Minimal Discriminants of Rational Elliptic Curves

Alvaro Cornejo (University of California-Santa Barbara), Owen Ekblad (University of Michigan-Dearborn), Marietta Geist (Carleton College),
Kayla Harrison (Eckerd College), and Abby Loe (Carleton College)

Pomona Research in Mathematics Experience (PRiME)

Abstract

By a rational elliptic curve, we mean a projective variety of genus 1 that admits a Weierstrass model of the form $y^2 = x^2 + Ax + B$ where A and B are integers. For a rational elliptic curve E, there is a unique quantity known as the minimal discriminant which has the property that it is the smallest integer (in absolute value) occurring in the $\mathbb{Q}$-isomorphism class of E. In 1975, Hellegouarch showed that for relatively prime integers a and b the elliptic curve $y^2 = x(x+a)(x-b)$ comes equipped with an easily computable minimal discriminant. Recently, Barrios extended this result to all rational elliptic curves with non-trivial torsion subgroups. This project gives a classification of minimal discriminant for rational elliptic curves that admit an isogeny of degree $N = 5, 6, 7, 8, 9, 13$.

Elliptic Curves

- A **Weierstrass model** is an implicit function E of the form
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
where each a_j is a rational number. When E is differentiable at every point on the curve, we say that E is **non-singular**.
- An **elliptic curve** is defined as a pair $(E, \mathcal{O})$ where E is a smooth projective curve of genus 1 and $\mathcal{O}$ is an element of E.
- Intuitively, a **rational elliptic curve** is the graph of a non-singular Weierstrass model E together with a point $\mathcal{O}$ not on E, often referred to as the "point at infinity."
- We define the $\mathbb{Q}$**-rational points** of an elliptic curve E as the set $E(\mathbb{Q})$ of points $(x, y) \in \mathbb{Q}^2$ satisfying the Weierstrass model of E.
- The set $E(\mathbb{Q})$ is a finitely-generated abelian group under its group law, portrayed graphically on the right, with identity $\mathcal{O}$.

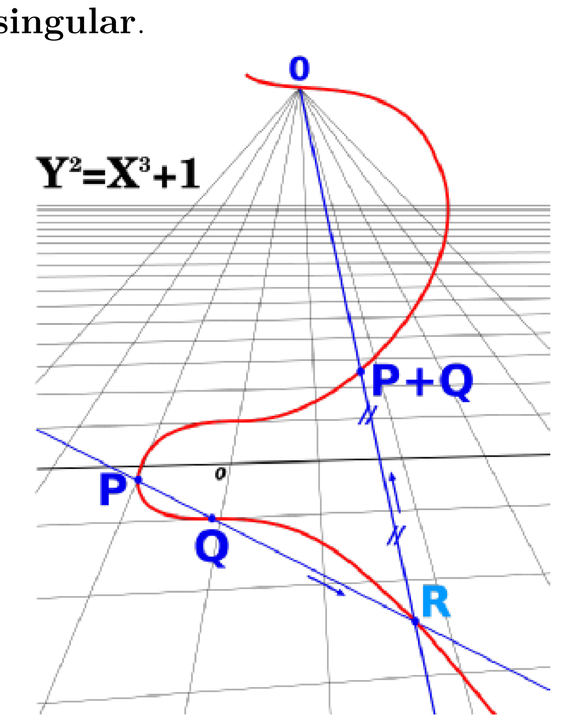

Figure 1: The group law of an elliptic curve.

- We define the **invariants** c_4 and c_6, the **discriminant** Δ, and the j**-invariant** j of an elliptic curve E to be
$$c_4 = a_1^4 + 8a_1^2a_2 - 24a_3a_1 + 16a_2^2 - 48a_4$$
$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)(2a_4 + a_1a_3) - 216\left(a_3^2 + 4a_6\right)$$
$$\Delta = \frac{c_4^3 - c_6^2}{1728} \qquad j = \frac{c_4^3}{\Delta}$$
- We say that E is $\mathbb{C}$**-isomorphic** to E' if and only if $j = j'$, where j is the j-invariant of E and j' is the j-invariant of E'.
- A $\mathbb{Q}$**-isogeny** between two elliptic curves E and E' is a non-constant morphism φ from E to E' such that $\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$ where φ is defined over $\mathbb{Q}$. If such a morphism exists, E and E' are said to be **isogenous** and in the same **isogeny class**.

