b}$ and $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O})$ are isomorphic. So $N(\mathfrak{b}) = l$ if and only if $N(\mathfrak{a} \cap \mathcal{O}) = l$. Similar argument holds for the inverse map. The unique factorization is a consequence of the multiplicative property from Lemma 108 (iii) and unique factorization in $\mathcal{O}_K$. □

We are now ready to fully characterize the number of horizontal isogenies.

Corollary 110. Let E be an ordinary elliptic curve, $j(E) \in V$, $\mathcal{O} = \operatorname{End}(E)$ an order with conductor c in imaginary quadratic field K with discriminant d_K. If $l \nmid c$, then the number of horizontal edges from $j(E)$ is $1 + \left(\frac{d_K}{l}\right)$, otherwise there are none.

Proof. If $l \mid c$, then there are no horizontal edges by Lemma 98. Otherwise, there are exactly $1 + \left(\frac{d_K}{l}\right)$ ideals of norm l in $\mathcal{O}$. The rest follows from the bijection between these ideals and horizontal l-isogenies.

$$\begin{tikzcd}
\text{Ideals in } \mathcal{O}_K \text{ of norm } l & \mathfrak{a} \arrow[r] & \mathfrak{a} \cap \mathcal{O} & \text{Ideals in } \mathcal{O} \text{ of norm } l & \mathfrak{a} \arrow[r] & {[\phi_{\mathfrak{a}}]} & \text{Classes of horizontal } l\text{-isogenies} \\
 & \mathfrak{a}\mathcal{O}_K & \mathfrak{a} \arrow[l] & & \mathfrak{a}_{\phi} & {[\phi]} \arrow[l] &
\end{tikzcd}$$

□

Before we look at vertical isogenies, let's use Lemma 108 to prove multiplicativity of norm. In general, it is not true that $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b})$, but as it turns out, this holds for ideals prime to the conductor:

Corollary 111. Let $\mathcal{O}$ be an order in imaginary quadratic field K with conductor c. Then $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ for any two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ prime to c.

Proof. Firstly, $N(\mathfrak{a}\mathfrak{b}) = N((\mathfrak{a}\mathfrak{b})\mathcal{O}_K) = N((\mathfrak{a}\mathcal{O}_K)(\mathfrak{b}\mathcal{O}_K))$. The norm in $\mathcal{O}_K$ is multiplicative hence $N((\mathfrak{a}\mathcal{O}_K)(\mathfrak{b}\mathcal{O}_K)) = N(\mathfrak{a}\mathcal{O}_K)N(\mathfrak{b}\mathcal{O}_K) = N(\mathfrak{a})N(\mathfrak{b})$. □

Lemma 108 has answered the question about horizontal edges. What about the vertical ones. We already know that if l divides the conductor of endomorphism ring of elliptic curve, then there is exactly one ascending isogeny and if l doesn't divide the conductor, there is none. What about the descending ones?

Lemma 112. Let E be an ordinary elliptic curve, $\mathcal{O} = \operatorname{End}(E)$ an order in imaginary quadratic field K with conductor c. Also denote $v = |\mathcal{O}_K/\mathbb{Z}[\pi]|$.

(i) If $l \nmid \frac{v}{c}$, then there are no descending isogenies from E.

(ii) If $l \mid \frac{v}{c}$ and $l \mid c$, then there are, up to isomorphism, l descending isogenies from E.

(iii) If $l \mid \frac{v}{c}$ and $l \nmid c$, then there are, up to isomorphism, $l - \frac{d_k}{l}$ descending isogenies from E.

Proof. (i) Assume for contradiction that there is a descending l-isogeny $E \to E'$. Then the conductor of $\operatorname{End}(E')$ is $lc \mid v$ which means $l \mid \frac{v}{c}$.

(ii) Let $\mathcal{O}_K = \mathbb{Z}[\tau_k]$. We have shown $\tau_K = \frac{\pi - a}{v}$ for appropriate $a \in \mathbb{Z}$ in Lemma 84. Since $c\tau_K \in \mathcal{O}$, we get $\frac{v}{c}c\tau_K = \pi - a \in \mathcal{O}$ and $\frac{v}{c} \mid \pi - a$. By the assumption $l \mid \pi - a$, which means that π fixes every subgroup of $E[l]$ and there are therefore $l + 1$ l-isogenies with domain E. Remembering that $l \mid c$, there is exactly one ascending isogeny and no horizontal isogenies, hence l descending l-isogenies. In the case of (iii) there are no ascending isogenies and $\frac{d_k}{l}+1$ horizontal isogenies which finishes the proof.

□

We finally arrive at the main theorem of this chapter which shows that V is a volcano in the sense of the Definition 53.

Theorem 113 ([Sut12])**.** Let V be an ordinary component of $G_l(\mathbb{F}_q)$ that does not contain 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 $1+\left(\frac{d_K}{l}\right)$, where d_K is the discriminant of the fraction field K of $\mathcal{O}$.

(iii) The depth of V is[3] $d=\frac{1}{2}\nu_l\left(\frac{T(\pi_E)^2-4q}{d_K}\right)$, for any $j(E)\in V$.

(iv) $l\nmid[\mathcal{O}_K:\mathcal{O}_0]$ and $[\mathcal{O}_i:\mathcal{O}_{i+1}]=l$ for $0\le i<d$.

(v) The depth of any $j(E)\in V$ is $\nu_l(c)$ where c is the conductor of $\operatorname{End}(E)$.

Proof. We have partitioned V into levels V_i in Lemma 95 with orders $\mathcal{O}_i$ and $[\mathcal{O}_i:\mathcal{O}_{i+1}]=l$. The subgraph on V_0 (consisting of horizontal edges) contains vertices with degree $1+\left(\frac{d_K}{l}\right)$ by Corollary 110, also $l\nmid[\mathcal{O}_K:\mathcal{O}_0]$. The parts (iii) and (iv) follow from Lemma 112.

It remains to show that V is l-volcano. For $i<d$, each vertex in V_i has degree $l+1$ by Lemma 112. For $i>0$, each vertex in V_i has exactly one neighbor in level V_{i-1} by Lemma 104. Finally, we have to prove that if there any loops in V_0 then $|V_0|=1$. We could prove it here but we will wait for more elegant proof.

□

Class group

It seems that we have almost fully described the ordinary components of $G_l(\mathbb{F}_q)$. However, one information about volcanoes remains undescribed: the size of the subgraph on V_0 and the number of loops in V_0. If the degree of V_0 is 0,1 or $|V_0|=1$, then there is nothing to think about. However, if $|V_0|>1$ and the degree is 2, then there are a priori two options for the crater as in the Figure 4.1. The goal is to prove that the right option never happens and more importantly to characterize the size of the cycle on the left. Recall that each directed edge from vertex $j(E)$ corresponds to a unique prime ideal containing l. We will expand upon this by identifying ideals in $\operatorname{End}(E)$ with sequences of horizontal edges we will call walks. Walks around the crater will help us characterize the size of the crater.

Definition 114 (Walk)**.** Let $\operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ be the set of j-invariants of elliptic curves over $\mathbb{F}_q$ with endomorphism ring isomorphic to $\mathcal{O}$. We define a *walk* on $\operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ as a sequence $(\mathfrak{l}_1,\mathfrak{l}_2,\ldots,\mathfrak{l}_n)$ of prime ideals $\mathfrak{l}_i\subseteq\mathcal{O}$ prime to conductor c of $\mathcal{O}$. An empty sequence will be called empty walk.

[3] $\nu_l(a)$ denotes the highest integer i such that $l^i\mid a$

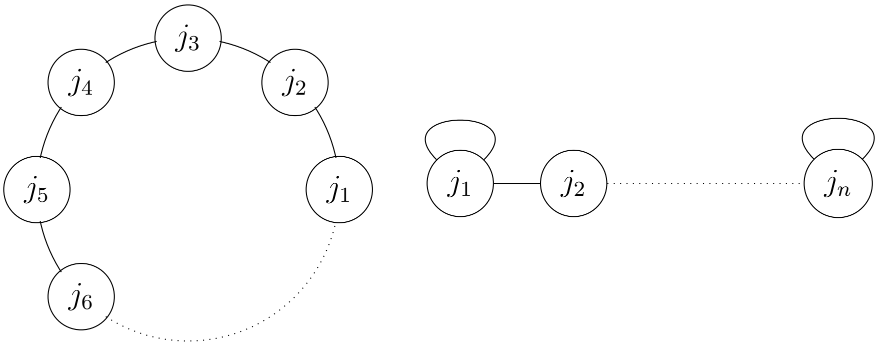


Figure 4.1: Two options for crater of degree 2

Recall that for each vertex $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ each prime ideal in $\mathcal{O}$ prime to conductor corresponds to a directed horizontal edge $j(E)$. If we fix a $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, then any walk $\alpha = (\mathfrak{l}_1, \mathfrak{l}_2, \dots, \mathfrak{l}_n)$ uniquely corresponds to a series of directed horizontal edges:

$$\begin{tikzcd} j(E) \arrow[r, "\mathfrak{l}_1"] & j(E_2) \arrow[r, "\mathfrak{l}_2"] & j(E_3) \arrow[r, "\mathfrak{l}_3"] & \cdots \arrow[r, "\mathfrak{l}_n"] & j(E_n) \end{tikzcd}$$

We say that the walk α from $j(E)$ *ends* in $j(E_n)$. We will show that the vertex $j(E_n)$ doesn't depend on the order of the ideals $\mathfrak{l}_1, \dots, \mathfrak{l}_n$, hence allowing us to uniquely assign to $j(E_n)$ the (commutative) product $\mathfrak{a} = \mathfrak{l}_1 \cdot \dots \cdot \mathfrak{l}_n$. All ideals assigned to $j(E_n)$ for different walks will form a class of ideals. In the end, we will show that these classes form a group called class group and the size of the crater will be an order of appropriate element of this class group.

Lemma 115. Let $\alpha = (\mathfrak{l}_1, \mathfrak{l}_2, \dots, \mathfrak{l}_n)$ be a walk on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ and E_1 an elliptic curve over $\mathbb{F}_q$ such that $j(E_1) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$. Denote the product $\mathfrak{a} = \mathfrak{l}_1\mathfrak{l}_2 \dots \mathfrak{l}_n$. There exists an isogeny $\phi : E_1 \to E_n$ with degree $\deg \phi = N(\mathfrak{a})$ such that $\ker \phi = E_1[\mathfrak{a}] = \{P \in E_1(\overline{\mathbb{F}}_q) \mid \alpha(P) = \infty \text{ for all } \alpha \in \mathfrak{a}\}$ and the walk α from $j(E_1)$ ends in $j(E_n)$.

Proof. The statement is trivial for $n = 1$. Let $\phi_1, \phi_2, \dots, \phi_n$ be any isogenies corresponding to $\mathfrak{l}_1, \mathfrak{l}_2, \dots, \mathfrak{l}_n$ such that domain of ϕ_1 is E_1 and domain E_i of ϕ_i is codomain of ϕ_{i-1} for $i = 2 \dots, n$:

$$\begin{tikzcd} E_1 \arrow[r, "\phi_1"] & E_2 \arrow[r, "\phi_2"] & E_3 \arrow[r, "\phi_3"] & \cdots \arrow[r, "\phi_n"] & E_n \end{tikzcd}$$

Denote $\phi = \phi_n\phi_{n-1} \dots \phi_1$, then

$$\deg(\phi) = \deg(\phi_n) \dots \deg(\phi_1) = N(\mathfrak{l}_1) \dots N(\mathfrak{l}_n) = N(\mathfrak{a})$$

It remains to prove that $\ker \phi = E_1[\mathfrak{a}]$. Suppose it's true for $n-1$, i.e. $\ker \phi' = E[\mathfrak{a}']$ where $\phi' = \phi_{n-1} \dots \phi_1$, $\mathfrak{a}' = \mathfrak{l}_1\mathfrak{l}_2 \dots \mathfrak{l}_{n-1}$. Then $\phi = \phi_n\phi'$, $\ker \phi_n = E_{n-1}[\mathfrak{l}_n]$ and

$$\ker \phi = \{P \in E(\overline{\mathbb{F}}_q) \mid \phi'(P) \in E_{n-1}[\mathfrak{l}_n]\} = \{P \mid \alpha\phi'(P) = \infty, \forall \alpha \in \mathfrak{l}_n\}$$

By Lemma 87 endomorphisms commute with horizontal isogenies and we can write

$$= \{P \mid \phi'\alpha(P) = \infty, \forall \alpha \in \mathfrak{l}_n\} = \{P \mid \alpha(P) \in E[\mathfrak{a}'], \forall \alpha \in \mathfrak{l}_n\} =$$

$$= \{P \mid \alpha'\alpha(P) = \infty \text{ for all } \alpha \in \mathfrak{l}_n, \alpha' \in \mathfrak{a}'\} =$$

$$= \{P \in E(\overline{\mathbb{F}}_q) \mid \alpha(P) = \infty \text{ for all } \alpha \in \mathfrak{a}'\mathfrak{l}_n\} = E[\mathfrak{a}'\mathfrak{l}_n] = E[\mathfrak{a}].$$

□

The fact that product of ideals is commutative translates into commutativity of horizontal isogenies as the following corollary states.

Corollary 116. Let $\alpha = (\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_n)$ be a walk on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ from $j(E)$ to $j(E_n)$. If σ is any permutation on the set $\{1, \ldots, n\}$ then the walk $\beta = (\mathfrak{l}_{\sigma(1)}, \mathfrak{l}_{\sigma(2)}, \ldots, \mathfrak{l}_{\sigma(n)})$ from $j(E)$ ends in $j(E_n)$.

So, as claimed, the end of walk from $j(E)$ doesn't depend on the order of ideals, rather on the product. If denote $I(\mathcal{O})$ the set of ideals of $\mathcal{O}$ prime to conductor, then every ideal $\mathfrak{a} \in I(\mathcal{O})$ can be uniquely factorized into a product of prime ideals prime to conductor. This yields a map $I(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) \to \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ defined as $(\mathfrak{a}, j(E)) \mapsto j(E')$ where the walk $\mathfrak{a}$ from $j(E)$ ends in $j(E')$. We will denote this map as $\mathfrak{a} \cdot j(E) = j(E')$.

Our objective is the crater. If the crater is a cycle then it means there is an ideal $\mathfrak{a}$ given by the walk around the crater for which $\mathfrak{a} \cdot j(E) = j(E)$. The following lemma shows that such ideal must be principal.

Lemma 117. Let E be ordinary elliptic curve over $\overline{\mathbb{F}}_q$ and $\mathfrak{a}$ be ideal of $\mathrm{End}(E)$. The isogeny $\phi_{\mathfrak{a}}$ is an endomorphism if and only if $\mathfrak{a}$ is generated by one element $\alpha \in \mathrm{End}(E)$, i.e. $(\alpha) = \mathfrak{a}$. In particular, $\mathfrak{a} \cdot j(E) = j(E)$ if and only if $\mathfrak{a}$ is principal.

Proof. If $\mathfrak{a} = (\alpha)$ then clearly $E[\mathfrak{a}] = \ker \alpha$. Corresponding isogenies differ up to an isomorphism over $\mathbb{F}_q$ which is endomorphism.

On the other hand if $\phi_{\mathfrak{a}}$ is an endomorphism, then $E[\mathfrak{a}] = \ker \phi_{\mathfrak{a}} = E[(\phi_{\mathfrak{a}})]$. This means that $\mathfrak{a} = (\phi_{\mathfrak{a}})$. □

Equipped with the Lemma 117 we can finally take care of the loops on the crater.

Lemma 118. If $j(E) \in V_0$ has a loop then $|V_0| = 1$.

