Minimal Discriminants of Elliptic Curves with a 4-Isogeny

Thea Nicholson (Xavier University of Louisiana), Louis Burns (Pomona College), & Jewel Aho (University of St. Thomas)

January 4, 2024

Why do we care about Elliptic Curves

Theorem (Pythagorean Theorem 1600 B.C.E.)

Let a, b, and c denote the sides of a right triangle, with c denoting the hypotenuse. Then

$$a^2 + b^2 = c^2.$$

Why do we care about Elliptic Curves

Theorem (Pythagorean Theorem 1600 B.C.E.)

Let a, b, and c denote the sides of a right triangle, with c denoting the hypotenuse. Then

$$a^2 + b^2 = c^2.$$

How many integer solutions can solve $a^2 + b^2 = c^2$?

Why do we care about Elliptic Curves

Theorem (Pythagorean Theorem 1600 B.C.E.)

Let a, b, and c denote the sides of a right triangle, with c denoting the hypotenuse. Then

$$a^2 + b^2 = c^2.$$

How many integer solutions can solve $a^2 + b^2 = c^2$?

- Infinitely Many!

Why do we care about Elliptic Curves

Theorem (Pythagorean Theorem 1600 B.C.E.)

Let a, b, and c denote the sides of a right triangle, with c denoting the hypotenuse. Then

$$a^2 + b^2 = c^2.$$

How many integer solutions can solve $a^2 + b^2 = c^2$?

- Infinitely Many!

Theorem (Fermat's Last Theorem)

If n is an integer greater than 2, then

$$a^n + b^n = c^n$$

has no nonzero integer solutions.

Fermat's Last Theorem

- For the next 357 years mathematicians would try to recreate the proof that Fermat claimed to have.

Fermat's Last Theorem

- For the next 357 years mathematicians would try to recreate the proof that Fermat claimed to have.
- In the early 1990's Andrew Wiles proved Fermat's Last Theorem by using elliptic curves. This proof relied on knowledge of the minimal discriminant of a special kind of elliptic curve.

Fermat's Last Theorem

- For the next 357 years mathematicians would try to recreate the proof that Fermat claimed to have.
- In the early 1990's Andrew Wiles proved Fermat's Last Theorem by using elliptic curves. This proof relied on knowledge of the minimal discriminant of a special kind of elliptic curve.
- Our Goal
  - Our goal for the summer was to make it easier for mathematicians to find the minimal discriminants of elliptic curves with a 4-isogeny. We also worked on finding when such elliptic curves have additive reduction.

Crash Course on Elliptic Curves

We define an **elliptic curve** $E/\mathbb{Q}$ to be given by the following equation

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

We define an **elliptic curve** $E/\mathbb{Q}$ to be given by the following equation

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

For an elliptic curve E, the **invariants** of the elliptic curve are

defined to be

$$c_4 = a_1^4 + 8a_1^2a_2 - 24a_1a_3 + 16a_2^2 - 48a_4$$
$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)\left(2a_4 + a_1a_3\right) - 216\left(a_2^3 + 4a_6\right)$$
$$\Delta = \frac{c_4^3 - c_6^2}{1728} \neq 0.$$

We define an **elliptic curve** $E/\mathbb{Q}$ to be given by the following equation

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

For an elliptic curve E, the **invariants** of the elliptic curve are

defined to be

$$c_4 = a_1^4 + 8a_1^2a_2 - 24a_1a_3 + 16a_2^2 - 48a_4$$
$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)(2a_4 + a_1a_3) - 216\left(a_2^3 + 4a_6\right)$$
$$\Delta = \frac{c_4^3 - c_6^2}{1728} \neq 0.$$

The **signature** of an elliptic curve E is $Sig(E) = (c_4, c_6, \Delta)$.