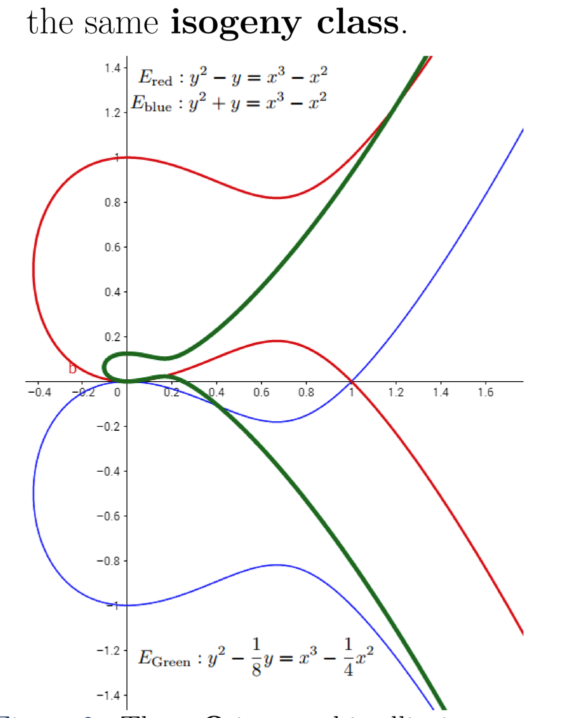

Figure 2: Three $\mathbb{Q}$-isomorphic elliptic curves.

- Let E and E' be isogenous rational elliptic curves, and suppose that ϕ is a $\mathbb{Q}$-isogeny between them. We say that ϕ is a $\mathbb{Q}$**-isomorphism** and an **admissible change of variables** if and only if
$$\phi(x,\ y) = (u^2x + r,\ u^3y + u^2sx + w)$$
where $u, s, r, w \in \mathbb{Q}$. If Δ, c_4, c_6 are associated to E and Δ', c_4', c_6' are associated to E', we have the relations $\Delta' = u^{-12}\Delta$, $c_6' = u^{-6}c_6$, and $c_4' = u^{-4}c_4$. Curves between which such a ϕ exists are said to be $\mathbb{Q}$**-isomorphic**.

Kraus's Theorem

- Let p be a prime. The p**-adic valuation** $v_p : \mathbb{Z} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ is a function defined as $v_p(n) = \max\{v \in \mathbb{Z}_{\geq 0} : p^v \mid n\}$ if $n \neq 0$, and $v_p(n) = \infty$ if $n = 0$.
- Suppose that α, β, and γ are integers satisfying $\gamma = \frac{\alpha^3 - \beta^2}{1728}$, with $\gamma \neq 0$. Then **Kraus's Theorem** asserts that there exists a rational elliptic curve E given by a Weierstrass model with integral coefficients having invariants $c_4 = \alpha$ and $c_6 = \beta$ if and only if
  (i) $v_3(\beta) \neq 2$, and
  (ii) either $\beta \equiv -1 \pmod 4$, or both $v_2(\alpha) \geq 4$ and $\beta \equiv 0$ or $8 \pmod{32}$.