Proof. Any loop corresponds to an ideal $\mathfrak{l}$ such that $\mathfrak{l} \cdot j(E) = j(E)$ hence $\mathfrak{l}$ is principal. If we assume $|V_0| > 1$, then there is another edge from $j(E)$ to $j(E') \neq j(E)$ which corresponds to an ideal $\mathfrak{l}'$. Moreover $\mathfrak{l}\mathfrak{l}' = (l)$. Since $\mathfrak{l}$ is principal by Lemma 117, then $\mathfrak{l}'$ is also principal, hence $j(E) = j(E')$ which is a contradiction. □

Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ be a walk around the crater from $j(E)$ (which ends in $j(E)$). The goal is to characterize the integer n. We know from Lemma 117 that $\mathfrak{l}_1 \cdot \ldots \cdot \mathfrak{l}_n$ is a principal ideal. Recall that each $\mathfrak{l}_i$ is one of the ideals $\mathfrak{l}$, $\mathfrak{l}'$ satisfying $\mathfrak{l}\mathfrak{l}' = (l)$ (Proposition 106). It follows again from Lemma 117 that all of the ideals $\mathfrak{l}_i$ are equal. Thus both the ideals $\mathfrak{l}$ and $\mathfrak{l}'$ give us two walks in opposite direction, in another words

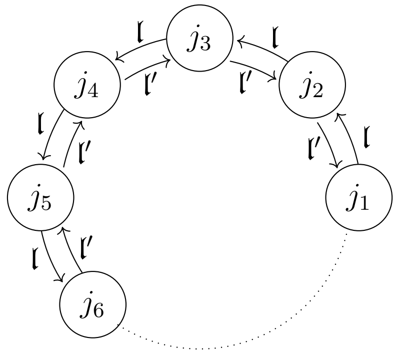


Figure 4.2: Orientation of the crater

orientation of the crater (see the Figure 4.2). If we pick, for example, the ideal $\mathfrak{l}$ then we want to find n such that $\mathfrak{l}^n \cdot j(E) = j(E)$ or equivalently $\mathfrak{l}^n = (\alpha)$ for some $\alpha \in \mathcal{O}$.

So it seems that we are interested in 'order of $\mathfrak{l}$ up to principal ideal'. This can be formalized. Consider the subset $P(\mathcal{O}) \subseteq I(\mathcal{O})$ of principal ideals. We define a relation on $I(\mathcal{O})$ as

$$\mathfrak{a} \sim \mathfrak{b} \iff (\alpha)\mathfrak{a} = (\beta)\mathfrak{b} \text{ for some } (\alpha), (\beta) \in P.$$

It can be easily proven straight up from the definition that this is an equivalence, but it is perhaps better to realize this from equivalent description

$$\mathfrak{a} \sim \mathfrak{b} \iff \mathfrak{a} \cdot j(E) = \mathfrak{b} \cdot j(E) \text{ for all } j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q).$$

The equivalence is a consequence of Lemma 117 and is of course true only for nonempty $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, but the other case is no interest to us. We thus have a factorization $I(\mathcal{O})/\sim$ by this equivalence.

Lemma 119. The set $I(\mathcal{O})/\sim$ with operation $[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$ is a group.

Proof. The operation is well defined: If $[\mathfrak{a}'] = [\mathfrak{a}]$, $[\mathfrak{b}'] = [\mathfrak{b}]$, then $(\alpha')\mathfrak{a}' = (\alpha)\mathfrak{a}$ and $(\beta')\mathfrak{b} = (\beta)\mathfrak{b}$. This yields $(\alpha'\beta')\mathfrak{a}'\mathfrak{b}' = (\alpha')\mathfrak{a}'(\beta')\mathfrak{b}' = (\alpha)\mathfrak{a}(\beta)\mathfrak{b} = (\alpha\beta)\mathfrak{a}\mathfrak{b}$ and $[\mathfrak{a}\mathfrak{b}] = [\mathfrak{a}'\mathfrak{b}']$. The operations is associative as the multiplication of ideals is associative. The neutral element is the class $P(\mathcal{O})$ of principal ideals. It remains to find inverse element for any $[\mathfrak{a}]$. This can be proven in general but for us, it suffices to consider the case when $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is nonempty. If we can pick $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ and $\mathfrak{a}(j(E)) = j(E')$ for some $j(E')$ then the walk of $\mathfrak{a}$ with opposite direction corresponds to some $\mathfrak{b}$ for which $\mathfrak{b}(j(E')) = j(E)$. Thus $(\mathfrak{b}\mathfrak{a})(j(E)) = j(E)$ and $\mathfrak{a}\mathfrak{b}$ is principal ideal, and in particular the class $[\mathfrak{a}\mathfrak{b}]$ is the neutral element. □

Definition 120. The group $(I(\mathcal{O})/\sim, \cdot) := \mathrm{Cl}(\mathcal{O})$ is called a class group.

The size of the crater can be now simply described.

Corollary 121. Let V be a l-volcano where order $\mathcal{O}_0$ in quadratic numberfield K corresponds to the crater V_0. Let $\mathfrak{l}$ be any prime ideal containing l in $\mathcal{O}_0$. The integer $|V_0|$ is the order of $\mathfrak{l}$ in $\mathrm{Cl}(\mathcal{O})$.

The class group is an important concept in number theory. It turns out that it is always finite. The cardinality $|\operatorname{Cl}(\mathcal{O})| = h(\mathcal{O})$ is called class number. Roughly speaking, the bigger the number $h(\mathcal{O}_K)$ is, the more the ring $\mathcal{O}_K$ fails to have unique factorization property in some sense. For example, if $h(\mathcal{O}_K) = 1$, then $\mathcal{O}_K$ is a unique factorization domain. We won't be going much deeper in the theory of class groups as it's quite advanced and we will be mainly interested in its application to cryptography in the next chapter. The most important fact about $\operatorname{Cl}(\mathcal{O})$ is its action on the set $\operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q)$.

Corollary 122. The map

$$\operatorname{Cl}(\mathcal{O}) \times \operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q) \to \operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q) \quad ([\mathfrak{a}], j) \mapsto \mathfrak{a} \cdot j,$$

which we will denote $[\mathfrak{a}] \cdot j$ is a free action of group $\operatorname{Cl}(\mathcal{O})$ on $\operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, i.e. for any $j \in \operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q)$:

(i) $[\mathfrak{a}] \cdot j = j$ if and only if $[\mathfrak{a}] = P(\mathcal{O})$

(ii) $[\mathfrak{a}] \cdot ([\mathfrak{b}] \cdot j) = [\mathfrak{a}\mathfrak{b}] \cdot j$

Theorem 123 ([Sil11a])**.** For any $j, j' \in \operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ there exists $\mathfrak{a} \in \operatorname{Cl}(\mathcal{O})$ such that $\mathfrak{a} \cdot j = j'$.

The theorem tells us that the action is transitive, but we will not prove this here. If we fix a $j(E) \in \operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, then since $\operatorname{Cl}(\mathcal{O})$ acts freely and transitively, for each $j \in \operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ there exists a unique element $\mathfrak{a} \in \operatorname{Cl}(\mathcal{O})$ such that $\mathfrak{a} \cdot j(E) = j$, thus we get the following corollary

Corollary 124. The set $\operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is either empty or its cardinality is $h(\mathcal{O}) = |\operatorname{Cl}(\mathcal{O})|$. In particular, either every elliptic curve E over $\overline{\mathbb{F}}_q$ with $\operatorname{End}(E) \cong \mathcal{O}$ is defined over $\mathbb{F}_q$ or none of them are.

We will be using class group action in terms of elements which correspond to so-called Elkies primes. Elkies prime for E is a prime such that $l \nmid t^2 - 4q$ and $\left(\frac{d_K}{l}\right) = 1$, i.e. primes for which the l-volcano of E is a cycle. The reason for our focus on Elkies primes is that the degree of all but finitely many prime degree isogenies is Elkies prime. Indeed, if ϕ is an l-isogeny from E then either $l \mid t^2 - 4q$ or $\left(\frac{d_K}{l}\right) = 1$ where the first condition is satisfied by finitely many primes but the latter is satisfied by roughly half of primes by Chebotarev's density theorem [SL96]. Second reason for usage of Elkies primes is that we can simply express corresponding elements of $\operatorname{Cl}(\mathcal{O})$:

Lemma 125. Let $\phi : E_1 \to E_2$ is an l-isogeny such that l is an Elkies prime and λ, μ be eigenvalues of π on $E[l]$.

(i) $(l, \pi - \lambda)(l, \pi - \mu) = (l)$ is the prime factorization of (l).

(ii) If the eigenspace of λ is $\ker(\phi)$ then $[\mathfrak{a}_\phi] = [(l, \pi - \lambda)]$.

Proof. For (i) we refer the reader to [Con18] and for (ii) it suffices to prove $\mathfrak{a}_\phi = (l, \pi - \lambda)$. Clearly, $(l, \pi - \lambda) \subseteq \mathfrak{a}_\phi$ and since $N(\mathfrak{a}_\phi) = N((l, \pi - \lambda)) = l$ we get an equality. □

Growing volcano

In the last part of this chapter, we will examine the field of definition of l-isogenies. We know that for any elliptic curve E there are $l+1$ l-isogenies defined over some extension. We will manage to describe the possible extensions as well as the field of definition of kernels of these isogenies. This will have an application in the next chapter as one of the ways to compute an isogeny is to find its kernel. Our main idea to approach this is to examine what happens to the depth of volcanoes when we change the field of definition, i.e. make a shift from $G_l(\mathbb{F}_q)$ to $G_l(\mathbb{F}_{q^k})$. Every vertex from $\mathbb{F}_q$ can be considered as a vertex from $\mathbb{F}_{q^k}$. Every edge between $j(E)$ and $j(E')$ corresponds to a class of isogenies defined over $\mathbb{F}_q$, which can also be considered as isogenies over $\mathbb{F}_{q^k}$. Thus we can write this as inclusion of graphs

$$G_l(\mathbb{F}_q) \subseteq G_l(\mathbb{F}_{q^k}).$$

If we pick a volcano $V \subseteq G_l(\mathbb{F}_q)$, the question is, how does the connected component $V(\mathbb{F}_{q^k}) \subseteq G_l(\mathbb{F}_{q^k})$ containing V looks like. New edges in $V(\mathbb{F}_{q^k})$ can appear only for the vertices on the floor V as others have full $l+1$ edges. Thus, as we go from V to $V(\mathbb{F}_{q^k})$, we can say that V *grows.*

For elliptic curve E over $\mathbb{F}_q$ and prime l, we will define four numbers:

- k_1 is the smallest number such that $E[l] \cap E(\mathbb{F}_{q^{k_1}}) \neq \{\infty\}$.
- k_2 is the smallest number such that $E[l] \subseteq E(\mathbb{F}_{q^{k_2}})$.
- i_1 is the smallest number for which exists an l-isogeny defined over $\mathbb{F}_{q^{i_1}}$ with domain E.
- i_2 is the smallest number for which exist,up to isomorphism, $l+1$ l-isogenies defined over $\mathbb{F}_{q^{i_2}}$ with domain E.

In the case of k_1, k_2 we are looking for field of definition of l-torsion points. Recall that Frobenius morphism satisfies: $\pi^r(P) = P$ if and only if $P \in E(\mathbb{F}_{q^r})$. Hence k_1 is the smallest integer such that $\pi^{k_1}(P) = P$ for at least one affine point $P \in E[l]$ and k_2 is the smallest integer that satisfies this for every point in $E[l]$.

Concerning the case of i_2, i_1, we know that E admits an l-isogeny over $\mathbb{F}_{q^r}$ for each $\mathbb{F}_{q^r}$-stable subgroup of $E[l]$ of order l. We have described (Lemma 43 and Remark 44) the existence of such subgroups by the eigenvalues of π_l: i_1 is the smallest integer such that π^{i_1} has at least one eigenvalue and i_2 is the smallest integer such that π^{i_2} has exactly one eigenvalue with geometric multiplicity 2. Before we move to finding i_1, i_2 we should realize that the eigenvalues of π_l can be described as roots of Frobenius polynomial modulo l as tells us the next lemma.

Lemma 126. Let E be an ordinary elliptic curve over $\mathbb{F}_q$ and l a prime. Denote π_l the restriction of π to $E[l]$. The characteristic polynomial of π_l as a linear map is $x^2 - tx + q \in \mathbb{Z}/l\mathbb{Z}[x]$.

Proof. If π_l has a eigenvalue λ with $\lambda P = \pi_l(P)$ for $P \in E[l]$, then $(\pi^2 - t\pi + q)P = (\lambda^2 - t\lambda + q)P = \infty$. This means that $\lambda^2 - t\lambda + q \equiv 0 \pmod{l}$. So any eigenvalue is a root of $x^2 - tx + q$ and since it has the same dimension as $E[l]$ then it must be the characteristic polynomial of π_l. For complete proof see [Sil11b]. □

To compute the desired i_1, i_2, k_1, k_2 we will split the situation to four cases based on whether E is already a domain of, up to isomorphism, 0,1,2 or $l+1$ isogenies. The result can be best described through the Table 4.1 which we will now explain:

	0	1	2	$l+1$
k_2	$\operatorname{lcm}(\operatorname{ord}(\omega_1), \operatorname{ord}(\omega_2))$	$l \operatorname{ord}(\omega_1)$	$\operatorname{lcm}(\operatorname{ord}(\omega_1), \operatorname{ord}(\omega_2))$	$\operatorname{ord}(\omega_1)$
k_1	$\operatorname{lcm}(\operatorname{ord}(\omega_1), \operatorname{ord}(\omega_2))$	$\operatorname{ord}(\omega_1)$	$\min(\operatorname{ord}(\omega_1), \operatorname{ord}(\omega_2))$	$\operatorname{ord}(\omega_1)$
i_2	$\operatorname{ord}(\omega_1\omega_2^{-1})$	l	$\operatorname{ord}(\omega_1\omega_2^{-1})$	1
i_1	$\operatorname{ord}(\omega_1\omega_2^{-1})$	1	1	1

Table 4.1: Columns represent four cases of number of isogenies from E and ω_1, ω_2 are roots of Frobenius chararacteristic polynomial over $\mathbb{F}_{l^2}$.

(i) Suppose E is a domain of $l+1$ l-isogenies, i.e π_l has one eigenvalue λ with geometric multiplicity 2. This means $\pi(P) = \lambda P$ for every $P \in E[l]$. Hence $k_1 = k_2$ is the smallest integer such that $\lambda^{k_1} \equiv 1 \pmod{l}$, which is the order $\operatorname{ord}(\lambda)$ of λ in $\mathbb{Z}/l\mathbb{Z}$. Trivially $i_1 = i_2 = 1$.

(ii) Suppose E is a domain of 2 l-isogenies, i.e π_l admits 2 distinct eigenvalues λ, μ. Trivially $i_1 = 1$. Both eigenvalues λ, μ have eigenspaces of dimension 1, generated by $P_\lambda, P_\mu \in E[l]$, which also form basis of $E[l]$. For any r and $a, b \in \mathbb{Z}/l\mathbb{Z}$: $\pi^r(aP_\lambda + bP_\mu) = a\lambda^r P_\lambda + b\mu^r P_\mu$. Hence

$$k_2 = \operatorname{lcm}(\operatorname{ord}(\lambda), \operatorname{ord}(\mu)) \text{ and } \quad k_1 = \min(\operatorname{ord}(\lambda), \operatorname{ord}(\mu)),$$

where if $k_1 = \operatorname{ord}(\lambda)$ then the l-point corresponding to k_1 is P_λ and vice versa. Furthermore, i_2 is the smallest integer such that there exists $\nu \in \mathbb{Z}/l\mathbb{Z}$ for which $\pi^{i_2}(P) = \nu P$ for all $P \in E[l]$. This means that $\lambda^{i_2} = \mu^{i_2} = \nu$ and $i_2 = \operatorname{ord}(\lambda\mu^{-1})$.

(iii) Suppose E is a domain of 1 l-isogeny, i.e π_l admits one eigenvalue λ with geometric multiplicity 1. This means that $\pi(P) = \lambda P$, $\pi(Q) = P + \lambda Q$ for some basis P, Q of $E[l]$. Since for each r: $\pi^r(Q) = r\lambda^r P + \lambda^r Q$, then $\pi^r(Q) = Q$ if and only if $l \mid r$ and $r \mid \operatorname{ord}(\lambda)$. Hence, $k_2 = l \operatorname{ord}(\lambda)$. If $\pi^{k_1}(aP + bQ) = aP + bQ$, then $\pi^{k_1}(aP + bQ) = (a + k_1)\lambda^{k_1} P + \lambda^{k_1} bQ$. Either $l \mid k_1$ or $a = 0$ and $k_1 = \operatorname{ord}(\lambda)$, but $l > \operatorname{ord}(\lambda)$ so $k_1 = \operatorname{ord}(\lambda)$. Finally, if $\pi^{i_2} P = \nu P$, $\pi^{i_2} Q = \nu Q$ for some $\nu \in \mathbb{Z}/l\mathbb{Z}$, then $\lambda^{i_2} = \nu$, $l \mid i_2$, which yields $i_2 = l$ and trivially $i_1 = 1$.

