Modular Curves and Minimal Discriminants

or, Modulus Curveous and the Minimus Discriminus

Alvaro Cornejo[1] Owen Ekblad[2] Marietta Geist[3]
Kayla Harrison[4] Abby Loe[3]

July 29, 2019

Outline

Introduction

Definitions

Definition (Weierstrass Equation)

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.

Definition (Weierstrass Equation)

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**.

Definitions

Definition (Weierstrass Equation)

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**.
- Conversely, when E is *not* differentiable everywhere, we say that E is **singular**.

Example of Non-Singular Weierstrass Model

assets/nonsingularexamples.PNG

Figure: A non-singular Weierstrass model

Examples of Singular Curves

assets/singularexamples.PNG

Figure: Two singular curves,
$y^2 = x^3 - 3x^2 + 3x - 1$ and $y^2 = x^3 + x^2$.

Definition (Elliptic Curve)

Suppose that E is a non-singular Weierstrass equation. Intuitively, a **rational elliptic curve** is the graph of E together with a point $\mathcal{O}$ not on the curve that is said to be the "point at infinity."

Elliptic Curves

Definition (Elliptic Curve)

Suppose that E is a non-singular Weierstrass equation. Intuitively, a **rational elliptic curve** is the graph of E together with a point $\mathcal{O}$ not on the curve that is said to be the "point at infinity."

- We can define an elliptic curve over any arbitrary field K, but this summer we focused on elliptic curves defined over the rational numbers.

Elliptic Curves

Definition (Elliptic Curve)

Suppose that E is a non-singular Weierstrass equation. Intuitively, a **rational elliptic curve** is the graph of E together with a point $\mathcal{O}$ not on the curve that is said to be the "point at infinity."

- We can define an elliptic curve over any arbitrary field K, but this summer we focused on elliptic curves defined over the rational numbers.
- We can also think about the rational points on elliptic curves!

Elliptic Curves

Definition (Elliptic Curve)

Suppose that E is a non-singular Weierstrass equation. Intuitively, a **rational elliptic curve** is the graph of E together with a point $\mathcal{O}$ not on the curve that is said to be the "point at infinity."

- We can define an elliptic curve over any arbitrary field K, but this summer we focused on elliptic curves defined over the rational numbers.
- We can also think about the rational points on elliptic curves!

Elliptic Curves

Definition (Elliptic Curve)

Suppose that E is a non-singular Weierstrass equation. Intuitively, a **rational elliptic curve** is the graph of E together with a point $\mathcal{O}$ not on the curve that is said to be the "point at infinity."

- We can define an elliptic curve over any arbitrary field K, but this summer we focused on elliptic curves defined over the rational numbers.
- We can also think about the rational points on elliptic curves!

Definition ($\mathbb{Q}$-rational Points)

The **$\mathbb{Q}$-rational points** are

$$E(\mathbb{Q}) = \left\{(x, y) \in \mathbb{Q}^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\}$$

$\mathbb{Q}$-rational points

The Group Law

We can define a group

The Group Law

We can define a group

Definition

Let E be an elliptic curve, and let P and Q be rational points on E. We define a group $(E, \bigoplus)$ by drawing a secant line through P, Q. R is where the secant line intersects E. $P \bigoplus Q$ is the intersection of E and the secant line through $R, \mathcal{O}_E$.

The Group Law

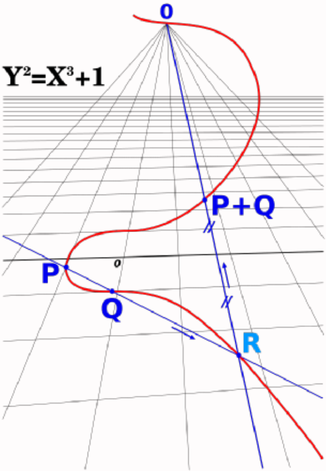

Figure: Group Law on Elliptic Curves

The Group Law

The identity is $\mathcal{O}_E$.

$P \bigoplus P$ is found not with a secant line, but with a tangent line.

Torsion Subgroup

Definition (Torsion Subgroup)

Let G be a group. The subgroup of G containing all elements of finite order in G is called the **torsion subgroup** of G and is denoted by G_{tors}.

Elliptic curves with nontrivial torsion subgroups are worthy of study

Torsion Subgroup

Definition (Torsion Subgroup)

Let G be a group. The subgroup of G containing all elements of finite order in G is called the **torsion subgroup** of G and is denoted by G_{tors}.

Elliptic curves with nontrivial torsion subgroups are worthy of study

Torsion Subgroup

Definition (Torsion Subgroup)

Let G be a group. The subgroup of G containing all elements of finite order in G is called the **torsion subgroup** of G and is denoted by G_{tors}.

Elliptic curves with nontrivial torsion subgroups are worthy of study

Theorem (Mazur's Torsion Theorem)

Let E be a rational elliptic curve and let C_N denote the cyclic group of N elements. Then

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

Torsion Subgroup

Definition (Torsion Subgroup)

Let G be a group. The subgroup of G containing all elements of finite order in G is called the **torsion subgroup** of G and is denoted by G_{tors}.

Elliptic curves with nontrivial torsion subgroups are worthy of study

Theorem (Mazur's Torsion Theorem)

Let E be a rational elliptic curve and let C_N denote the cyclic group of N elements. Then

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

Torsion Subgroup

Definition (Torsion Subgroup)

Let G be a group. The subgroup of G containing all elements of finite order in G is called the **torsion subgroup** of G and is denoted by G_{tors}.

