UiO : Department of Mathematics
University of Oslo

Isogeny Graphs and Isogeny Volcanoes

Hana Barakzahi

Master's Thesis, Spring 2020

This master's thesis is submitted under the master's programme *Mathematics*, with programme option *Mathematics*, at the Department of Mathematics, University of Oslo. The scope of the thesis is 60 credits.

The front page depicts a section of the root system of the exceptional Lie group E_8, projected into the plane. Lie groups were invented by the Norwegian mathematician Sophus Lie (1842–1899) to express symmetries in differential equations and today they play a central role in various parts of mathematics.

Contents

Introduction

Isogeny graphs are a type of graphs, where the vertices represent elliptic curves and the edges represent isogenies. I will examine some of the structures of these graphs in this thesis. It turns out that the majority of the components of such a graph will be *volcanoes*, see Definition 4.5. This has applications in cryptography and number theory, because many algorithms are made more efficient by exploiting this structure. In most elliptic curve cryptography one is dependent on computing an elliptic curve with a given number of points over a fixed field. The *complex multiplication method* in Remark 4.8 uses the volcano structure to compute such an elliptic curve.

The first two chapters are background information about elliptic curves and isogenies, where I have included the necessary definitions and results that are needed to build the theory of chapter 3 and chapter 4. I have used [8] as reference for most of the first two chapter. In chapter 3 I will define, examine and derive some results about the isogeny graph. In chapter 4 I will define what a p-volcano is and show that most of the *components* of an p isogenous graph will be p-volcanoes. For these two chapter, I have essentially used [9] as reference. In appendix A I have listed some j-invariants of supersingular elliptic curves over finite fields because I needed them to make some of the examples of the thesis. In appendix B I have included some of the many isogeny graphs that I have computed as examples. In appendix C I have included tables that show some statistics of some isogeny graphs. In appendix D I have included code snippets of *Isogenic*, which is the program I made in connection to this thesis to compute the isogeny graphs and calculate the statistics.

I will construct the isogeny graphs using the modular polynomials, see Theorem 3.1. Usually it is the other way around. As mentioned in Example 3.1, the modular polynomials are calculated with the algorithm from [2]. This algorithm uses the volcano structure of chapter 4 to construct the modular polynomials. But all the results of chapter 4 in this thesis, are based on the modular polynomials. To make the isogeny graphs without the modular polynomials I would have to construct them using Velu's formula, see Section 2.5. As you can see from Example 2.1, it takes a lot of work to construct only one isogeny. I would not have been able to make enough isogeny graphs to study them as I wished to in this thesis if I had to construct the isogeny graphs with Velu's formula.

Chapter 1

Elliptic Curves

Let K be a perfect field and $\bar{K}$ an algebraic closure of K.

1.1 Weierstrass Equation

By a *Weierstrass curve (w-curve)* I will mean the solution set of a Weierstrass equation, which in the projective space $\mathbb{P}^2$ is the equation

$$Y^2Z + a_1XYZ + a_2YZ^2 = X^3 + a_3X^2Z + a_4XZ^2 + a_5Z^3, \tag{1.1}$$

where a_1, a_2, a_3, a_4 and $a_5 \in \bar{K}$. The point $\mathcal{O} = [0, 1, 0]$ satisfies the equation and is the unique point at the line at infinity.

One can get an equation with non-homogenous coordinates by substituting x with X/Z and y with Y/Z,

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5. \tag{1.2}$$

The solution set of this equation plus the point at infinity is also then a w-curve.

Definition 1.1. The w-curve is said to be *defined over K* when $a_1, a_2, a_3, a_4, a_5 \in K$. Points $P = (x, y)$ on a w-curve are said to be *K-rational* if $x, y \in K$.

1.2 Simpler Weierstrass Equation and Isomorphic w-curves

Definition 1.2. Let C_1 and C_2 be w-curves. A *morphism* from C_1 to C_2 is a map of the form

$$\phi\colon C_1 \to C_2, \qquad \phi = [f_1(x, y), f_2(x, y)]$$

where each f_i is on the form $f_i(x, y) = g_i(x, y)/h_i(x, y)$ where $g_i(x, y)$ and $h_i(x, y)$ are polynomials in two variables and have the property that for each $P \in C_1$, $h_i(P) \neq 0$.

Definition 1.3. Two w-curves C_1 and C_2 are *isomorphic* if there are morphisms $\phi_1 : C_1 \to C_2$ and $\phi_2 : C_2 \to C_1$ such that $\phi_1 \circ \phi_2$ is the identity map on C_2 and $\phi_2 \circ \phi_1$ is the identity map on C_1.

Theorem 1.1. *If char*$(K) \neq 2, 3$ *then the* w*-curve in Equation* (1.2) *is isomorphic to*

$$y^2 = x^3 + Ax + B \tag{1.3}$$

where $A = -27((a_1^2 + 4a_3)^2 - 24(2a_4 + a_1a_2))$ *and* $B = -54(-(a_1^2 + 4a_3)^3 + 36(a_1^2 + 4a_3)(2a_4 + a_1a_2) - 216(a_2^2 + 4a_5))$

Proof. The map

$$\phi\colon C_1 \to C_2, \qquad \phi(x, y) = \left(x, \frac{1}{2}(y - a_1x - a_2)\right) \tag{1.4}$$

from one w-curve to another, is a morphism:

Writing it as a linear transformation

$$\phi(x, y) = \begin{bmatrix} 1 & 0 \\ -1/2a_1 & 1/2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0 \\ -a_2 \end{bmatrix}$$

shows that it has an inverse

$$\phi^{-1}(x, y) = \begin{bmatrix} 1 & 0 \\ a_1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} - \begin{bmatrix} 0 \\ -1/2a_2 \end{bmatrix}.$$

So there exists an morphism from the first w-curve (1.2) to the other (1.4) that has an inverse.

The w-curves, C_1 and C_2, must hence be isomorphic. Therefore replacing y with $\frac{1}{2}(y - a_1x - a_2)$[1], which gives

$$y^2 = 4x^3 + (a_1^2 + 4a_3)x^2 + (2a_1a_2 + 2a_4)x + 3a_2^2 + 4a_5, \tag{1.5}$$

gives a simplified version of equation (1.2) (as long as the characteristic of K is not 2).

By also assuming that the characteristic of K is not 3, one can simplify further by replacing x with $\frac{x - 3(a_1^2 + 4a_3)}{36}$ and y with $\frac{y}{108}$,[2], which also is a morphism with an inverse, giving the simpler Weierstrass equation in the theorem. □

Two w-curves that are isomorphic may be given by different Weierstrass equations. But the following result narrows the possibilities.

Theorem 1.2. *If two w-curves are defined by* $y^2 = x^3 + a_1x + b_1$ *and* $y^2 = x^3 + a_2x + b_2$ *then they are isomorphic if and only if* $a_2 = u^4a_1$ *and* $b_2 = u^6b_1$ *for some* $u \in K \setminus \{0\}$.

Proof. See [8] in the proof of Theorem 10.1, chapter III.10. □

[1]Suggestion for this replacement was found in Silverman
[2]This replacement suggestion is also found in Silverman

1.3 The Discriminant Δ

For each Weierstrass equation (1.1) there is a quantity, the *discriminant* denoted Δ, defined as

$$\begin{aligned}\Delta = &-(a_1^2+4a_3)^2(a_1^2a_5+4a_3a_5-a_1a_2a_4+a_3a_2^2-a_4^2)-8(2a_4+a_1a_2)^3\\ &-27(a_2^2+4a_5)^2+9(a_1^2+4a_3)(2a_4+a_1a_2)(a_2^2+4a_5).\end{aligned}$$

If the characteristic of K is not 2 or 3 then the discriminant can be simplified to

$$\Delta = -16(4A^3+27B^2)$$

where A and B are as in Equation (1.3).

Definition 1.4. Let

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_2YZ^2 - X^3 - a_3X^2Z - a_4XZ^2 - a_5Z^3$$

Then the solution of $F(X,Y,Z)=0$ is a w-curve. A point P at a w-curve, C, is *nonsingular* if the Jacobi matrix of $F(X,Y,Z)$ at P has rank 1.

Definition 1.5. An *elliptic curve* is a w-curve where all the points on the w-curve are nonsingular.

Theorem 1.3. *A w-curve given by a Weierstrass equation is an elliptic curve if and only if* $\Delta \neq 0$.

Proof. See [8], chapter III.1, Proposition 1.4a i). □

1.4 The j-invariant

For each Weierstrass equation the j-invariant, denoted j, is defined as

$$j = \frac{((a_1^2+4a_3)^2-24(2a_4+a_1a_2))^3}{\Delta}.$$

If char$(K) \neq 2,3$, then j is simplified to

$$j = -1728\frac{(4A)^3}{\Delta}.$$

Where A is as in Equation (1.3).

It is called the j-invariant because it identifies isomorphism classes of elliptic curves over $\bar{K}$.

Theorem 1.4. *Two elliptic curves are isomorphic over $\bar{K}$ if and only if they both have the same j-invariant.*

Proof See [8], chapter III.1 b). □

Theorem 1.5. *Let $j_0 \in \bar{K}$. Then there exists an elliptic curve defined over K whose j-invariant is equal to j_0.*

Proof See [8], chapter III.1 c).

1.5 The Group Law

Theorem 1.6. *Let E be an elliptic curve defined by Equation* (1.1) *and let $l \subset \mathbb{P}^2$ be a line. Then $l \cap E$ consists of exactly three, not necessarily distinct, points.*

Proof. Since the degree of the Weierstrass equation is three, the line l must intersect E at three points. This is a result of Bèzout's theorem. □

Now I will define an *addition* operation for points on an elliptic curve.

Definition 1.6. Let *addition*, denoted as $+$, on an elliptic curve E be defined as the following. Let $P, Q \in E$ and let l be the line through P and Q. If $P = Q$ then l is the tangent line of E at P. Because of the theorem above this line will intersect at a third point on E, say R. Let l' be the line through R and $\mathcal{O}$. This line will also intersect E at a third point. Denote this third point by $P + Q$.

The algorithm for computing addition given points in affine coordinates is given in the following theorem.

Theorem 1.7. *Let E be an elliptic curve given by*

$$E\colon y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5.$$

Let $P_1 = (x_1, y_1) \in E$, then

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_2). \tag{1.6}$$

Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3) \in E$. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_2 = 0$, then

$$P_1 + P_2 = \mathcal{O}.$$

Otherwise $P_1 + P_2 = P_3$ where

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_3 - x_1 - x_2 \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_2. \end{aligned}$$

And where λ and ν are defined as following when $x_1 \neq x_2$

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\ \nu &= \frac{y_1x_2 - y_2x_1}{x_2 - x_1}. \end{aligned}$$

If $x_1 = x_2$ then

$$\begin{aligned} \lambda &= \frac{3x_1^2 + 2a_3x_1 + a_4 - a_1y_1}{2y_1 + a_1} \\ \nu &= \frac{-x_1^3 + a_4x_1 + 2a_5 - a_2y_1}{2y_1 + a_1x_1 + a_2}. \end{aligned}$$

Proof. See [8], chapter III.2., Group Law Algorithm 2.3. □

Theorem 1.8. *The addition defined in Definition 1.6 has the following properties*

1. *Let l be a line that intersects E at P, Q and R. Then $(P+Q)+R=\mathcal{O}$.*
2. *$P+\mathcal{O}=P$ for all $P \in E$.*
3. *$P+Q=Q+P$ for all $P, Q \in E$.*
4. *$(P+Q)+R=P+(Q+R)$ for all $P, Q, R \in E$.*

Proof. See [8], chapter III.2., Proposition 2.2. □

Theorem 1.9. *The addition defined in Definition 1.6 together with $\mathcal{O}$ as identity, makes E into an abelian group. Furthermore, If E is defined over K, then*

$$E(K)=\{(x,y) \in K^2 \colon y^2+a_1xy+a_2y=x^3+a_3x^2+a_4x+a_5\} \cup \{\mathcal{O}\}$$

is a subgroup of E.

Proof. The first statement follows from Theorem 1.8 2-4. The second statement is true because the operations used in the Weierstrass equation are field operations so that the result must also be in that field. □

Example 1.1. Let $K=F_5$ and let E be the elliptic curve

$$E\colon y^2+x^3+3,$$

defined over K. To find out what the K-rational points besides $\mathcal{O}$ on E are, I can check all the 25 candidates (x,y) where $x, y \in F_5$. That gives me that

$$\{\mathcal{O},(1,2),(2,1),(3,0),(1,3),(2,4)\}$$

are the K-rational points on E.