(iv) Finally, we assume that E is a domain of no l-isogenies, i.e that π has no eigenvalues on $E[l]$. Any l-isogeny from E defined over $\mathbb{F}_{q^{i_1}}$ will be descending from Lemma 103. Thus, $j(E)$ will lie on top of the crater of l-volcano, having $l+1$ edges and $i_1 = i_2$. Consider matrix A of π_l in any basis. Although A doesn't have any eigenvalues we can consider A over $\mathbb{F}_{l^2}$ where it has two eigenvalues as its characteristic equation is a quadratic polynomial in $\mathbb{F}_l$ which must split in $\mathbb{F}_{l^2}$. Thus A can be expressed as $P^{-1}JP = A$ where J, P are matrices over $\mathbb{F}_{l^2}$ and $J = \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix}$ is in Jordan normal form. Also $A^{i_2} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ for appropriate $\lambda \in \mathbb{Z}/l\mathbb{Z}$. This means that $J^{i_2} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ and $\omega_1^{i_2} = \omega_2^{i_2} = \lambda$. If for any r $\omega_1^r = \omega_2^r$, then $\omega_1^r \in \mathbb{F}_l$. So $i_2 = \mathrm{ord}(\omega_1\omega_2^{-1})$. Finally, $k_1 = k_2 = \mathrm{lcm}(\mathrm{ord}(\omega_2), \mathrm{ord}(\omega_1))$.

Example 127. Consider the curve $E : y^2 = x^3 + 16x + 6$ over $\mathbb{F}_{23}$. Using any point counting algorithm to find $|E(\mathbb{F}_{23})|$ we conclude that $T(\pi) = -4$ and the characteristic polynomial is $x^2 + 4x + 23$. Assuming $l = 5$:

$$x^2 + 4x + 23 = (x-2)(x-4) \pmod 5.$$

Since $\mathrm{ord}(2) = 4$ and $\mathrm{ord}(4) = 2$ we get that $k_2 = 4$ and $k_1 = 2$. This means we can find five 5-torsion points in $E(\mathbb{F}_{23})$ and the whole $E[5]$ in $E(\mathbb{F}_{23^4})$

Moreover, there are two 5-isogenies from E and the third column of Table 4.1 is relevant to us. Clearly $i_1 = 1$ and $i_2 = \mathrm{ord}(2 \cdot 4^{-1}) = \mathrm{ord}(3) = 4$. Indeed, we can see in the Figure 127 that the 5-volcano of E grows as we go to $\mathbb{F}_{23^4}$.

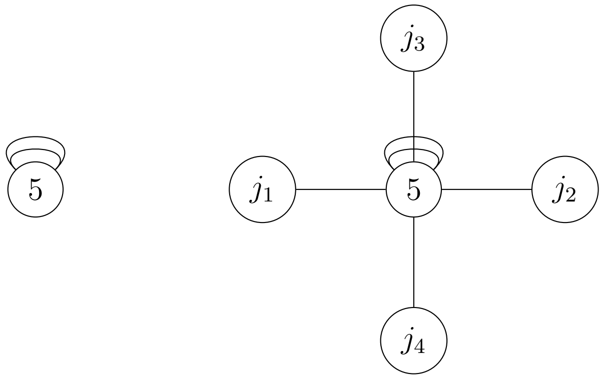


Figure 4.3: 5-volcano of $j(E) = 5$ in $\mathbb{F}_{23}$ and $\mathbb{F}_{23^4} = \mathbb{F}_{23}[z]/(z^4 + 3z^2 + 19z + 5)$ where $j_1 = 12z^2 + 16z$, $j_2 = 5z^3 + 11z^2 + 4z + 18$, $j_3 = 7z^3 + 13z^2 + 20z + 15$, $j_4 = 11z^3 + 10z^2 + 6z + 10$

Corollary 128. Let E_1, E_2 be elliptic curves over $\mathbb{F}_q$ and $\phi : E_1 \to E_2$ an l-isogeny over $\mathbb{F}_{q^n}$. If r is the smallest integer such that $\ker(\phi) \subseteq E(\mathbb{F}_{q^r})$ then $r \mid l^2 - 1$. Moreover, if ϕ is defined over $\mathbb{F}_q$ then $r \mid l - 1$.

Chapter 5

Isogenies in cryptography

We have so far focused on the theoretical background of isogenies. The purpose of this chapter is to use our gained knowledge and show applications of isogenies and isogeny volcanoes for practical problems in cryptography. Firstly, we will go through algorithms for computing isogenies.

Remark 129. For measuring the complexity of algorithms, we will be using the big-O notation. We will always be working over some fixed finite field, or a ring (polynomial ring) whose operations (addition, subtraction, multiplication) are by no means constant. It would be cumbersome to be constantly dealing with the complexity of those operations. We will therefore use the *algebraic complexity*: If we say that the complexity of an algorithm A is $O(f(n))$ we mean that the number of ring (field) operations in A is $O(f(n))$. The multiplication of polynomials will be often needed whose complexity will be denoted $M(n)$[1]. Sometimes we will also use the soft-O notation $\tilde{O}(f(n))$ which is just a shorthand for $O(f(n)(\log^k(f(n)))$ for some k. See [PCS11] for introduction to algebraic complexity.

Any isogeny is determined by its domain, codomain and rational maps. By Theorem 26, we can also represent any isogeny by its kernel uniquely, up to isomorphism. However, the theorem is purely existential and doesn't tell us how can we find such separable isogeny (rational maps and codomain) if we are given the kernel. The answer bring the famous Vélu formulas due to Jacques Vélu. For simplicity, we will state them for odd order isogenies. Full theorem can be found in [Was08].

Theorem 130. Let $E_1 : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_q$ and G a finite subgroup of $E_1(\overline{\mathbb{F}}_q)$ of odd order. Denote $P = (x_P, y_P)$ for each $P \in G$. There exists a separable isogeny $\alpha : E_1 \to E_2$ defined over $\overline{\mathbb{F}}_q$ satisfying $\ker(\alpha) = G$ and

- E_2 is given by $y^2 = x^3 + (a - 5v)x + b - 7w$ where $v = \sum_{P \in G \setminus \{\infty\}} 3x_P^2 + a$ and $w = \sum_{P \in G \setminus \{\infty\}} 2y_P^2 + 3x_P^3 + ax_P$.
- $\alpha(x, y) = (\alpha_1(x), \alpha_2(x)y)$ is given by

$$\alpha_1(x) = x + \sum_{P \in G \setminus \{\infty\}} \left(\frac{3x_P^2 + a}{x - x_P} + \frac{2y_P^2}{(x - x_P)^2} \right),$$

[1] It can be shown $M(n) \in O(n \log(n) \log(\log(n)))$ [GJ13]

$$\alpha_2(x) = 1 - \sum_{P \in G \setminus \{\infty\}} \left(\frac{3x_P^2 + a}{(x - x_P)^2} + \frac{4y_P^2}{(x - x_P)^3} \right).$$

Lemma 131 ([Shu09])**.** Let $\phi : E \to E'$ be an isogeny of degree l defined over $\mathbb{F}_q$. Let d be the smallest integer satisfying $\ker(\phi) \subseteq E(\mathbb{F}_{q^d})$. The time complexity of computing Vélu formulas is $O(lM(d))$.

As we know from Corollary 128, the degree d is in $O(l)$. The time complexity of computing Vélu formulas is therefore $O(lM(l))$. This algorithm assumes that we represent the kernel as a set of points in some extension but we can also represent it using the kernel polynomial:

Definition 132 (Kernel polynomial)**.** Kernel polynomial of isogeny $\phi : E_1 \to E_2$ over $\mathbb{F}_q$ is defined as[2]

$$f(x) = \prod_{P \in \ker(\phi) \setminus \{\infty\}} (x - x_P) \in \overline{\mathbb{F}}_q[x]$$

This doesn't seem simpler as we need at least $\deg f = |\ker(\phi)| - 1$ coefficients in $\overline{\mathbb{F}}_q$. But as it turns out, it can be easily seen that $f \in \mathbb{F}_q[x]$. The fact that $f \in \mathbb{F}_q[x]$ is equivalent to $(f(x))^q = f(x)$. Every monic polynomial is uniquely determined by its roots. If we therefore prove that the map $x \mapsto x^q$ only permutes the roots, then we are done. However, this follows from the fact that Frobenius endomorphism π satisfies $\pi(\ker(\phi)) = \ker(\phi)$ by Lemma 24.

Lemma 133. The kernel polynomial of any separable isogeny of degree n defined over $\mathbb{F}_q$ lies in $\mathbb{F}_q[x]$ and has degree $n - 1$.

David Kohel in his thesis [Koh96] found a way to compute the rational maps and codomain directly from the kernel polynomial, thus completely avoiding any extension field.

Lemma 134 ([MS11])**.** Let $\phi : E_1 \to E_2$ be an isogeny over $\mathbb{F}_q$ with kernel polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then

$$\phi(x, y) = \left(\frac{g(x)}{f(x)}, \left(\frac{g(x)}{f(x)} \right)' \right),$$

$$g(x) = f(x)(lx - a_{n-1}) - (3x^2 + a)f'(x) - 2(x^3 + ax + b)\left(f''(x) + \frac{(f'(x))^2}{f(x)} \right).$$

Lemma 135 ([Shu09])**.** If $\phi : E_1 \to E_2$ is an isogeny of degree n defined over $\mathbb{F}_q$, then the Kohel's formulas can be computed in $O(M(n)) = \tilde{O}(n)$.

[2] Some authors define the kernel polynomial of n-isogeny for n odd as the square root of f. This is well defined as each factor $(x - x_P)$ appears in the factorization of f twice for (x_P, y_P) and $(x_P, -y_P)$

So it seems that Kohel's algorithm is nearly optimal considering the size of kernel is n. Nonetheless, these formulas are only part of the story of computing isogenies. What if we are in a situation without any representation of kernel. For example, the following problem, which is relevant to us.

Problem 1. Given elliptic curve E over $\mathbb{F}_q$ and prime l find all j-invariants which are neighbours to $j(E)$ in $G_l(\mathbb{F}_q)$.

There are basically two main methods to approach this. First one utilizes the algorithms by Vélu or Kohel. In order to use them, we have to find the kernel. Recall that for any l-isogeny $\ker(\phi)$ is a subgroup of $E[l]$ and similarly the kernel polynomial f_ϕ of ϕ divides the kernel polynomial[3] f_l of $[l]$. If the rational maps for $[l]$ are $[l](x, y) = \left(\frac{u(x)}{v(x)}, \frac{u(x)}{v(x)}y\right)$ (these can be computed using addition formulas on E), then f_l must divide v^2 in $\mathbb{F}_q[x]$. We are therefore looking for polynomials of degree $l-1$ which divide v^2. Hence we factorize v over $\mathbb{F}_q$ and use Kohel's formulas for any factors whose product is a degree l polynomial. The complexity of this algorithm is dominated by factorization of v, which can be done in $\tilde{O}(l^3)$ using the Cantor-Zassenhaus algorithm [CZ81].

The second method relies on the fact that we actually don't need to compute any rational maps. We just need the j-invariants. Recall that for each prime l there exists a modular polynomial Φ_l satisfying for any $j(E_1), j(E_2) \in \mathbb{F}_q$:

$$\Phi_l(j(E_1), j(E_2)) = 0 \iff E_1 \text{ and } E_2 \text{ are } l\text{-isogenous.}$$

Thus the solution to Problem 1 reduces to factorization of $\Phi_l(j(E_1), x) \in \mathbb{F}_q[x]$ which has degree $l+1$. The modular polynomials seem to be a good solution for constructing volcanoes. Nonetheless, there are several issues the reader should be aware of:

- The complexity of the best algorithms for constructing $\Phi_l(X, Y)$ is $O(l^3(\log l)^4)$. The leader between them is due to Sutherland [BLS10] which utilizes isogeny volcanoes.
- Size of $\Phi_l(X, Y)$ is in $O(l^3 \log l)$.

Because of the time to generate modular polynomial, it is only slightly better than the first method where we have to find and factorize l-th division polynomial. However, in practice the modular polynomials are precomputed and stored in databases [Sut18] as they don't depend on the elliptic curve we are using. Other polynomials with similar properties can be used [KZ98].

Example 136. The modular polynomial Φ_2 is

$$-X^2Y^2 + X^3 + 1488X^2Y + 1488XY^22 + Y^3 - 162000X^2 + 40773375XY -$$

$$162000Y^2 + 8748000000X + 8748000000Y - 157464000000000$$

[3] The kernel polynomial of $[l]$ is often called l-th division polynomial

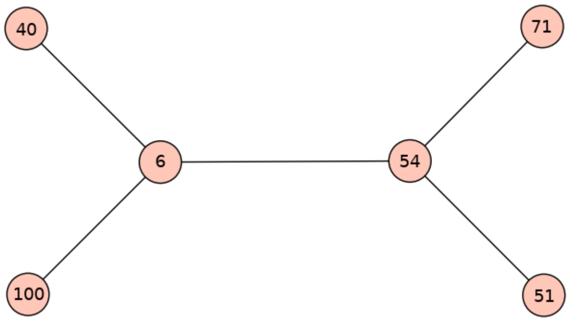


Figure 5.1: 2-volcano of $E : y^2 = x^3 + 3x + 86$ over $\mathbb{F}_{101}$

If we consider a curve $E : y^2 = x^3 + 3x + 86$ over $\mathbb{F}_{101}$ with $j(E) = 54$ then its neighbors in $G_2(\mathbb{F}_{101})$ are the roots of

$$\Phi_2(x, 54) = x^3 + 74x^2 + 10x + 90 = (x + 30)(x + 50)(x + 95).$$

Modular or division polynomial allow us to compute neighbors of any vertex in $G_l(\mathbb{F}_q)$. Using any graph searching algorithm we can thus explore any volcano. We will see that through this 'isogeny climbing' we are able to gain knowledge about given elliptic curve including: endomorphism ring, identifying supersingularity or trace of Frobenius endomorphism.

Computing endomorphism ring

The knowledge of the endomorphism ring of ordinary elliptic curve E gives us the depth of E in its l-volcano V_l for every prime number l: If c is the conductor of $\mathrm{End}(E)$ in $\mathcal{O}_K$, then the depth of E in V_l is $\nu_l(c)$ (Theorem 113). However, we can turn this around. If we are somehow able to compute depth of E in each of its l-volcano V_l, then we know $\nu_l(c)$ for every prime l and consequently c and $\mathrm{End}(E)$ as any order is uniquely determined by its conductor. Since $c \mid v$, where $v^2 = \frac{t^2-4q}{d_k}$, it suffices to find $\nu_l(c)$ for every $l \mid v$.

How do we compute the depth of $j(E)$ in V_l? The depth of $j(E)$ is the distance from the crater but we have no way to recognize the crater while searching through the volcano. We will rather search for the vertices on the floor which are precisely the vertices with only one neighbor. The algorithm FindFloor will go as follows. If $j(E)$ has only one neighbor, $j(E)$ is on the floor and the algorithm terminates. Otherwise $j(E)$ has $l + 1$ neighbors. We pick any 3 of them and repeat the previous step for each one of them. Since there are at most two non-descending isogenies from each vertex, one of the 3 neighbors must be closer to the floor than $j(E)$. Repeating this process must terminate after s steps where s is the distance of $j(E)$ from the floor. Since the depth of the volcano is $\nu_l(v)$:

$$\nu_l(c) = \nu_l(v) - s$$

```
Algorithm 1: FindFloor($E, \Phi_l$)
    Result: Find the distance from $j(E)$ to the floor of its $l$-volcano
    distance $\leftarrow$ 0
    Find 3 roots $j_1, j_2, j_3$ of $\Phi(j(E), x)$. Otherwise return 0.
    while True do
        for $i = 1, 2, 3$ do
            Find root $j_i'$ of $\Phi(j_i, x)/(x - j_i)$. Otherwise return distance.
        end
        distance+=1
        $j_i \leftarrow j_i'$
    end
    Return distance
```

Example 137. Let $E : y^2 = x^3 + 103x + 667$ be an elliptic curve over $\mathbb{F}_{907}$ with $j(E) = 659$ and trace $t = 8$. Then $t^2 - 4q = 8^2 - 4 \cdot 907 = -3564 = -2^2 \cdot 3^4 \cdot 11$. Since $-11 \equiv 1 \pmod 4$ then $d_K = -11$ and $v = 2 \cdot 3^2$. We therefore have to find depth of $j(E)$ in its 2-volcano V_2 and 3-volcano V_3 whose depths are 1 and 2 respectively.