Modular Curves and Minimal Discriminants

- Let E be a rational elliptic curve given by the Weierstrass model
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
We say $E_{\min}$ is a **global minimal model** of E if
(i) each of $a_1, a_2, a_3, a_4, a_6, c_4, c_6$, and Δ are integers, and
(ii) the value $|\Delta|$ is minimal over all $\mathbb{Q}$-isomorphic elliptic curves to E.
We call Δ the **minimal discriminant** of $E_{\min}$ and denote it by $\Delta_E^{\min}$, and we call the quantities c_4 and c_6 of a global model the associated quantities to a minimal model.
- By an **isomorphism class of triples** we mean that (E_1, E_1', π_1) is equivalent to (E_2, E_2', π_2) if and only if there exist isomorphisms $\varphi : E_1 \to E_2$ and $\varphi' : E_1' \to E_2'$ such that $\pi_2 \circ \varphi = \varphi' \circ \pi_1$.
- The **modular curve** $X_0(N)$ for $N \geq 2$ parametrizes isomorphism classes of triples (E_1, E_2, π) where $\pi : E_1 \to E_2$ is an isogeny with $\ker \pi \cong C_N$, where C_N is the cyclic group of order N.
- For the modular curve $X_0(N)$ to be of genus 0 it is necessary and sufficient that $N = 1, 2, \ldots, 10, 12, 13, 16, 18$, or 25.
- Let $X_0(N)$ be a genus 0 modular curve and recall that $\mathbb{P}^1(\mathbb{Q})$ is bijective to $\mathbb{Q} \cup \{\infty\}$. Then there exists a birational map $\varphi : \mathbb{P}^1(\mathbb{Q}) \to X_0(N)$ defined by
$$\varphi(t : 1) = [E_1(t), E_2(t), \pi_t]$$
with the property that if $t \in \mathbb{Q}$ then $E_1(t)$ and $E_2(t)$ are elliptic curves over $\mathbb{Q}$ with $\pi_t : E_1(t) \to E_2(t)$ a $\mathbb{Q}$-isogeny and $\ker \pi_t \cong C_N$. We can use this to parametrize elliptic curves $E_{N,1}(t)$ and $E_{N,2}(t)$, where $t = b/a$ with $a, b \in \mathbb{Z}$, and, utilizing Kraus's Theorem, we are able to classify minimal discriminants of representative curves of $E_{N,1}(t)$ and $E_{N,2}(t)$.
- For example, consider the elliptic curves $E_{8,1}(t)$ and $E_{8,2}(t)$, defined as
$$E_{8,1}(t) : y^2 = x^3 - 27a_{4,1}(t)\,x - 54a_{6,1}(t)$$
$$E_{8,2}(t) : y^2 = x^3 - 27a_{4,2}(t)\,x - 54a_{6,2}(t)$$
where $a_{4,1}(t) = t^4 + 60t^3 + 134t^2 + 60t + 1$, $a_{4,2}(t) = 16\,t^4 - 16\,t^2 + 1$, $a_{6,1}(t) = \left(t^4 - 132\,t^3 - 250\,t^2 - 132\,t + 1\right)\left(t^2 + 6\,t + 1\right)$, and, lastly, $a_{6,2}(t) = \left(32\,t^4 - 32\,t^2 - 1\right)\left(2\,t^2 - 1\right)$.
- If we set $t = b/a$, then we can explicitly compute the discriminant and invariants of these curves, and by making use of admissible changes of variables and Kraus's Theorem, we can completely classify the minimal discriminant of these curves. This methodology can be utilized for arbitrary $E_{N,1}(t)$ and $E_{N,2}(t)$, which led us to our theorem below.

Theorem (CEGHL)

Let $a, b \in \mathbb{Z}$ be coprime, let $(E_{N,1}, E_{N,2}, \pi_N) \in X_0(N)$, and suppose that

$f_5 = 125a^2 + 22ab + b^2$ is 4^{th} power free if $N = 5$,
$f_7 = 49a^2 + 13ab + b^2$ is 6^{th} power free if $N = 7$,
and $f_{13} = \left(13a^2 + 5ab + b^2\right)\left(13a^2 + 6ab + b^2\right)$ is 6^{th} power free if $N = 13$.

Then the minimal discriminant of $E_{N,j}$ is $u_{N,j}^{-12}\Delta_{N,j}$, where $u_{N,j}$ is one of the possibilities given below:

$(N,1)$	$(5,1)$	$(6,1)$	$(7,1)$	$(8,1)$	$(9,1)$	$(13,1)$
$u_{N,1}$ divides	50	6	98	8	9	26

$(N,2)$	$(5,2)$	$(6,2)$	$(7,2)$	$(8,2)$	$(9,2)$	$(13,2)$
$u_{N,2}$ divides	10	4	14	2	3	26

Moreover, there are necessary and sufficient conditions on a, b to determine exactly the value of $u_{N,j}$ as summarized in the following:

(N,j)	Conditions on $u_{N,j}$
$(5,1)$	$u_{N,j} = 50 \iff v_5(b) \geq 3$ where $2 \nmid a$
	$u_{N,j} = 25 \iff v_5(b) \geq 3$ where $2 \mid a$
	$u_{N,j} = 5 \iff v_5(b) = 2$
	$u_{N,j} = 2 \iff v_5(b) = 1$ where $2 \nmid a$
	$u_{N,j} = 1 \iff v_5(b) = 1$ where $2 \mid a$ or $v_5(b) = 0$
$(5,2)$	$u_{N,j} = 10 \iff v_5(b) \geq 3$ where $2 \nmid a$
	$u_{N,j} = 5 \iff v_5(b) \geq 3$ where $2 \mid a$
	$u_{N,j} = 2 \iff v_5(b) \leq 2$ where $2 \nmid a$
	$u_{N,j} = 1 \iff v_5(b) \leq 2$ where $2 \mid a$
$(6,1)$	$u_{N,j} = 6 \iff v_3(b) = 1$ where $2 \mid b$ and $ab \equiv 6 \mod 9$
	$u_{N,j} = 3 \iff v_3(b) = 1$ where $2 \nmid b$ and $ab \equiv 6 \mod 9$
	$u_{N,j} = 2 \iff 2 \mid b$ and $v_3(b) \neq 1$ or $v_3(b) = 1$ with $ab \equiv 3 \mod 9$
	$u_{N,j} = 1 \iff 2 \nmid b$ and $v_3(b) \neq 1$ or $v_3(b) = 1$ with $ab \equiv 3 \mod 9$
$(6,2)$	$u_{N,j} = 4 \iff v_2(b) = 1$
	$u_{N,j} = 2 \iff v_2(b) \geq 2$
	$u_{N,j} = 1 \iff v_2(b) = 0$