Now I want to add all the points using the addition defined in Definition 1.6, using the algorithms from Theorem 1.7 and the results from Theorem 1.8. According to Theorem 1.8 adding whichever point P to $\mathcal{O}$ you get $\mathcal{O}$. To add $(1,2)$ with itself I will use the algorithms from Theorem 1.7. Comparing E to the affine Weierstrass equation from Equation (1.2) gives,

$$a_1=0, \quad a_2=0, \quad a_3=0, \quad a_4=0, \quad a_5=3.$$

According to Equation (1.2), if $x_1=x_2$, which in the case where I want to add the point $(1,2)$ to itself is true, then I have to first check if $y_1+y_2+a_1x_2+a_2=0$.

$$y_1+y_2+a_1x_2+a_2=2+2+0+0=4 \neq 0.$$

Now the algorithm from Theorem 1.7 says that $(1,2)+(1,2)=(x_3,y_3)$, where

$$\begin{aligned}
x_3 &= \lambda^2+a_1\lambda-a_3-x_1-x_2 \\
&= \lambda^2-1-1 \\
&= \lambda^2-2, \\
y_3 &= -(\lambda+a_1)x_3-\nu-a_2 \\
&= -(\lambda)(\lambda^2-2)-\nu
\end{aligned}$$

where, when $x_1 = x_2$,

$$\begin{aligned}\lambda &= \frac{3x_1^2 + 2a_3x_1 + a_4 - a_1y_1}{2y_1 + a_1} \\ &= \frac{3 * 1^2 + 2 * 0 + 0 - 0}{2 * 2} \\ &= 3 * 4^1 = 2 \text{ mod } 5. \\ \nu &= \frac{-x_1^3 + a_4x_1 + 2a_5 - a_2y_1}{2y_1 + a_1x_1 + a_2} \\ &= \frac{-1^3 + 0 + 2 * 3 - 0}{2 * 2 + 0 + 0} \\ &= \frac{0}{4} \\ &= 0.\end{aligned}$$

So

$$\begin{aligned}(1,2) + (1,2) &= (\lambda^2 - 2, -\lambda(\lambda^2 - 2) - \nu) \\ &= (2, -4) \\ &= (2, 1).\end{aligned}$$

Now I want to add $(2,1)$ to $(3,0)$. The algorithm from Theorem 1.7 says that

$$(2,1) + (3,0) = (\lambda^2 + a_1\lambda - a_3 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_2)$$

where, when $x_1 \neq x_2$,

$$\begin{aligned}\lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\ &= \frac{0 - 1}{3 - 2} \\ &= -1 = 4 \text{ mod } 5, \\ \nu &= \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \\ &= \frac{1 * 3 - 1 * 0}{3 - 2} \\ &= 3\end{aligned}$$

So

$$\begin{aligned}(2,1) + (3,0) &= (4^2 - 2 - 3, -4(4^2 - 2 - 3) - 3) \\ &= (-4, -4) = (1, 3).\end{aligned}$$

When adding $(2,1)$ and $(2,4)$, the algorithm says that if $x_1 = x_2$ as here, then I have to check if $y_1 + y_2 + a_1x_2 + a_2 = 0$

$$y_1 + y_2 + a_1x_2 + a_2 = 1 + 4 + 0 + 0 = 0$$

So

$$(2,1) + (2,4) = \mathcal{O}$$

Using the algorithm to calculate $P_1 + P_2$ for all $P_1, P_2 \in E/K$, except when $P_1 \neq P_2$ and $P_2 \neq P_1$ because addition is commutative according to 3. in Theorem 1.8, gives the result,

$$\begin{aligned}
\mathcal{O} + \mathcal{O} &= \mathcal{O}\\
\mathcal{O} + (1,2) &= (1,2)\\
\mathcal{O} + (2,1) &= (2,1)\\
\mathcal{O} + (3,0) &= (3,0)\\
\mathcal{O} + (1,3) &= (1,3)\\
\mathcal{O} + (2,4) &= (2,4)\\
(1,2) + (1,2) &= (2,1)\\
(1,2) + (2,1) &= (3,0)\\
(1,2) + (3,0) &= (2,4)\\
(1,2) + (1,3) &= \mathcal{O}\\
(1,2) + (2,4) &= (1,3)\\
(2,1) + (2,1) &= (2,4)\\
(2,1) + (3,0) &= (1,3)\\
(2,1) + (1,3) &= (1,2)\\
(2,1) + (2,4) &= \mathcal{O}\\
(3,0) + (3,0) &= \mathcal{O}\\
(3,0) + (1,3) &= (2,1)\\
(3,0) + (2,4) &= (1,2)\\
(1,3) + (1,3) &= (2,4)\\
(1,3) + (2,4) &= (3,0)\\
(2,4) + (2,4) &= (2,1).
\end{aligned}$$

As one can see the K-rational points on E are closed under the addition defined in Definition 1.6. Setting up the addition table for the K-rational points of E, see Table 1.1, shows that the 6 K-rational points of E is the cyclic, abelian group of 6 elements, which is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

+	$\mathcal{O}$	**(1,2)**	**(2,1)**	**(3,0)**	**(1,3)**	**(2,4)**
$\mathcal{O}$	$\mathcal{O}$	(1,2)	(2,1)	(3,0)	(1,3)	(2,4)
(1,2)	(1,2)	(2,1)	(3,0)	(2,4)	$\mathcal{O}$	(1,3)
(2,1)	(2,1)	(3,0)	(2,4)	(1,3)	(1,2)	$\mathcal{O}$
(3,0)	(3,0)	(2,4)	(1,3)	$\mathcal{O}$	(2,1)	(1,2)
(1,3)	(1,3)	$\mathcal{O}$	(1,2)	(2,1)	(2,4)	(3,0)
(2,4)	(2,4)	(1,3)	$\mathcal{O}$	(1,2)	(3,0)	(2,1)

Table 1.1

Theorem 1.10. *Let E be an elliptic curve. The equations in the algorithm from Theorem 1.7 define morphisms*

$$+\colon E \times E \to E, \qquad (P_1, P_2) \mapsto P_1 + P_2 \tag{1.7}$$

$$-: E \to E, \qquad P \mapsto -P \tag{1.8}$$

Proof. See [8], chapter III.3., Theorem 3.6. □

Chapter 2

Isogenies

Definition 2.1. Let E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism that sends the identity of E_1 to the identity of E_2.

By $\phi\colon E_1 \to E_2, \phi = \{\mathcal{O}\}$ I will mean the isogeny that sends all points of E_1 to the identity element of E_2.

Definition 2.2. Two elliptic curves E_1 and E_2 are *isogenous* if there exists an isogeny $\phi \neq \{\mathcal{O}\}$ from E_1 to E_2.

Definition 2.3. An isogeny is said to be *defined over* K if its coefficients are in K.

Theorem 2.1. *Let $\phi\colon E_1 \to E_2$ be an isogeny. Then ϕ must be either constant or surjective.*

Proof. See [8], chapter II.2., Theorem 2.3. □

Theorem 2.2. *Let $\phi\colon E_1 \to E_2$ be an isogeny. Then ker ϕ must be a finite group.*

Proof. See [8], chapter III.4., Corollary 4.9. □

2.1 Degree of an Isogeny and Separable Isogenies

Let $K(E)$ be the function field of E over K.

Let E_1 and E_2 be elliptic curves defined over K and let $\phi\colon E_1 \to E_2$ be a non-constant isogeny defined over K. I will define $\phi^*\colon K(E_2) \to K(E_1)$ as

$$\phi^* f = f \circ \phi.$$

Then $K(E_1)$ will be a finite extension of $\phi^*(K(E_2))$. For proof see [8], chapter II.2., Theorem 2.4. Now I can define what the *degree* of an isogeny should be.

Definition 2.4. Let $\phi\colon E_1 \to E_2$ be an isogeny defined over K. If ϕ is constant then define the *degree of* ϕ to be

$$\text{deg } \phi = 0.$$

Otherwise define the *degree of* ϕ to be

$$\text{deg } \phi = [K(E_1) : \phi^* K(E_2)].$$

Definition 2.5. An isogeny is defined to be *separable* when the field extension $K(E_1)/\phi^* K(E_2)$ is separable.

Theorem 2.3. *Let $\phi\colon E_1 \to E_2$ be an isogeny. If ϕ is separable, then*

$$\#\textit{ker}\ \phi = \textit{deg}\ \phi.$$

Proof. See [8], chapter III.4., Theorem4.10c). □

Theorem 2.4. *Let E_1, E_2 and E_3 be elliptic curves defined over K , let $\phi\colon E_1 \to E_2$ and $\psi\colon E_1 \to E_3$ be isogenies defined over K, where ψ is separable, and let ker$(\phi) \subset$ ker(ψ). Then there exists a unique isogeny $\lambda\colon E_2 \to E_3$, that is defined over K, such that $\psi = \lambda \circ \phi$.*

Proof. See [8], chapter III.4., Corollary 4.11. □

2.2 Two Relevant Isogenies

The following is an example of an isogeny.

Definition 2.6. For each $m \in \mathbb{Z}$ define the *multiplication-by-m-map* $[m]\colon E \to E$ by

$$[m](P) = P + \cdots + P$$

where P is added to itself m times, if $m > 0$. For $m < 0$ set

$$[m](P) = [-m](-P).$$

And if $m = 0$ set

$$[0](P) = \mathcal{O}.$$

Theorem 2.5. *The multiplication-by-m-map is an isogeny and it has degree equal to m^2.*

Proof. The group law operation on elliptic curves is a morphism according to theorem (1.8) and so by induction adding P to itself m times will also be a morphism. And $\mathcal{O}$ is sent to $\mathcal{O}$. Hence the map is an isogeny. For proof of the degree of the multiplication-by-m-map see [8], chapter III.4, the discussion at page 69. □

Theorem 2.6. *The multiplication-by-m-map is separable if and only if char$(K) \nmid m$.*

Proof. See [9], lecture 6, Theorem 6.24. □

Definition 2.7. Let $m \in \mathbb{Z}$ and $m \geq 1$. The *m-torsion subgroup of* ***E***, denoted $E[m]$, is the set of points of E of order m.

$$E[m] = \{P \in E\colon [m]P = \mathcal{O}\}$$

The kernel of the multiplication-by-m-map is the m-torsion subgroup.

Theorem 2.7. *Let $m \in \mathbb{Z}$ such that char$(K) \nmid m$, then*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Proof. See [8], chapter III.6, corollary 6.4. □

Another example of an important isogeny, that I will use in this thesis, is the Frobenius map. Which fixes the K-rational points of an elliptic curve and sends the other points to other points at the same curve.

Definition 2.8. Let $K = \mathbb{F}_q$ be a finite field with q elements. The *qth-power Frobenius map* is the map

$$\phi \colon E \to E$$

where

$$\phi(X, Y) = (X^q, Y^q).$$

Theorem 2.8. *The Frobenius map fixes the K- rational points on the elliptic curve:*

$$x^q = x \text{ for any } x \in F_q$$

$$y^q = y \text{ for any } x \in F_q$$

Proof. This is true because of Fermat's little theorem. □

Theorem 2.9. *The Frobenius map is an isogeny.*

Proof. See [8]. □

2.3 The Dual Isogeny

Theorem 2.10. *Let $\phi \colon E_1 \to E_2$ be a non-constant isogeny with degree m. Then there exists a unique isogeny $\hat{\phi} \colon E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [m]$.*

Proof. See [8], chapter III.6., Theorem 6.1. □

Uniqueness in the theorem is not uniqueness up to isomorphism.

Definition 2.9. The unique isogeny in Theorem 2.10, denoted by $\hat{\phi}$, is called the *dual isogeny* of ϕ if $\phi \neq [0]$. If $\phi = [0]$ then the dual isogeny of ϕ is set to be $\hat{\phi} = [0]$ as well.

Theorem 2.11. *Let $\phi \colon E_1 \to E_2$ be an isogeny and let deg $\phi = m$. Then*

1. $$\hat{\phi} \circ \phi = [m] \text{ on } E_1$$

   and

   $$\phi \circ \hat{\phi} = [m] \text{ on } E_2$$

2. *Let $\psi \colon E_2 \to E_3$ be another isogeny. Then*

   $$\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$$

3. *Let $\lambda \colon E_1 \to E_2$ be another isogeny. Then*

   $$\widehat{\lambda + \phi} = \hat{\lambda} + \hat{\phi}$$

4. *For all $m \in \mathbb{Z}$,*
$$\widehat{[m]} = [m]$$
5. *deg $\hat{\phi}$ = deg ϕ*
6. $\hat{\hat{\phi}} = \phi$

Proof. See [8], chapter III.6., Theorem 6.2. □

2.4 End(E) and Aut(E)

Let the set of isogenies between two elliptic curves E_1 and E_2 be denoted by Hom(E_1, E_2) and define addition between isogenies as

$$(\phi + \psi)(P) = \phi(P) + \psi(P). \tag{2.1}$$

Where $+$ in the right hand side of the equation is the addition of elliptic curves as defined in Definition 1.6. This will be a new morphism. And $\phi = \{\mathcal{O}\}$ is also a isogeny. From this follows:

Theorem 2.12. *Hom(E_1, E_2) given with addition as defined in (2.1) is a group with $\{\mathcal{O}\}$ as the identity element.*

Proof. See [8] □

Let $E_1 = E_2$. Then composing isogenies in Hom(E, E) is allowed, so define multiplication between isogenies as

$$(\phi\psi)(P) = \phi(\psi(P)). \tag{2.2}$$

Let End(E) = Hom(E, E).

Theorem 2.13. *The two operations isogeny addition defined in equation (2.1) and composing isogenies as the multiplication defined in equation (2.2) makes End(E) into a ring.*

Proof. See [8] □

Let Aut(E) denote the set of the invertible elements of End(E).

Theorem 2.14. *Aut(E) is a group.*

Proof. See [8] □

End(E) is therefore called the *endomorphism ring of E* and Aut(E) is called the *automorphism group of E*.

Theorem 2.15. *Let E/K be an elliptic curve. If $j(E) \neq 0$ and $j(E) \neq 1728$ then Aut(E) consists of only two elements. The identity automorphism $id\colon E \to E$ where $id(P) = P$ and the automorphism $-\colon E \to E$ where $-(P) = -P$. When char(K) $\neq 2$ and char(K) $\neq 3$ and if $j(E) = 0$ #Aut(E)$= 6$ and for $j(E) = 1728$ #Aut(E)$= 4$. If char(K) $= 2$ and $j(E) = 0 = 1728$ then #Aut(E) $= 24$. If char(K) $= 3$ and $j(E) = 0 = 1728$ then Aut(E) $= 12$.*

Proof. See [8], chapter III.10., Theorem 10.1. and the proof of Theorem 10.1. □

2.5 Constructions of Isogenies (Velu's Formula)

Theorem 2.16. *Let E_1 be an elliptic curve and let $G \subset E_1$ be a finite subgroup of E. Then there exists a unique elliptic curve E_2 and a separable isogeny $\phi\colon E_1 \to E_2$ such that*

$$\textit{ker}\ \phi = G.$$

Proof. See [8], chapter III.4., Proposition 4.12. □

If two isogenies are constructed for a fixed subgroup G of E, then they have the same kernel equal to G. Which means that they must be isomorphic. Hence ϕ from the above theorem is unique up to isomorphism.