Examples of Elliptic Curves

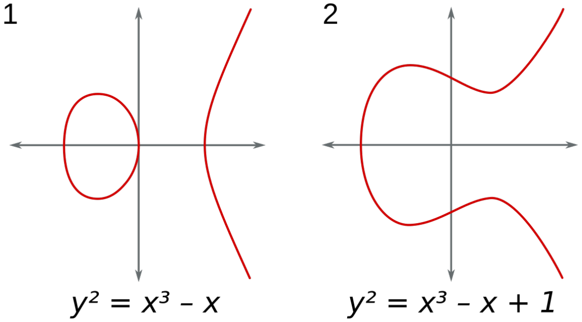
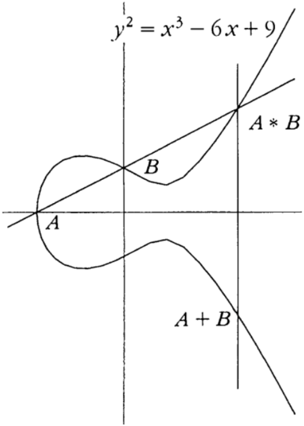
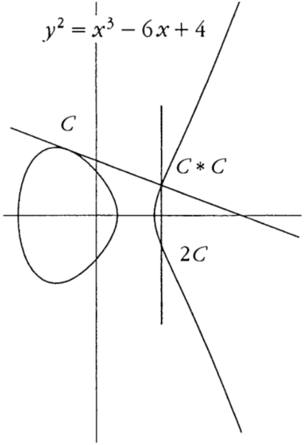


Figure: elliptic curve examples

Group Structures





Elliptic Curves

Given an elliptic curve

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

with each a_i a rational number, one can transform and/or scale the graph of E to obtain an isomorphic elliptic curve

$$E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

with the property that each a_i' is an integer and the discriminant Δ' of E' is "minimal" in the sense that $|\Delta'|$ is the smallest discriminant that can be attained from E via translations and/or scalings.

Elliptic Curves

Given an elliptic curve

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

with each a_i a rational number, one can transform and/or scale the graph of E to obtain an isomorphic elliptic curve

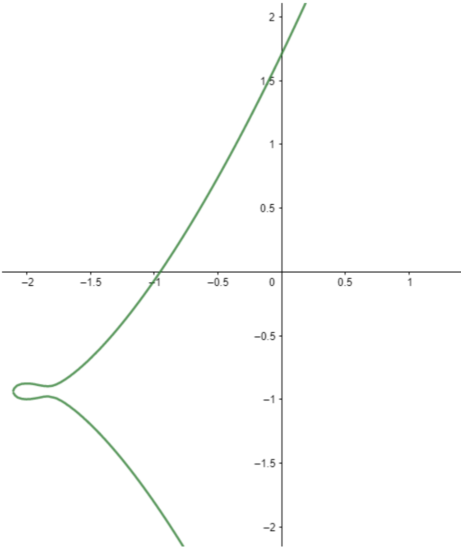
$$E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$$

with the property that each a'_i is an integer and the discriminant Δ' of E' is "minimal" in the sense that $|\Delta'|$ is the smallest discriminant that can be attained from E via translations and/or scalings.

Definition

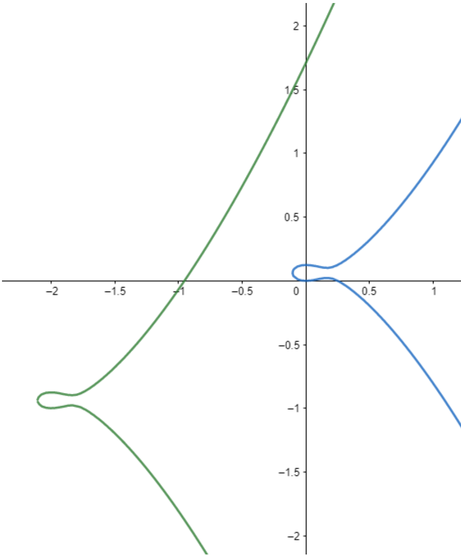
We say that E' is a **global minimal model** for E, and call Δ' **the minimal discriminant of** E. The signature of E' is **the minimal signature** of E, and is denoted by $\mathrm{sig}_{\min}(E) = (c'_4, c'_6, \Delta')$.

As an example, consider the elliptic curve E_{green} : $y^2 + \frac{15}{8}y = x^3 + \frac{23}{4}x^2 + 11x + \frac{49}{8}$. Then $\text{sig}(E_{\text{green}}) = \left(1, \frac{-19}{8}, \frac{-11}{4096}\right)$.



