Elliptic Curves: Minimal Discriminants and Additive Reduction

Jewel Aho [1] Louis Burns [2] Thea Nicholson [3]

[1]University of St. Thomas [2]Pomona College [3]Xavier University of Louisiana

Abstract

Elliptic curves over $\mathbb{Q}$ that admit a cyclic isogeny of degree n are parameterizable. In this project, we consider the family of parameterized elliptic curves corresponding to an isogeny class degree of 4. We classify their minimal discriminants and give necessary and sufficient conditions for determining the primes at which additive reduction occurs.

Elliptic Curves

- Let $\mathbb{Q}$ be the field of rational numbers. We define an **elliptic curve** $E/\mathbb{Q}$ as a curve given by an (affine) Weierstrass model

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

where $a_i \in \mathbb{Q}$ and every point on the curve has a unique tangent. We also include a point at infinity $\mathcal{O}$. If each $a_i \in \mathbb{Z}$, then we say that E is given by an **integral Weierstrass model**.

- The **signature** of an elliptic curve E is $\mathrm{Sig}(E) = (c_4, c_6, \Delta)$ where c_4, c_6, and Δ are the invariants of E defined to be

$$c_4 = a_1^4 + 8a_1^2a_2 - 24a_1a_3 + 16a_2^2 - 48a_4$$
$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)(2a_4 + a_1a_3) - 216\left(a_3^2 + 4a_6\right)$$
$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$

Kraus's Theorem, 1989

Let $\alpha, \beta, \gamma \in \mathbb{Z}$ with $\alpha^3 - \beta^2 = 1728\gamma \neq 0$. Then there exists some integral Weierstrass model E with $\mathrm{Sig}(E) = (\alpha, \beta, \gamma)$ 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 $\beta \equiv 0, 8 \mod 32$.

Isomorphisms

- Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$. We say that E_1 and E_2 are **$\mathbb{Q}$-isomorphic**, denoted $E_1 \cong_{\mathbb{Q}} E_2$, if and only if there exist $u, r, s, w \in \mathbb{Q}, u \neq 0$ such that we have a map

$$E_1 \longrightarrow E_2 \text{ where } (x, y) \longmapsto (u^2x + r, u^3y + u^2sx + w).$$

- We define the **$\mathbb{Q}$-isomorphism class** of E_1, denoted $[E_1]_{\mathbb{Q}}$, to be the set of all elliptic curves that are $\mathbb{Q}$-isomorphic to E_1.
- Denote $\mathrm{Sig}(E_1) = (c_4, c_6, \Delta)$ and $\mathrm{Sig}(E_2) = (c_4', c_6', \Delta')$. If $E_1 \cong_{\mathbb{Q}} E_2$, then we have the following relationship

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

Minimal Discriminants and Global Minimal Models

- Let $E/\mathbb{Q}$ be an elliptic curve. The **minimal discriminant** of E, denoted Δ_E^{min}, is the discriminant of an integral Weierstrass model that is $\mathbb{Q}$-isomorphic to E and satisfies:

$$|\Delta_E^{min}| = \min\{|\Delta_{E/\mathbb{Q}}| : F \cong_{\mathbb{Q}} E \text{ and } F \text{ is an integral model}\}.$$

We say that E is given by a **global minimal model** if it is given by an integral model with discriminant Δ_E^{min}.

- Let $E/\mathbb{Q}$ be an elliptic curve and let F be a global minimal model for E. The **minimal signature** of E is

$$\mathrm{Sig}_{min}(E) = \mathrm{Sig}(F) = \left(c_4, c_6, \Delta_E^{min}\right).$$

- We say that E has **additive reduction** at p if $p \mid gcd(c_4, \Delta_E^{min})$. Similarly, we say that E has **semistable reduction** at p if E does not have additive reduction at p.