(N,j)	Conditions on $u_{N,j}$ (continued)
$(7,1)$	$u_{N,j} = 98 \iff v_7(b) = 2, v_7(f_7) = 5,$ and $ab \equiv 1,2 \mod 4$
	$u_{N,j} = 49 \iff v_7(b) = 2, v_7(f_7) = 5,$ and $ab \equiv 0,3 \mod 4$
	$u_{N,j} = 14 \iff v_7(b) \geq 3$ and $ab \equiv 1,2 \mod 4$
	$u_{N,j} = 7 \iff v_7(b) \geq 3$ and $ab \equiv 0,3 \mod 4$
	$u_{N,j} = 2 \iff 4 \nmid ab$ and above conditions do not hold
	$u_{N,j} = 1 \iff$ all above conditions do not hold
$(7,2)$	$u_{N,j} = 14 \iff v_7(b) = 2, v_7(f_7) = 5,$ and $ab \equiv 1,2 \mod 4$
	$u_{N,j} = 7 \iff v_7(b) = 2, v_7(f_7) = 5,$ and $ab \equiv 0,3 \mod 4$
	$u_{N,j} = 2 \iff ab \equiv 1,2 \mod 4$ and above conditions do not hold
	$u_{N,j} = 1 \iff$ all above conditions do not hold
$(8,1)$	$u_{N,j} = 6 \iff v_2(a-b) \geq 3$
	$u_{N,j} = 3 \iff v_2(a-b) = 2$
	$u_{N,j} = 2 \iff v_2(a-b) = 13$
	$u_{N,j} = 1 \iff v_2(a-b) = 0$
$(8,2)$	$u_{N,j} = 2 \iff v_2(a) \geq 1$ or $v_2(b^2 - a^2) \geq 4$
	$u_{N,j} = 1 \iff$ all above conditions do not hold
$(9,1)$	$u_{N,j} = 9 \iff v_2(a-b) \geq 2$
	$u_{N,j} = 3 \iff v_2(a-b) = 1$
	$u_{N,j} = 1 \iff v_2(a-b) = 0$
$(9,2)$	$u_{N,j} = 3 \iff v_2(a-b) \geq 2$ or $3 \mid a$
	$u_{N,j} = 1 \iff v_2(a-b) \leq 1$ or $3 \nmid a$
$(13,j)$	$u_{N,j} = 26 \iff v_{13}(b) \geq 1$ and either $b \equiv 2 \mod 4$ or $v_2(a) \geq 2$
	$u_{N,j} = 13 \iff v_{13}(b) \geq 1$ and either $b \not\equiv 2 \mod 4$ or $v_2(a) \leq 1$
	$u_{N,j} = 2 \iff v_{13}(b) = 0$ and either $b \equiv 2 \mod 4$ or $v_2(a) \geq 2$
	$u_{N,j} = 1 \iff v_{13}(b) = 0$ and either $b \not\equiv 2 \mod 4$ or $v_2(a) \leq 1$