The polynomial $\Phi_2(x, j(E)) = x^3 + 650x^2 + 690x + 178 \in \mathbb{F}_{907}[x]$ has three roots $574, 548, 42 \in \mathbb{F}_{907}$, so $j(E)$ is not on the floor. However, $\Phi_2(x, 574)$ has only one root 659. Thus $j(E)$ has depth 0 in V_2.

For V_3, we find that $\Phi_3(x, j(E)) = x^4 + 418x^3 + 457x^2 + 47x + 177$ has only one root. Hence, E is on the floor and its depth is 2. The desired conductor is then $c = 2^0 \cdot 3^2 = 9$. Since $\mathcal{O}_K = \mathbb{Z}[\tau_K]$ where $\tau_K = \frac{d_K + \sqrt{d_K}}{2} = \frac{-11 + \sqrt{11}i}{2}$, we conclude that $\text{End}(E) \cong \mathbb{Z}\left[\frac{-99 + 9\sqrt{11}i}{2}\right]$.

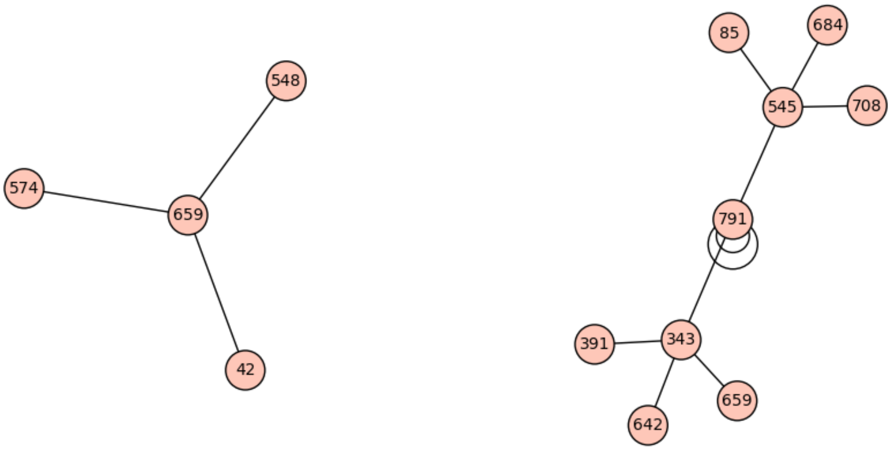


Figure 5.2: 3-volcano V_3 and 2-volcano V_2 of $E : y^2 = x^3 + 103x + 667$ over $\mathbb{F}_{907}$

The trace t of Frobenius endomorphism can be computed in polynomial time using SEA-algorithm. Afterwards, we have to factorize v which can be done using number field sieve in subexponential time. The rest depends on complexity of FindFloor. In FindFloor for each prime l, we have to in each step factorize a polynomial of degree $l + 1$, which can be done in $O(l^3)$. Overall complexity may be exponential in $\log q$. We must keep in mind that we are always limited by the modular polynomials. If one of the primes l dividing v is large, computing the modular polynomial becomes infeasible. Other algorithms have been therefore found using more sophisticated methods. One of them, described in [BGSV09], uses horizontal walks. We will show the main idea on an example provided by the authors.

Example 138. Let $E : y^2 = x^3 - 3x + b$ over $\mathbb{F}_q$ where

$$q = 5027255188393102140809144871023564674 9/$$

$$9046609804985766800866998654318435688 47$$

$$b = 1426295789578376474298752473282119957 0/$$

$$8602432930077355375750270514536634943 06$$

Using the SEA algorithm we can compute $t = 1200$, $d_K = -7$ and $v = 2{\cdot}127{\cdot}p_1 p_2 p_3 p_4$ where $p_1 = 582509$, $p_2 = 582511$, $p_3 = 852857$ and $p_4 = 2305843009213693951$. We can deal with 2 and 127 using isogeny exploration as before but it would be hopeless trying to generate modular polynomial for p_4. The authors, Bisson and Sutherland, found another way to determine whether $p_i \mid c$ for each $i = 1, 2, 3, 4$ where c is conductor of $\mathcal{O} \cong \mathrm{End}(E)$. We will show the main idea on p_1.

Let $\mathcal{O}_1$,$\mathcal{O}_2$ be orders in $\mathcal{O}_K$ with conductors $\frac{v}{p_1}, p_1$ respectively. The conductors haven been chosen in such a way that

$$\text{if } p_1 \mid c \text{ then } \mathcal{O} \subseteq \mathcal{O}_2, \text{ otherwise } \mathcal{O}_1 \subseteq \mathcal{O}.$$

First important part of the algorithm is to find a *relation*. Relation R will mean a sequence of integers $e_1, \dots, e_k$ and a sequence of Elkies prime numbers $l_1, \dots, l_k$ for E. If we assign to each prime l_i an ideal class $\mathfrak{l}_i \in \mathrm{Cl}(\mathcal{O})$ containing prime ideal of norm l_i (we have two options for each such choice of ideal class), then the relation corresponds to a horizontal walk $(\mathfrak{l}_1^{e_1}, \dots, \mathfrak{l}_k^{e_k})$ from $j(E)$.

To every such relation R and an order $\mathcal{O}$ we will assign a number

$$R_{\mathcal{O}} = |\{\tau \in \{-1, 1\}^{\{1,\dots,k\}} \mid \mathfrak{l}_1^{\tau(1)e_1} \dots \mathfrak{l}_k^{\tau(k)e_k} = 1\}|.$$

Notice, that the number doesn't depend on our choice of ideal classes. Similarly, we denote $R_{\mathcal{O}_1}$ and $R_{\mathcal{O}_2}$. The motivation behind $R_{\mathcal{O}}$ is the following: If R is a relation satisfying $R_{\mathcal{O}_1} > R_{\mathcal{O}_2}$, then

$$p_1 \mid c \iff R_{\mathcal{O}} < R_{\mathcal{O}_1}. \tag{5.1}$$

Hence if we find such relation R then we are finished. It remains to justify the claim (5.1) and explain how can we find the relation R.

By Lemma 108 there is a map $I(\mathcal{O}) \to I(\mathcal{O}_K)$ which maps each ideal $\mathfrak{a}$ (prime to c) to $\mathfrak{a}\mathcal{O}_K$. If $\mathfrak{a}$ is principal then so is $\mathfrak{a}\mathcal{O}_K$. This induces a homomorphism of groups $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K)$ (considering part (iii) of Lemma 108). One can generalize this to any inclusion of orders $\mathcal{O} \subseteq \mathcal{O}'$. It follows that $R_{\mathcal{O}} \le R_{\mathcal{O}'}$ and in particular

$$\mathcal{O} \subseteq \mathcal{O}_2 \Rightarrow R_{\mathcal{O}} \le R_{\mathcal{O}_2} \text{ and } \mathcal{O}_1 \subseteq \mathcal{O} \Rightarrow R_{\mathcal{O}_1} \le R_{\mathcal{O}}$$

We can now prove (5.1). Assume $R_{\mathcal{O}_1} > R_{\mathcal{O}_2}$ for some relation R. If $p_1 \mid c$ then $\mathcal{O} \subseteq \mathcal{O}_2$ and consequently $R_{\mathcal{O}} \leq R_{\mathcal{O}_2} < R_{\mathcal{O}_1}$. On the other hand if $p_1 \nmid c$ then $\mathcal{O}_1 \subseteq \mathcal{O}$ and $R_{\mathcal{O}_1} \leq R_{\mathcal{O}}$.

All class group actions are performed using binary quadratic forms, but we will not explain this any further here. The search for R such that $R_{\mathcal{O}_1} < R_{\mathcal{O}_2}$ is done by searching through $\mathrm{Cl}(\mathcal{O}_1)$ and testing the inequality. But how can we compute $R_{\mathcal{O}}$ when we don't even know how $\mathcal{O}$ looks like, that is our goal after all. This is the second most important part of the algorithm: We actually perform the relations as walks, as we have abstractly pictured them. The integer $R_{\mathcal{O}}$ can be thought of as the number of walks from $j(E)$ back to $j(E)$ where for each step we make a choice for one of two edges. If we therefore try all of these, we will find $R_{\mathcal{O}}$.

In our case, there is a relation[4]

$$(2^{2533}, 11^{752}, 29^2, 37^{47}, 79, 113, 149, 151, 347, 431)$$

for which $R_{\mathcal{O}_1} = 2$ and $R_{\mathcal{O}_2} = 0$. To find $R_{\mathcal{O}}$, we need to compute modular polynomials of these primes, which is considerable improvement from computing Φ_{p_1}. One can find out that $R_{\mathcal{O}} = 0$ which implies $p_1 \mid c$.

Identifying ordinary curves

This thesis is based on particular structure, volcano, which is composed of ordinary curves. We have seen that supersingular curves behave in different manner in terms of isogeny graphs. The idea may arise: Is it possible to design an algorithm, based on this knowledge, to determine whether given curve is supersingular? At first, we will go through a few algorithms for determining supersingularity used in practice:

The most direct approach is to use efficient point-counting algorithm to determine t and verify that $p \mid t$. The Schoof's algorithm can find t in $O(\log^8 q)$.

Faster but non-deterministic algorithm is used for elliptic curves over $\mathbb{F}_p$. The idea is: If E is supersingular then $(p+1)P = \infty$ for all $P \in E(\mathbb{F}_p)$. On the other hand, if E is ordinary then at most $\frac{8\sqrt{p}}{(\sqrt{p}-1)^2}$ points satisfy this. Hence, by picking random points in E we should recognize whether E is supersingular. One can generalize this for curves over $\mathbb{F}_{p^2}$. For further info see [Sut11]. Expected running time of this algorithm is $\tilde{\mathcal{O}}(\log^2 p)$. The algebra system Sage uses combination of this algorithm and point counting algorithm already discussed.

Third algorithm, we should explain, uses the properties of isogeny graphs with modular polynomials. The fact that l-isogeny graph of supersingular curve E over $\mathbb{F}_{p^2}$ is $l+1$-regular means that $\Phi_l(x, j(E))$ splits completely in $\mathbb{F}_{p^2}[x]$ and this holds for every prime $l \neq p$. The polynomial $\Phi_l(x, j(E))$ can also split for ordinary E but only for finitely many primes l as each such splitting corresponds to divisor of $t^2 - 4p^2$. If we therefore find enough primes, for which the modular polynomial splits then E is supersingular. We can be more precise in how many primes is enough: If $l_1, \ldots, l_k$ are primes for which $\Phi_{l_i}(x, j(E))$ splits completely and $l_1 l_2 l_3 \ldots l_k > 2p$

[4] Reader may notice that 2 is in the relation even though it's not an Elkies prime. One can take exception for 2 as is explained in the paper.

then $l_1 l_2 l_3 \dots l_k > 2p \geq |t|$ and $l_1^2 l_2^2 l_3^2 \dots l_k^2 > t^2 > t^2 - 4p^2$. If E were to be ordinary then each l_i^2 divides $t^2 - 4p^2$ and therefore also their product divides $t^2 - 4p^2$ which is contradiction and E must be supersingular. If we have precomputed modular polynomials, then the complexity of this algorithm is in $\widetilde{O}(\log^4 q)$.

Sutherland came up with usage of isogeny volcanoes in [Sut11] for determining supersingularity. The idea is again to search for the floor, i.e. vertex with one neighbor. If we are on a volcano, we are bound to find it using FindFloor. On the other hand if we have a supersingular curve, then its component in $G_l(\mathbb{F}_{p^2})$ must be regular graph of order $l + 1$ and therefore doesn't contain any vertex of degree 1. The algorithm FindFloor, as it stands, would never terminate on supersingular component being stuck in infinite loop. On the other hand, the number of iterations for ordinary E is bounded by the depth d of the volcano. Since $l^{2d} \mid t^2 - 4q$, then $2d < \log_l(|t^2 - 4q|) < \log_l(4p^2) = 2\log_l(2p)$. Hence, if the algorithm doesn't stop in less then $\log_l(2p)$ iterations then the input is supersingular curve. It would seem that we are again limited by modular polynomials, but there is no reason to choose any other l than 2. Thus, the algorithm needs only Φ_2. Concerning the complexity, the hardest part is computing roots of cubic polynomials. The total expected time is $O(\log^3 q \log^2(\log q))$, which makes it the leading algorithm for proving that given elliptic curve is supersingular.

```
Algorithm 2: IsSupersingular($E$)
  Result: True if $E$ is supersingular and false otherwise.
  if $j(E) \notin \mathbb{F}_{p^2}$ then return False
  Find three roots $j_1, j_2, j_3$ of $\Phi_2(j(E), X)$. Otherwise return False
  $j'_1 \leftarrow j(E)$, $j'_2 \leftarrow j(E)$, $j'_3 \leftarrow j(E)$
  for $k \leftarrow 1$, to $\lfloor \log_2 p \rfloor + 1$ do
      for $i \leftarrow 1,2,3$ do
          $f_i(X) \leftarrow \Phi_2(j_i, X)/(X - j'_i)$
          $j'_i \leftarrow j_i$
          if $f_i(X)$ does not have root in $\mathbb{F}_{p^2}$ then return False
          $j_i \leftarrow$ root of $f_i(X)$
  return True
```

Key exchange

The goal of key exchange is for two parties, communicating over a public channel, to agree on a common secret. One of the simplest protocols is Diffie-Hellman key exchange. We will briefly summarize it in the context of ECDH and show an equivalent protocol based on isogenies and class group.

Two parties, Alice and Bob, agree on public parameters: elliptic curve E over field $\mathbb{F}_q$ and point $G \in E(\mathbb{F}_q)$ of order n. Alice and Bob then pick a secret integer a and b respectively. They compute points $A = aG$ and $B = bG$ and exchange them. Finally, each of them multiplies recieved point by their secret integer, thus getting a shared secret $bA = aB = abG$. Security of Diffie-Helmann protocol is based upon the discrete logarithm problem: Given points $G \in E$, $A \in \langle G \rangle$, it is hard to find integer a such that $aG = A$.

The hardness of the DL problem as well as relatively easy scalar multiplication aG has been the reason for usage of the discrete logarithm problem in cryptographic protocols. However, in the context of quantum computation, new attacks on this problem has appeared. The most popular, Schor's algorithm, invented in 1994 [Sho94], has shown that DLP can indeed be efficiently solved on quantum computers as well as integer factorization. There is therefore a need for new hard problems, resistant to quantum computers. Promising results brings the isogeny based cryptography with the following problem.

Problem 2. Given two isogenous curves E_1 and E_2, find an isogeny $\phi : E_1 \to E_2$.

We have seen that finding isogeny in any context is exponentially hard in the degree. Hence, for large degrees the Problem 2 is computationally hard to solve. The idea might be to use ϕ as a secret key with E_1, E_2 as public keys. However, computing any isogeny of large degree is hard even without any conditions given by public keys. Thus this problem misses the desired assymetry of easy computation and hard attack: Remember, in the DLP it is easy to compute $A = aG$ and hard to find a. A more practical problem is therefore used using isogenies of smooth degree. We say that any isogeny has smooth degree, if the degree is divisible only by small primes, i.e. bounded by some fixed constant.

Problem 3. Given two isogenous elliptic curves E_1 and E_2, find an isogeny of smooth degree $\phi : E_1 \to E_2$.

Assuming that this is a hard problem, how can we implement this into any Diffie-Hellman type protocol. The classical Diffe-Hellman is based on a map $\mathbb{Z} \times G \to G$ defined as $(a, G) \mapsto aG$. If we fix the generator G then the inverse of the map $a \mapsto aG$ must be hard to compute.

If we had some sort of group of isogenies H, then the isogeny equivalent would be a map $\phi \mapsto \phi(E)$ for some fixed elliptic curve E and isogeny $\phi \in H$. Finding the inverse to this map is the Problem 3. We don't have at our hand any such group H but we have the class group, where each element corresponds to a horizontal isogeny. Morever, we have the action $\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) \to \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$. The action is free and transitive so any fixed elliptic curve can be thought of as a generator of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ as in the Diffie-Hellman protocol. We can now try to formulate the protocol, mimicking the original DH:

- Public parameters are an elliptic curve E with endomorphism ring $\mathcal{O}$, a vector $k = ([\mathfrak{l}_1], \dots, [\mathfrak{l}_n])$ of generators of $\mathrm{Cl}(\mathcal{O})$ such that each ideal $\mathfrak{l}_i$ has small norm (bounded by some constant).
- Alice and Bob pick secret vectors $a = (a_1, \dots, a_n)$, $b = (b_1, \dots, b_n)$ of integers corresponding to ideals $A = \prod_{i=1}^{n} \mathfrak{l}_i^{a_i}$ and $B = \prod_{i=1}^{n} \mathfrak{l}_i^{b_i}$.
- Each of them computes $j(E_a) = [A] \cdot j(E)$ and $j(E_b) = [B] \cdot j(E)$ and exchange the results.