Isogenies

- We say that $\pi : E_1 \to E_2$ is an **isogeny** if π is a surjective group homomorphism $\pi : E_1 \to E_2$. The $\ker \pi$ is finite and we define the **degree** of the isogeny to be $\# \ker \pi$. We say that an isogeny π is **cyclic** if $\ker \pi \cong \mathbb{Z}/n\mathbb{Z}$, and we say that π is an **n-isogeny**.
- Consider two elliptic curves over $\mathbb{Q}$, i.e. $E_1 : y^2 = x^3 + A_1x + B_1$ and $E_2 : y^2 = x^3 + A_2x + B_2$. It turns out that all cyclic isogenies $\pi : E_1 \to E_2$ are of the form

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

where $f(x) \in \mathbb{Q}(x)$ and $c \in \mathbb{Q} \setminus \{0\}$

- The **isogeny class** of E is the set

$$\mathrm{Iso}(E) = \{[F]_{\mathbb{Q}} : F \text{ is isogenous to } E\}$$

The isogeny class (over $\mathbb{Q}$) of an elliptic curve E defined over $\mathbb{Q}$ is the set of all isomorphism classes of elliptic curves defined over $\mathbb{Q}$. The **isogeny class degree** is the largest n-isogeny that occurs between elements of the set.

- The **isogeny graph** of E is the graph whose vertices are elements of $\mathrm{Iso}(E)$, and the edges of the graph correspond to isogenies of prime degrees between representatives of vertices.
- At a given prime, isogenous elliptic curves have the same reduction types.

Families of Elliptic Curves

Theorem (Barrios, 2023)

Let $E/\mathbb{Q}$ be an elliptic curve that has isogeny class degree equal to 4. Then there are $a, b, d \in \mathbb{Z}$ with $gcd(a, b) = 1$ and d is squarefree such that the isogeny class of E is $\{[F_{4,i}(a, b, d)]_{\mathbb{Q}}\}_{i=1}^{4}$. Moreover, the isogeny graph of E is given in the figure below.

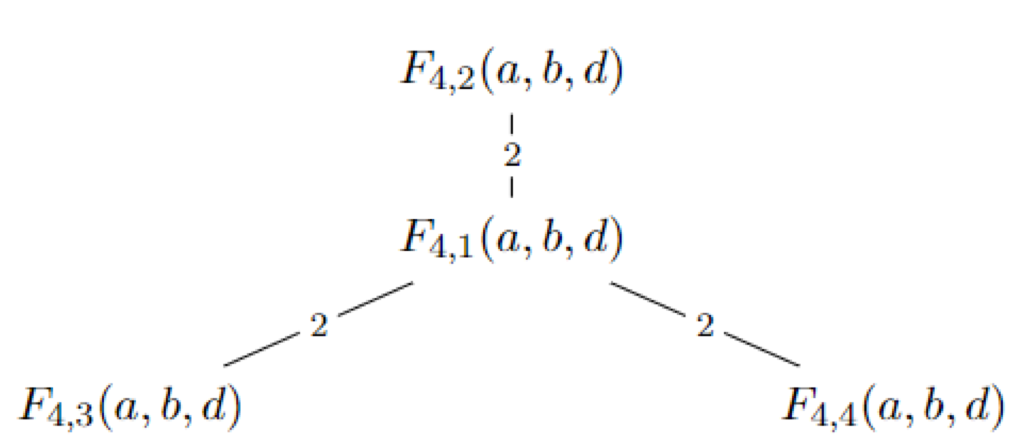

Figure: Isogeny graph of degree 4

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

Example

$$F_{4,1}(16, -17, -5) : y^2 = x^3 - 1440x^2 + 108800x,$$
$$F_{4,2}(16, -17, -5) : y^2 = x^3 + 600x^2 + 115600x,$$
$$F_{4,3}(16, -17, -5) : y^2 = x^3 + 2880x^2 + 1638400x,$$
$$F_{4,4}(16, -17, -5) : y^2 = x^3 - 5280x^2 + 6400x$$

Theorem 1 (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 in the table 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	$a \equiv 1 \mod 4$		$(2, 2, 2, 2)$
	$a \not\equiv 1 \mod 4$		$(1, 1, 1, 1)$