Modified Szpiro Ratios

- Denoted $P = (a, b, c)$, an ABC **triple** is a triple of relatively prime non-zero integers a, b, and c where $a + b = c$.
- The **quality** of an ABC triple $P = (a, b, c)$ is the quantity
$$q(P) = \frac{\log\ \max\{|a|, |b|, |c|\}}{\log\,(abc)}.$$
The ABC **conjecture** states that for all $\varepsilon > 0$ there are only finitely many ABC triples satisfying $q(P) > 1 + \varepsilon$.
- If a prime p divides $\gcd(c_4, \Delta)$ then we say that E has **additive reduction at** p. Otherwise, we say that E is **semistable at** p, and if E is semistable at all primes, we call E **semistable**.
- We define the **conductor** of a rational elliptic curve E as the quantity
$$N_E = \prod_{p \mid \Delta_E^{\min}} p^{f_p},$$
where $f_p = 1$ if E is semistable at p, and $2 + \delta_p$ if E, has additive reduction at at p, and δ_p is a function that depends on the primes.
- If two elliptic curves E and E' are isogenous, then $N_E = N_{E'}$.
- Let E be a rational elliptic curve with minimal discriminant $\Delta_E^{\min}$ and invariants c_4 and c_6. By a **modified Szpiro ratio**, we mean the quantity
$$\sigma_m(E) = \frac{\log\ \max\{|c_4^3|,\ c_6^2\}}{\log\ N_E}.\quad \text{If } \sigma_m(E) > 6, \text{ we say } E \text{ is } \textbf{good}.$$
If two elliptic curves E and E' are isogenous, then $\sigma_m(E) = \sigma_m(E')$.
- The **modified Szpiro conjecture** states that for all $\varepsilon > 0$ there are only finitely many rational elliptic curves E satisfying $\sigma_m(E) > 6 + \varepsilon$.
- The Modified Szpiro Conjecture and ABC Conjecture are equivalent, and the explicit ABC Conjecture implies Fermat's Last Theorem for $n \geq 6$.

Database of Elliptic Curves

- The ABC@Home project was a home-computing project that sought to compute good ABC triples. By 2011, they met their goal of computing 23.8 million good ABC triples, after which they ceased operations. Similarly, we wanted to find good elliptic curves with specified isogeny, so we constructed a database of elliptic curves.
- To construct the database of elliptic curves, we used the modular curve $X_0(N)$, and found curves admitting isogeny degrees of $N = 6, 7, 8, 9, 10, 12, 13$, and 16.
- We define S as the set
$$S = \left\{ \frac{b}{a}\ \middle|\ \gcd(a, b) = 1 \text{ and } 1 \leq a, b \leq 650 \right\},$$
and consider the subset $\{E_{N,1}(t), E_{N,2}(t)\}$ such that $t \in S$.
- Recall that any rational elliptic curve E has a global minimal model $E_{\min}$. There is also a **reduced minimal model** of E given by a Weierstrass model
$$y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$$
where the reduced minimal model is a global minimal model, with $b_1, b_3 \in \{0, 1\}$ and $b_2 \in \{-1, 0, 1\}$. The reduced minimal model of E is unique.
- Using the elements of S as parameters for $E_{N,1}(t)$ and $E_{N,2}(t)$, and assuring uniqueness by checking reduced minimal models were distinct, we were able to write a computer program to produce the database in Figure 3, containing over 21,000,000 unique elliptic curves with specified isogeny.

Isogeny Class	No. of Unique Curves	Good Elliptic Curves	Largest MSR	Smallest MSR	Lower Bound?
$X_0(6)$	3,112,892	425	7.66	2.84	
$X_0(7)$	3,112,926	2	618	2.025	2?
$X_0(8)$	2,334,693	2268	12.794	2.795	
$X_0(9)$	3,112,925	886	13.395	3.01	3?
$X_0(10)$	3,112,924	23	7.31	2.76	
$X_0(12)$	2,810,469	15,664	10.98	4.03	4?
$X_0(13)$	3,112,926	0	5.9	2.21	
$X_0(16)$	2,334,693	6759	12.79	3.37	

Figure 3: Database of elliptic curves

- Below are histograms showing the distribution of Modified Szpiro Ratios (MSRs) for elliptic curves of isogeny degree $N = 8$ and 12. It is noteworthy that as the MSRs grow larger, the number of elliptic curves with these MSRs appears to decay almost exponentially. It is also noteworthy that the MSRs appear to have a lower bound. For example, curves with isogeny degree 12 appear to have MSRs bounded below by 4.

