Minimal Discriminants for Elliptic Curves with Non-Trivial Isogeny

Alyssa Brasse[1] Nevin Etter[2] Gustavo Flores[3] Drew Miller[4] Summer Soller[5]

[1]Hunter College [2]Washington and Lee University [3]Carleton College [4]University of California Santa Barbara [5]University of Utah

August 2, 2021

Outline

Elliptic Curves

Definition

*An **Elliptic Curve** over $\mathbb{Q}$ is the set of complex numbers (x, y) that satisfy the equation*

$$y^2 = x^3 + Ax + B$$

together with a point "at infinity" denoted $\mathcal{O}$, where $A, B \in \mathbb{Q}$ satisfy $4A^3 + 27B^2 \neq 0$.

Why are Elliptic Curves Important?

- The "applications" answer

Why are Elliptic Curves Important?

- The “applications” answer
    - Cryptography

Why are Elliptic Curves Important?

- The “applications” answer
  - Cryptography
- The “mathematics” answer

Why are Elliptic Curves Important?

- The "applications" answer
  - Cryptography
- The "mathematics" answer
  - Bridge between algebra and geometry

Elliptic Curve Theorems

Theorem (Mordell-Weil, 1922)

The set of rational points $E(\mathbb{Q})$ has the structure of a finitely generated abelian group with identity element $\mathcal{O}$.

Theorem (Mazur, 1977)

Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup, the subgroup of points of finite order, is isomorphic to one of the following possibilities:

$$E(\mathbb{Q})_{tors} \cong \begin{cases} C_N, & N = 1, 2, \ldots, 10, 12 \\ C_2 \times C_N, & N = 1, 2, 3, 4. \end{cases}$$

Weierstrass Form of an Elliptic Curve

The **Weierstrass form** of an elliptic curve over $\mathbb{Q}$ is given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where each $a_j \in \mathbb{Q}$. We say E is given by an **integral Weierstrass model** if each $a_j \in \mathbb{Z}$.

Weierstrass Form of an Elliptic Curve

The **Weierstrass form** of an elliptic curve over $\mathbb{Q}$ is given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where each $a_j \in \mathbb{Q}$. We say E is given by an **integral Weierstrass model** if each $a_j \in \mathbb{Z}$.
Define the quantities associated to E by

$$\begin{aligned} c_4 &= a_1^4 + 8a_1^2a_2 - 24a_1a_3 - 48a_4 \\ c_6 &= -(a_1^2 + 4a_2)^3 + 36(a_1^2 + 4a_2)(2a_4 + a_1a_3) - 216(a_3^2 + 4a_6) \\ \Delta &= \frac{c_4^3 - c_6^2}{1728}, \qquad j(E) = \frac{c_4^3}{\Delta}. \end{aligned}$$

We call Δ the **discriminant** and $j(E)$ the j-**invariant** of E.

Isomorphisms of Elliptic Curves

An elliptic curve E' is $\mathbb{Q}$-isomorphic to E if E' arises from E via an **admissible change of variables**

$$x \longmapsto u^2x + r \qquad y \longmapsto u^3y + u^2sx + w,$$

where $u, r, s, w \in \mathbb{Q}$ and $u \neq 0$.

Isomorphisms of Elliptic Curves

An elliptic curve E' is $\mathbb{Q}$-isomorphic to E if E' arises from E via an **admissible change of variables**

$$x \longmapsto u^2x + r \qquad y \longmapsto u^3y + u^2sx + w,$$

where $u, r, s, w \in \mathbb{Q}$ and $u \neq 0$.
Let c_4', c_6', Δ', and j' be the quantities associated to E'. Then,

$$c_4' = u^{-4}c_4, \quad c_6' = u^{-6}c_6, \quad \Delta' = u^{-12}\Delta, \quad j' = j$$

Isomorphisms of Elliptic Curves

An elliptic curve E' is $\mathbb{Q}$-isomorphic to E if E' arises from E via an **admissible change of variables**

$$x \longmapsto u^2x + r \qquad y \longmapsto u^3y + u^2sx + w,$$

where $u, r, s, w \in \mathbb{Q}$ and $u \neq 0$.
Let c_4', c_6', Δ', and j' be the quantities associated to E'. Then,

$$c_4' = u^{-4}c_4, \quad c_6' = u^{-6}c_6, \quad \Delta' = u^{-12}\Delta, \quad j' = j$$

If E and E' are $\mathbb{Q}$-isomorphic, we say E' is in the $\mathbb{Q}$-**isomorphism class** of E, which we denote $E' \in [E]_{\mathbb{Q}}$.