- Alice computes $[A] \cdot j(E_b)$ and Bob $[B] \cdot j(E_a)$, obtaining the secret key $[A] \cdot j(E_b) = [A] \cdot ([B] \cdot (j(E))) = [AB] \cdot j(E) = [B] \cdot j(E_a)$.

The ideal action is computed through isogenies. Recall that for every $j(E)$ every element $[\mathfrak{a}]$ of $\mathrm{Cl}(\mathcal{O})$ corresponds to a walk from $j(E)$ to $[\mathfrak{a}] \cdot j(E)$. So the secret keys are in fact walks on the graph of horizontal isogenies. As it usually is in cryptographic protocols, we need the set of possible keys to be large and random in order to prevent any brute force attacks. We therefore use Elkies primes (Corollary 125). By design, we have picked ideals with smooth degree which means that every step of the walk is determined by small degree isogeny. Any such l-isogeny $\phi : E \to E'$ has kernel $E[(l, \pi - \lambda)]$ for appropriate λ. There are two main methods to compute one step $[(l, \pi - \lambda)] \cdot j(E)$, both in the spirit of the discussed methods of exploring volcanoes.

The second method, called Elkies, utilizes modular polynomials. For Elkies prime l_i, the polynomial $\Phi_{l_i}(j(E), x) \in \mathbb{F}_q[x]$ has two roots j_1, j_2 which are neighbors of $j(E)$ in the l_i-volcano (cycle). However, we have no way to distinguish the j-invariants by the scalar λ. So we compute isogeny $\phi : E \to E_1$, for which $j(E_1) = j_1$, by method of Elkies [Sch95]. Then we find a nontrivial element $P \in \ker(\phi)$. This can be done by finding roots of kernel polynomial of ϕ. We verify that $\pi(P) = \lambda P$. If it's not the case, we have chosen the wrong direction and $[(l_i, \pi - \lambda)]j(E) = j_2$. Otherwise $[(l_i, \pi - \lambda)]j(E) = j_1$. This seems costly, especially determining the correct direction. However, we only have to do this for the first step of $\mathfrak{l}_i^n$.

Here we provide the algorithms FirstStep and NextStep from [FKS18].

```
Algorithm 3: ElkiesFirstStep
  Input: $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, prime $l$, scalar $\lambda$
  Output: $[(l, \pi - \lambda)] \cdot j(E)$
  $j_1, j_2 \leftarrow$ roots of $\Phi_l(X, j(E))$ in $\mathbb{F}_q$
  $I \leftarrow \mathrm{Isogeny}(j(E), j_1, l)$
  $x \leftarrow$ root of KernelPolynomial($I$) in $\overline{\mathbb{F}}_q$
  $Q \leftarrow (x, y) \in E$
  if $\pi(P) = \lambda \cdot P$ then return $j_1$ else return $j_2$
```

```
Algorithm 4: ElkiesNextStep
  Input: $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, prime $l$, scalar $\lambda$, $j$
  Output: $[(l, \pi - \lambda)] \cdot j(E)$
  return root of $\Phi_l(X, j(E))/(X - j)$ in $\mathbb{F}_q$
```

The second method utilizes the other approach of computing isogenies, that is by Velu/Kohel formulae, hence called VeluWalk as presented in [FKS18]. VeluWalk will not have a problem with determining direction of first step, so it is a series of VeluSteps, which we will describe. Computation of isogenies by Velu or Kohel needs the kernel in some form. We have already discussed that finding the kernel polynomial by factoring kernel polynomial of $[l]$ is not faster, however, in the case of Elkies primes it is possible to speed it up in some cases.

The main idea of VeluStep is to simply find any generating point P of kernel of l_i-isogeny assuming that $P \in E(\mathbb{F}_{q^r})$ where r is small enough. Recall that r is the multiplicative order of λ (Table 4.1). Finding P is done by randomly choosing points from $E(\mathbb{F}_{q^r})$ and multiplying them by N/l where $N = |E(\mathbb{F}_{q^r})|$. There is a problem that using this algorithm we can always go in the direction of the eigenvalue λ but not the other. If s is the order of the other eigenvalue then it may happen that $r \mid s$ and $E[l] \subseteq E(\mathbb{F}_{q^s})$. In this case we would have no control in which kernel does the point P lie if any. Authors of [FKS18] got around this by forcing $p \equiv -1 \pmod{l_i}$, which enabled them switching directions by switching between quadratic twists. The authors chose primes p of the form

$$p = \prod_i l_i - 1.$$

This puts considerable constrain on possible primes p and also on trace t of π. Nonetheless, if the order r is not large VeluWalk is faster than ElkiesWalk. Choosing elliptic curve with the appropriate trace is done simply by randomly choosing elliptic curves and using efficient point counting algorithm.

```
Algorithm 5: VeluStep
  Input: $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, prime $l$, scalar $\lambda$, $N = |E(\mathbb{F}_{q^r})|$
  Output: $(l, \pi - \lambda) \cdot j(E)$
  $P \leftarrow \mathrm{random}(E(\mathbb{F}_{q^r}))$
  while $(N/l) \cdot P = \infty$ do
      $P \leftarrow \mathrm{random}(E(\mathbb{F}_{q^r}))$
  $f \leftarrow \prod_{i=0}^{(l-1)/2} (X - (i \cdot P)_x)$
  $E' \leftarrow \mathrm{Kohel}(E, f)$
  return $E'$
```

Possible attacks

The potential attacker wants to find the secret key. This means, given two j-invariants $j(E)$, $j(E')$ find a walk from $j(E)$ to $j(E')$. We can determine whether E and E' are isogenous (not on mutually twisted components) in polynomial time with algorithms for counting points on elliptic curve. So finding secret key is essentially breaking the Problem 3.

The best classical algorithm in context of asymptotic complexity is due to Galbraith, Hess and Smart [GHS02]. The idea is to start random walks from $j(E)$ and $j(E')$ until we found a collision, i.e. vertex which is on both walks.

First step for the attacker is to check whether E and E' have maximal endomorphism ring, i.e. $\mathrm{End}(E) \cong \mathrm{End}(E') \cong \mathcal{O}_K$. If it is not the case, there exist a prime l dividing the conductors and l-volcanoes V_1, V_2 such that $j(E_1) \in V_1$ and $j(E_2) \in V_2$. Moreover, $j(E_1)$, $j(E_2)$ don't lie on the surfaces. The attacker can climb in both V_1 and V_2 on the surfaces with $j(E_1') \in V_1$, $j(E_2') \in V_2$ and solve the Problem 3 for these curves. The reason for this climbing is that elliptic curves on the surfaces have smaller class groups and consequently the set of $\mathrm{Ell}_{\mathcal{O}_K}(\mathbb{F}_q)$ is smaller. Because of this, most proposed protocols demand that $\mathcal{O} = \mathcal{O}_K$. In the Figure 5.3, you can see two horizontal isogeny graphs with endomorphism ring $\mathcal{O}_K$ and $\mathcal{O}$ with conductor 2.

Second step is to generate a set of primes P such that corresponding prime ideals generate the class group $\mathrm{Cl}(\mathcal{O}_K)$. Otherwise the attacker would not be able

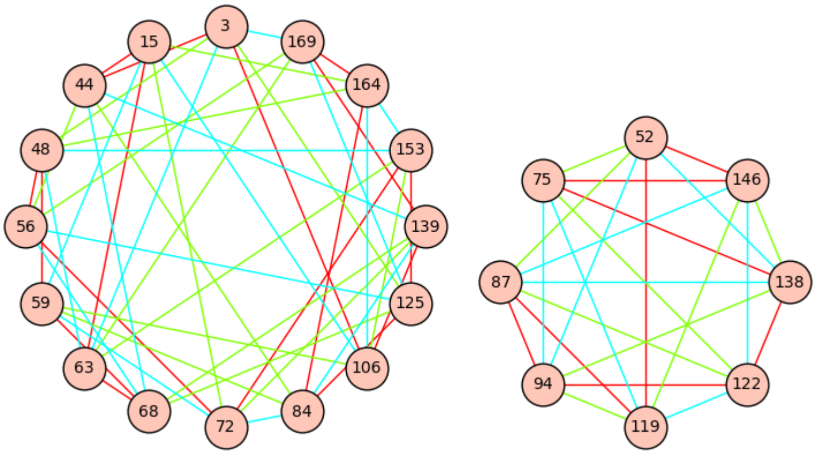


Figure 5.3: Left: $\mathrm{Ell}_{\mathcal{O}_K}(\mathbb{F}_{173})$, right: $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_{173})$ where $\mathcal{O}$ has conductor 2.

to perform walks throughout the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ and possibly not be able to find the collision. Moreover, the set P must be large enough so that the walks seem random. The attacker samples random sequences of primes from P, thus generating walks from $j(E)$ and $j(E')$ until collision of both walks is found. The collision search is done through pollard rho type algorithm, which we will not go through here, but the expected time is in $\mathcal{O}(\sqrt{h(\mathcal{O}_K)})$ by the birthday paradox which is typically $\mathcal{O}(q^{1/4})$.

Better assymptotic complexity has been found for the quantum computers. At the beginning, we have stated that both the discrete logarithm and integer factorization problems can be broken in polynomial time with quantum computers. They are actually both instances of the hidden subgroup problem:

Problem 4. Given a group G, a set X and a function $f : G \to X$ for which exists a subgroup $H \subseteq G$ satisfying $f(h_1) = f(h_2) \iff h_1 h_2^{-1} \in H$, find generators of H.

We will show that discrete logarithm on elliptic curve is a hidden subgroup problem. Let E be an elliptic curve, $P, Q \in E$ points such that $Q = xP$ for $x \in \mathbb{Z}_n$, where P has order n. Consider the homomorphism of groups $f : \mathbb{Z}_n \times \mathbb{Z}_n \to E$ defined by $f(a, b) = aP - bQ$. The kernel of f are the points (a, b) such that $aP - bQ = aP - bxP = \infty$ which is equivalent to $a = bx$ and $(a, b) = b(x, 1)$. Thus if we define $H = \langle (x, 1) \rangle \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$, we get the hidden subgroup problem for the subgroup H.

Kitaev generalized the Schor's polynomial algorithm to hidden subgroup problem for finitely generated abelian group [Kit95]. The isogeny path problem can be in some cases similarly generalized to hidden shift problem:

Problem 5. Given group G, set X and two injective functions $f_1, f_2 : G \to X$ for which exists an element $s \in G$ satisfying $f_1(g) = f_2(gs)$ for any $g \in G$, find s.

The generalization of isogeny path problem to this hidden shift problem is trivial: For $j(E)$ and $j(E')$ define two maps $f_1, f_2 : \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Ell}_{\mathcal{O}_K}(\mathbb{F}_q)$ as $f_1(\mathfrak{a}) = \mathfrak{a} \cdot j(E)$ and $f_2(\mathfrak{a}) = \mathfrak{a} \cdot j(E')$. The shift s is the unique ideal $\mathfrak{b}$ satisfying $\mathfrak{b} \cdot j(E) = j(E')$.

The hidden shift problem can actually be reduced to hidden subgroup problem, but with nonabelian group (as opposed to Kitaev's algorithm for abelian groups) and there is no known algorithm that solves this. However, Kuperberg came with subexponential quantum time algorithm in [Kup05]. Practical uses of this this algorithm are debated but remain a potential problem.

Supersingular key exchange

Although, there has been considerable effort to make the key exchange on ordinary graphs practical, nowadays it remains an ancestor of now popular and widely studied key exchange on supersingular graphs. We have seen that in order to speed up the computation of group action by using VeluWalk we have put constraints on the prime $p = \prod_i l_i - 1$. However, if we are bold enough and put $t = 0$ then

$$|E(\mathbb{F}_q)| = \prod_i l_i.$$

Hence we effortlessly gain a lot of subgroups (kernels of isogenies) for VeluWalk and we don't have to worry about their field of definition as they are defined over $\mathbb{F}_q$. By forcing $t = 0$, we have chosen supersingular curve and even though the endomorphism ring of supersingular curves is not an imaginary quadratic field and we have no class group, it is possible to restrain to endomorphisms over $\mathbb{F}_p$. This yields, in general, a ring isomorphic to either $\mathbb{Z}[\sqrt{-p}]$ or to $\mathbb{Z}[(1+\sqrt{-p})/2]$ as shown in [Sch95]. We can then apply our theory of complex multiplication to these rings. As a result of this, the popular CSIDH [CLM+18], has been introduced which uses only VeluWalk for computing isogeny steps. Additionally, no subexponential quantum attack is known similar to Kuperberg's approach.

Point counting

We have seen that we are often in need of finding the cardinality $|E(\mathbb{F}_q)|$, or equivalently by $|E(\mathbb{F}_q)| = q + 1 - t$, finding the trace t of Frobenius endomorphism:

- If we want to compute the endomorphism ring $\mathrm{End}(E)$ we need to factorize $t^2 - 4q$.
- Determining whether $p \mid t$ tells us whether E is supersingular or ordinary.
- In order to setup a practical key exchange we need to find E such that $|E(\mathbb{F}_q)|$ is divisible by small primes.

The current state-of-the-art point counting algorithm for elliptic curves over finite field of large characteristic is the SEA algorithm. The heart of SEA is the Schoof's algorithm later improved by Elkies and Atkin. We will briefly go through the ideas of these algorithms. More thorough introduction can be found in [Sch95]. Fouquet and Morain have come up with application of isogeny volcanoes for point counting in [FM02]. Building up on this paper, we will in the next chapter propose possible improvements in the context of elliptic curves over optimal extension fields.

Schoof's algorithm

The idea of Schoof's algorithm is to compute t modulo small primes. By Hasse's theorem $-2\sqrt{q} < t < 2\sqrt{q}$. So if we determine t modulo $l_1, \ldots, l_n$ satisfying

$$\prod_{i=1}^{n} l > 4\sqrt{q},$$

then we have determined t.

Finding t modulo 2 is straightforward: $2 \mid 0$ if and only if $2 \mid |E(\mathbb{F}_q)|$, which is true if and only if there exists $P \in |E(\mathbb{F}_q)|$ of order 2. Points of order 2 are of the form $(x_P, 0)$ as $P = -P$. Thus, x_P is the root of $x^3 + ax + b \in \mathbb{F}_q[x]$. We could use some factorization method but it is easier to simply compute $\gcd(x^q - x, x^3 + ax + b)$. The overall complexity is $O(\log^3(p))$.

For $l > 2$ we make use of the characteristic polynomial of π: $\pi^2 + q = t\pi$. If $P \in E[l]$ then also $\pi(P), qP \in E[l]$ and we can write

$$\pi^2(P) + q_l P = t_l \pi(P), \tag{5.2}$$

where $0 \leq q_l, t_l < l$ are remainders of q, t modulo l. Since we can compute left side of the equation, we can determine t_l by repeated addition of $\pi(P)$ until the equation holds. It remains to find at least one $P \in E[l]$. Recall that there exists a kernel polynomial $\psi_l \in \mathbb{F}_q[x]$(called division polynomial) for $[l]$ whose at least one root is equal to x_P. We could simply compute and factorize ψ_l but it is better to directly use ψ_l as follows: If we express (5.2) in the coordinates we get

$$(x^{q^2}, y^{q^2}) + q_l \cdot (x, y) = t_l \cdot (x^q, y^q), \tag{5.3}$$

for $(x, y) \in E[l]$. We can consider (5.3) as an equation in $\mathbb{F}_q(x, y)$ modulo $y^2 - x^3 - ax - b$, and ψ_l and find t_l as discussed. The complexity of finding t_l for each l is in $O(l^5 \log^2(q))$. Using the prime number theorem we can estimate the number of primes needed to be $O(\log(q))$ each of size $O(\log(q))$. Thus, making the complexity of the whole algorithm to be $O(\log^8(q))$. Although this is a polynomial algorithm, in practice the large degrees of the division polynomials (ψ_l has degree $\frac{l^2-1}{2}$) are an obstacle making the algorithm not very efficient.