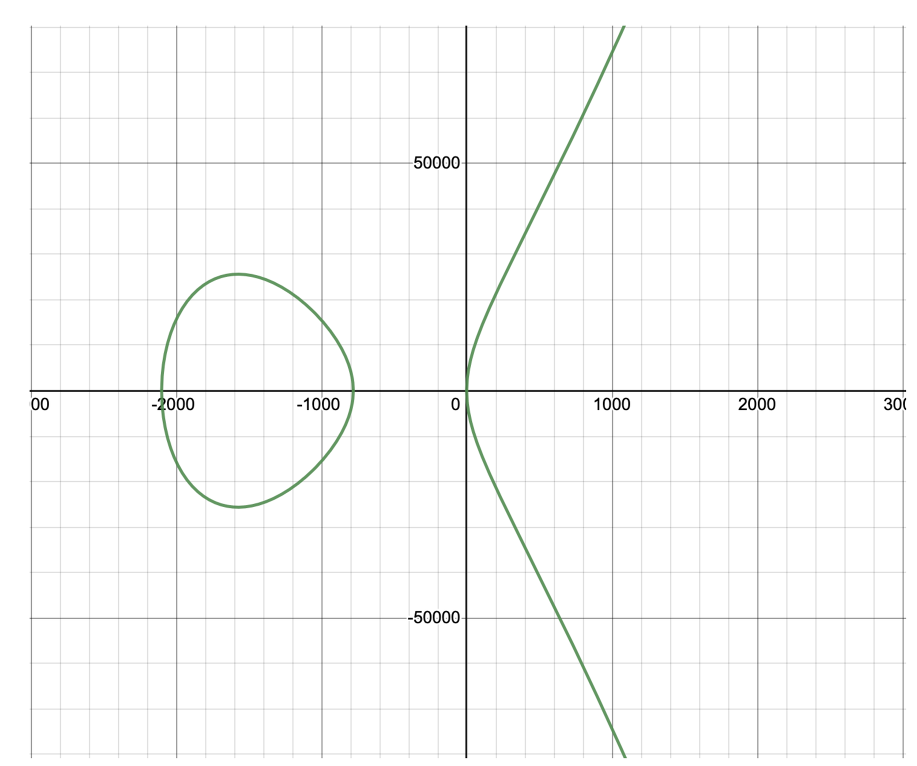

Figure: $F_{4,3}(16, -17, -5)$

Example

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

$$F_{4,1}(16, -17, -5) : y^2 = x^3 - 1440x^2 + 108800x$$
$$Sig(E) = (2^{12} \cdot 3 \cdot 5^2 \cdot 7 \cdot 13, 2^{18} \cdot 3^4 \cdot 5^4 \cdot 11, 2^{36} \cdot 5^6 \cdot 17^2)$$

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

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

Theorem 2 (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, then $F_{4,i}$ has additive reduction at a prime p if and only if p is listed in the table below and the corresponding conditions on a, b, d are satisfied.

p	Conditions	
≥ 2	$v_p(d) = 1$	
2	$v_2(a) \geq 8$	$bd \not\equiv 3 \mod 4$
	$5 \leq v_2(a) \leq 7$	
	$v_2(a) = 4$	$v_2(a + 16b) \leq 7$
		$bd \not\equiv 1 \mod 4$
	$1 \leq v_2(a) \leq 3$	
	$v_2(a) = 0$	$a \not\equiv 1 \mod 4$

Corollary

Let $a, b, d \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and d squarefree. If $F_{n,i}(a, b, d)$ is an elliptic curve, then $F_{n,i}$ is semistable if and only if $|d| = 1$ and either (i) $v_2(a) \geq 8$ with $bd \equiv 3 \mod 4$, (ii) $v_2(a) = 8$ with $v_2(a + 16b) \geq 8$ and $bd \equiv 1 \mod 4$, or (iii) $a \equiv 1 \mod 4$.

Example

Let $E = F_{4,1}(16, -17, -5)$. From the table above, we can determine that E has additive reduction at 5 and semistable reduction at all other primes.

Future Work

This project focused on elliptic curves with isogeny class degree equal to 4, and ongoing work aims to determine the minimal discriminants and primes of additive reduction for elliptic curves with isogeny class degree $n > 1$.

References

[1] A.J. Barrios. *Minimal models of rational elliptic curves with non-trivial torsion*, Res. Number Theory 8 (2022), no. 1, Paper No. 4., 39 pp.

[2] A.J. Barrios. *Explicit classification of isogeny graphs of rational elliptic curves*, Int. J. Number Theory 19 (2023), no. 4, 913–936.

[3] A. Kraus. *Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique*, Acta Arith.54(1989), no.1, 75–80.

[4] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, Volume 106. Second Edition (2009).

Acknowledgements

- Dr. Alex Barrios (University of St. Thomas)
- Fabian Ramirez (University of California Irvine)
- Dr. Edray Herber Goins (Pomona College), and our fellow PRiME participants.
- Department of Mathematics, Pomona College
- Research at PRiME was supported by the National Science Foundation award DMS-2113782. Any opinions, findings, and conclusions or recommendations expressed in this article are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.