Isomorphisms of Elliptic Curves

An elliptic curve E' is $\mathbb{Q}$-isomorphic to E if E' arises from E via an **admissible change of variables**

$$x \longmapsto u^2x + r \qquad y \longmapsto u^3y + u^2sx + w,$$

where $u, r, s, w \in \mathbb{Q}$ and $u \neq 0$.
Let c_4', c_6', Δ', and j' be the quantities associated to E'. Then,

$$c_4' = u^{-4}c_4, \quad c_6' = u^{-6}c_6, \quad \Delta' = u^{-12}\Delta, \quad j' = j$$

If E and E' are $\mathbb{Q}$-isomorphic, we say E' is in the $\mathbb{Q}$-**isomorphism class** of E, which we denote $E' \in [E]_{\mathbb{Q}}$.
Composition of isomorphisms affects u multiplicatively:

$$E_1 \xrightarrow{u_1} E_2 \xrightarrow{u_2} E_3 \implies \Delta_3 = u_2^{-12}\Delta_2 = u_2^{-12}u_1^{-12}\Delta_1$$

Examples

Suppose we have elliptic curves

$$E : y^2 + 81xy + 24786y = x^3 + 324x^2$$
$$E' : y^2 + xy = x^3 - 43x + 105.$$

They are isomorphic via the change of variables

$$x \longmapsto 9^2x - 648 \quad y \longmapsto 9^3y - 9^2 \cdot 36x + 13851.$$

That is, $(u, r, s, w) = (9, -648, -36, 13851)$.

Examples

Suppose we have elliptic curves

$$E : y^2 + 81xy + 24786y = x^3 + 324x^2$$

$$E' : y^2 + xy = x^3 - 43x + 105.$$

They are isomorphic via the change of variables

$$x \longmapsto 9^2x - 648 \quad y \longmapsto 9^3y - 9^2 \cdot 36x + 13851.$$

That is, $(u, r, s, w) = (9, -648, -36, 13851)$.
One can show that E has discriminant 652977088344072 and E' has discriminant 2312.
Note that

$$652977088344072 = 2^3 \cdot 3^{24} \cdot 17^2 \quad \text{and} \quad 2312 = 2^3 \cdot 17^2.$$

GeoGebra example!

Minimal Discriminants

We say E defined by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is a **global minimal model** if each $a_j \in \mathbb{Z}$ and Δ is minimal over all $\mathbb{Q}$-isomorphic curves:

$$\Delta_E = \min\{|\Delta_{E'}| \in \mathbb{Z} : \Delta_{E'} \text{ is the discriminant of } E' \in [E]_{\mathbb{Q}}\}$$

The discriminant associated with a global minimal model is called the **minimal discriminant**.

Additive Reduction

- We say E has **additive reduction** at a prime p if $p \mid \gcd(c_4, \Delta^{\min})$ where c_4 is associated to a global minimal model of E.

Additive Reduction

- We say E has **additive reduction** at a prime p if $p \mid \gcd(c_4, \Delta^{\min})$ where c_4 is associated to a global minimal model of E.
- We say E is **semistable at a prime** p if it does not have additive reduction at a prime p.

Additive Reduction

- We say E has **additive reduction** at a prime p if $p \mid \gcd(c_4, \Delta^{\min})$ where c_4 is associated to a global minimal model of E.
- We say E is **semistable at a prime** p if it does not have additive reduction at a prime p.
- We say E is **semistable** if E is semistable at every prime.

Additive Reduction

Example

Suppose we have the elliptic curves

$$E : y^2 + 81xy + 24786y = x^3 + 324x^2$$

$$E' : y^2 + xy = x^3 - 43x + 105.$$

A global minimal model of E is given by E'.
We saw that E' has minimal discriminant $2312 = 2^3 \cdot 17^2$.
We have that $\Delta_{E'}^{\min} = 2^3 \cdot 17^2$ and $c_4 = 5 \cdot 7 \cdot 59$, so we have that E' is semistable.

