Minimal Discriminants of 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

Abstract

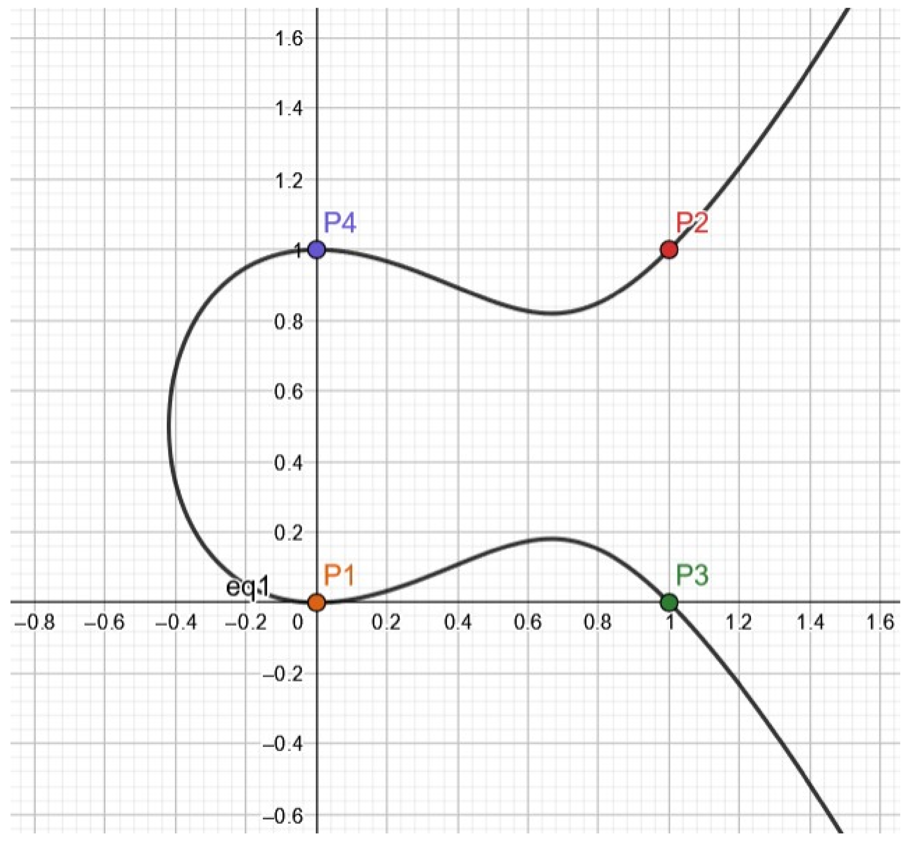
For a positive integer N, we say that an elliptic curve E admits an N-isogeny if E has a cyclic subgroup of order N. Such elliptic curves are parametrizable, and by studying the explicit equations corresponding to the modular curve $X_0(N)$, we prove results about the minimal discriminants of elliptic curves with a non-trivial isogeny over the rational numbers.

Elliptic Curves

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 $4A^3 + 27B^2 \neq 0$. There is a natural group structure of the points on an elliptic curve where $\mathcal{O}$ is the identity.



An elliptic curve parameterized by $X_1(5)$

More generally, elliptic curves can be written in their **Weierstrass form**:

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

where $a_j \in \mathbb{Q}$. If instead each $a_j \in \mathbb{Z}$, we say E is in **integral Weierstrass form**.

Elliptic Curves Cont.

Associated to an elliptic curve are the quantities c_4, c_6, and Δ which can be easily computed from the coefficients of the elliptic curve. We have the identity

$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$

We call Δ the **discriminant** of the elliptic curve.

The following is a useful theorem for determining whether there exists an integral Weierstrass model with given c_4 and c_6:

Kraus' Theorem

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. $\nu_2(\beta) \neq 2$, and
2. - $\beta \equiv -1 \pmod 4$ if β is odd,
   - $\nu_2(\alpha) \geq 4$ and $\beta \equiv 0$ or $8 \pmod{32}$ if β is even.