I will now show how to construct isogenies using Velu's formula. See [12]. Let $\text{char}(K) \neq 2, 3$. Let E_1 be an elliptic curve and choose G a subgroup of E_1. Then by Theorem 2.16 there exists a unique elliptic curve, let me call it E_2, and an isogeny $\phi\colon E_1 \to E_2$, such that its kernel is G. Velu's formula will construct an isogeny with G as the kernel explicitly as a rational function and give the Weierstrass equation of E_2. The following are the steps.

1. Choose an elliptic curve, E_1, on simple Weierstrass form.

$$E\colon y^2 = x^3 + ax + b \tag{2.3}$$

2. Choose a subgroup G of E_1 with odd order.

3. Because G is a group, if $P \in G$ then $-P \in G$ as well. Partition $G - \{\mathcal{O}\}$ into G^+ and G^- where $P \in G^+$ if and only if $-P \in G^-$. Now for each point $P \in G^+$ calculate the quantities

$$g_P^x = 3x_P^2 + a, \qquad g_P^y = -2y_P,$$

$$v_P = 2g_P^x, \qquad u_P = (g_P^y)^2,$$

$$v = \sum_{P \in G^+} v_P, \qquad w = \sum_{P \in G^+} u_P + x_P v_P.$$

4. Now the isogeny $\phi\colon E_1 \to E_2$ will be

$$\phi(x, y) = \left(x + \sum_{P \in G^+} \frac{v_P}{x - x_P} - \frac{u_P}{(x - x_P)^2}, y - \sum_{P \in G^+} \frac{2u_P y}{(x - x_P)^3} + v_P \frac{y - y_P - g_P^x g_P^y}{(x - x_P)^2} \right)$$

5. where E_2 is

$$E_2\colon y^2 = x^3 + (a - 5v)x + (b - 7w).$$

Remark 2.1. Because I have simplified some by writing the equation for the elliptic curve on simple Weierstrass form, the field K can not have characteristic 2 or 3 with this method. Also, I have done some simplifications so that the algorithm can be as simple as the steps above, and a consequence of that is that the order of the chosen subgroup G can not be an even number. To see how to construct an isogeny when $\text{char}(K)$ is 2 or 3 or when the order of G is even, see [12].

Example 2.1. Let $K = F_5$ be the finite field with 5 elements. Let E_1 be

$$E_1 \colon y^2 = x^3 + 1 \tag{2.4}$$

Then there are 6 F_5-rational points on E_1. $\{\mathcal{O}, (0,1), (0,4), (4,0), (2,2), (2,3)\}$. This set must be a group by Theorem 1.9. I found the F_5-rational points of E_1 by checking all the possibilities (x, y) where $0 \leq x \leq 5$ and $0 \leq y \leq 5$. Hence, for F_5 there were only 25 coordinates to check. For bigger fields there exists algorithms to do this.

Now I will have to choose a subgroup of this group. The order of a subgroup must divide the order of group. Hence the nontrivial possibilities are of order 2 or 3. The identity $\mathcal{O}$ must be in the group. Then choosing freely the next point, $(0,1)$. To make a subgroup I must then also include $-(0,1)$. To find out which point that is, i will use the algorithm defined in Equation (1.6) from Theorem 1.7, which gives

$$\begin{aligned} -(0,1) &= (0,-1) \\ &= (0,4). \end{aligned}$$

Now $G = \{\mathcal{O}, (0,1), (0,4)\}$ is a subgroup. This will be the kernel of the isogeny I am constructing. Now I will partition $G - \mathcal{O}$ into $G^+ = \{(0,1)\}$ and $G^- = \{(0,4)\}$. Now I can calculate the four quantities from step 3 above. There is only one point in G^+, (0, 1). Hence

$$g_P^x = 0, \qquad g_P^y = -2,$$

$$v_P = 0, \qquad u_P = 4,$$

$$v = 0, \qquad w = 4.$$

And the isogeny $\phi \colon E_1 \to E_2$ will be

$$\phi(x,y) = \left(x - \frac{4}{x^2}, y - \frac{8y}{x^3}\right).$$

Where E_2 is

$$E_2 \colon y^2 = x^3 + 3.$$

There are 6 F_5-rational points on E_2, $\{\mathcal{O}, (3,0), (1,2), (1,3), (2,1), (2,4)\}$. This is the group from Example 1.1 seen in Table 1.1. The subgroup G of F_5-rational points on E_2 has the cosets G and $\{(2,2), (2,3), (4,0)\}$. ϕ will send the points of G to $\mathcal{O}$ and the points of $\{(2,2), (2,3), (4,0)\}$ to $(3,0)$.

Chapter 3

Isogeny Graphs

In this chapter I will define a type of graph that will show which elliptic curves that are isogenous, by making the vertices of the graph represent elliptic curves and the edges represent isogenies.

3.1 The N-Isogeny Graph $G_N(F_q)$

First I will introduce a polynomial in $\mathbb{Z}[X, Y]$, that will actually give the j-invariants of elliptic curves that are isogenous by a certain type of isogeny, as its zeros.

By a *cyclic isogeny* I will mean an isogeny where the kernel is a cyclic group. By a *N-isogeny* I will mean an isogeny with N elements in the kernel.

Theorem 3.1. *There exists a polynomial, $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$, for $N \in \mathbb{Z}$, that is symmetric in X and Y with degree $N + 1$ in both X and Y, such that the following holds. For all $j_1, j_2 \in K$, $\Phi_N(j_1, j_2) = 0$ over K if and only if j_1 and j_2 are the j-invariants of elliptic curves defined over K that are related by a cyclic isogeny of degree N defined over K.*

Proof. See [9], lecture 21. □

I will call the polynomial from Theorem 3.1, the *N-modular polynomial*.

Remark 3.1. It makes sense to look at $\Phi_N(X, Y)$ over K because the coefficients of $\Phi_N(X, Y)$ are in $\mathbb{Z}$ and there is a ring homomorphism from $\mathbb{Z}$ to any field K. By a coefficient c of $\Phi_N(X, Y)$ in K, I will mean the image of c by the unique ring homomorphism from $\mathbb{Z}$ to K, sending 1 to the identity element of K.

Remark 3.2. The j-invariants do not determine the elliptic curves uniquely. If K is algebraically closed the j-invariants determine the elliptic curves uniquely up to isomorphism. If K is not an algebraically closed field, then there may be two (or more) different elliptic curves over K that have the same j-invariants but that are not isomorphic over K. I will discuss this further in Section 3.3.

Remark 3.3. The pair (j_1, j_2) does not determine a cyclic isogeny uniquely either, not even up to isomorphism. In Section 3.2 I will discuss the requirements needed for the pair to define an isogeny uniquely up to isomorphism.

I will now define a type of graph for each $N \in \mathbb{Z}$ and each finite field K. Let the vertices of the graph be the elements of $K = F_q$. Because of Theorem 1.5 each element in F_q is the j-invariant of an elliptic curve defined over K. Let the edges be all pairs (j_1, j_2) between vertices $j_1, j_2 \in F_q$ if there exists an cyclic N-isogeny, defined over K, from an elliptic curve with j-invariant equal to j_1 to an elliptic curve with j-invariant equal to j_2.

But first I will define what the multiplicity of a zero of $\Phi_N(X, Y)$ should be.

Definition 3.1. Let the *multiplicity* of a root (j_1, j_2) of $\Phi_N(X, Y)$ be the multiplicity of j_2 as a root of $\Phi_N(j_1, Y) = \Phi_N(Y)$.

Remark 3.4. I could have just as well defined the multiplicity of (j_1, j_2) as the multiplicity of j_1 as a root of $\Phi_N(X, j_2)$. Of course if j_2 is a root of $\Phi_N(j_1, Y)$, then j_1 is a root of $\Phi_N(X, j_2)$ and because $\Phi_N(X, Y)$ is symmetric in X and Y, if j_2 is a root of $\Phi'_{N,X=j_1}(Y)$ then j_1 is a root of $\Phi'_{N,Y=j_2}(X)$. Hence, the multiplicity of j_2 as a root of $\Phi_N(j_1, Y)$ is the same as the multiplicity of j_1 as a root of $\Phi_N(X, j_2)$.

Definition 3.2. Let $K = F_q$ be a finite field and let $N \in \mathbb{Z}$. The N-*isogenious graph* $G_N(K)$ is the directed graph with the vertex set equal to F_q and edges (j_1, j_2), present with multiplicity, where $j_1, j_2 \in K$, will be the zeros of $\phi_N(X, Y)$.

Each vertex will represent the j-invariant of (several) elliptic curves defined over K and because of Theorem 3.1 the zeros (j_1, j_2) of $\Phi_N(X, Y)$ will give the edges.

The dual isogeny ensures that $\Phi_N(j_1, j_2) = \Phi_N(j_2, j_1)$. So, if (j_1, j_2) is an edge in the graph then (j_2, j_1) is also an edge on the graph. If the multiplicity of (j_1, j_2) is also the same as the multiplicity of (j_2, j_1) then I will represent both directed edges with one undirected edge. However, there may be graphs where there are pairs of vertices j_1, j_2 where the multiplicity of (j_1, j_2) is not the same as the multiplicity of (j_2, j_1). Between such vertices there will be drawn directed edges. I will explain more how this can happen later in this chapter.

Example 3.1. Choosing $N = 3$ and $q = 7$, I want to draw the graph $G_3(F_7)$. The vertices will be the set $F_q = \{0, 1, 2, 3, 4, 5, 6\}$. The edges are the the zeros of $\Phi_3(X, Y)$ in F_7. The polynomial $\Phi_3(X, Y)$ itself can be found at [7] where it is calculated based on the algorithms from [2].

$$\begin{aligned}\Phi_3(X,Y) &= 1855425871872000000000X + 1855425871872000000000Y\\ &- 770845966336000000XY + 452984832000000X^2\\ &+ 452984832000000Y^2 + 8900222976000X^2Y + 8900222976000XY^2\\ &+ 2587918086X^2Y^2 + 36864000X^3 + 36864000Y^3\\ &- 1069956X^3Y - 1069956Xy^3 + 2232X^3Y^2 + 2232X^2Y^3\\ &- X^3Y^3 + X^4 + Y^4\\ &= X + Y + 2XY + 6X^2 + 6Y^2 + 6X^2Y + 6XY^2 + 5X^2Y^2 + 5X^3\\ &+ 5Y^3 + X^3Y + XY^3 + 6X^3Y^2 + 6X^2Y^3 + 6X^3Y^3 + X^4 + Y^4 \text{ mod } 7\end{aligned}$$

$$\begin{aligned}\Phi_3(X,Y) &= 0 \text{ mod } 7\\ (X,Y) &\in \{(0,0),(0,3),(2,2),(3,0),(4,5),(5,4),(6,6)\}\end{aligned}$$

To find the multiplicity of $(0,0)$ I will find the multiplicity of 0 in $\Phi_3(0,Y)$, according to Definition 3.1.

$$\begin{aligned}\Phi_{3,X=0}(Y) &= Y^4 + 5Y^3 + 6Y^2 + Y \text{ mod } 7\\ \Phi'_{3,X=0}(Y) &= 4Y^3 + Y^2 + 5Y + 1 \text{ mod } 7\\ \Phi'_{3,X=0}(0) &= 1 \neq 0 \text{ mod } 7\end{aligned}$$

Thus, the multiplicity of $(0,0)$ is 1. Similarly, to find the multiplicity of $(0,3)$ I must find the multiplicity of 3 in $\Phi_3(0,Y)$.

$$\begin{aligned}\phi_{3,X=0}(Y) &= Y^4 + 5Y^3 + 6y^2 + Y\\ \phi'_{3,X=0}(Y) &= 4Y^3 + Y^2 + 5Y + 1\\ \phi'_{3,X=0}(3) &= 0 \text{ mod } 7\\ \phi''_{3,X=0}(Y) &= 5Y^2 + 2Y + 5\\ \phi''_{3,X=0}(3) &= 0 \text{ mod } 7\\ \phi'''_{3,X=0}(Y) &= 3Y + 2\\ \phi''''_{3,X=0}(3) &= 4 \neq 0 \text{ mod } 7\end{aligned}$$

So the multiplicity of $(0,3)$ is 3. Now I want to find the multiplicity of $(3,0)$. To do so I must find the multiplicity of 0 in $\phi_3(3,Y)$.

$$\begin{aligned}\phi'_{3,X=3}(Y) &= 4Y^3 + 4Y^2 + 4\\ \phi'_{3,X=3}(0) &= 4 \neq 0\end{aligned}$$

So $(3,0)$ has multiplicity 1.
Calculate the remaining edges in similar fashion.

(0, 0) with multiplicity 1
(0, 3) with multiplicity 3
(2, 2) with multiplicity 1
(3, 0) with multiplicity 1
(4, 5) with multiplicity 1
(5, 4) with multiplicity 1
(6, 6) with multiplicity 4

Thus, the graph of $G_3(F_7)$ will be as in Figure 3.1.

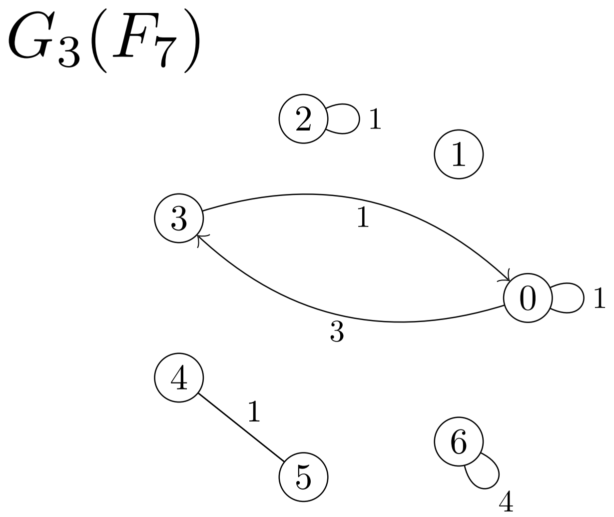

Figure 3.1: This is the 3-isogeny graph where the vertex set is the set of elements of F_7

Figure 3.1 shows a drawing of graph $G_3(F_7)$. There are 7 vertices, which are the j-invariants of elliptic curves. and some vertices have edges between them and some vertices dont. [1]

3.2 Edges Representing Isomorphism Classes of (Cyclic) Isogenies

If choosing N such that $\mathrm{char}(K) \nmid N$ then the kernel of a cyclic isogeny with N elements will be a separable isogeny by Theorem 2.6. Two separable isogenies are isomorphic if they have the same number of elements in the kernel. Therefore if $\mathrm{char}(K) \nmid N$, the multiplicity of an edge (j_1, j_2) will be the number of isomorphism classes of isogenies that exist between elliptic curves having j_1 and j_2 as j-invariants. The other graphs where $\mathrm{char}(K) \mid N$ are graphs where the edges still represent the existence of an isogeny between some elliptic curves having those vertices as j-invariants, but the multiplicities no longer represent the number of isomorphism classes of isogenies.