Elkies's and Atkin's approach

We will restrict to the case of E ordinary with $j(E) \neq 0, 1728$. For $j(E) = 0, 1728$ there are better methods for point counting based on the knowledge of endomorphism ring [Sch95]. The chances of encountering supersingular curve are slim and there are methods to quickly determine this.

Atkin's method utilizes the l-th modular polynomial with degree $l + 1$ instead of the division polynomial. The idea is based on the following Proposition [Sch95]:

Proposition 139. Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with $j(E) \neq 0, 1728$. Let $\Phi_l(j, x) = f_1 \ldots f_s$ be the factorization of $\Phi_l(j, x) \in \mathbb{F}_q[x]$ as a product of irreducible polynomials. Finally, let r be the smallest integer such that $E[l] \subseteq E(\mathbb{F}_{q^r})$. Then there are the following possibilities for the degrees of $f_1, \ldots, f_s$:

(i) $\deg(f_1) = \cdots = \deg(f_{s-1}) = 1$ and $\deg(f_s) = l$ if $l \mid t^2 - 4q$.

(ii) $\deg(f_1) = \deg(f_2) = 1$ and $\deg(f_3) = \cdots = \deg(f_s) = r$ if $\mid t^2 - 4q$ is square modulo l.

(iii) $\deg(f_1) = \cdots = \deg(f_s) = r$ if $\mid t^2 - 4q$ is not a square modulo l.

The knowledge of r restricts the possibilities for t_l as t_l is the root of $x^2-tx+q = 0$ modulo l. To compute r we can either factorize $\Phi_l(j,x)$ in $\mathbb{F}_q[x]$ or, as Atkin does, find i such that $\gcd(x^{q^i} - x, \Phi_l(j,x)) = \Phi_l(j,x)$. In another words find i such that $\Phi_l(j,x)$ splits into linear factors in $\mathbb{F}_{q^i}[x]$. Atkin actually doesn't use the modular polynomial but some related modular functions. The algorithm isn't polynomial as it uses a baby-step-giant-step type algorithm to determine t from all values of r, but it is still practical for moderately large q.

Elkies's approach only works for primes l for which x^2-tx+q splits modulo l. By Cheboratev's theorem [SL96] this applies in roughly half the cases. If we can acquire the root λ of x^2-tx+q, then $t \equiv \lambda + q/\lambda \pmod{l}$. We know that if x^2-tx+q splits modulo l then E admits at least one l-isogeny ϕ whose kernel satisfies $\pi(P) = \lambda P$ for each $P \in \ker(\phi)$. We can therefore add $P + \cdots + P$ until we get $\pi(P)$. Similarly to original Schoof, Elkies does this in terms of coordinates, i.e.: $(x^q, y^q) = \lambda \cdot (x,y)$ where the equation is done modulo $y^2 - x^3 - ax - b$ and modulo the square root of kernel polynomial of ϕ, which is a polynomial of degree $\frac{l-1}{2}$.

Clever combination of Schoof's algorithm with Elkies's and Atkin's ideas results in the SEA algorithm, which is a probabilistic algorithm with time running in $\tilde{O}(\log^4(q))$. Sage implements SEA together with algorithms for small characterstics through PARI-GP for more efficiency.

Chapter 6

Practical implementation

The purpose of this chapter is to present a possible improvement for the algorithm of Fouquet and Morain in [FM02], which utilizes isogeny volcanoes for counting points of elliptic curves. Secondly, as a part of this thesis, implementation of various functions concerning isogenies and isogeny volcanoes in Sage was written which are missing in the official implementation.

Isogeny volcanoes and Schoof's algorithm

The term 'volcano' was first introduced in the paper Isogeny Volcanoes and the SEA Algorithm by Mireille Fouquet and François Morain [FM02]. Authors followed on the work by David Kohel and gave a complete description of volcanoes and explained how we can travel through volcanoes using modular polynomials. At the end, authors proposed application for counting points of elliptic curve. The idea, as in Schoof's algorithm, is to compute trace t modulo primes $l = 2, 3, \ldots$ with the alteration that for each such prime l we obtain the depth of l-volcano through isogeny climbing. If a curve E over $\mathbb{F}_q$ has an l-volcano of depth n then

$$l^{2n} \mid t^2 - 4q$$

Moreover, if the crater is one vertex with one loop or two vertices connected by one edge then $l \mid d_K$ and $l^{2n+1} \mid t^2 - 4q$. Thus, by isogeny climbing we can determine $t^2 \pmod{l^{2n+e}}$ where $e \in \{0, 1\}$. If $l \neq 2$, then $x^2 \equiv t^2 \pmod{l^{2n+e}}$ has two solutions for x, which differ by sign. To determine the sign of t modulo l^{2n+e}, we compute t modulo l by one of the methods discussed (Schoof's or Elkies approach). We repeat this for primes $l_1, \ldots, l_k$ with corresponding depths $n_1, \ldots, n_k$ (and $e_i \in \{0, 1\}$) until

$$\prod_{i=1}^{k} l_i^{2n_i+e_i} > 4\sqrt{q}.$$

This could be a potential improvement as we don't have to compute t modulo higher primes and avoid high degree division polynomials (rather using modular polynomials for isogeny climbing). However, there seem to be two main issues with this approach:

- For $l = 2$, we can't determine $t \bmod 2^{2n+e}$ from the knowledge of t^2 modulo 2^{2n+e} by the same method. The equation $x^2 \equiv t^2 \pmod{l^{2n+e}}$ can have more than two solutions and computing t modulo 2 tells us nothing. Fouquet admits that this situation is left open in [Fou01].
- For each curve there is only a finite amount of primes l for which corresponding l-volcanoes have nonzero depth. Furthermore, the number $D = t^2 - 4q$ behaves as a random integer, and we can't expect it to be divisible by large squares.

We can support the gravity of these two problems by real data. The Table 6.1 shows the average depth of l-volcano for $l = 2, 3, 5, 7, 11$. For each bit size $8, 16, 32, 64$ we have generated 10 primes and for each such prime p 100 ordinary elliptic curves over $\mathbb{F}_p$. The numbers then represent the average depth of volcanoes of these 1000 curves. One can see that the average elliptic curve is not suitable for the algorithm using isogeny volcanoes as the depth is zero. Moreover, the most relevant prime for volcanoes is $l = 2$. This is unfortunate as the case $l = 2$ is the one which is missing. Notice that that the depths don't as much vary with different bit sizes. We will therefore from now on focus on the case of primes of size 16 bits and similarly $l = 2, 3, 5$ as higher primes are evidently not as relevant.

	$l = 2$	$l = 3$	$l = 5$	$l = 7$	$l = 11$
8 bit	0.687	0.129	0.066	0.034	0.006
16 bit	0.904	0.205	0.079	0.024	0.008
32 bit	0.859	0.212	0.079	0.022	0.012
64 bit	0.953	0.196	0.052	0.026	0.012

Table 6.1: The average depth of l-volcano over field $\mathbb{F}_p$ of size $8, 16, 32, 64$ bits.

We present a solution for the problem with $l = 2$ and propose the usage of the algorithm for non-prime finite fields which seem to have volcanoes with bigger depths. The following lemma is the basis for our algorithm for $l = 2$.

Lemma 140. Let E be an ordinary elliptic curve over $\mathbb{F}_q$ and $t = T(\pi_E)$. Suppose $2^n \mid t^2 - 4q$ for some $n \in \mathbb{N}$:

(i) If $n < 3$ then $t \equiv 0 \pmod 2$

(ii) If $3 \leq n$ then $t \equiv 2 \pmod 4$

(iii) If $5 \leq n$ and t_0 is a square root of $4q \pmod{2^n}$ satisfying $t_0 \equiv 2 \pmod 8$ then

$$t \equiv t_0 \pmod{2^{n-2}} \iff 8 \mid E(\mathbb{F}_q),$$

otherwise $t \equiv -t_0 \pmod{2^{n-2}}$. Moreover, $q \equiv 1 \pmod 8$.

Proof. The cases (i) and (ii) are trivial as $2 \nmid q$. We proceed to (iii). Let t_0 be any square root of $4q \pmod{2^n}$. Either $t_0 \equiv 2 \pmod 8$ or $t_0 \equiv 6 \pmod 8$ as $4 \nmid t_0$. Without loss of generality assume the latter (otherwise pick $-t_0$). Then

$$t^2 - t_0^2 = (t - t_0)(t + t_0) \equiv 0 \pmod{2^n}$$

If it were to happen $8 \mid t - t_0$ and $8 \mid t + t_0$, then $4 \mid t$, which is contradiction with (ii). So either $t \equiv t_0 \pmod{2^{n-2}}$ or $t \equiv -t_0 \pmod{2^{n-2}}$. Moreover, $t \equiv t_0 \pmod{2^{n-2}}$ if and only if $t \equiv 2 \pmod 8$, which is true if and only if $q + 1 - |E(\mathbb{F}_q)| \equiv 2$. Since $t^2 \equiv 4 \pmod 8$, then $q \equiv 1 \pmod 8$. It follows that $q + 1 - |E(\mathbb{F}_q)| \equiv 2 \pmod 8$ if and only if $8 \mid |E(\mathbb{F}_q)|$. □

The lemma can summarized as follows: If we find through isogeny climbing that $t^2 \equiv 4q \pmod{2^{2n+e}}$, then we compute a square root t_0 of $4q \pmod{2^{2n+e}}$ such that $t_0 \equiv 2 \pmod 8$. Afterwords, we compute the sign $t \equiv \pm t_0 \pmod{2^{2n+e-2}}$ by determining whether $8 \mid |E(\mathbb{F}_q)|$ (see Algorithm 6).

Algorithm 6: Find $t \pmod{2^{n-2}}$

```
Input: Elliptic curve $E$ for which $2^n \mid t^2 - 4q$, $n \geq 5$, $q \equiv 1 \pmod 8$
Output: $t \pmod{2^{n-2}}$
$t_0 \leftarrow$ square of $4q$ modulo $2^n$
if $t_0 \equiv 6 \pmod 8$ then $t_0 \leftarrow -t_0 \pmod{2^{n-2}}$ else $t_0 \leftarrow t_0 \pmod{2^{n-2}}$
if is_order_divisible_by_8(E) then return $t_0$ else return $-t_0$
```

It remains to show how to decide whether $8 \mid |E(\mathbb{F}_q)|$. If $8 \mid E(\mathbb{F}_q)$ then either $E(\mathbb{F}_q)$ contains a point of order 8 or $\mathbb{Z}_4 \times \mathbb{Z}_2 \subseteq E[4] \cap E(\mathbb{F}_q)$. The latter case means there are at least four points of order 4 in $E(\mathbb{F}_q)$. The algorithm will compute gradually points of order 2, 4 and 8. If it doesn't find enough points of order 4 or any point of order 8, then it will return $8 \nmid E(\mathbb{F}_q)$ and the opposite otherwise. The following lemma tells us how to compute such points and the result is Algorithm 7.

Lemma 141. If $E : y^2 = x^3 + ax + b$ is an elliptic curve over $\mathbb{F}_q$ then

(i) any point $(x, y) \in E(\mathbb{F}_q)$ of order 4 satisfies $-x^6 - 5ax^4 + 5a^2x^2 - 20bx^3 + a^3 + 4abx + 8b^2 = 0$

(ii) any point $(x, y) \in E(\mathbb{F}_q)$ of order 8 satisfies $-x^4 + 2ax^2 - a^2 + 8bx + 4(x^3 + ax + b)r = 0$ for appropriate point $(r, s) \in E(\mathbb{F}_q)$ of order 4.

Proof. The statement is an application of addition formulas. □

To show practical usage of Algorithms 6 and 7, we have compared three algorithms for point counting:

- Original Schoof's algorithm implemented in Sage in [Lou16].
- Algorithm based upon the paper by Fouquet and Morain, which we implemented in Sage using pseudocodes provided in the paper [FM02].
- Our algorithm building up on Fouqet and Morain with the improvement $l = 2$.

```
Algorithm 7: is_order_divisible_by_8
Input: Elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$
Output: True if $8 \mid E(\mathbb{F}_q)$ and False otherwise
counter $\leftarrow 0$
foreach root $r$ of $-x^6 - 5ax^4 + 5a^2x^2 - 20bx^3 + a^3 + 4abx + 8b^2$ do
    if $r$ defines point $(r, y_r) \in E(\mathbb{F}_q)$ then
        counter$+= 1$
        $g \leftarrow -x^4 + 2ax^2 - a^2 + 8bx + 4(x^3 + ax + b)r$
        if $g$ has a root in $\mathbb{F}_q$ then return True
    end
end
return counter$\geq 2$
```

We have generated 5 primes of size 16 bits and for each prime 100 elliptic curves whose 2-volcano has depth at least 2. The average time, in seconds, of each algorithm can be seen in Table 6.2. Each row corresponds to one of the five primes.[1]

Schoof	Fouquet and M.	$l = 2$ improvement
0.109	0.121	0.094
0.113	0.104	0.087
0.123	0.122	0.094
0.115	0.134	0.105
0.113	0.117	0.105

Table 6.2: Comparing the times of point counting algorithms for elliptic curves with 2-volcanoes of large depth. Each cell is an average time in seconds.

We have shown that we can deal with the case $l = 2$. However, this doesn't solve the second problem with sporadic occurrences of volcanoes of nonzero depth. We can at least partially get around this by choosing appropriate fields. We claim that elliptic curves over fields $\mathbb{F}_q$ for $q = p^m$, m even, tend to have volcanoes with bigger depths. We can support this by statistical evidence: We have generated 10 random primes of size 16 bits. For each such prime p and $m = 2, 3, 4$ we have generated random prime p_m of the same bit size as p^m, thus getting 10 pairs of fields $(\mathbb{F}_{p^m}, \mathbb{F}_{p_m})$. We compared each pair of fields by generating 100 ordinary elliptic curves and computing the average depth of l-volcano for $l = 2, 3, 5$. In Table 6.3, you can see the result where each cell is of the form h_1/h_2 where h_1, h_2 are the average depths for $\mathbb{F}_{p^m}$, $\mathbb{F}_{p_m}$ respectively.

One of the explanation for the bigger depths of 2-volcanoes over non-prime fields is the following: From the Lemma 140, if $n \geq 5$ then necessarily $q \equiv 1 \pmod 8$. This is always satisfied for q square, in particular for $q = p^2, p^4$. Similar ideas may hold for other primes then 2.

[1] The reader should be aware that since all computation are done in Sage (as opposed to more time effective language C, for example) the purpose of the timings is solely for comparisons of the algorithms.

	$l=2$	$l=3$	$l=5$
$m=2$	1.326/0.913	0.369/0.128	0.093/0.024
$m=3$	1.037/0.910	0.202/0.222	0.042/0.021
$m=4$	1.432/0.922	0.352/0.147	0.093/0.064

Table 6.3: Each cell contains h_1/h_2 where h_1, h_2 are the average depths of l-volcanoes over $\mathbb{F}_{p^m}$, $\mathbb{F}_{p_m}$ respectively.

It seems that isogeny volcanoes for point counting might be more appropriate for non-prime fields. Again, we have compared the three point counting algorithms, this time for field $\mathbb{F}_p^m$. We have generated 10 random primes of size 16 bits and for each such prime and $m = 1, 2, 3$ generated 10 elliptic curves over $\mathbb{F}_{p^m}$. The resulting comparison of the three algorithms can be seen in Table 6.4 where each cell contains the average time for computing one trace in seconds.

	Schoof	Fouquet and M.	$l=2$ improvement
$m=1$	0.091	0.074	0.061
$m=2$	10.83	9.82	9.40
$m=3$	42.10	39.54	39.74

Table 6.4: Comparing point counting algorithms. Each cell is an average time in seconds for elliptic curve over $\mathbb{F}_{p^m}$

.

Finally, we would like to discuss point counting algorithms as an application to cryptography. There are three fields used in cryptographic protocols:

- Prime fields $\mathbb{F}_p$
- Binary fields $\mathbb{F}_{2^n}$
- Optimal extension fields introduced by Bailey and Paar in [BP98]. An optimal extension field (OEF) is a field $\mathbb{F}_{p^m}$ such that $p = 2^n \pm c$ where $\log_2(c) \leq n/2$ and an irreducible polynomial $x^m - \omega$ exists over $\mathbb{F}_p$. It can be shown that under some conditions OEF brings faster finite field arithmetic for elliptic curves.