Computing Minimal Discriminants

- Tate's algorithm (1975)
- Laska's algorithm (1982)
- Kraus-Laska-Connell algorithm (1991)

Frey Curve

The **Frey Curve**, named for Gerhard Frey, is defined by

$$F(a,b) : y^2 = x(x+a)(x-b),$$

where a and b are coprime positive integers with a even. Its discriminant is $\Delta = (4ab(a+b))^2$.

Frey Curve

The **Frey Curve**, named for Gerhard Frey, is defined by

$$F(a,b) : y^2 = x(x+a)(x-b),$$

where a and b are coprime positive integers with a even. Its discriminant is $\Delta = (4ab(a+b))^2$.

Theorem (Hellegouarch, 1975)

The minimal discriminant of $F(a,b)$ is $\Delta^{min} = u^{-12}\Delta$, where

$$u = \begin{cases} 2 & \textit{if } a \equiv 0 \pmod{16} \textit{ and } b \equiv 3 \pmod 4 \\ 1 & \textit{otherwise.} \end{cases}$$

Fermat's Last Theorem

Pomona College

Theorem (Wiles and Taylor, 1995)

Fermat's equation

$$x^n + y^n = z^n$$

has no integer solutions for $n \geq 3$ *such that* $xyz \neq 0$

- Consider the corresponding Frey Curve $F(a^n, b^n) : y^2 = x(x + a^n)(x - b^n)$ taking the values to make $F(a^n, b^n)$ to be semi-stable.
- If Fermat's last theorem were not true, this curve would not be modular

Minimal Discriminant for Frey Curve

- $\gcd(a, b, c) = 1$ which means exactly one of a^n, b^n or c^n must be even,so we can relabel and call the even term a^n.
- Similarly, we can rearrange terms so $b^n \equiv 3 \mod 4$.
- For $F(a^p, b^p) : y^2 = x(x + a^p)(x - b^p)$ where $p \geq 5$, the minimal discriminant is:$\left(\frac{a^p b^p c^p}{16}\right)^2$.
- $a^p \equiv 0 \mod 16$ and $b^p \equiv 3 \mod 4$.

Extension of Hellegouarch

- The Frey curve comes equipped with an easily computable minimal discriminant.
- Barrios extended Hellegourch's result to all elliptic curves with a non-trivial torsion subgroup.
- We focused on extending this result to all elliptic curves that have a non-trivial isogeny.

Kraus' Theorem

Theorem (1989)

Let $\alpha, \beta, \gamma \in \mathbb{Z}$ *with* $\gamma \neq 0$ *be such that* $\alpha^3 - \beta^2 = 1728\gamma$*. There exists an integral Weierstrass model with* $c_4 = \alpha$ *and* $c_6 = \beta$ *if and only if*

1. $v_3(\beta) \neq 2$*, and*
2. - $\beta \equiv -1 \pmod 4$ *if* β *is odd*
   - $v_2(\alpha) \geq 4$ *and* $\beta \equiv 0$ *or* $8 \pmod{32}$ *if* β *is even.*

Kraus' Theorem Example

- We verify that $F : y^2 + 18xy + 189y = x^3$ is an integral model using Kraus' Theorem. Note that for $F_{9,2}$, we have
- $c_4 = 9(36a^2 - 6ab + b^2)(6a + b)b$ and $c_6 = -27(324a^4 - 108a^3b + 54a^2b^2 + 6ab^3 + b^4)(18a^2 + 6ab - b^2)$.
- Plugging in $a = 1$ and $b = 6$ yields $c_4 = 23328$ and $c_6 = -2047032$. This means that $v_3(c_6) = 9$, $v_2(c_4) = 5$, and $c_6 \equiv 8 \pmod{32}$. Kraus tells us that an integral model with these invariants exists!

Isogenies

- An **isogeny** $\pi : E \to E'$ is a nonzero surjective group homomorphism with finite kernel between elliptic curves.

Isogenies

- An **isogeny** $\pi : E \to E'$ is a nonzero surjective group homomorphism with finite kernel between elliptic curves.
- When this occurs, we say that E and E' are **isogenous**.

Isogenies

- An **isogeny** $\pi : E \to E'$ is a nonzero surjective group homomorphism with finite kernel between elliptic curves.
- When this occurs, we say that E and E' are **isogenous**.
- We say an isogeny has degree N if $|\ker \pi| = N$.