[1] Remember when I have drawn single undirected edges there are actually 2 edges between the vertices. For example from vertex 4 to vertex 5 there is one directed edge. And one directed edge from 5 to 4.

If also choosing N to be a prime, then an isogeny of degree N will have a kernel of N elements. And a finite group with a prime number of elements must be a cyclic group. Therefore, when N is a prime, the cyclic isogenies are all the isogenies of degree N.

3.3 Vertices Representing Isomorphism Classes of Elliptic Curves

As discussed in Remark 3.2, each element in a finite field K is the j-invariant of an elliptic curve by Theorem 1.5. Since K is not algebraically closed, Theorem 1.4 does not apply. Hence there may be two or more elliptic curves having the same j-invariant, and therefore are isomorphic over $\bar{K}$, but that are not isomorphic over K. For a $j \in K$, let E be an elliptic curve such that its j-invariant is j. I will call the set of all elliptic curves that are isomorphic to E for $Twist((E, O)/K)$.

Theorem 3.2. *Assume that char$(K) \neq 2, 3$ and let*

$$n = \begin{cases} 2 & \textit{if } j(E) \neq 0, 1728, \\ 4 & \textit{if } j(E) = 1728, \\ 6 & \textit{if } j(E) = 0. \end{cases}$$

Then Twist$((E, O), K)$ is canonically isomorphic to $K^*/(K^*)^n$.

Proof. See [8], chapter X.5, proposition 5.4 and corollary 5.4.1. □

Corollary 3.1. *Let $K = F_q$ be a finite field where $q \neq 2, 3$. For each element $j \in F_q$ such that $j \neq 0, 1728$ mod q, there are two isomorphism classes of elliptic curves over K that have j as their j-invariants.*

Proof. Since $j \neq 0, 1728$ mod q, $n = 2$ in Theorem 3.2. And so

$$\text{Twist}((E, O)/K) = K^*/(K^*)^2 = \mathbb{Z}/2\mathbb{Z}.$$

There are two elements in $\mathbb{Z}/2\mathbb{Z}$. □

Even though there are two different elliptic curves having the same j-invariant this does not pose a problem for the definition of isogeny graphs and the results about them in this chapter because of the following results.

Theorem 3.3. *Let E_1 be an elliptic curve, defined over $K = F_q$, and let E_2, also defined over $K = F_q$, be another elliptic curve with the same j-invariant as E_1. Then there is an F_q-rational isogeny of degree p from E (to some other elliptic curve) if and only if there is an F_q-rational isogeny of degree p from E_2.*

Proof. See [4]. □

Theorem 3.4. *Let E_1 be an elliptic curve, defined over $K = F_q$, and let E_2, also defined over $K = F_q$, be another elliptic curve with the same j-invariant as E_1. Then*

$$\textbf{\textit{End}}(E_1) \cong \textbf{\textit{End}}(E_2)$$

Proof. See [4]. □

3.4 Some Expected Structures in the N-Isogenous Graph

Example 3.2. When looking at Figure 3.2, the graph of $G_2(F_7)$ shows that there exists an isogeny of degree 2 from an elliptic curve with j-invariant equal to 2 to an elliptic curve with j-invariant equal to 0. Let's call it $\phi\colon E(2) \to E(0)$. From $G_3(F_7)$ shown in Figure 3.3 one can see that there exists an isogeny of degree 3 from an elliptic curve with j-invariant equal to 0 to an elliptic curve with j-invariant equal to 3. I will call this isogeny for $\psi\colon E(0) \to E(3)$. If two such isogenies exists, I can compose the isogenies to a new cyclic isogeny $\psi \circ \phi\colon E(2) \to E(3)$. For each point $P \in (\psi \circ \phi)(E_2)$, $\#\psi^{-1}(P) = \text{deg}\psi = 3$. And for each point Q in $\phi(E_2)$, $\#\phi^{-1}(Q) = 2$. Hence $\text{deg}(\psi \circ \phi) = 2 \cdot 3 = 6$. Hence this isogeny must exist as an edge in the graph of $G_6(F_7)$ where the edges represent isogenies of degree 6. Looking at this graph in Figure 3.4 shows that there indeed exists an edge between the vertices 2 and 3. The same applies to any other cyclic isogenies from different N-isogenous graphs over the same finite field, not only for 2 and 3.

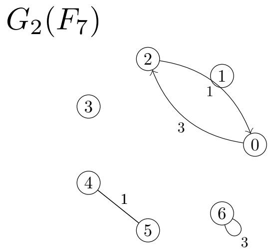

Figure 3.2: This is the 2-isogeny graph where the vertex set is the elements of F_7

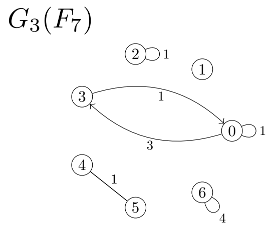

Figure 3.3: This is the 3-isogeny graph where the vertex set is the set of elements of F_7

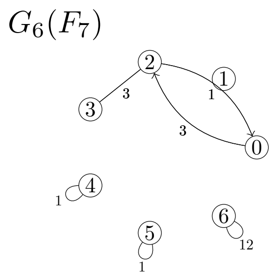

Figure 3.4: This is the 6-isogeny graph where the vertex set is the set of elements of F_7

Actually, all isogenies can be decomposed into a composition of isogenies of prime degree as in Example 3.2.

Theorem 3.5. *Let E_1 and E_2 be elliptic curves over K and let $\phi\colon E_1 \to E_2$ be a separable isogeny that is defined over K. Then*

$$\phi = \phi_1 \circ \cdots \circ \phi_k \circ [m]$$

where $\phi_1, \ldots, \phi_k$ are isogenies with a prime degree defined over K.

Proof. Let the degree of ϕ be $d = p_1^{e_1} \cdots p_k^{e_k}$ where p_i are primes. Because ϕ is separable, its kernel is a group with d elements. This group has subgroups $\mathbb{Z}/p_i\mathbb{Z}$ for each p_i that divide d. Because of Theorem 2.16 there exist isogenies, ϕ_i, with these groups as kernels. Now for each i, $\text{ker}(\phi_i) \subset \text{ker}(\phi)$, and so Theorem 2.4 says that there must exist a unique isogeny λ defined over K, such that $\phi = \lambda \circ \phi_i$. Hence ϕ must be composed of at least k isogenies, all of which have prime degree. Now let m be the largest integer such that $E[m] \subset ker(\phi)$. Then there must be some isogeny with $E[m]$ as kernel by Theorem 2.16. Of course the multiplication-by-m-map has $E[m]$ as its kernel. Then ϕ must be composed of $\psi \circ [m]$ for some isogeny ψ. □

Example 3.3. For every power of prime q, there is also the Frobenius endomorphism on elliptic curves defined over the finite field F_q. Recall that the identity element is here $\mathcal{O} = [0, 1, 0]$. So to find the kernel of a Frobenius map I have to solve the equations $x^q = 0$ and $y^q = 1$. The solutions are all $(0, w)$ such that w is the q-th root of 1. Since there are q q-th root of 1, there must be q elements in the kernel of the Frobenius map.

Endomorphisms are represented in the N-isogenous graph as self-loops. Therefore, due to the existence of the Frobenius endomorphism, the graphs of $G_q(F_q)$ are expected to have self-loops for all its vertices. The figures Figure 3.5-Figure 3.7 below shows examples of such graphs, which indeed agree with the observation.

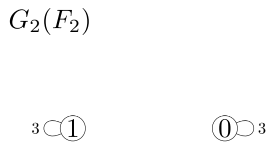

Figure 3.5: This is the 2-isogeny graph where the vertex set is the elements of F_2

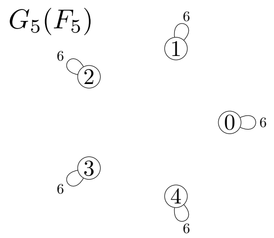

Figure 3.6: This is the 5-isogeny graph where the vertex set is the set of elements of F_5

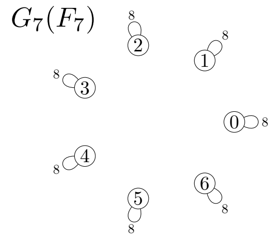

Figure 3.7: This is the 7-isogeny graph where the vertex set is the set of elements of F_7

3.5 Number of Edges from a Given Vertex

Theorem 3.6. *Let E/K be an elliptic curve with j-invariant not equal to 0 or 1728 and let $p \neq char(K)$ be a prime. The number of isomorphism classes of isogenies defined over K from E is either 0, 1, 2 or $p + 1$.*

Proof. See [9]. □

Theorem 3.7. *Let K be a finite field. Let E_1 and E_2 be elliptic curves defined over K. If $End(E_1) \cong End(E_2)$, then the number of isomorphism classes of isogenies from E_1 are the same as the number of isomorphism classes of isogenies from E_2.*

Proof. See [4] □

Looking at the N-isogenous graphs in the examples so far, some vertices have undirected edges between them while some have directed edges from them. The existence of the dual isogeny ensures that if there exists an edge (j_1, j_2) then there must exists an edge (j_2, j_1). From the earlier discussion, when char$(K) \nmid N$ the multiplicity of the edges represents isomorphism classes of isogenies. But there is no guarantee that the number of isomorphic isogenies from an elliptic curve E_1 to an elliptic curve E_2 is the same as the number of isomorphic isogenies from E_2 to E_1.

Theorem 3.8. *Let E_1 and E_2 be elliptic curves. If $j(E_1) = 0$ and $j(E_2) \neq 0$ or $j(E_1) = 1728$ and $j(E_2) \neq 1728$, then there exist isogenies $\phi\colon E_1 \to E_2$ and $\psi\colon E_1 \to E_2$ that are different but isomorphic, but such that their dual isogenies $\hat{\phi}\colon E_2 \to E_1$ and $\hat{\psi}\colon E_2 \to E_1$ are not isomorphic.*

Proof. Let $\phi\colon E_1 \to E_2$ be an isogeny such that $\ker(\phi) \neq \{\mathcal{O}\}$ and let $\lambda\colon E_2 \to E_2$ be an automorphism. The kernel of an automorphism consists of $\mathcal{O}$ only. Therefore composing λ with ϕ in the following order will make the kernel remain as the kernel of ϕ,

$$\ker(\lambda \circ \phi) = \ker(\phi).$$

Hence $\lambda \circ \phi$ is isomorphic to ϕ. Let $\widehat{\lambda \circ \phi}$ be the dual isogeny of $\lambda \circ \phi$ and $\hat{\phi}$ the dual isogeny of ϕ. Then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$

where $\hat{\lambda}\colon E_2 \to E_2$ and $\hat{\phi}\colon E_2 \to E_1$. In this order, the kernel of $\hat{\phi} \circ \hat{\lambda}$ is not automatically the same as the kernel of $\hat{\phi}$. Hence $\widehat{\lambda \circ \phi}$ might not be isomorphic to $\hat{\phi}$. This implies that if there are different amount of automorphisms on one elliptic curve E_1 than on another E_2, then the number of isomorphic isogenies from E_1 to E_2 will be different than the number of isomorphic isogenies from E_2 to E_1. Since there are two automorphisms on elliptic curves where the j-invariant is not equal to 0 or 1728 and more than two automorphisms on an elliptic curve where the j-invariant is 0 or 1728, see Theorem 2.15, the number of isomorphic isogenies from E_1 to E_2 can only differ from the number of isomorphic isogenies from E_2 to E_1 if $j(E_1) = 0$ and $j(E_2) \neq 0$ or if $j(E_1) = 1728$ and $j(E_2) \neq 1728$. □

Hence the multiplicities, representing the number of isomorphism classes of isogenies, of one edge in $G_N(K)$ can be different from the edge in the opposite direction. Therefore the edges where there is not the same number of isomorphism classes of isogenies one way as in the opposite direction will have directed edges with different multiplicity. Whereas the edges that have the same multiplicity in both directions, will not need to be directed on the figures.

Theorem 3.9. *Let E_1 and E_2 be two elliptic curves with j-invariants j_1 and j_2 respectively. If $j_1 = 0$ and $j_2 \neq 0$, then the edge (j_1, j_2) will have multiplicity 3 and the edge (j_2, j_1) will have multiplicity 1 in $G_N(K)$. If $j_1 = 1728$ and $j_2 \neq 1728$ then the edge (j_1, j_2) will have multiplicity 2 and (j_2, j_1) will have multiplicity 1 in $G_N(K)$.*

Proof. See [9] □

Chapter 4

Isogeny Volcanoes

In this chapter I will study the isogeny graphs more and illuminate some of its structure.

In the succeeding I will not only assume that $\text{char}(K) \nmid N$, but that N is a prime. Hence the N-isogenous graph will be called the p-isogenous graph. K will be a finite field with a prime number of elements. And so I will examine the structure of the p-isogenous graph over F_q for primes p and q.

4.1 Supersingular and Ordinary Components

Let a *path* be a sequence of directed edges between vertices, such that the end vertex of one edge is the start vertex of the next. Then let a *connected* subgraph of the isogeny graph be a subgraph where there is a path from each vertex to every other vertex. I will now partition each isogeny graph into connected subgraphs. I will call each such subgraph a *component* of the $G_p(F_q)$ graph.