It is beyond the scope of this text to go deeper into the theory of OEF. However, as a practical cryptographical example we use our algorithm to generate a cryptographically strong elliptic curve over optimal extension field. We call elliptic curve E strong if it satisfies the following:

- $|E(\mathbb{F}_q)| = k \cdot r$ with r prime and $k \leq 4$ to avoid pollard-rho attack.
- The order of q in $\mathbb{F}^\times$ is at least $\log^2(q)$ to avoid MOV attack (see [CFA+12])

There are two methods to obtain cryptographically strong curve. First one utilizes methods of complex multiplication [Bai01] and is restricted to curves with small discriminant d_K. The second one, randomly chooses curves and uses efficient point

p^2	Schoof	Fouquet and M.	$l = 2$ improvement
4274675161	52.13	123.84	52.53
4273367641	24.96	45.15	26.93
4282000969	25.10	30.37	69.37
4263175849	57.82	117.53	61.71
4280168929	91.61	74.98	54.94

Table 6.5: Times to generate cryptographically strong curve over $\mathbb{F}_{p^2}$ using three point counting algorithms.

counting algorithm to verify the two conditions on strong curves. We will use the second method and compare the three presented algorithms to obtain strong curves.

We conclude that even though we have managed to improve the original ideas by Fouquet and Morain, isogeny volcanoes doesn't seem to be in general useful for point counting. However, the study of isogeny volcanoes in non-prime fields could provide an interesting direction for further research.

Isogenies in Sage

For the computational purposes, including Schoof's algorithm with volcanoes, we have created several classes in Sage implementing: isogenies, endomorphisms, isogeny volcanoes, endomorphism ring and class group action. We will compare them with official implementation in Sage v09 ([SGE]) and show basic functionality on examples. More thorough documentation showing all features is in appendix.

The official Sage implementation of isogenies over finite fields is based on the class `EllipticCurveIsogeny`. This class implements isogenies using the Vélu and Kohel formulae. However, the functionality is limited. For example, the following is not implemented:

- Isogenies with noncyclic kernel
- Inseparable isogenies
- Generating isogenies using kernel not defined over base field

```
Warning: Only cyclic, separable isogenies are
implemented (except for [2]). Some algorithms
may need the isogeny to be normalized.
```

We provide a new class `Isogeny` which manages to solve these problems and provide further functions useful for isogeny computations including:

- Factorization of isogenies into prime degree isogenies
- Transformation of rational maps into standard form
- Computation of kernel in any extension

- Isomorphisms of isogenies
- Addition of isogenies with the same domain and codomain
- Dual isogeny for separable isogenies (the official implementation is limited)

```
sage: EllipticCurve(GF(23),[15,9])
sage: Isogeny(E,kernel_polynomial = x^3+22*x^2+7*x+16)
Isogeny of degree 6 from Elliptic Curve defined by...

## As opposed to official implementation:
sage: EllipticCurveIsogeny(E,kernel = x^3+22*x^2+7*x+16)
NotImplementedError: For basic Kohel's algorithm,
if the kernel degree is even then the kernel must
be contained in the two torsion.
```

Our implementation of isogenies allowed us to create a subclass `Endomorphism` of class `Isogeny`. Endomorphisms of elliptic curves are not implemented in Sage at all as the class `EllipticCurveIsogeny` is limited to only small subset of isogenies, unable to support endomorphisms which are in general inseparable and don't have cyclic kernel.

One of the key feature of the class `Endomorphism` is the correspondence between rational maps of endomorphisms and appropriate elements in quadratic number field K. For example, we can pass to constructor element of K:

```
sage: K.<c> = Numberfield(E.frobenius_polynomial())
sage: Endomorphism_ring(E,element = c-3)
Endomorphism of degree 23 on Elliptic Curve defined
by y^2 = x^3 + 12*x + 4 over Finite Field of size 23
```

Furthemore, as computation of endomorphism ring is not implemented in sage in any form we created a class `Endomorphism_ring`, which finds endomorphism ring of given curve.

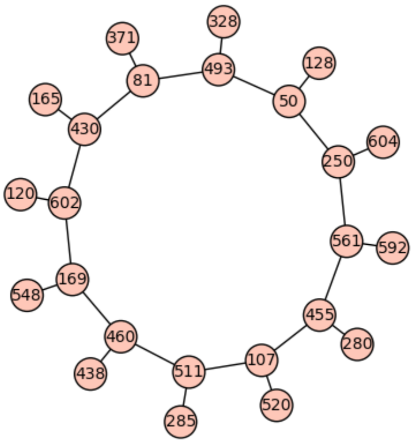
```
sage: E = EllipticCurve(GF(23),[12,4])
sage: O = Endomorphism_ring(E); O
Endomorphism ring of Elliptic Curve defined
by y^2 = x^3 + 12*x + 4 over Finite Field of size 23
sage: O.conductor()
1
```

The algorithm is based on finding depths of volcanoes as was explained in previous chapter. The function `volcano_depth` provides this (which implements the algorithms of [FM02]). Based on `volcano_depth`, Schoof's algorithm with isogeny volcanoes has been implemented.

```
sage: E = EllipticCurve(GF(607), [350,514])
sage: volcano_depth(E,2)
1
```

Implementation of isogeny volcanoes in Sage is completely missing. We therefore provide our class Volcano.

```
sage: E = EllipticCurve(GF(607), [350,514])
sage: V = Volcano(E,2); V
Isogeny 2-volcano of depth 1 over Finite Field of
size 607
sage: V.plot()
```



Constructor of Volcano is based on breadth-first search algorithm using modular polynomials or Vélu algorithms (one can choose). One of the features of this Class is a computation of extension over which volcano has given depth, which is based on the section *Growing volcano* from Chapter 4. The purpose of the class Volcano is mainly visual. To obtain depth of the volcano it is more appropriate to use function volcano_depth. We have also implemented Algorithm 2 in the function is_supersingular.

Key exchange

We will now show an example of Diffie-Hellman key exchange based on the action of class group using implemented function horizontal_walk as well as other classes already mentioned. Class group action on ellipitc curves is not supported in Sage.

Alice and Bob agree on a public prime p and an elliptic curve E. They also verify that the class group is large enough and that E is ordinary.

```
sage: p = 3*2*3*5*7*11*13*17*19-1
sage: E = EllipticCurve(GF(p),[2558103,24391662])
sage: K.<x> = NumberField(E.frobenius_polynomial())
sage: K.class_number()
9216
sage: is_supersingular(E)
False
```

Avoiding possible attacks by isogeny climbing, Alice and Bob should pick curve with maximal endomorphism ring:

```
sage: Endomorphism_ring(E).conductor()
1
```

Next step for them is to generate a secret key, which will be in this case a list of triples (l, λ, n) where l is an Elkies prime, λ an eigenvalue of π_l (determining the direction) and n is the number of steps. If $n < 0$ we consider $-n$ steps in the direction of the other eigenvalue.

```
sage: A = ([(3, 2, 602),(5, 4, 7253),
(7, 5, -3275), (11, 9, 4404),
(13, 12, -7215), (19, 8, -6567)]
sage B = [(3, 2, 2326), (5, 4, -1532),
(7, 5, -190), (11, 9, 1889),
(13, 12, 5211), (19, 8, 5628)])
```

Each of them then computes an action of their key (the element of class group) on the curve E using the function `horizontal_walk` which we have implemented based on the algorithms VeluWalk and ElkiesWalk (recall Algorithms 5, 3 and 4). One can choose which one of them to use but Vélu's approach is limited by the condition of $p \equiv -1 \pmod{l}$ for each l.

```
sage:AE = horizontal_walk(E,A), AE
Elliptic Curve defined by y^2 = x^3 +
20616365*x + 12507225 over Finite Field of size 29099069
sage:BE = horizontal_walk(B,A), BE
Elliptic Curve defined by y^2 = x^3 + 1521470*x + 26872156
over Finite Field of size 29099069
```

Finally, they exchange the elliptic curves AE and BE and apply their keys. The shared secret is the resulting j-invariant.

```
sage:BAE = horizontal_walk(AE,B), BAE
Elliptic Curve defined by y^2 = x^3 + 6749168*x + 9329299
over Finite Field of size 29099069
sage:ABE = horizontal_walk(BE,A), ABE
Elliptic Curve defined by y^2 = x^3 + 13448780*x +
26542762 over Finite Field of size 29099069
sage: ABE.j_invariant(), BAE.j_invariant()
(17791384, 17791384)
```

The function `horizontal_walk` is also used in the class `Volcano` as a part of Vélu algorithms to compute neighbours in given volcano.

Conclusion

This thesis explored the theory and applications of isogeny volcanoes. Any beginner in the isogeny based cryptography might find several obstacles in understanding the theory as the current literature is prepared for readers with a wide range of background knowledge. We have managed to build up the theory using only elementary methods over finite fields, thus hopefully providing better insight into the field. This text should be a good starting point for anyone ambitious enough to understand the subject deeply.

On the other hand, obstacles can be found in more practical problems, which we have pointed out in the official Sage implementation. Evidently, the implementation behind isogenies, isogeny volcanoes, endomorphisms rings, class group action is either completely missing or limited for anyone trying to understand and use these tools in theory or practical problems. We have therefore completed this implementation to some level. However, future work on this lies ahead in terms of optimization and preparation for integration to official implementation.

With these practical and theoretical tools at our hand, we have tried to solve some incomplete results from [FM02] using isogeny volcanoes for point counting. Although the isogeny volcanoes might not lie in the future of point counting, we have managed to solve the incomplete result from the paper for computing the trace modulo higher powers of two. Furthermore, we proposed a hypothesis concerning the height of volcanoes for non-prime fields, which could be an interesting direction in the study of isogeny volcanoes.

Hopefully, the reader should be convinced that isogeny volcanoes offer a powerful tool to understand elliptic curves in both the theory and applications to cryptography. The field around isogenies still has many open questions and incomplete results, some of which we have managed to solve, including practical problems one might find in available implementations.

Chapter 7

Appendix

Here we provide documentation of our implementation of isogenies and isogeny volcanoes. Firstly, we prove Lemma 141, which is the basis for Algorithm 7

Lemma 142. If $E : y^2 = x^3 + ax + b$ is an elliptic curve over $\mathbb{F}_q$, then

(i) any point $(x, y) \in E(\mathbb{F}_q)$ of order 4 satisfies $-x^6 - 5ax^4 + 5a^2x^2 - 20bx^3 + a^3 + 4abx + 8b^2 = 0$

(ii) any point $(x, y) \in E(\mathbb{F}_q)$ of order 8 satisfies $-x^4 + 2ax^2 - a^2 + 8bx + 4(x^3 + ax + b)r = 0$ for appropriate point $(r, s) \in E(\mathbb{F}_q)$ of order 4.

Proof. (i) For any point (x, y) of order 4 the point $[2](x, y)$ is point of order 2. Through addition formulas on E as stated in [Was08] we can write:

$$[2](x, y) = (m^2 - 2x, m(x - (m^2 - 2x)) - y), \text{ where } m = \frac{3x^2 + a}{2y},$$

Since points of order 2 are precisely those with y-coordinate 0 then necessarily

$$0 = m(x - (m^2 - 2x)) - y = \frac{3x^2 + a}{2y}\left(x - \left(\frac{(3x^2 + a)^2}{4y^2} - 2x\right)\right) - y.$$

Multiplying by $8y^3$ gets us

$$0 = (3x^2 + a)\left(4xy^2 - \left((3x^2 + a)^2 - 8xy^2\right)\right) - 8y^4.$$

After substitution of y^2 by $x^3 + ax + b$ we should arrive to

$$0 = (3x^2 + a)\left(12x(x^3 + ax + b) - (3x^2 + a)^2\right) - 8(x^3 + ax + b)^2.$$

The rest is simple rudimentary algebra.

(ii) We proceed in similar way for point of order 8. This time if $m^2 - 2x = r$ where r is the root of the polynomial from (i). We therefore plug it in and verify. □

Class Isogeny

We can construct `Isogeny` using:

- Kernel polynomial[1]

  ```
  sage: E = EllipticCurve(GF(59),[10,36])
  sage: x = PolynomialRing(GF(59),’x’).gen()
  sage: Isogeny(E,kernel_polynomial = x^2+45*x+22)
  Isogeny of degree 5 from Elliptic Curve defined
  by y^2 = x^3 + 10*x + 36 over Finite Field of size 59
  to Elliptic Curve defined by y^2 = x^3 + 29*x + 27
  over Finite Field of size 59
  ```

- Kernel as a list of points. As opposed to `EllipticCurveIsogeny`, these points can lie in any extension of base field of E.

  ```
  sage: k2 = GF(59^2)
  sage: z = k2.gen()
  sage: E2 = E.change_ring(k2)
  sage: kernel = [E2(40,20*z + 49),
  E2(40,39*z + 10), E2(33,29*z + 15),
  E2(33,30*z + 44),E2(0)]
  sage: Isogeny(E, kernel = kernel)
  Isogeny of degree 5 from Elliptic Curve defined
  by y^2 = x^3 + 10*x + 36 over Finite Field of size 59
  to Elliptic Curve defined by y^2 = x^3 + 29*x + 27
  over Finite Field of size 59
  ```

- Rational maps and codomain.

  ```
  sage: x,y = PolynomialRing(GF(59),[’x’,’y’]).gens()
  sage: maps =
  ((x^5 - 28*x^4 + 12*x^3 + 21*x^2 - 17*x - 18)/(x^4 -
  28*x^3 + 4*x^2 - 26*x + 12), (x^6*y + 17*x^5*y -
  3*x^4*y - 19*x^3*y + 17*x^2*y - 9*x*y + 7*y)/(x^6
  + 17*x^5 + 5*x^4 + 10*x^3 - 8*x^2 + 27*x + 28))
  sage: E3 = EllipticCurve(GF(59),[29,27])
  sage: Isogeny(E, rational_maps = maps, codomain = E3)
  Isogeny of degree 5 from Elliptic Curve defined
  by y^2 = x^3 + 10*x + 36 over Finite Field of size 59
  to Elliptic Curve defined by y^2 = x^3 + 29*x + 27
  over Finite Field of size 59
  ```

[1] Contrarily to the text we use the term kernel polynomial for the square root of our definition of kernel polynomial in order to be consistent with the current implementation in Sage.