Isomorphisms of Elliptic Curves

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

$$x \mapsto u^2x + r \quad y \mapsto u^3y + u^2sx + w,$$

where $u, r, s, w \in \mathbb{Q}$ and $u \neq 0$. If c_4', c_6', and Δ' are the quantities associated with E', then

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

Observe that if E_1 is isomorphic to E_2 via a change of variables in which $u = u_1$ and E_2 is isomorphic to E_3 via a change of variables with $u = u_2$, then the discriminant of E_3 can be written as

$$\Delta_3 = u_2^{-12}\Delta_2 = u_2^{-12}u_1^{-12}\Delta_1.$$

In other words, $\mathbb{Q}$-isomorphisms affect the quantities associated to an elliptic curve multiplicatively.

Minimal Discriminants

We say the elliptic curve 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 its discriminant Δ is minimal over all curves $\mathbb{Q}$-isomorphic to E. That is,

$$\Delta_E = \min\{|\Delta_{E'}| \in \mathbb{Z} : E' \text{ is } \mathbb{Q}\text{-isomorphic to } E.\}$$

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

In general, it is not easy to compute the minimal discriminant of an elliptic curve. There are existing algorithms by Tate (1975), Laska (1982), and later Laska, Kraus, and Connell (1991).

Isogenies

An **isogeny** $\pi : E \to E'$ between elliptic curves is a nonzero surjective group homomorphism with finite kernel. If the kernel has size N, we say π is an N-isogeny. An isogeny $\pi : E \to E'$ can be written in the form

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

for some rational function $f(x)$ and rational constant $c \neq 0$.

Our Project

Let $n = 2, 3, \ldots, 10, 12, 13, 16, 18, 25$. Elliptic curves with non-trivial n-isogeny can be parameterized in terms of a family of n-isogenous, non-isomorphic curves $F_{n,k}(a, b, d)$ for some coprime a, b and some integers d and k. Using this parameterization, we aim to classify the minimal discriminants of each curve $F_{n,k}$ in terms of arithmetic conditions on the integers a, b, d. Doing so classifies the minimal discriminants of elliptic curves with an n-isogeny.

Main Theorem

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:

n	p	Condition on a, b	$(\nu_p(u_{n,i}))_i$
6	2	$\nu_2(b) \leq 1$	$(1, 0, 1, 2)$
		$\nu_2(b) = 2$	$(2, 0, 2, 2)$
		$\nu_2(b) \geq 3$	$(3, 1, 3, 3)$
	3	$\nu_3(b) = 0$	$(0, 0, 0, 0)$
		$\nu_3(b) = 1$	$(1, 1, 0, 0)$
		$\nu_3(b) \geq 2$	$(2, 2, 1, 1)$
8	2	$\nu_2(b) = 0$	$(1, 0, 0, 0, 0, 1)$
		$\nu_2(b) = 1$	$(2, 1, 1, 1, 1, 2)$
		$\nu_2(b) = 2$, $\nu_2(a + \frac{b}{4}) = 1$, and $\nu_2(a - \frac{b}{4}) = 2$	$(4, 3, 4, 2, 2, 2)$
		$\nu_2(b) = 2$, $\nu_2(a + \frac{b}{4}) = 1$, and $\nu_2(a - \frac{b}{4}) \geq 3$	$(5, 4, 5, 3, 3, 3)$
		$\nu_2(b) = 2$ and $\nu_2(a + \frac{b}{4}) = 2$	$(4, 4, 3, 2, 2, 2)$
		$\nu_2(b) = 2$ and $\nu_2(a + \frac{b}{4}) \geq 3$	$(5, 5, 4, 3, 3, 3)$
		$\nu_2(b) \geq 3$	$(3, 2, 2, 2, 3, 2)$
9	3	$\nu_3(b) = 0$	$(1, 0, 0)$
		$\nu_3(b) \geq 1$ and $\nu_3(a - \frac{b}{3}) = 0$	$(1, 1, 0)$
		$\nu_3(b) = 1$ and $\nu_3(a - \frac{b}{3}) = 1$	$(2, 1, 0)$
		$\nu_3(b) = 1$ and $\nu_3(a - \frac{b}{3}) > 1$	$(3, 2, 1)$

Further Work

We are in the process of classifying the minimal discriminants of curves that admit an n-isogeny for the remaining values of n.

Acknowledgements

We would like to thank:

- Pomona College for making PRiME 2021 possible
- The NSA for funding this project (NSA H98230-21-1-0015)
- Dr. Edray Goins, Dr. Rachel Davis, and especially Dr. Alex Barrios for their guidance and expertise throughout this experience.