Consider the elliptic curve E_{green} : $y^2 + \frac{15}{8}y = x^3 + \frac{23}{4}x^2 + 11x + \frac{49}{8}$. Then $\text{sig}(E_{\text{green}}) = \left(1, \frac{-19}{8}, \frac{-11}{4096}\right)$.

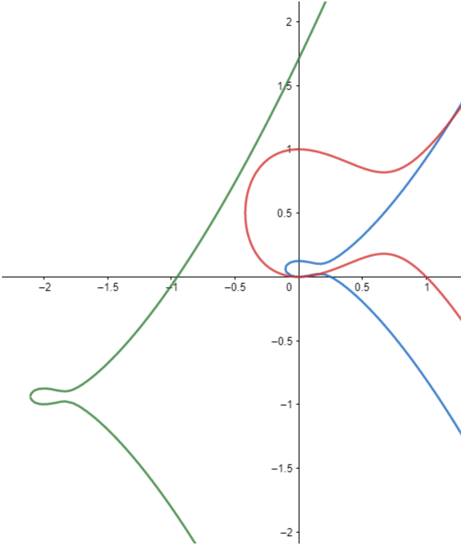
Next, we translate E_{green} to attain $E_{\text{blue}} : y^2 - \frac{1}{8}y = x^3 - \frac{1}{4}x^2$. It turns out that $\text{sig}(E_{\text{green}}) = \text{sig}(E_{\text{blue}})$.



As an example, consider the elliptic curve E_{green} : $y^2 + \frac{15}{8}y = x^3 + \frac{23}{4}x^2 + 11x + \frac{49}{8}$. Then $\text{sig}(E_{\text{green}}) = \left(1, \frac{-19}{8}, \frac{-11}{4096}\right)$.

Next, we translate E_{green} to obtain $E_{\text{blue}} : y^2 - \frac{1}{8}y = x^3 - \frac{1}{4}x^2$. It turns out that $\text{sig}(E_{\text{green}}) = \text{sig}(E_{\text{blue}})$.

Lastly, we scale E_{blue} to obtain $E_{\text{red}} : y^2 - y = x^3 - x^2$, which is a global minimal model for E_{green}. In particular, $\text{sig}_{\text{min}}(E_{\text{green}}) = \text{sig}(E_{\text{red}}) = (16, -152, -11)$.



Isogenies

- In the same way that E and E' can be isomorphic we can find two elliptic curves that have a group homomorphism between them. We call that mapping an isogeny.

Isogenies

- In the same way that E and E' can be isomorphic we can find two elliptic curves that have a group homomorphism between them. We call that mapping an isogeny.

Definition

We say that $f : E \to E'$ is an **isogeny** if f is a surjective group homomorphism. If $\ker f \cong \mathbb{Z}/n\mathbb{Z}$, then we call f an **n-isogeny** and we say n is the degree of the n-isogeny.

Isogenies

- In the same way that E and E' can be isomorphic we can find two elliptic curves that have a group homomorphism between them. We call that mapping an isogeny.

Definition

We say that $f : E \to E'$ is an **isogeny** if f is a surjective group homomorphism. If $\ker f \cong \mathbb{Z}/n\mathbb{Z}$, then we call f an **n-isogeny** and we say n is the degree of the n-isogeny.

Example

$$E : y^2 = x^3 - 1440x^2 + 108800x$$

The origin $P = (0, 0)$ of E is a point of order 2. Then we get the isogeny $E' = E$ mod P

$$E' : y^2 = x^3 + 2880x^2 + 1638400x$$

Isogenies

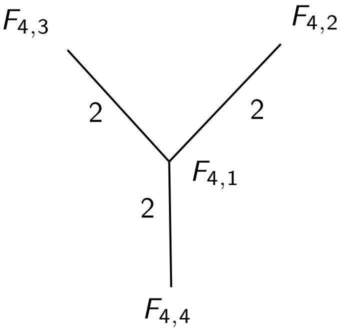
The study of elliptic curves that have isogeny class degree equal to 4 is equivalent to understanding the parameterized elliptic curves $F_{4,i}(a, b, d)$ for $i = 1, 2, 3, 4$ that are given below:

$$F_{4,1}(a, b, d) : y^2 = x^3 + (ad - 16bd)x^2 - 16abd^2x$$
$$F_{4,2}(a, b, d) : y^2 = x^3 + (ad + 8bd)x^2 + 16b^2d^2x$$
$$F_{4,3}(a, b, d) : y^2 = x^3 + (32bd - 2ad)x^2 + (a^2d^2 + 32abd^2 + 256b^2d^2)x$$
$$F_{4,4}(a, b, d) : y^2 = x^3 - (2ad + 64bd)x^2 + a^2d^2x$$