The kernel of the multiplication-by-q-map is $E[q]$. Since q is prime, the number of elements in $E[q]$ is either q or 1. So either

$$E[q] \cong \mathbb{Z}/q\mathbb{Z} \tag{4.1}$$

or

$$E[q] \cong \{0\}. \tag{4.2}$$

Consequently the elliptic curves can be distinguished into two cases.

Definition 4.1. The elliptic curves where the kernel of the multiplication-by-q map is isomorphic to $\mathbb{Z}/q\mathbb{Z}$ are called *ordinary elliptic curves* and the elliptic curves where the kernel of the multiplication-by-q map is trivial are called *supersingular elliptic curves*.

Theorem 4.1. *Let $\phi\colon E_1 \to E_2$ be an isogeny. Then E_1 is supersingular if and only if E_2 is supersingular. And E_1 is ordinary if and only if E_2 is ordinary.*

Proof. See [9], lecture 14, Theorem 14.1 □

Because of Theorem 4.1, the vertices in the components of the p-isogeny graph will either all be j-invariants of supersingular elliptic curves or ordinary elliptic curves. Accordingly, I will call the components where all the vertices are j-invariants of supersingular elliptic curves for *supersingular components* and the components of the graph where all the vertices are j-invariants of ordinary elliptic curves for *ordinary components*.

To see which j-invariants are vertices of supersingular components see Appendix A. To categorize which components of $G_p(F_q)$ are ordinary in the examples below, I will check if a vertex in the component is supersingular or not over F_q.

Example 4.1. Over F_{23} the j-invariants of supersingular elliptic curves are 0, 3, and 19 (see Appendix A). In $G_2(F_{23})$ all three are vertices in the same (and only) supersingular component shown in Figure B.27. This is not always the case. Over F_{53} the j-invariants of supersingular elliptic curves are 0, 46 and 50. In $G_2(F_{53})$ there are two supersingular components. They are shown in Figure 4.2 and Figure 4.3.

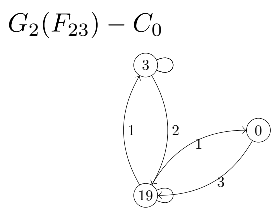

Figure 4.1: This is a supersingular component of the 2-isogeny graph where the vertex set is the elements of F_{23}

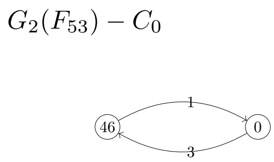

Figure 4.2: This is a supersingular component of the 2-isogeny graph where the vertex set is the set of elements of F_{53}

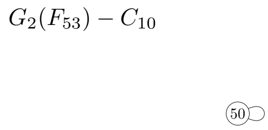

Figure 4.3: This is another supersingular component of the 2-isogeny graph where the vertex set is the set of elements of F_{53}

Remark 4.1. Some post quantum cryptography systems have been proposed given by hard problems based on the supersingular components.

1. Given two vertices, finding a sequence of isogenies between the two vertices in a supersingular component of the isogeny graph is hard. Which makes computing isogenies between two supersingular elliptic curves a hard problem.
2. Computing the endomorphism ring of a supersingular elliptic curve.
3. Computing the maximal order (see Definition 4.2) isomorphic to the endomorphism ring of a supersingular elliptic curve.

[3] proposed a PQC hash function which is based on the hard problem of finding a sequence of n-isogenies for a small prime n between supersingular elliptic curves. There are also key exchange protocols based on the above hard problems. See [6] and [5]. There are signature schemes, see [13] and public key encryption systems, see [6]. There are also public key encryption algorithm and key encapsulation mechanism, based on these hard problems, that is per today in the second round of NIST post-quantum cryptography standardization competition. See [1].

4.2 Horizontal and Vertical Edges

Definition 4.2. Let $\mathcal{K}$ be a $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. An *order* of $\mathcal{K}$ is a subring $\mathcal{R}$ of $\mathcal{K}$ that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Definition 4.3. Let the *Endomorphism algebra* $\text{End}^0(E)$ be defined as

$$\text{End}^0(E) = \text{End}(E) \otimes \mathbb{Q}.$$

Theorem 4.2. *If E is an ordinary elliptic curve, then $End^0(E) = \mathcal{K}$ is an imaginary quadratic field.*

Proof. See [9], lecture 14, Theorem 14.5. □

For each $m \in \mathbb{Z}$ there is a multiplication-by-m isogeny. If these are the only isogenies from E to itself, then End(E)$\cong \mathbb{Z}$. But over fintite fields F_q, the Frobenius endomorphism π_E is an example of an isogeny that is not in $\mathbb{Z}$. Therefore $\mathbb{Z}[\pi_E] \subseteq \text{End}(E)$. One says that E has *complex multiplication* when End(E) is not $\mathbb{Z}$. The following theorem shows which possibilities there are for End(E) to be.

Theorem 4.3. *Let E/K be an elliptic curve over a finite field $K = F_q$. The Endomorphism ring, End(E), of E is one and only one of the following*

1. *an order in an imaginary quadratic field*
2. *an order in a quaternion algebra*

Proof. For 1. see theorem 14.5 and for 2. see theorem 14.18, lecture 14 in [9]. □

As explained in Theorem 4.3 there are two possibilities for $\text{End}(E)$ when E is defined over a finite field. The following theorem show another way one could define ordinary and supersingular that has to do with the relationship between E being an ordinary or supersingular elliptic curve and $\text{End}(E)$.

Theorem 4.4. *Let K be a finite field and let E be an elliptic curve defined over K. Then E is ordinary if and only if* **End**(E) *is an order in an imaginary quadratic field.*

Proof. By the definition of order in Definition 4.2 and the definition of endomorphism algebra in Definition 4.3 $\text{End}(E)$ must be an order in $\text{End}^0(E)$. And by Theorem 4.2, $\text{End}^0(E)$ is an imaginary quadratic field. Thus, $\text{End}(E)$ is an order in an imaginary quadratic field. □

Theorem 4.5. *Let $\phi\colon E_1 \to E_2$ be an isogeny between ordinary elliptic curves. Then*

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

Proof. See theorem 23.3 from [9]. □

The following theorem show that there are more to know about the relationship between endomorphism rings of E_1 and E_2 other than that both are orders in the same imaginary quadratic field.

Theorem 4.6. *Let $\phi \colon E_1 \to E_2$ be an isogeny of degree p between ordinary elliptic curves E_1 and E_2 and let End$(E_1) \cong \mathcal{O}_1$ and End$(E_2) \cong \mathcal{O}_2$, where $\mathcal{O}_1$ and $\mathcal{O}_2$ are orders in the endomorphism algebras of E_1 and E_2. Then the following three are the only possibilities for $\mathcal{O}_1$ and $\mathcal{O}_2$.*

1. $\mathcal{O}_1 = \mathcal{O}_2$
2. $[\mathcal{O}_1 \colon \mathcal{O}_2] = p$
3. $[\mathcal{O}_2 \colon \mathcal{O}_1] = p$

Proof. Since E_1 and E_2 are ordinary elliptic curves, then $\text{End}^0(E_1) = \text{End}^0(E_2)$ by Theorem 4.5, is an imaginary quadratic field by Theorem 4.2. By Theorem 4.4, both $\text{End}(E_1) = \mathcal{O}_1$ and $\text{End}(E_2) = \mathcal{O}_2$ are orders in imaginary quadratic fields, and so they must both be the orders in the same imaginary quadratic field.

Now, let $\alpha \colon E_1 \to E_1$ be an isogeny. Then $\alpha \in \text{End}(E_1)$, and let it be represented as $\alpha \in \mathcal{O}_1$. And let $\beta \colon E_2 \to E_2$ also be an isogeny. Then $\beta \in \text{End}(E_2)$. And let β be the equivalent element in $\mathcal{O}_2$. Now the isogeny $\hat{\phi} \circ \beta \circ \phi$ is in $\text{End}(E_1)$, represented by $p\beta \in \mathcal{O}_1$. And the isogeny $\phi \circ \alpha \circ \hat{\phi}$ is in $\text{End}(E_2)$. Represented by $p\alpha \in \mathcal{O}_2$. So for each $\alpha \in \mathcal{O}_1$, $p\alpha$ is in $\mathcal{O}_2$. And for each $\beta \in \mathcal{O}_2$, $p\beta$ is in $\mathcal{O}_1$. □

Definition 4.4. Let $\phi \colon E_1 \to E_2$, $\mathcal{O}_1$ and $\mathcal{O}_2$ be as in Theorem 4.6. By the theorem there are three possibilities for $\mathcal{O}_1$ and $\mathcal{O}_2$. So ϕ can be distinguished by what the relation between the orders are. I will call ϕ *horizontal* if $\mathcal{O}_1 = \mathcal{O}_2$ and *vertical* if ϕ is not horizontal. the vertical isogenies can be further distinguished into two types. I will call ϕ *descending* if $[\mathcal{O}_1 \colon \mathcal{O}_2] = p$ and I will call ϕ *ascending* if $[\mathcal{O}_2 \colon \mathcal{O}_1] = p$.

Theorem 4.7. *Let E be an elliptic curve defined over K such that its endomorphism ring is isomorphic to an order in an imaginary quadratic field. Then there are 0 or 1 ascending p-isogenies from E depending on whether $p \nmid [\mathcal{O}_K \colon \mathcal{O}]$ or not, where $\mathcal{O}_K$ is maximal order in End$^0(E)$.*

Proof. Lemma 23.6 of lecture 23 from [9]

Theorem 4.8. *Let E_1 be an ordinary elliptic curve where End$(E_1) \cong \mathcal{O}$, then the number of (isomorphism classes of) isogenies $\phi \colon E_1 \to E_2$ where End$(E_2) \cong \mathcal{O}$ is either 0, 1 or 2.*

Proof. See chapter 25 of [4]. □

Remark 4.2. The number of (isomorphism classes of) isogenies from E_1 in Theorem 4.8 are still as in Theorem 3.6 but the number of isogenies from E_1 to an elliptic curve with the same endomorphism ring are 0, 1 or 2. The other isogenies from E_1 will vertical isogenies.

4.3 p-Volcanoes

Definition 4.5. Let $G_p(F_q)$ be the p-isogenous graph with the vertex set equal to F_q where q is prime. A *p-volcano* in $G_p(F_q)$ is a connected, undirected subgraph, that allows self-loops and multi-edges, whose vertices are partitioned into one or more *levels* $V_0, \ldots, V_d$ such that the following hold:

1. The subgraph on V_0 (the *surface*) is a regular graph of degree at most 2.
2. For $i > 0$, each vertex in V_i has exactly one edge to a vertex in level V_{i-1}. These are the only edges in the graph except for the edges in V_0.
3. For $i < d$, each vertex in V_i has degree $p + 1$.

Where the *degree* of a vertex j will be the number of roots of $\Phi_p(j, Y)$ counted with multiplicity. And the *degree* of a regular graph will be the degree of any of its vertices.

Remark 4.3. From the first look it might seem like 1. in Definition 4.5 is contradicting to 3. in terms of the degree of the vertices of V_0, but 1. says that the vertices of the subgraph V_0, has degree at most 2. Thus, the edges from vertices in V_0, that are not in the subgraph V_0 are not counted in 1. While in 3. the vertices of V_i for $i < d$ are seen as vertices of the whole graph.

Proposition 4.1. *Subgraphs of isogeny graphs that are regular graphs of degree at most two are volcanoes of depth $d = 0$. Such graphs can be categorized into one of the following types of regular graphs. A graph consisting of*

1. *one single vertex with no edges, which I will call a trivial component,*
2. *one vertex with one or two self-loops,*
3. *two vertices with one or two edges between them or*
4. *a cyclic graph with three or more vertices.*

Proof. A regular graph of degree at most two is a connected, undirected graph. Partitioning a regular graph of degree at most two into one level V_0 makes the graph satisfy 1. Because $d = 0$ requirement 2. and 3. from Definition 4.5 are always also true. □

Example 4.2. Figure 4.4 shows a component of $G_2(F_3)$. It consists of a vertex and a self-loop. So this is a regular graph of degree 1. Figure 4.5 shows a component of $G_2(F_7)$ consisting of two vertices and an edge between them. This is a regular graph of degree 1. Figure 4.6 shows a component of $G_3(F_{23})$. It consists of three vertices, where each vertex has two edges to two vertices. This is a regular graph of degree 2. Figure 4.7 shows a component of $G_3(F_{59})$. It consists of a regular graph of degree 2. By Proposition 4.1 these four components are volcanoes of depth 0.

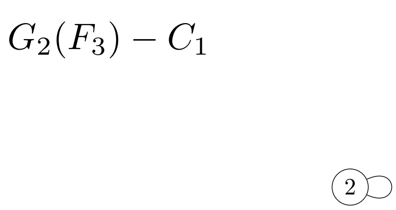

Figure 4.4: Component of $G_2(F_3)$

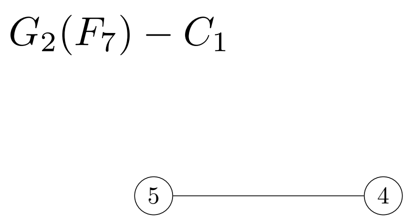

Figure 4.5: Component of $G_2(F_7)$

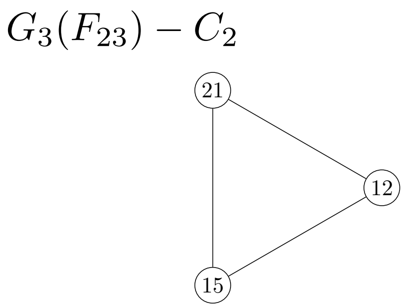

Figure 4.6: Component of $G_3(F_{23})$

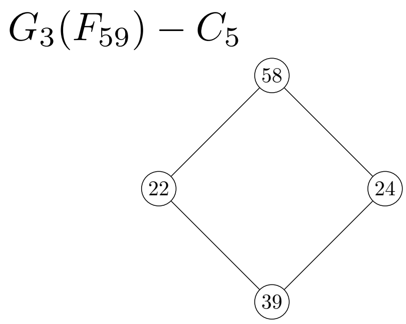

Figure 4.7: Component of $G_3(F_{59})$

Example 4.3. Figure 4.8 shows a component of $G_2(F_{17})$. If partitioned into $V_0 = \{10\}$ and $V_1 = \{6, 1\}$, then $d = 1$ and V_0 consists of one vertex with one self-loop, which is a regular graph of degree one. So requirement 1. from Definition 4.5 is satisfied. $6 \in V_1$ has exactly one edge and it is to vertex 10 $\in V_0$ and $1 \in V_1$ has exactly one edge which goes to $10 \in V_0$. Which means that 2. from Definition 4.5 is also satisfied. There is only one level such that $i < d = 1$, V_0. From 10, which is the only vertex in V_0, there is an edge to vertex 6, one edge from 10 to vertex 1 and one edge from 10 to itself vertex 10. Which means that the degree of each vertex in V_i for $i < d$, which is just the vertex 10, is $3 = 2 + 1 = p + 1$. Thus, requirement 3. from Definition 4.5 is also satisfied. Hence the component of $G_2(F_{17})$ drawn in Figure B.18 is a 3-volcano.