Isogenies

- An **isogeny** $\pi : E \to E'$ is a nonzero surjective group homomorphism with finite kernel between elliptic curves.
- When this occurs, we say that E and E' are **isogenous**.
- We say an isogeny has degree N if $|\ker \pi| = N$.
- In particular, a **cyclic** isogeny of degree N has $\ker \pi \cong C_N$. An isogeny of degree N is also called an N-isogeny.

Isogenies

- If $E : y^2 = x^3 + Ax + B$ and $E' : y^2 = x^3 + A'x + B'$ then an isogeny $\phi : E \to E'$ can be written as

$$\phi(x, y) = \left(f(x), c\frac{\mathrm{d}}{\mathrm{d}x}f(x)\right)$$

for some $f(x) \in \mathbb{Q}(x)$ with $c \in \mathbb{Q}$ and $c \neq 0$.

Example of Isogeny

- Taking 2 curves in the 8-isogeny,
  $a4 : y^2 = x^3 - 23003136x + 31708938240$ and
  $a2 : y^2 = x^3 - 21344256x + 37951635456$
- $f(x) = \frac{x^2 - 2688\,x + 331776}{x - 2688}$ and $c = 1$

ISogeny.png

Figure: 24.a Isogeny Class

Example of Isogeny

24.a1.png

Figure: 24.a1

24.a2.png

Figure: 24.a2

Modular Curves

We say that $(E_1, E_1', \pi_1) \sim (E_2, E_2', \pi_2)$ if and only if there exist isomorphisms $\phi : E_1 \to E_2$ and $\phi' : E_1' \to E_2'$ such that

$$\begin{tikzcd} E_1 \arrow[r, "\pi_1"] \arrow[d, "\phi"] & E_1' \arrow[d, "\phi'"] \\ E_2 \arrow[r, "\pi_2"] & E_2' \end{tikzcd}$$

Modular Curves

We say that $(E_1, E_1', \pi_1) \sim (E_2, E_2', \pi_2)$ if and only if there exist isomorphisms $\phi : E_1 \to E_2$ and $\phi' : E_1' \to E_2'$ such that

$$\begin{array}{ccc} E_1 & \xrightarrow{\pi_1} & E_1' \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'} \\ E_2 & \xrightarrow{\pi_2} & E_2' \end{array}$$

Definition (Modular Curves)

The modular curve $X_0(N)$ parameterizes isomorphism classes of triples (E, E', π), where $\pi : E \to E'$ is a cyclic N-isogeny.

Here we consider $N = 1, 2, \ldots, 10, 12, 13, 16, 18, 25$. This is where the genus of $X_0(N)$ is 0.

These parameterizations are made explicit:

Fricke Parameterizations

If two elliptic curves E and E' are isogenous over $\mathbb{Q}$, there exists $t \in \mathbb{Q}$ such that the j-invariants of E and E' are given by $j_{n,1}(t)$ and $j_{n,2}(t)$, respectively:

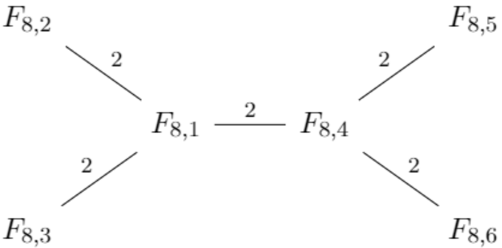
TABLE 1. The Fricke Parameterizations: j-invariants $j_{n,i}$

n	$j_{n,1}(t)$	$j_{n,2}(t)$
6	$\frac{(t+12)^3(t^3+252t^2+3888t+15552)^3}{t^6(t+8)^2(t+9)^3}$	$\frac{(t+6)^3(t^3+18t^2+84t+24)^3}{t(t+8)^3(t+9)^2}$
8	$\frac{(t^4+240t^3+2144t^2+3840t+256)^3}{t(t-4)^8(t+4)^2}$	$\frac{(t^4-16t^2+16)^3}{t^2(t^2-16)}$
9	$\frac{(t+6)^3(t^3+234t^2+756t+2160)^3}{(t-3)^8(t^3-27)}$	$\frac{t^3(t^3-24)^3}{t^3-27}$

Parameterizations exist for the other values of N, but they are omitted.