- Already constructed isogeny instance of `EllipticCurveIsogeny`.

```
sage: x = PolynomialRing(GF(59),'x').gen()
sage: poly = x^2+45*x+22
sage: isg = EllipticCurveIsogeny(E,kernel = poly)
sage: E4 = EllipticCurve(GF(59),[36,1])
sage: isg2 = Isogeny(E,isogeny = isg, codomain = E4)
sage: isg2
Isogeny of degree 5 from Elliptic Curve defined
by y^2 = x^3 + 10*x + 36 over Finite Field of size 59
to Elliptic Curve defined by y^2 = x^3 + 36*x + 1
over Finite Field of size 59
```

As we can see, we can force codomain to constructor (in any construction above) if it is isomorphic to valid codomain of given isogeny. We can also change it later by `.change_codomain()` and print out the isomorphism.

```
sage: E5 = EllipticCurve(GF(59),[29,27])
sage: isg2.change_codomain(E5); isg2
Isogeny of degree 5 from Elliptic Curve defined by
y^2 = x^3 + 10*x + 36 over Finite Field of size 59
to Elliptic Curve defined by y^2 = x^3 + 29*x + 27
over Finite Field of size 59
sage: isg2.isomorphism()
(-13*x, 24*y)
```

Class `Isogeny` has methods implementing usual properties including: `domain()`, `codomain()`, `degree()`, `kernel_polynomial()`,`kernel()`, `rational_maps()` and `separable()`:

```
sage: E = EllipticCurve(GF(101),[89,68])
sage: isg = Isogeny(E, x+50)
sage: isg.domain()
Elliptic Curve defined by y^2 = x^3 + 89*x +
68 over Finite Field of size 101
sage: isg.codomain()
Elliptic Curve defined by y^2 = x^3 + 50*x +
99 over Finite Field of size 101
sage: isg.degree()
3
sage: isg.rational_maps()
((x^3 - x^2 + 3*x - 18)/(x^2 - x - 25),
(x^3*y + 49*x^2*y - 2*x*y - 16*y)/(x^3 +
49*x^2 + 26*x - 38))
sage: isg.kernel()
[(51 : 10 : 1), (51 : 91 : 1),(0 : 1 : 0)]
```

```
sage: isg(isg.kernel()[0])
(0 : 1 : 0)
sage: isg.kernel_polynomial()
x+50
sage: isg.separable()
True
```

Dual isogeny is implemented for separable isogenies:

```
sage: isg.dual()
Isogeny of degree 3 from Elliptic Curve defined by
y^2 = x^3 + 50*x + 99 over Finite Field of size 101
to Elliptic Curve defined by y^2 = x^3 + 89*x + 68
over Finite Field of size 101
```

Both the composition and addition of isogenies is supported:

```
sage: isg+isg
Isogeny of degree 12 from Elliptic Curve defined
by y^2 = x^3 + 89*x + 68 over Finite Field of size
101 to Elliptic Curve defined by y^2 = x^3 + 50*x +
99 over Finite Field of size 101
sage: isg-isg
Zero isogeny from Elliptic Curve defined by
y^2 = x^3 + 89*x + 68 over Finite Field of size 101
to Elliptic Curve defined by y^2 = x^3 + 50*x + 99
over Finite Field of size 101
sage: E2 = isg.codomain()
sage: isg2 = Isogeny(isg.codomain(),
kernel_polynomial = x+52, codomain = E)
sage: isg2*isg
Isogeny of degree 9 from Elliptic Curve defined
by y^2 = x^3 + 89*x + 68 over Finite Field of
size 101 to Elliptic Curve defined by y^2 = x^3
+ 89*x + 68 over Finite Field of size 101
```

Inseparable isogenies are implemented. Every inseparable isogeny can be decomposed to $\alpha = \alpha_s \pi_p^r$ by Lemma 28. We can specify the integer r by argument `frobenius_power`:

```
sage: E = EllipticCurve(GF(101),[89,68])
sage: isg = Isogeny(E, x+50, frobenius_power = 1)
Isogeny of degree 303 from Elliptic Curve defined by
y^2 = x^3 + 89*x + 68 over Finite Field of size 101 to
Elliptic Curve defined by y^2 = x^3 + 50*x + 99 over
Finite Field of size 101
sage: isg.separable()
```

```
False
sage: isg.inseparable_degree()
101
```

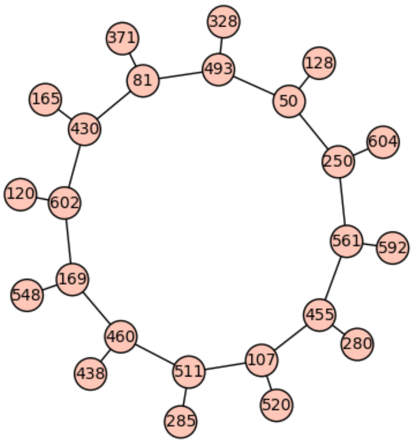
Finally, we bring a method that can factorize any separable isogeny to a list of prime isogenies (based on the Lemma 28).

```
sage: isg = Isogeny(E, x+50, frobenius_power = 0)
sage: (isg+isg).isogeny_factors()
[Isogeny of degree 2 from Elliptic Curve
defined by y^2 = x^3 + 89*x + 68 over Finite
Field in z2 of size 101^2 to Elliptic Curve
defined by y^2 = x^3 + 21*x + 73 over Finite
Field in z2 of size 101^2,
Isogeny of degree 2 from Elliptic Curve defined
by y^2 = x^3 + 21*x + 73 over Finite Field in z2
of size 101^2 to Elliptic Curve defined by y^2 =
x^3 + 10*x + 9 over Finite Field in z2 of size 101^2,
Isogeny of degree 3 from Elliptic Curve defined
by y^2 = x^3 + 10*x + 9 over Finite Field in z2
of size 101^2 to Elliptic Curve defined by y^2 =
x^3 + 93*x + 74 over Finite Field in z2 of size 101^2]
```

Isogeny volcanoes in Sage

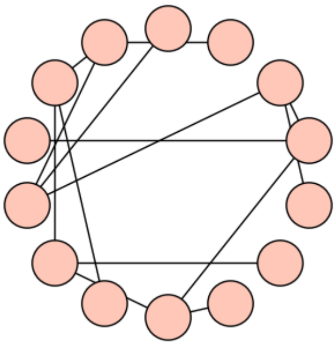
The constructor for Volcano has two arguments: elliptic curve and degree.

```
sage: from libr.volcano import Volcano
sage: E = EllipticCurve(GF(607), [350,514])
sage: V = Volcano(E,2); V
Isogeny 2-volcano of depth 1 over Finite Field of
size 607
sage: V.plot()
```



Method `.plot()` has optional arguments `figsize`, `vertex_size`, `vertex_labels`, `layout` which are the same as corresponding methods of igraph in Sage.

```
sage: E = EllipticCurve(GF(743),[622,90])
sage: Volcano(E,2).plot(figsize = (5,5), vertex_size =
800,layout = 'circular', vertex_labels = False)
```



We can print out all usual properties of volcano: individual levels (crater in particular), depth, neighbors to each vertex (parent and children), depth of each vertex.

```
sage: E = EllipticCurve(GF(607), [350,514])
sage: V.level(1)
[285, 438, 520, 548, 280, 120, 592, 165, 604, 371, 128, 328]
sage: V.depth()
1
sage: V.crater()
[511, 460, 107, 169, 455, 602, 561, 430, 250, 81, 50, 493]
sage: V.neighbors(107)
[(520, 1), (511, 1), (455, 1)]
sage: V.volcano_parent(107)
None
sage: V.volcano_children(107)
[520]
sage: V.vertex_depth(107)
0
sage: V.degree()
2
```

One can also call methods `.vertices()` and `edges()` to acquire corresponding lists. Only ordinary curves are of course implemented and graphs containing j-invariant 0, 1728 may behave funny, so warning is always displayed. One can also use the method `special` to check whether we have these special vertices on volcano.

```
sage: E_0 = EllipticCurve_from_j(GF(101)(0))
sage: V = Volcano(E_0,2); V
```

```
Curve with j_invariant 0 or 1728 found, may malfunction.
Isogeny 2-volcano of depth 0 over Finite Field of
size 101
sage: V.special()
True
```

If one doesn't want to see any warning, it is possible to put `special = False` in the constructor

```
sage: Volcano(E_0,2,special = False)
Isogeny 2-volcano of depth 0 over Finite Field of size 101
```

The algorithm for computing volcanoes uses be default modular polynomials, so a `database_kohel` is required to be installed in sage. One can pass as an argument to constructor to construct the volcanoes using Velu algorithms, hence not be bounded by the finite database (the highest available Φ_l is for $l = 127$).

```
sage: E = EllipticCurve(GF(607), [350,514])
sage: V2 = Volcano(E,2,Velu=True)
Isogeny 2-volcano of depth 1 over Finite Field of
size 607
```

When using Velu algorithm, there is an upper bit limit (100) on the size of extension that contains kernels. One can pass to constructor different limit.

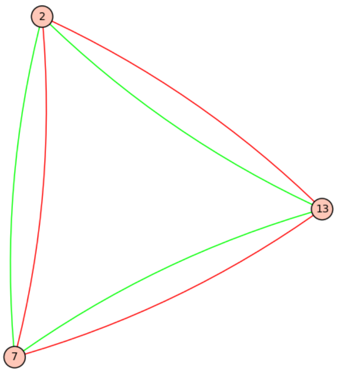
```
sage: E2 = EllipticCurve(GF(577),[11,114])
sage: Volcano(E2,127) #Kohel database is limited
FileNotFoundError ...
sage: Volcano(E2,127, Velu = True,  upper_bit_limit= 120)
Isogeny 127-volcano of depth 0 over Finite Field of size 577
```

Furthermore based on the section Growing volcano of Chapter 4, a method `.expand_volcano` is implemented, which finds an extension such that given volcano has depth at least d where d is passed as an argument.

```
sage: V3 = Volcano(E,3), V3
Isogeny 3-volcano of depth 0 over Finite Field of
size 607
sage: V3.expand_volcano(3)
Isogeny 3-volcano of depth 3 over Finite Field in z3 of
size 607^3
```

We can also plot the graph of several prime degree isogenies at the same time using class `Isogeny_graph`, which takes as an argument elliptic curve E and a list of primes. The methods `.edges()` and `.vertices()` are also available. Plotting is the same as in the class `Volcano`.

```
sage: from libr.volcano import Isogeny_graph
sage: E = E = EllipticCurve(GF(17),[3,16])
sage: G = Isogeny_graph(E,[3,5])
sage: G.plot()
```



Endomorphism ring in Sage

The constructor for class `Endomorphism_ring` takes as an argument elliptic curves over finite field.

```
sage: E = EllipticCurve(GF(23),[12,4])
sage: O = Endomorphism_ring(E); O
Endomorphism ring of Elliptic Curve defined
by y^2 = x^3 + 12*x + 4 over Finite Field of size 23
sage: O.conductor()
1
sage: O.field()
Number Field in c with defining polynomial x^2 - 3*x + 23
```

By calling `.order()`, we can get the instance of class Order implemented in Sage. The class `Endomorphism` is a subclass of Isogeny class, thus we can construct endomorphisms as isogenies.

```
sage: f = x^10 + 13*x^9 + 4*x^8 + 8*x^7 + 6*x^6 +
20*x^5 + 11*x^4 + 5*x^3 + 15*x + 4
end = Endomorphism(E,kernel_polynomial = f)
Endomorphism of degree 21 on Elliptic Curve defined
by y^2 = x^3 + 12*x + 4 over Finite Field of size 23
```

In addition, we can print out corresponding element of order in quadratic number field. This requires computing endomorphism ring with class `Endomorphism_ring`.

```
sage: end.order_element(), end.order_element().parent()
(c - 2, Number Field in c with
defining polynomial x^2 - 3*x + 23)
```

We can also pass as an argument to constructor an element of the order:

```
sage: end = Endomorphism_ring(E,element = c-2); end
Endomorphism of degree 21 on Elliptic Curve defined
by y^2 = x^3 + 12*x + 4 over Finite Field of size 23
```

The methods for dual and trace of endomorphism and trace are also implemented:

```
sage: end.trace()
-1
sage: end.dual()
Endomorphism of degree 21 on Elliptic Curve defined
by y^2 = x^3 + 12*x + 4 over Finite Field of size 23
sage: end.dual().order_element()
-c+1
## One can see (c-2)+(-c+1) = -1 = trace
```

Horizontal walks, Schoof's algorithm and other functions

The function horizontal_walk takes as an argument an elliptic curve and a list of triplets of the form (l, λ, n) where l is Elkies prime, λ is an eigenvalue of π_l and n is the number of steps along the ideal $(l, \pi - \lambda)$. Optional argument is algorithm, which is by default 'Elkies' but if algorithm = "Velu" is passed then Vélu algorithms are used. Implementation is based on Algorithms 3, 4 and 5.

```
sage: from libr.horizontal_walk import horizontal_walk
sage: p = 3*2*3*5*7*11*13*17*19-1
sage: E = EllipticCurve(GF(p),[2558103,24391662])
sage: A = [(3, 2, 50),(5, 4, 72),
(7, 5, -32), (11, 9, 44),
(13, 12, -72), (19, 8, -65)]
sage: horizontal_walk(E,A)
25832645
sage: horizontal_walk(E,A,algorithm = 'Velu')
25832645
```

The function volcano_schoof computes the trace of given elliptic curve E. The algorithm is based on the work of Fouquet and Morain in [FM02] with addition of our algorithm for case $l = 2$.

```
sage: from libr.volcano_schoof import volcano_schoof
sage: E = EllipticCurve(GF(17),[3,16])
sage: volcano_schoof(E)
3
```

The computation of depth of volcano through algorithms due to Fouquet and Morain is available with function volcano_depth.

```
sage: from libr.volcano_depth import volcano_depth
sage: E = EllipticCurve(GF(101),[3,16])
sage: volcano_depth(E,2)
1
```

Algorithm 2 is implemented through function `is_supersingular`:

```
sage: from libr.supersingular import is_supersingular
sage: E = EllipticCurve(GF(101),[1,1])
sage: is_supersingular(E)
False
sage: E = EllipticCurve(GF(101),[0,1])
sage: is_supersingular(E)
True
```

For easier understanding of the implementation we have prepared files in Jupyter Notebook with all the examples presented.

Bibliography

[Bai01] Harald Baier. Elliptic curves of prime order over optimal extension fields for use in cryptography. In C. Pandu Rangan and Cunsheng Ding, editors, *Progress in Cryptology — INDOCRYPT 2001*, pages 99–107, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[BGSV09] Bisson, Gaetan, Sutherland, and Andrew V. Computing the endomorphism ring of an ordinary elliptic curve over a finite field, Mar 2009.

[BLS10] Reinier Broker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *arXiv e-prints*, page arXiv:1001.0402, January 2010.

[BP98] Daniel V. Bailey and Christof Paar. Optimal extension fields for fast arithmetic in public-key algorithms. In *CRYPTO*, 1998.

[CFA$^+$12] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition*. Chapman and Hall/CRC, 2nd edition, 2012.

[CLM$^+$18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. Csidh: An efficient post-quantum commutative group action. *Lecture Notes in Computer Science Advances in Cryptology – ASIACRYPT 2018*, page 395–427, 2018.

[Con18] Keith T. Conrad. The conductor ideal. https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf, 2018.

[Cox13] David A. Cox. *Primes of the form* $p = x^2 + y^2n$. John Wiley and Sons, Inc, 2013.

[CZ81] David G. Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. 1981.

[DF04] David Steven Dummit and Richard M. Foote. *Abstract algebra*. John Wiley and Sons, Inc., 2004.

[DF18] Luca De Feo. Exploring isogeny graphs. https://defeo.lu/, 2018.

[FKS18] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. Cryptology ePrint Archive, Report 2018/485, 2018. https://eprint.iacr.org/2018/485.

[FM02] Mireille Fouquet and François Morain. Isogeny volcanoes and the sea algorithm. *Lecture Notes in Computer Science Algorithmic Number Theory*, page 276–291, 2002.

[Fou01] Mireille Fouquet. Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques. thèse, École polytechnique, 2001.

[GHS02] Steven D. Galbraith, Florian Hess, and Nigel P. Smart. Extending the GHS Weil descent attack. In *Advances in cryptology–EUROCRYPT 2002 (Amsterdam)*, volume 2332 of *Lecture Notes in Computer Science*, pages 29–44. Springer, Berlin, 2002.

[GJ13] Joachim Von Zur Gathen and Gerhard Jurgen. *Modern Computer Algebra*. Cambridge University Press, 2013.

[Kit95] A. Yu. Kitaev. Quantum measurements and the Abelian Stabilizer Problem. *arXiv e-prints*, pages quant–ph/9511026, November 1995.

[Koh96] David R. Kohel. Endomorphism rings of elliptic curves over finite fields. 1996.

[Kup05] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, July 2005.

[KZ98] Kaneko and Zagier. Supersingular j-invariants, hypergeometric series and atkin's orthogonal polynomials., Jan 1998.

[Lou16] Gerard Jacques Louw. Elliptic curve cryptography. 2016.

[MS11] Dustin Moody and Daniel Shumow. Analogues of velu's formulas for isogenies on alternate models of elliptic curves. Cryptology ePrint Archive, Report 2011/430, 2011. https://eprint.iacr.org/2011/430.

[PCS11] Burgisser Peter, Michael Clausen, and Mohammad Amin Shokrollahi. *Algebraic complexity theory*. Springer, 2011.

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7(1):219–254, 1995.

[SGE] Sage. http://www.sagemath.org/.

[Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[Shu09] Daniel Shumow. Isogenies of Elliptic Curves: A Computational Approach. *arXiv e-prints*, page arXiv:0910.5370, October 2009.

[Sil11a] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer, 2011.

[Sil11b] Joseph H. Silverman. *The arithmetic of elliptic curves*. World Publishing Company, 2011.

[SL96] P. Stevenhagen and H. W. Lenstra. Chebotarev and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996.

[ST15] Joseph H. Silverman and John Torrence Tate. *Rational points on elliptic curves*. Springer, 2015.

[Sut11] Andrew V. Sutherland. Identifying supersingular elliptic curves. *arXiv e-prints*, page arXiv:1107.1140, July 2011.

[Sut12] Andrew Sutherland. Isogeny volcanoes. *arXiv e-prints*, August 2012.

[Sut17] Andrew Sutherland. Lectures on elliptic curves. https://math.mit.edu/classes/18.783/2017/index.html, 2017.

[Sut18] Andrew V. Sutherland. Modular polynomials. https://math.mit.edu/~drew/ClassicalModPolys.html, 2018.

[Was08] Lawrence C. Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2008.