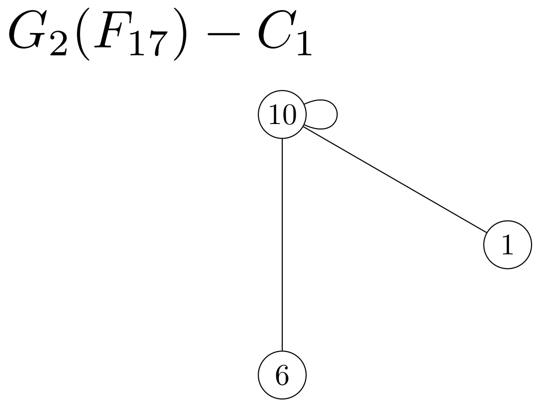

Figure 4.8: Component of $G_2(F_{17})$

Example 4.4. There are two components of $G_2(F_{53})$ that are 2-volcanoes of depth 2. These are ordinary components. Look at Figure 4.9 and choose $V_0 = \{17\}, V_1 = \{7\}$ and $V_2 = \{1, 35\}$. For Figure 4.10, choose $V_0 = \{39\}, V_1 = \{8, 22, 42\}$ and $V_2 = \{5, 11, 12, 13, 14, 40\}$.

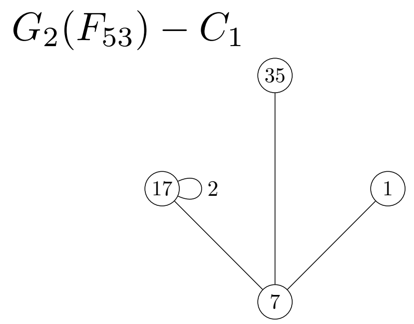

Figure 4.9: Component of $G_2(F_{53})$

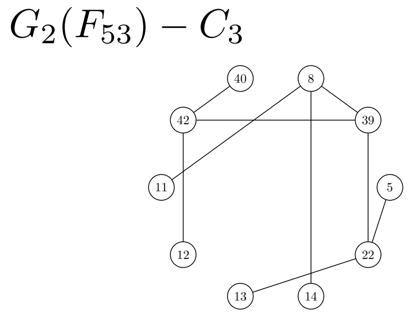

Figure 4.10: Component of $G_2(F_{53})$

Example 4.5. The following are two examples of 2-volcanoes that have depth 3. These are ordinary components. In Figure 4.11 choose $V_0 = \{120\}, V_1 = \{163\}, V_2 = \{95, 99\}$ and $V_3 = \{36, 58, 150, 227\}$. In Figure 4.12, choose $V_0 = \{332\}, V_1 = \{301\}, V_2 = \{235, 280\}$ and $V_3 = \{48, 62, 297, 336\}$.

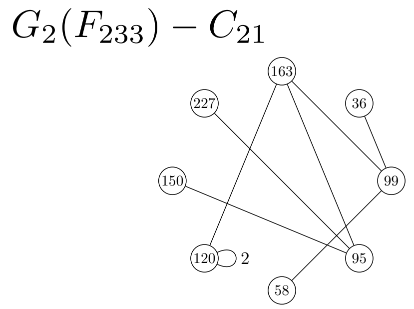

Figure 4.11: Component of $G_2(F_{233})$

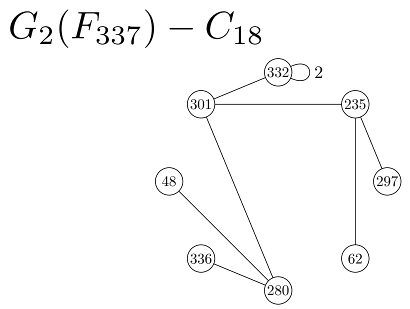

Figure 4.12: Component of $G_2(F_{337})$

Example 4.6. Supersingular components can also be volcanoes. Figure 4.13 and Figure 4.14 show two examples. Figure 4.13 shows a 3-volcano of depth 1, with $V_0 = \{41\}$ and $V_1 = \{50\}$. Figure 4.14 shows a 3-volcano of depth 2, with $V_0 = \{100\}$, $V_1 = \{65\}$ and $V_2 = \{36, 8\}$.

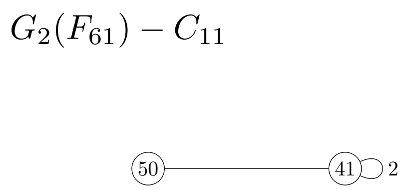

Figure 4.13: Component of $G_2(F_{61})$

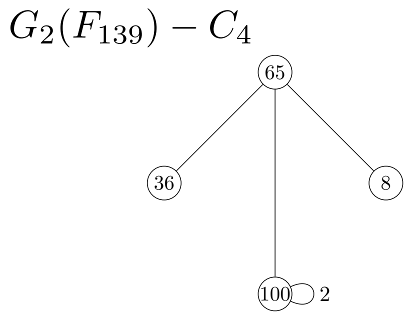

Figure 4.14: Component of $G_2(F_{139})$

Theorem 4.9. *Each ordinary component of the p-isogeny graph $G_p(F_q)$, excluding the components that contain the 0 or the 1728 vertices, is a p-volcano.*

Proof. The vertices in ordinary components represent j-invariants of elliptic curves where the only automorphisms are 1 and -1 according to Theorem 2.15. Therefore as explained in Section 3.5 all edges (j_1, j_2) will have the same multiplicity as (j_2, j_1). Hence the graph of these components do not need to be directed.

Because of Theorem 4.5, the endomorphism rings of all the elliptic curves in the component will be orders in the same imaginary quadratic field. The levels in a p-volcano will be the vertices that are j-invariant of elliptic curves having the same endomorphism rings.

Choosing a subgraph of an ordinary component where all the vertices are j-invariant of elliptic curves that have isomorphic endomorphism rings, will be a regular graph because of Theorem 3.7. This regular graph must have degree 0,1 or 2 due to Theorem 4.8. Hence requirement 1. from Definition 4.5 is satisfied in all ordinary components.

Which level V_i a j-invariant is going to be in, is determined by the p-adic valutaion of the conductor of $[\mathcal{O}_K : \mathcal{O}]$. (See [9] for details). By Theorem 4.7 every j-invariant of an elliptic curve that have isomorphic endomorphism rings and its conductor divisible by p has maximum one ascending p-isogeny from it. Hence requirement 2 from Definition 4.5 is satisfied.

It follows from Theorem 3.6 and Theorem 4.7 that there can only be one isogeny from the vertices in level d, hence requirement 3 from Definition 4.5 is satisfied. □

4.4 Applications

Theorem 4.9 is the base for many algorithms used in cryptography and number theory. I will briefly mention some of the algorithms. In the core of some of these algorithms is an algorithm that finds the vertices in level V_d. Level V_d is called the *floor* in many algorithms.

Remark 4.4. The idea behind finding the floor algorithm is that you start with a vertex j in an ordinary component of $G_p(F_q)$. Then by Theorem 4.9 the component must be a p-volcano, lets say of depth d. By the definition of a p-volcano then, either the degree of the vertex j is 1 or $p+1$. If deg $j = 1$ then $j \in V_d$ if deg $j = p + 1$, then $j \notin V_d$. So pick first an ordinary j-invariant. If this is not a vertex already on the floor, the algorithm will make a sequence of vertices that leads to the floor. Given a modular polynomial $\Phi_p(X, Y)$ over F_q, each step of this algorithm will have an expected time of $O(p^2\mathbf{M}(m) + \mathbf{M}(mn)m)$, where $\mathbf{M}(m)$ is the time it takes to multiply two m-bit integers and $m = \log q$. See [11] for details of the algorithm and proof of the time consumption. there is also a slightly modified version of this algorithm in [11], which finds the shortest path to the floor.

Remark 4.5. The two algorithms in Remark 4.4 which are based on the theory of this thesis can be used to make a Las Vegas algorithm to identify supersingular j-invariants. See section 3.2 in [11]. This algorithm will

(m^2) expected time, where $m = \log q$. The best known Las Vegas algorithms without this theory has an expected running time of (m^4) according to [11].

Remark 4.6. To compute the endomorphism rings of elliptic curves over F_q is usually hard and the running time for such an algorithm usually is exponential in $\log q$. But because of Theorem 4.6 one can use horizontal isogenies to compute the endomorphism rings. See [11] for details. Under the assumption of the General Riemann Hypothesis, this algorithms will have a sub-exponential running time. For details and proof of these claims see section 3.3 of [11].

Remark 4.7. Using the finding floor algorithms which are based on the volcano structure again, [11] has proposed an algorithm that can compute Hilbert class polynomials. The Hilbert class polynomials are important in the complex multiplication method in Remark 4.8 below, which is an important algorithm in elliptic curve cryptography.

Remark 4.8. The complex multiplication method is a method to construct an elliptic curve with a given number of rational points over a fixed field. This method is extensively used in elliptic curve cryptography and elliptic curve primality proving.

Let $Ell_{\mathcal{O}} = \{j(E) \colon E/K s.t. \mathrm{End}(E) \cong \mathcal{O}\}$ and let the *Hilbert class polynomial*, $H_D(X)$, be defined by

$$H_D(X) = \Pi_{j \in Ell_{\mathcal{O}}(\mathbb{C})}(X - j).$$

Start with an equation

$$DV^2 = 4q - t^2. \tag{4.3}$$

where q is prime. Then let j be any root of $H_D(X)$, except 0 or 1728. Now set

$$k = \frac{j}{1728 - j} \bmod q.$$

Then the curve

$$y^2 = x^3 + 3kc^2x + 2kc^3 \tag{4.4}$$

has j-invariant j for any nonzero $c \in F_q$. So pick $c = 1$. According to Corollary 3.1 there are two elliptic curves with the same j-invariant. One must have order $q + t + 1$ and the twist must have order $q - t + 1$. Choose a random point on the elliptic curve. To check which one it is, just pick a random point at the elliptic curve and multiply by either $q+t+1$ or $q-t+1$. If you get the identity element $\mathcal{O}$ then that is the order, if not then the other one is the order. For proof and details see section 3.4 of [11].

The part of this method that is dependent on the theory of this thesis is the computation of the Hilbert class polynomials. The algorithm for computing the Hilbert class polynomials is heavily based on the volcano structure of the components because the finding floor algorithms are used in two of the critical steps. Under the General Riemann Hypothesis this algorithm runs in quasi-linear expected time in size of $H_D(X)$. See section 3.4 of [11] and [10].

4.5 Statistics and Findings

In Appendix C I have calculated some statistics for isogeny graphs for some pairs of p and q. In the next remarks I will comment the findings.

Remark 4.9. Looking at the tables in Appendix C, we observe that the number of isogenies in an isogeny graph $G_p(F_q)$ will roughly be the same size as F_q. This is more visible when looking at the isogeny graphs with the bigger fields Table C.7-Table C.10.

Remark 4.10. Looking at the number of components, the number of ordinary components and the number of supersingular components in Table C.1-Table C.6, shows that most of the components are ordinary components and there are very few supersingular components.

Remark 4.11. The number of components seem to be about half of the number of isogenies. This is again, also more visible looking at the tables for the bigger fields, Table C.7-Table C.10. This means, that in average there is about 2 isogenies per component. That is not many enough to make volcanoes of big depth. Also comparing the number of components to the number of non-trivial components, shows that most of the components are trivial-components. From looking at looking at Table C.10, about 70% of all the components are trivial components. Therefore, if one pick an ordinary j-invariant, which, because of Theorem 4.9, will be a volcano, and wishes to make a path to the floor of the volcano, as one would want in the applications above, the probability for the path to be longer than 1, is low. It would be interesting to find exactly what the probability is to get volcanoes of certain depths for pairs of p and q.

Proposition 4.2. *Following table shows the number of p-volcanoes of depth $d = 2$ and $d = 3$ in $G_p(F_q)$ for $2 \leq p \leq 7$ and $2 \leq q \leq 293$.*

$2 \leq q \leq 293$	d=2	d=3
$p = 2$	55	6
$p = 3$	5	0
$p = 5$	0	0
$p = 7$	0	0

There are no volcanoes of depth larger than 3 for $2 \leq p \leq 7$ and $2 \leq q \leq 293$.

Proof. I checked this manually by computing all the isogeny graphs for p and q as in the proposition, and counting. There are too many graphs to include in the thesis but they were all computed using the code in Appendix D □

Remark 4.12. It makes sense that there are less p-volcanoes of high depth for bigger p in the same range of primes q, because as mentioned in Remark 4.9 the number of isogenies in each $G_p(F_q)$ is almost q, but for larger p, the degree of the vertices of p-volcanoes are $p + 1$ and so for bigger p there are more edges (isogenies) needed for each p-volcano of the same size.