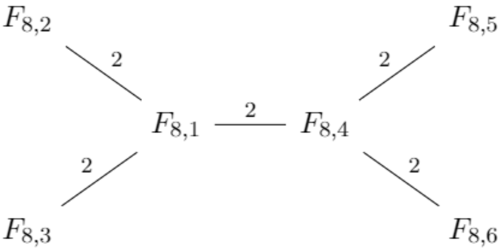
Fricke Parameterizations

Let $n \geq 2$ be an integer such that $X_0(n)$ has genus 0. As part of our research project, we consider various parameterized families of elliptic curves $F_{n,i}(a, b, d)$ with the property that they parameterize isogenous elliptic curves that admit a degree n isogeny.



Fricke Parameterizations

Let $n \geq 2$ be an integer such that $X_0(n)$ has genus 0. As part of our research project, we consider various parameterized families of elliptic curves $F_{n,i}(a,b,d)$ with the property that they parameterize isogenous elliptic curves that admit a degree n isogeny.



These families are related to the Fricke parameterizations by the following theorem:

Fricke Parameterizations

Theorem (Barrios)

Let $n \geq 2$ be an integer such that $X_0(n)$ has genus 0 and suppose E is a rational elliptic curve such that its isogeny degree is n. Then there are integers a, b, d such that $\gcd(a, b) = 1$ and the following hold:

(1) E is $\mathbb{Q}$-isomorphic to $F_{n,k}(a, b, d)$ for some k,

(2) $j_{n,1}\left(\frac{b}{a}\right) = j(F_{n,l}(a, b, d))$ and $j_{n,2}\left(\frac{b}{a}\right) = j(F_{n,h}(a, b, d))$ for some l and h,

(3) The isogeny class of E is $\left\{[F_{n,i}(a, b, d)]_{\mathbb{Q}}\right\}_i$.

Above, $j_{n,i}(t)$ refers to the Fricke parameterization.

Our Task

We aim to classify the minimal discriminants of elliptic curves with non-trivial isogeny.

So far, we have classified the minimal discriminants of 6-, 8-, and 9-isogenous elliptic curves in terms of arithmetic conditions on the parameters a and b, taking $d = 1$.

Our Task

Lemma

If E is a rational elliptic curve given by an integral Weierstrass model with invariants c_4 and c_6 and discriminant Δ, then there is a unique positive integer u such that

$$c_4' = u^{-4}c_4, \qquad c_6' = u^{-6}c_6, \qquad \textit{and} \qquad \Delta_E^{\textit{min}} = u^{-12}\Delta$$

where $\Delta_E^{\textit{min}}$ is the minimal discriminant of E and c_4' and c_6' are the invariants associated to a global minimal model of E.

Main Theorem

Theorem (B.,E.,F.,M.,S.)

Let $n = 6,\ 8,$ or 9 and consider the elliptic curves $F_{n,i} = F_{n,i}(a, b, 1)$. Let $\Delta_{n,i}$ denote the discriminant of $F_{n,i}$. Then the minimal discriminant of $F_{n,i}$ is $u^{-12}\Delta_{n,i}$ where u is uniquely determined from the p-adic valuations given in the following table:

Results

n	p	Condition on a, b	$(v_p(u_{n,i}))_i$
6	2	$v_2(b) = 0$	$(1, 0, 1, 2)$
		$v_2(b) = 1$	$(2, 0, 1, 2)$
		$v_2(b) = 2$	$(3, 0, 2, 2)$
		$v_2(b) \geq 3$	$(3, 1, 3, 3)$
	3	$v_3(b) = 0$	$(0, 0, 0, 0)$
		$v_3(b) = 1$	$(1, 1, 0, 0)$
		$v_3(b) \geq 2$	$(2, 2, 1, 1)$
8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$
9	3	$v_3(b) = 0$	$(1, 0, 0)$
		$v_3(b) \geq 1$ and $v_3(a - \frac{b}{3}) = 0$	$(1, 1, 0)$
		$v_3(b) = 1$ and $v_3(a - \frac{b}{3}) = 1$	$(2, 1, 0)$
		$v_3(b) = 1$ and $v_3(a - \frac{b}{3}) > 1$	$(3, 2, 1)$

How to Use the Table

This is the table that displays our results for the 6 curves of the 8-Isogeny:

8	2	$v_2(b)=0$	$(1,2,?,0,0,1)$
		$v_2(b)=1$	$(2,?,?,1,1,2)$
		$v_2(b)=2$ and $v_2(a^2-\frac{b^2}{16})\geq 4$	$(5,?,?,?,3,3)$
		$v_2(b)=2$ and $v_2(a^2-\frac{b^2}{16})\leq 3$	$(4,?,?,?,2,2)$
		$v_2(b)=2$ and $v_2(a+\frac{b}{4})=0$	$(3,?,?,?,2,2)$
		$v_2(b)=2$, $v_2(a+\frac{b}{4})=1$, and $v_2(a-\frac{b}{4})\leq 2$	$(4,?,?,?,2,2)$
		$v_2(b)=2$, $v_2(a+\frac{b}{4})=1$, and $v_2(a-\frac{b}{4})\geq 3$	$(5,?,?,?,3,3)$
		$v_2(b)=2$ and $v_2(a+\frac{b}{4})=2$	$(5,?,?,?,2,2)$
		$v_2(b)=2$ and $v_2(a+\frac{b}{4})\geq 3$	$(5,?,?,?,3,3)$
		$v_2(b)\geq 3$	$(3,?,?,2,3,2)$

How to Use the Table

This is the table that displays our results for the 6 curves of the 8-Isogeny:

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

But how do we read it? Lets try some examples.

How to Use the Table: curve 6, $a = 1$, $b = 7$

Pomona College

Example: Try to find the u value of the 6th curve of the 8-Isogeny when $a = 1$ $b = 7$. $F_{8,6}(1,7) : y^2 = x^3 - 164x^2 + 256x$
$b = 7 = 7 \cdot 1 = 7 \cdot 2^0$. So the $v_2(b) = 0$.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

How to Use the Table: curve 6, $a = 1$, $b = 7$

Find the condition that is satisfied when $v_2(b) = 0$.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

How to Use the Table: curve 6, $a = 1$, $b = 7$

Now since we are finding the u value when for the 6th curve of the 8-Isogeny, we look at the 6th column to find our answer.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

How to Use the Table: curve 6, $a = 1$, $b = 7$

Now since we are finding the u value when for the 6th curve of the 8-Isogeny, we look at the 6th column to find our answer.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

So for the 6th curve of the 8-Isogeny, $v_2(u) = 1$, so $u = 2$ when $a = 1$ and $b = 7$.

How to Use the Table: Curve 1, $a = 59$, $b = 20$

Now lets try this example: Find the u value of the 1st curve of the 8-isogeny when $a = 59$ and $b = 20$.

$F_{8,1}(59, 20) : y^2 + 160xy - 35389440y = x^3 - 221184x^2$

$b = 20 = 4 \cdot 5 = 2^2 \cdot 5$. So $v_2(b) = 2$.

$a + \frac{b}{4} = 59 + \frac{20}{4} = 64 = 2^6$. So $v_2(a + \frac{b}{4}) = 6$.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

How to Use the Table: Curve 1, $a = 59$, $b = 20$

Find the condition that is satisfied when $v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 6$.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

How to Use the Table: Curve 1, $a = 59$, $b = 20$

Now since we are finding the u value when for the 1st curve of the 8-Isogeny, we look at the 1st column to find our answer.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

How to Use the Table: Curve 1, $a = 59$, $b = 20$

Now since we are finding the u value when for the 1st curve of the 8-Isogeny, we look at the 1st column to find our answer.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

So for the 1st curve of the 8-Isogeny, $v_2(u) = 5$, so $u = 32$ when $a = 59$ and $b = 20$.

How to Use the Table: Curve 5, $a = 117$, $b = 68$

One more example: Find the u value of the 5th curve of the 8-isogeny when $a = 117$ and $b = 68$.

$F_{8,5}(117, 68) : y^2 = x^3 - 866848x^2 + 21381376x$

$b = 68 = 4 \cdot 17 = 2^2 \cdot 17$. So $v_2(b) = 2$.

$a + \frac{b}{4} = 117 + \frac{68}{4} = 134 = 2 \cdot 67$. So $v_2(a + \frac{b}{4}) = 1$.

$a - \frac{b}{4} = 117 - \frac{68}{4} = 100 = 4 \cdot 25 = 2^2 \cdot 25$. So $v_2(a - \frac{b}{4}) = 2$.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

How to Use the Table: Curve 5, $a = 117$, $b = 68$

Find the condition that is satisfied when $v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) = 2$.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

How to Use the Table: Curve 5, $a = 117$, $b = 68$

Now since we are finding the u value when for the 5th curve of the 8-Isogeny, we look at the 5th column to find our answer.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

How to Use the Table: Curve 5, $a = 117$, $b = 68$

Now since we are finding the u value when for the 5th curve of the 8-Isogeny, we look at the 5th column to find our answer.