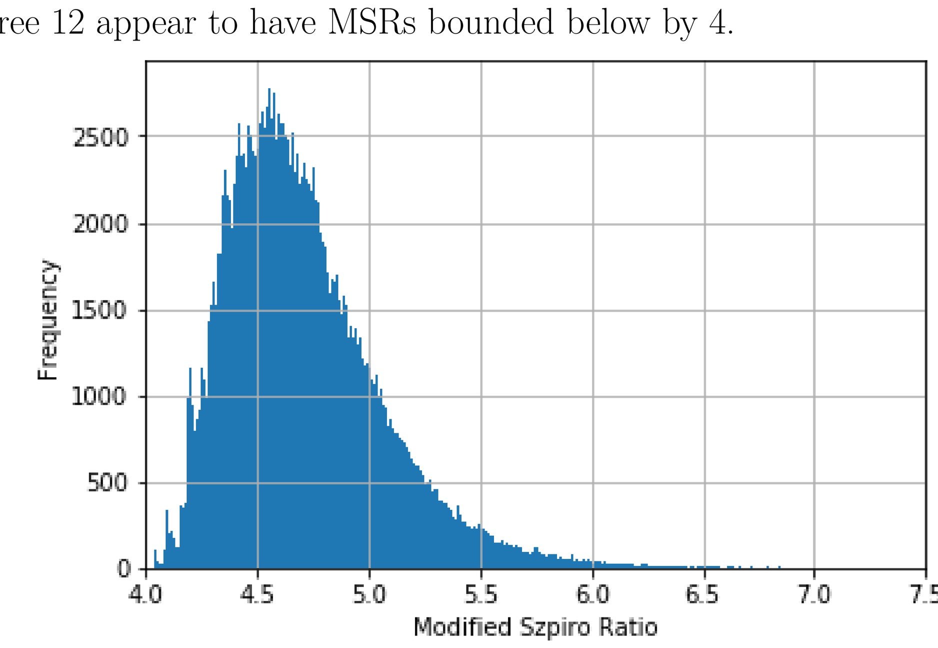

Figure 4: Modified Szpiro ratios for $X_0(12)$

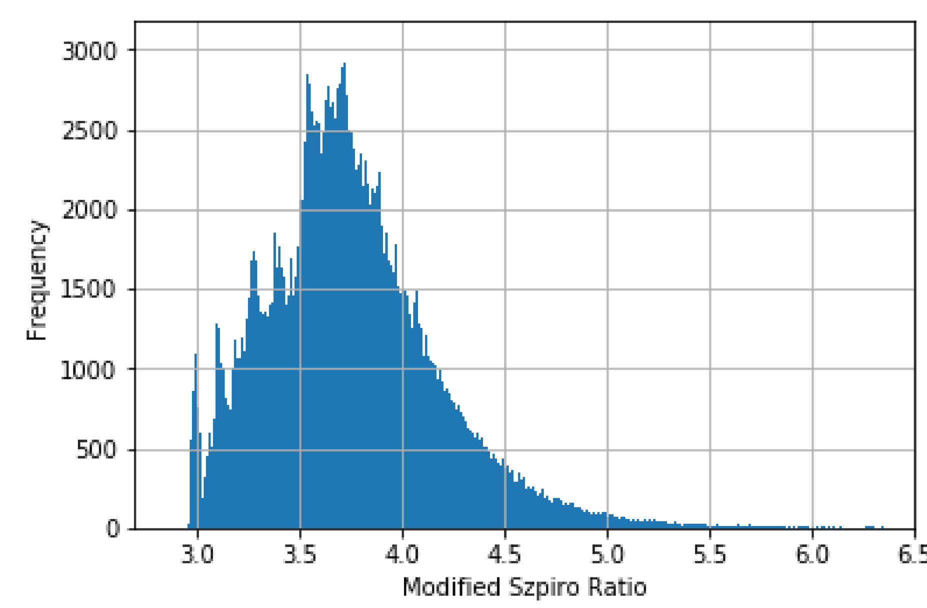

Figure 5: Modified Szpiro ratios for $X_0(8)$

Future Work

Going forward, we hope to finish classifying minimal discriminants for elliptic curves admitting isogeny degree of $N = 2, 3, 4, 10, 11, 12, 13, 16, 18$, and 25, and to generate more elliptic curves with non-trivial isogeny. Moreover, we hope to articulate a conjecture about lower bounds of modified Szpiro ratios of elliptic curves of non-trivial isogeny.

References

[1] A. Barrios, "Modular Curves and the Modified Szpiro Conjecture" (2019)
[2] S. Lang, "Old and New Conjectured Diophantine Inequalities." *Bulletin of The American Mathematical Society* (1990)
[3] T. Weston, "The Modular Curves $X_0(11)$ and $X_1(11)$" (2012)

Acknowledgements

We would like to acknowledge Dr. Alexander Barrios (Carleton College), Dr. Edray Herber Goins (Pomona College), Alia Curtis (Scripps College), Dr. Tim McEldowney (West Virginia University), the Department of Mathematics at Pomona College, the National Science Foundation (DMS-1560394), and viewers like you. Thank you.