Moreover, $Sig(F_{4,1}(a, b, d)) = (16a^2d^2 + 256abd^2 + 4096b^2d^2,$
$-64a^3d^3 - 1536a^2bd^3 + 24576ab^2d^3 + 262144b^3d^3,$
$4096a^4b^2d^6 + 131072a^3b^3d^6 + 1048576a^2b^4d^6)$

Isogeny Graphs

In the notation $F_{4,i}$, 4 is the **isogeny class degree**, i is an index denoting a vertex on an **isogeny graph**, and each edge corresponds to a 2-isogeny between elliptic curves.



Kraus's Theorem

Theorem (Kraus's Theorem, 1989)

Let $\alpha, \beta, \gamma \in \mathbb{Z}$ with $\alpha^3 - \beta^2 = 1728\gamma$ with $\alpha \neq 0$. Then there is an elliptic curve, E, with integer coefficients and with $Sig(E) = (\alpha, \beta, \gamma)$ if and only if

1. $v_3(\beta) \neq 2$
2. *Either* $\beta \equiv -1 \mod 4$ *or both* $v_2(\alpha) \geq 4$ *and* $\beta \equiv 0, 8 \mod 32$.

More About Isomorphic Elliptic Curves

Definition (Isomorphic)

Let E and E' be elliptic curves over $\mathbb{Q}$. We say that E and E' are **isomorphic**, denoted $E \cong E'$, if and only if there exist $u, r, s, w \in \mathbb{Q}, u \neq 0$ such that we have a map

$$E \longrightarrow E' \text{ where } (x, y) \longmapsto (u^2x + r, u^3y + u^2sx + w).$$

More About Isomorphic Elliptic Curves

Definition (Isomorphic)

Let E and E' be elliptic curves over $\mathbb{Q}$. We say that E and E' are **isomorphic**, denoted $E \cong E'$, if and only if there exist $u, r, s, w \in \mathbb{Q}, u \neq 0$ such that we have a map

$$E \longrightarrow E' \text{ where } (x, y) \longmapsto (u^2x + r, u^3y + u^2sx + w).$$

Denote $Sig(E) = (c_4, c_6, \Delta)$ and $Sig(E') = (c_4', c_6', \Delta')$. If $E \cong E'$, then we have the following relationship

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

Results!

Theorem (A.,B.,N., 2023)

Let $a, b, d \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and d squarefree. If $F_{4,i}(a, b, d)$ is an elliptic curve with discriminant $\Delta_{4,i}$, then the minimal discriminant of $F_{4,i}(a, b, d)$ is $u_i^{-12}\Delta_{4,i}$ where u_i is given below.

$v_2(a)$	Additional conditions		(u_1, u_2, u_3, u_4)
≥ 8	$bd \equiv 3 \mod 4$		$(8, 4, 8, 16)$
	$bd \not\equiv 3 \mod 4$		$(4, 2, 4, 8)$
$6, 7$			$(4, 2, 4, 8)$
5	d is even		$(4, 2, 4, 8)$
	d is odd		$(4, 2, 4, 4)$
4	$v_2(a + 16b) \geq 8$	$bd \equiv 1 \mod 4$	$(8, 4, 16, 8)$
		$bd \not\equiv 1 \mod 4$	$(8, 4, 8, 4)$
	$v_2(a + 16b) < 8$	d is even	$(8, 4, 8, 4)$
		d odd, $v_2((a + 16b)^2 - 256ab) \geq 12$	$(8, 4, 8, 4)$
		d odd, $v_2((a + 16b)^2 - 256ab) < 12$	$(8, 4, 4, 4)$
3	d is even		$(4, 2, 4, 4)$
	d is odd		$(2, 2, 2, 2)$
2			$(2, 2, 2, 2)$
1	d is even		$(2, 2, 2, 2)$
	d is odd		$(1, 1, 1, 1)$
0	$a \equiv 1 \mod 4$		$(2, 2, 2, 2)$
	$a \not\equiv 1 \mod 4$		$(1, 1, 1, 1)$

Our Theorem!!