Proposition 4.3. *p-volcanoes in $G_p(F_q)$ can at most have depth $q-1$.*

Proof. Follows from Definition 4.5, of p-volcano: There can maximum be q vertices in a subgraph of $G_p(F_q)$. If one wants to make a 2-volcano with maximum depth then there must be a vertex in each level. And that is by definition a 2-volcano of depth $q-1$. □

Remark 4.13. In p-volcanoes for $p > 2$, there must be more than one vertex in most of the levels to satisfy requirement 3 of Definition 4.5 about the degree of the vertices. Therefore, the depth must be even less then $q-1$. Also, the proof of Proposition 4.3 assumes that there are q vertices in the p-volcano, this can only happen if all of $G_p(F_q)$ is connected. But as seen in the graphs of Figure B.1-Figure B.55 and the statistics of Table C.1-Table C.10, there are no isogeny graphs where that happens, and actually isogeny graphs are made out of many components, much more than one. Hence, the highest depth of a p-volcano in $G_p(F_q)$ must probably be much less than $q-1$.

4.6 Further Studies

As mentioned in Section 4.5 there are few p-volcanoes of high depth. From the discussions from Section 4.2 and the proof of Theorem 4.9 it looks like the depth of the p-volcano, a j-invariant is a part of, is dependent on the endomorphism ring of the elliptic curve with that j-invariant. It would be interesting to count and make statistics on which j-invariants are more often part of p-volcanoes of high depth and give an estimate for the probability of p-volcanoes with given depths d for pairs p and q.

Appendix A

Table of j-Invariants of Supersingular Elliptic Curves over F_p

In the following table I have listed j-invariants of supersingular elliptic curves over finite fields with a prime number of elements. Ranging from $2 \le p \le 293$.

First I used the fact that 0 is the j-invariant of a supersingular elliptic curve over F_p if and only if $p = 2 \bmod 3$ and 1728 (mod p) is the j-invariant of a supersingular elliptic curve if and only if $p = 3 \bmod 4$. See [8], in the proof of theorem 4.1, chapter V.

The other j-invariants of supersingular elliptic curves over F_p I found by calculating the roots of the polynomial

$$H_p(t) = \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 t^i$$

over F_p, see [8] theorem 4.1b), chapter V.

p	j	p	j
2	0	131	0, 25=1728 (mod 131), 10, 28, 31, 50, 62, 82, 94, 113
3	0=1728 (mod 3)	137	0, 22, 78, 136
5	0	139	60=1728 (mod 139), 8, 36, 44, 65, 100
7	6=1728 (mod 7)	149	0, 12, 30, 62, 68, 74, 103
11	0, 1=1728 (mod 11)	151	67=1728 (mod 151), 29, 101, 124, 143, 148, 150
13	5	157	79, 134, 150
17	0, 8	163	98, 127
19	18=1728 (mod 19), 7	167	0, 58=1728 (mod 167), 15, 27, 30, 59, 89, 112, 131, 132, 151
23	0, 3=1728 (mod 23), 19	173	0, 17, 24, 42, 85, 102, 159
29	0, 2, 25	179	0, 117=1728 (mod 179), 22, 35, 61, 112, 120, 121, 140, 171
31	23=1728 (mod 31), 2, 4	181	36, 64, 146, 173, 175
37	8	191	0, 9=1728 (mod 191), 16, 41, 46, 55, 66, 106, 107, 138, 150, 169, 176
41	0, 3, 28, 32	193	42, 169
43	41, 8	197	0, 22, 72, 120, 131
47	0, 36=1728 (mod 47), 9, 10, 44	199	136=1728 (mod 199), 8, 40, 61, 64, 90, 98, 140, 147
53	0, 46, 50	211	40=1728 (mod 211), 28, 82, 114, 148, 198
59	0, 17=1728 (mod 59), 15, 28, 47, 48	223	167=1728 (mod 223), 49, 128, 193, 195, 210, 221
61	9, 41, 50	227	0, 139=1728 (mod 227), 30, 110, 114, 132, 147, 160, 191, 201
67	53=1728 (mod 67), 66	229	27, 60, 93, 172, 214
71	0, 24=1728 (mod 71), 17, 40, 41, 48, 66	233	0, 11, 85, 177, 183, 187
73	9, 56	239	0, 55=1728 (mod 239), 68, 105, 107, 113, 185, 192, 193, 214, 215, 217, 218, 225, 235
79	69=1728 (mod 79), 15, 17, 21, 64	241	8, 28, 64, 93, 216, 240
83	0, 68=1728 (mod 83), 17, 28, 50, 67	251	0, 222=1728 (mod 251), 4, 24, 30, 35, 64, 101, 139, 185, 199, 207, 213, 232
89	0, 6, 7, 13, 52, 66	257	0, 30, 115, 121, 139, 198, 223, 249
97	1, 20	263	0, 150=1728 (mod 263), 31, 37, 55, 85, 107, 108, 110, 141, 149, 184, 208
101	0, 3, 21, 57, 59, 64, 66	269	0, 5, 92, 111, 122, 142, 189, 197, 199, 200, 215
103	80=1728 (mod 103), 23, 24, 34, 69	271	102=1728 (mod 271), 23, 47, 69, 98, 125, 141, 148, 202, 236, 240
107	0, 16=1728 (mod 107), 47, 72, 81, 94	277	61, 195, 244
109	17, 41, 43	281	0, 5, 48, 84, 90, 109, 130, 133, 249, 252
113	0, 54, 72, 99	283	30=1728 (mod 283), 21, 60, 78, 122, 251
127	77=1728 (mod 127), 73, 95, 125, 126	293	0, 48, 88, 89, 124, 127, 141, 212, 243

Table A.1

Appendix B

Examples of Isogeny Graphs

This appendix contains figures showing isogeny graphs $G_p(F_q)$ for primes $2 \leq p \leq 11$ and $2 \leq q \leq 11$, such that $q \nmid p$.

$G_2(F_3)$

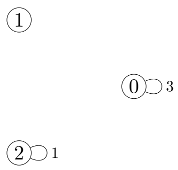

Figure B.1

$G_3(F_2)$

Figure B.2

$G_5(F_2)$

Figure B.3

$G_2(F_5)$

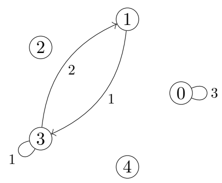

Figure B.4

$G_3(F_5)$

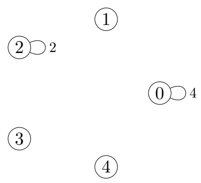

Figure B.5

$G_5(F_3)$

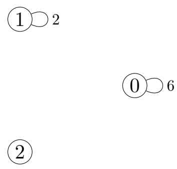

Figure B.6

$G_2(F_7)$

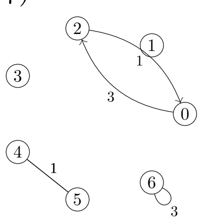

Figure B.7

$G_3(F_7)$

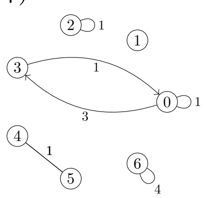

Figure B.8

$G_5(F_7)$

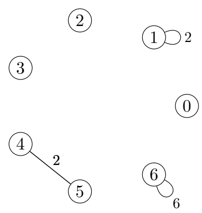

Figure B.9

$G_2(F_{11})$

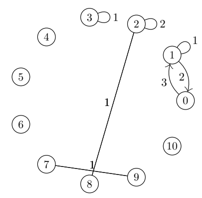

Figure B.10

$G_3(F_{11})$

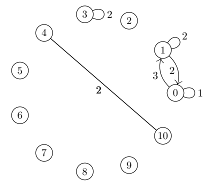

Figure B.11

$G_5(F_{11})$

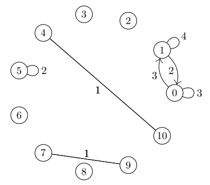

Figure B.12

Isogeny graphs where $q \geq 13$ will be complex, so I will present the graphs component by component. Figure B.13 - Figure B.16 show the non-trivial components of $G_2(F_{13})$.

$G_2(F_{13}) - C_0$

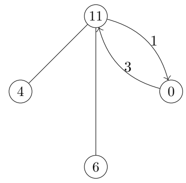

Figure B.13

$G_2(F_{13}) - C_1$

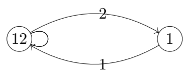

Figure B.14

$G_2(F_{13}) - C_2$

Figure B.15

$G_2(F_{13}) - C_3$

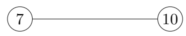

Figure B.16

Figure B.17-Figure B.20 show non-trivial components of $G_2(F_{17})$.

$G_2(F_{17}) - C_0$

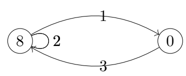

Figure B.17

$G_2(F_{17}) - C_1$

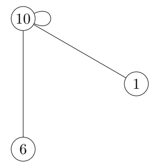

Figure B.18

$G_2(F_{17}) - C_2$

Figure B.19

$G_2(F_{17}) - C_3$

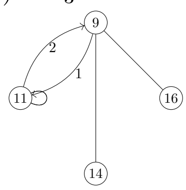

Figure B.20

Figure B.21-Figure B.26 show non-trivial components of $G_2(F_{19})$.

$G_2(F_{19}) - C_0$

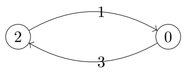

Figure B.21

$G_2(F_{19}) - C_1$

Figure B.22

$G_2(F_{19}) - C_2$

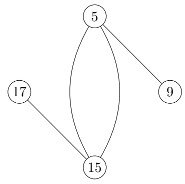

Figure B.23

$G_2(F_{19}) - C_3$

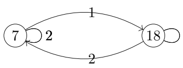

Figure B.24

$G_2(F_{19}) - C_4$

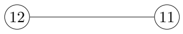

Figure B.25

$G_2(F_{19}) - C_5$

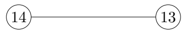

Figure B.26

Figure B.27-Figure B.32 show non-trivial components of $G_2(F_{23})$.

$G_2(F_{23}) - C_0$

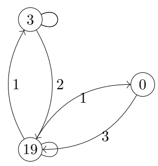

Figure B.27

$G_2(F_{23}) - C_1$

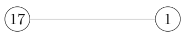

Figure B.28

$G_2(F_{23}) - C_2$

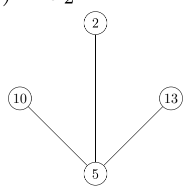

Figure B.29

$G_2(F_{23}) - C_3$

Figure B.30

$G_2(F_{23}) - C_4$

Figure B.31

$G_2(F_{23}) - C_5$

Figure B.32

Figure B.33-Figure B.38 show non-trivial components of $G_2(F_{29})$.

$G_2(F_{29}) - C_0$

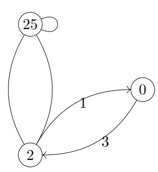

Figure B.33

$G_2(F_{29}) - C_1$

Figure B.34

$G_2(F_{29}) - C_2$

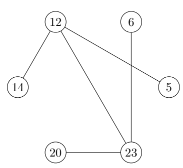

Figure B.35

$G_2(F_{29}) - C_3$

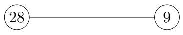

Figure B.36

$G_2(F_{29}) - C_4$

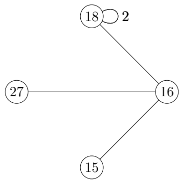

Figure B.37

$G_2(F_{29}) - C_5$

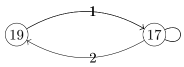

Figure B.38

Figure B.39-Figure B.46 show non-trivial components of $G_2(F_{31})$.

$G_2(F_{31}) - C_0$

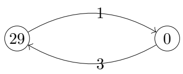

Figure B.39

$G_2(F_{31}) - C_1$

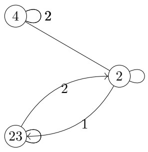

Figure B.40

$G_2(F_{31}) - C_2$

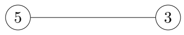

Figure B.41

$G_2(F_{31}) - C_3$

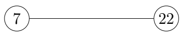

Figure B.42

$G_2(F_{31}) - C_4$

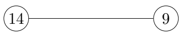

Figure B.43

$G_2(F_{31}) - C_5$

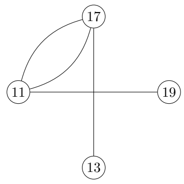

Figure B.44

$G_2(F_{31}) - C_6$

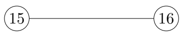

Figure B.45

$G_2(F_{31}) - C_7$

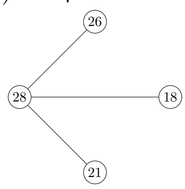

Figure B.46

Figure B.47-Figure B.55 show non-trivial components of $G_2(F_{37})$.

$G_2(F_{37}) - C_0$

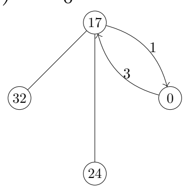

Figure B.47

$G_2(F_{37}) - C_1$

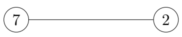

Figure B.48

$G_2(F_{37}) - C_2$

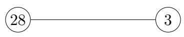

Figure B.49

$G_2(F_{37}) - C_3$

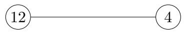

Figure B.50

$G_2(F_{37}) - C_4$

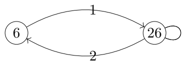

Figure B.51

$G_2(F_{37}) - C_5$

Figure B.52

$G_2(F_{37}) - C_6$

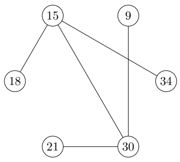

Figure B.53

$G_2(F_{37}) - C_7$

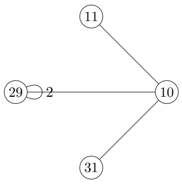

Figure B.54

$G_2(F_{37}) - C_8$

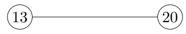

Figure B.55

Appendix C

Tables of Statistics

In this chapter I have collected some of the statistics that I have calculated for $G_p(F_q)$. I have calculated all the statistics using the program Isogenic which I made in connection with this thesis. See Appendix D for more information. Each table shows statistics for a fixed p which will determine which modular polynomial is used. For Table C.1-Table C.6, the following is an explanation of what statistics that is included.