8	2	$v_2(b) = 0$	$(1, 2, ?, 0, 0, 1)$
		$v_2(b) = 1$	$(2, ?, ?, 1, 1, 2)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \geq 4$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a^2 - \frac{b^2}{16}) \leq 3$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 0$	$(3, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \leq 2$	$(4, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$, $v_2(a + \frac{b}{4}) = 1$, and $v_2(a - \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) = 2$	$(5, ?, ?, ?, 2, 2)$
		$v_2(b) = 2$ and $v_2(a + \frac{b}{4}) \geq 3$	$(5, ?, ?, ?, 3, 3)$
		$v_2(b) \geq 3$	$(3, ?, ?, 2, 3, 2)$

So for the 5th curve of the 8-Isogeny, $v_2(u) = 2$, so $u = 4$ when $a = 117$ and $b = 68$.

Torsion Method

The torsion method works when our elliptic curves $F_{n,i}$ have a non-trivial point of finite order. If this is the case, then there is a classification for the minimal discriminant of such elliptic curves. Consequently, our second method deduces the minimal discriminant of $F_{n,i}$ by using this classification.

Torsion Method Techniques: 6th Isogeny, 2nd Curve

Let $A = 9a$, $B = -9a - b$, and $d = \gcd(A, B)$. Then,

$$F_{6,2} = E_{C_6}(A, B) : y^2 + (a-b)xy - (A^2B + AB^2)y = x^3 - (AB + B^2)x^2$$

By the classification of minimal discriminants of elliptic curves with non-trivial torsion, the minimal discriminant of $F_{6,2}$ is

$$u^{-12}d^{-12}\Delta_{F_{6,2}} \text{ where } u = \begin{cases} 2 & \text{if } \nu_2(\frac{A}{d} + \frac{B}{d}) \geq 3 \\ 1 & \text{if } \nu_2(\frac{A}{d} + \frac{B}{d}) \leq 2 \end{cases}$$

Using the Torison Method: The 6-Isogeny

$$\begin{tikzcd}
F_{6,1} \arrow[r, dash, "2"] \arrow[d, dash, "3"] & F_{6,2} \arrow[d, dash, "3"] \\
F_{6,3} \arrow[r, dash, "2"] & F_{6,4}
\end{tikzcd}$$

Thank you!

Questions?

We would like to thank Dr. Alex Barrios of the Pomona Research in Mathematics Experience as well as Dr. Edray Goins and Dr. Rachel Davis. Our work was funded by the National Security Agency (H98230-21-1-0015).

Example: 2nd Curve of the 6-Isogeny

$A : 9a \qquad B : -9a - b$

Step 1: If $p \mid \gcd(A, B)$, $p \neq 3$, then

$9a \equiv 0 \mod p \to p \mid a$

$9a - b \equiv 0 \mod p \to p \mid b$

This is a contradiction as a and b are relatively prime.

$3 \mid \gcd(A, B) \to 3 \mid 9a + b \to 3 \mid b$

Example: 2nd Curve of the 6-Isogeny

Step 2:

$$v_3(\gcd(A,B)) = \begin{cases} 0 & \text{if } v_3(b) = 0 \\ 1 & \text{if } v_3(b) = 1 \\ 2 & \text{if } v_3(b) \geq 2 \end{cases}$$

Example: 2nd Curve of the 6-Isogeny

Step 3: Find u' values using Theorem 4.4: $T = C_6$, which has:
$u' = 2$ if $v_2(A + B) \geq 3$
$u' = 1$ if $v_2(A + B) \leq 2$
Note that $A + B = -b$, so $v_2(A + B) = v_2(b)$

Example: 2nd Curve of the 6-Isogeny

Results:

$v_3(b) = 0$ and $v_2(b) \leq 2$, then $u = 1$

$v_3(b) = 0$ and $v_2(b) \geq 3$, then $u = 2$

$v_3(b) = 1$ and $v_2(b) \leq 2$, then $u = 3$

$v_3(b) = 1$ and $v_2(b) \geq 3$, then $u = 6$

$v_3(b) \geq 2$ and $v_2(b) \leq 2$, then $u = 9$

$v_3(b) \geq 2$ and $v_2(b) \geq 3$, then $u = 18$