$v_2(a)$	Additional conditions		(u_1, u_2, u_3, u_4)
≥ 8	$bd \equiv 3 \mod 4$		$(8, 4, 8, 16)$
	$bd \not\equiv 3 \mod 4$		$(4, 2, 4, 8)$
$6, 7$			$(4, 2, 4, 8)$
5	d is even		$(4, 2, 4, 8)$
	d is odd		$(4, 2, 4, 4)$
4	$v_2(a + 16b) \geq 8$	$bd \equiv 1 \mod 4$	$(8, 4, 16, 8)$
		$bd \not\equiv 1 \mod 4$	$(8, 4, 8, 4)$
	$v_2(a + 16b) < 8$	d is even	$(8, 4, 8, 4)$
		d odd, $v_2((a + 16b)^2 - 256ab) \geq 12$	$(8, 4, 8, 4)$
		d odd, $v_2((a + 16b)^2 - 256ab) < 12$	$(8, 4, 4, 4)$
3	d is even		$(4, 2, 4, 4)$
	d is odd		$(2, 2, 2, 2)$
2			$(2, 2, 2, 2)$
1	d is even		$(2, 2, 2, 2)$
	d is odd		$(1, 1, 1, 1)$
0	$a \equiv 1 \mod 4$		$(2, 2, 2, 2)$
	$a \not\equiv 1 \mod 4$		$(1, 1, 1, 1)$

Example

Consider $F_{4,i}(a, b, d)$ where $(a, b, d) = (16, -17, -5)$. Then

$$v_2(a) = 4$$

Example

Consider $F_{4,i}(a, b, d)$ where $(a, b, d) = (16, -17, -5)$. Then

$$v_2(a) = 4$$

$$v_2(a + 16b) = v_2(16 + 16(-17)) = v_2(16(1 - 17)) = 8$$

Example

Consider $F_{4,i}(a, b, d)$ where $(a, b, d) = (16, -17, -5)$. Then

$$v_2(a) = 4$$

$$v_2(a + 16b) = v_2(16 + 16(-17)) = v_2(16(1 - 17)) = 8$$

and

$$bd \equiv 17 \cdot 4 \mod 4 \equiv 1 \mod 4$$

Example

Consider $F_{4,i}(a, b, d)$ where $(a, b, d) = (16, -17, -5)$. Then

$$v_2(a) = 4$$

$$v_2(a + 16b) = v_2(16 + 16(-17)) = v_2(16(1 - 17)) = 8$$

and

$$bd \equiv 17 \cdot 4 \mod 4 \equiv 1 \mod 4$$

By the table, we have $(u_1, u_2, u_3, u_4) = (8, 4, 16, 8)$. As a consequence, we have that

$$\Delta_1^{min} = 8^{-12}(2^{36} \cdot 5^6 \cdot 17^2) = 5^6 \cdot 17^2$$
$$\Delta_2^{min} = 4^{-12}(-1 \cdot 2^{24} \cdot 5^6 \cdot 17^4) = -1 \cdot 5^6 \cdot 17^4$$
$$\Delta_3^{min} = 16^{-12}(2^{48} \cdot 5^6 \cdot 17) = 5^6 \cdot 17$$
$$\Delta_4^{min} = 8^{-12}(2^{36} \cdot 5^6 \cdot 17) = 5^6 \cdot 17$$

Whats Next?

We just looked at the family of elliptic curves with isogeny class degree 4, but there are so many other families of elliptic curves. Namely, those with isogeny class degree n where

$$n \in \{2, 3, \cdots, 10, 12, 13, 16, 18, 25\}$$

Acknowledgements

We would like to give a big thanks to Alex Barrios (University of St. Thomas) and Fabian Ramirez (UCI) for teaching us about elliptic curves! Thank you, Dr. Goins, for running PRIME! As well as NSF (DMS-2113782) for sponsoring PRIME last year!