1. In the first columns I have listed prime numbers q that represent which finite fields F_q the isogeny graphs use as its vertex set. In this way the isogeny graph $G_p(F_q)$ will be fixed for each row of the tables.
2. In the second column I have calculated the number of isomorphism classes of isogenies that exist between elliptic curves with j-invariants as elements of F_p. This will be the same as the number of directed edges counting with multiplicity of $G_p(F_q)$.
3. In the third column I have calculated the number of components of $G_p(F_q)$.
4. In the fourth column I have calculated the number of non-trivial components of $G_p(F_q)$.
5. In the fifth column I have calculated the number of ordinary components of $G_p(F_q)$.
6. In the sixth column I have calculated the number of supersingular components of $G_p(F_q)$.

Remark C.1. Of course, because of Theorem 4.1, the number of ordinary components (the number in the fourth column) plus the number of supersingular components (the number in the fifth column) must be equal to the number of components (the number in the third column).

$p = 2$ q	Number of isogenies	Number of components	Number of non-trivial components	Number of ordinary components	Number of super-singular components
5	7	4	2	3	1
7	9	5	3	4	1
11	13	8	4	7	1
13	17	8	4	7	1
17	21	10	4	9	1
19	23	12	6	11	1
23	25	14	6	13	1
29	35	16	6	15	1
31	35	18	8	17	1
37	39	21	9	20	1
41	49	21	7	20	1
43	45	25	11	24	1
47	51	26	10	25	1
53	55	29	11	27	2
59	67	32	12	31	1
61	65	33	13	31	2
67	69	38	16	37	1
71	77	39	15	38	1
73	77	38	14	37	1
79	81	44	18	43	1
83	87	45	17	43	2
89	97	45	15	43	2
97	101	50	18	49	1
101	109	52	18	49	3
103	107	55	21	54	1
107	109	58	22	56	2
109	111	58	22	56	2
113	115	59	21	57	2
127	129	68	26	67	1
131	139	69	25	67	2

Table C.1

$p=2$ q	Number of isogenies	Number of components	Number of non-trivial components	Number of ordinary components	Number of super-singular components
137	139	71	25	69	2
139	143	75	29	73	2
149	155	77	27	74	3
151	153	81	31	80	1
157	161	81	29	79	2
163	165	87	33	86	1
167	171	88	32	87	1
173	177	90	32	86	4
179	185	94	34	92	2
181	185	94	34	92	2
191	197	101	37	100	1
193	195	99	35	98	1
197	199	102	36	99	3
199	203	105	39	104	1
211	213	113	43	111	2
223	227	117	43	116	1
227	231	119	43	116	3
229	233	118	42	115	3
233	235	119	41	116	3
239	245	125	45	124	1
241	245	123	43	120	3
251	259	130	46	127	3
257	261	130	44	126	4
263	265	138	50	137	1
269	277	137	47	132	5
271	275	143	53	142	1
277	279	143	51	141	2
281	287	142	48	138	4
283	287	148	54	146	2
293	297	150	52	145	5

Table C.2

$p = 3$ q	Number of isogenies	Number of components	Number of non-trivial components	Number of ordinary components	Number of super-singular components
5	6	5	2	4	1
7	12	5	4	4	1
11	14	9	3	8	1
13	20	8	6	7	1
17	20	13	4	12	1
19	28	11	8	10	1
23	28	16	4	15	1
29	34	20	5	19	1
31	44	16	11	15	1
37	42	21	13	20	1
41	48	28	7	27	1
43	46	24	14	22	2
47	56	30	6	29	1
53	56	34	7	33	1
59	70	38	8	37	1
61	72	32	20	30	2
67	68	37	20	35	2
71	84	44	8	43	1
73	78	40	23	38	2
79	92	40	24	37	3
83	88	51	9	50	1
89	94	57	12	56	1
97	100	53	29	51	2
101	110	62	11	61	1
103	110	54	31	50	4
107	112	64	10	63	1
109	116	58	33	55	3
113	114	71	14	70	1
127	136	65	37	61	4
131	144	78	12	77	1

Table C.3

$p=3$ q	Number of isogenies	Number of components	Number of non-trivial components	Number of ordinary components	Number of super-singular components
137	138	83	14	82	1
139	150	71	40	67	4
149	154	88	13	87	1
151	164	77	44	72	5
157	162	82	44	79	3
163	164	87	46	85	2
167	178	95	11	94	1
173	178	100	13	99	1
179	186	106	16	105	1
181	190	94	52	90	4
191	204	111	15	110	1
193	198	101	54	99	2
197	202	113	14	112	1
199	214	101	57	95	6
211	218	110	60	105	5
223	230	116	63	110	6
227	232	130	16	128	2
229	238	119	65	115	4
233	236	137	20	136	1
239	254	135	15	134	1
241	250	125	68	120	5
251	262	145	19	144	1
257	258	151	22	150	1
263	274	151	19	150	1
269	276	156	21	155	1
271	288	137	76	129	8
277	284	142	75	139	3
281	284	164	23	163	1
283	286	147	77	141	6
293	298	163	16	162	1

Table C.4

$p = 5$ q	Number of isogenies	Number of components	Number of non-trivial components	Number of ordinary components	Number of super-singular components
7	12	6	3	5	1
11	18	8	4	7	1
13	18	11	5	10	1
17	28	13	6	12	1
19	30	12	6	11	1
23	40	15	6	14	1
29	42	20	10	19	1
31	46	20	10	19	1
37	38	28	10	27	1
41	58	27	13	26	1
43	48	29	9	27	2
47	76	28	9	27	1
53	58	36	11	34	2
59	82	34	14	33	1
61	72	39	19	38	1
67	72	44	12	42	2
71	98	41	17	40	1
73	74	51	15	49	2
79	96	45	19	44	1
83	106	47	10	45	2
89	104	54	24	53	1
97	98	66	18	64	2
101	120	61	27	60	1
103	116	63	16	60	3
107	122	64	15	60	4
109	118	66	30	65	1
113	118	72	17	69	3
127	138	77	18	73	4
131	162	73	29	72	1

Table C.5

$p=5$ q	Number of isogenies	Number of components	Number of non-trivial components	Number of ordinary components	Number of super-singular components
137	144	86	20	84	2
139	154	79	33	78	1
149	164	87	37	86	1
151	168	85	35	84	1
157	160	101	24	99	2
163	166	101	21	99	2
167	206	90	16	87	3
173	184	105	23	100	5
179	198	101	41	100	1
181	192	105	45	104	1
191	224	105	41	104	1
193	196	123	28	121	2
197	202	123	27	119	4
199	216	112	46	111	1
211	224	116	46	115	1
223	232	132	24	126	6
227	250	126	20	120	6
229	234	132	56	131	1
233	242	143	30	139	4
239	278	129	49	128	1
241	250	138	58	137	1
251	280	138	54	137	1
257	270	153	29	148	5
263	296	142	21	136	6
269	280	152	62	151	1
271	286	149	59	148	1
277	278	170	32	167	3
281	302	157	63	156	1
283	292	164	26	159	5
293	304	171	29	164	7

Table C.6

$p = 2$ q	Number of isogenies	Number of components	Number of non-trivial components
1009	1011	509	173
1013	1017	512	174
1019	1025	521	181
1021	1025	517	177
1031	1037	528	184
1033	1035	520	176
1039	1043	535	189
1049	1057	526	176
1051	1053	541	191
1061	1067	536	182

Table C.7

$p = 3$ q	Number of isogenies	Number of components	Number of non-trivial components
1009	1014	516	265
1013	1016	551	44
1019	1028	548	38
1021	1030	519	267
1031	1046	555	39
1033	1038	526	269
1039	1054	525	272
1049	1054	583	58
1051	1058	534	274
1061	1064	581	50

Table C.8

$p = 5$ q	Number of isogenies	Number of components	Number of non-trivial components
1009	1018	549	213
1013	1016	568	63
1019	1044	534	194
1021	1028	556	216
1031	1066	543	199
1033	1034	603	87
1039	1058	551	205
1049	1062	558	208
1051	1062	557	207
1061	1066	570	216

Table C.9

$p = 2$ q	Number of isogenies	Number of components	Number of non-trivial components
10007	10009	5053	1717
10009	10013	5014	1678
10037	10041	5037	1691
10039	10041	5089	1743
10061	10067	5049	1695
10067	10069	5090	1734
10069	10073	5057	1701
10079	10087	5090	1730
10091	10097	5091	1727
10093	10097	5064	1700

Table C.10

Appendix D

Source Code

This appendic shows parts of the source code for the calculations of the isogeny graphs.

polynomial.py

```
from sympy import (degree, diff, symbols)

(x, y) = symbols('x y')

class Polynomial:
    """
      Polynomial
    """
    def __init__(self, n, p, lists):
        self.p = p
        self.n = n
        self.lists = lists
        self.zeros = None
        self.multiplicities = None
        (x_list, y_list, c_list) = self.lists
        tmp_mod_poly = 0
        for i in range(len(x_list)):
            tmp_mod_poly += (c_list[i]%p)*x**(x_list[i])*y**(y_list[i])
            if x_list[i] != y_list[i]:
                tmp_mod_poly += (c_list[i]%p)*y**(x_list[i])*x**(y_list[i])
        self.mod_poly = tmp_mod_poly

    def make_list_of_roots(self):
        n = self.n
        p = self.p
        self.zeros = []
        for i in range(p):
            for j in range(p):
                if self.eval_mod_poly(i, j) % p == 0:
                    self.zeros.append((i, j))
```

```
        marshal.dump(self.zeros, open(filepath, 'wb'))
        return self.zeros

    def find_multiplicity_of_roots(self, xval, yval, p):
        multiplisitet = 0
        polynomial_in_y = self.eval_only_x(xval, p)
        i_counter = 0
        for i in range(degree(polynomial_in_y)):
            derivative_of_poly = diff(polynomial_in_y, y, i) % p
            evaluation_of_polynomial = derivative_of_poly.subs(y,

            i_counter = i
            if evaluation_of_polynomial == 0:
                multiplisitet = multiplisitet + 1
            else:
                break
        return multiplisitet
```

isogeny_graph.py

```
import networkx as nx

def list_components(roots):
    G = nx.Graph(roots)
    adj_lists = {}

    for cl in nx.connected_components(G):
        adj_lists[list(cl)[0]] = []
        for k in cl:
            adj_lists[list(cl)[0]] = adj_lists[list(cl)[0]]+[(k, m)
            for m in G.adj[k].keys()]
    for key in adj_lists.keys():
        adj_lists[key] = zeros_ex_duals(adj_lists[key])
    return [adj_lists[key] for key in adj_lists.keys()]

def count_components(list_of_roots, list_of_components, p):
    number_of_components = len(list_of_components)
    vertices_in_roots = []
    [vertices_in_roots.extend([root[0],root[1]])
    for root in list_of_roots]
    for vertice in range(p):
        if vertice not in vertices_in_roots:
            number_of_components = number_of_components + 1
    return number_of_components

def count_isogenies(list_of_roots, list_of_multiplicities):
    number_of_isogenies = 0
    for root in list_of_roots:
            number_of_isogenies = number_of_isogenies
```

```
                + list_of_multiplicities[list_of_roots.index(root)]
    return number_of_isogenies

def is_supersingular(given_component, p):
    j_in_given_component = []
    [j_in_given_component.extend([root[0], root[1]])
    for root in given_component]
    if any(j in j_in_given_component for j in supersingulars[p]):
        return True
    else:
        return False

def count_ordinary_volcanoes(components, p):
    volcanoes = 0
    ordinary_vertices = []
    for component in components:
        if not is_supersingular(component, p):
            volcanoes = volcanoes + 1
            [ordinary_vertices.extend([root[0], root[1]])
            for root in component]
    for j in range(p):
        if j not in supersingulars[p]:
            if j not in ordinary_vertices:
                volcanoes = volcanoes + 1
    return volcanoes

def count_supersingular_components(components, p):
    number_of_ss_components = 0
    ss_vertices = []
    for component in components:
        if is_supersingular(component, p):
            [ss_vertices.extend([root[0], root[1]]) for root in component]
            number_of_ss_components = number_of_ss_components + 1
    for j in supersingulars[p]:
        if j not in ss_vertices:
            number_of_ss_components = number_of_ss_components + 1
    return number_of_ss_components
```

References

[1] Reza Azarderakhsh et al. *SIKE - Supersinuglar Isogeny Key Encapsulation*. URL: https://sike.org.

[2] Reinier Broker, Kristin Lauter, and Andrew V. Sutherland. **?**Modular Polynomials via Isogeny Volcanoes**?** In: *Mathematics of Computation 81* (2012), pp. 1201–1231.

[3] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. **?**Cryptographic hash functions from expander graphs**?** In: *Journal of Cryptology* (2009), pp. 93–113.

[4] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.

[5] Steven D. Galbraith, Christphe Petit, and Javier Silva. *Identification protocols and signature shcemes based on supersingular isogeny problems*.

[6] David Jao, Luca De Feo, and Jérôme Plût. **?**Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies**?** In: *journal of mathematical cryptology* 8 (2012), pp. 209–247.

[7] *Modular Polynomials*. URL: https://math.mit.edu/~drew/ClassicalModPolys.html.

[8] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Dordrecht, Heidelberg, London, New York: Springer, 2016.

[9] Andrew Sutherland. *Elliptic Curve Lectures for Spring 2017*. URL: https://math.mit.edu/classes/18.783/2019/lectures.html.

[10] Andrew V. Sutherland. **?**Computing Hilbert class polynomials with the Chinese Remainder Theorem**?** In: *Mathematics of Computation* (2009), pp. 501–538.

[11] Andrew V. Sutherland. **?**Isogeny Volcanoes**?** In: *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, 2012, 507-530* (2013).

[12] J. Vélu. **?**Isogenies entre courbes elliptiques**?** In: *Comptes rendus de l'Académie des Sciences* (1971), pp. 238–241.

[13] Younghoo Yoo et al. **?**A post-quantum digital scheme based on supersingular isogenies**?** In: *financial Cryptography and Data Security - 21st International Conference, FC 2017, Silema, Malta, April 3-7* (2017).