Elliptic curves with nontrivial torsion subgroups are worthy of study

Theorem (Mazur's Torsion Theorem)

Let E be a rational elliptic curve and let C_N denote the cyclic group of N elements. Then

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

Remark If we define an elliptic curve over two different fields, it is possible that the cyclic subgroups are different.

Definition (c_4, c_6, Δ)

We define c_4, c_6, Δ as the following:

$$c_4 = a_1^4 + 8a_1^2 a_2 - 24a_3 a_1 + 16a_2^2 - 48a_4$$

$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)(2a_4 + a_1 a_3) - 216\left(a_3^2 + 4a_6\right)$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728}, \text{ (we call } \Delta \text{ the discriminant of } E\text{)}$$

Isomorphism

Definition (c_4, c_6, Δ)

We define c_4, c_6, Δ as the following:

$$c_4 = a_1^4 + 8a_1^2 a_2 - 24a_3 a_1 + 16a_2^2 - 48a_4$$

$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)(2a_4 + a_1 a_3) - 216\left(a_3^2 + 4a_6\right)$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728}, \text{ (we call } \Delta \text{ the discriminant of } E\text{)}$$

Definition (Isomorphism)

We say that $\phi : G \to H$ is an isomorphism if ϕ preserves group structure.

Isomorphism

Definition (c_4, c_6, Δ)

We define c_4, c_6, Δ as the following:

$$c_4 = a_1^4 + 8a_1^2 a_2 - 24 a_3 a_1 + 16 a_2^2 - 48 a_4$$

$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)(2a_4 + a_1 a_3) - 216\left(a_3^2 + 4a_6\right)$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728}, \text{ (we call } \Delta \text{ the discriminant of } E\text{)}$$

Definition (Isomorphism)

We say that $\phi : G \to H$ is an isomorphism if ϕ preserves group structure.

Isomorphism

Definition (c_4, c_6, Δ)

We define c_4, c_6, Δ as the following:

$$c_4 = a_1^4 + 8a_1^2 a_2 - 24a_3 a_1 + 16a_2^2 - 48a_4$$

$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)(2a_4 + a_1 a_3) - 216\left(a_3^2 + 4a_6\right)$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728}, \text{ (we call } \Delta \text{ the discriminant of } E\text{)}$$

Definition (Isomorphism)

We say that $\phi : G \to H$ is an isomorphism if ϕ preserves group structure.

Definition

We define the ***j*-invariant** of an elliptic curve E to be

$$j = \frac{c_4^3}{\Delta}$$

Isomorphism

Definition (c_4, c_6, Δ)

We define c_4, c_6, Δ as the following:

$$c_4 = a_1^4 + 8a_1^2 a_2 - 24a_3 a_1 + 16a_2^2 - 48a_4$$

$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)(2a_4 + a_1 a_3) - 216\left(a_3^2 + 4a_6\right)$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728}, \text{ (we call } \Delta \text{ the discriminant of } E\text{)}$$

Definition (Isomorphism)

We say that $\phi : G \to H$ is an isomorphism if ϕ preserves group structure.

Definition

We define the j-**invariant** of an elliptic curve E to be

$$j = \frac{c_4^3}{\Delta}$$

Isomorphism

Definition (c_4, c_6, Δ)

We define c_4, c_6, Δ as the following:

$$c_4 = a_1^4 + 8a_1^2a_2 - 24a_3a_1 + 16a_2^2 - 48a_4$$

$$c_6 = -\left(a_1^2 + 4a_2\right)^3 + 36\left(a_1^2 + 4a_2\right)(2a_4 + a_1a_3) - 216\left(a_3^2 + 4a_6\right)$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728}, \text{ (we call } \Delta \text{ the discriminant of } E\text{)}$$

Definition (Isomorphism)

We say that $\phi : G \to H$ is an isomorphism if ϕ preserves group structure.

Definition

We define the j-**invariant** of an elliptic curve E to be

$$j = \frac{c_4^3}{\Delta}$$

- When the *j*-invariants of two elliptic curves are the same we can say they are isomorphic over $\mathbb{C}$. However, this does not mean they are isomorphic over $\mathbb{Q}$.

$\mathbb{Q}$ – *Isomorphisms*

- When the j-invariants of two elliptic curves are the same we can say they are isomorphic over $\mathbb{C}$. However, this does not mean they are isomorphic over $\mathbb{Q}$.

  $y^2 = x^3 + 1$ and $y^2 = x^3 - 1$ have the same j-invariant of zero, but they are not $\mathbb{Q}$-isomorphic.

- When the j-invariants of two elliptic curves are the same we can say they are isomorphic over $\mathbb{C}$. However, this does not mean they are isomorphic over $\mathbb{Q}$.

  $y^2 = x^3 + 1$ and $y^2 = x^3 - 1$ have the same j-invariant of zero, but they are not $\mathbb{Q}$-isomorphic.
- Instead, we find that if we map $(x, y) \mapsto (i^2x, i^3y)$, and E_1, E_2 are isomorphic over $\mathbb{Q}(i)$

The Admissible Change of Variables

Proposition

Let K be a field, and E and E' be elliptic curves defined by a Weierstrass model. If $\phi : E \to E'$ is a K-isomorphism such that $\phi(\mathcal{O}_E) = \phi(\mathcal{O}_{E'})$, then $\phi(x, y) = (u^2x + r, u^3y + u^2sx + w)$ where $u, s, r, w \in K$.

The Admissible Change of Variables

Proposition

Let K be a field, and E and E' be elliptic curves defined by a Weierstrass model. If $\phi : E \to E'$ is a K-isomorphism such that $\phi(\mathcal{O}_E) = \phi(\mathcal{O}_{E'})$, then $\phi(x, y) = (u^2x + r, u^3y + u^2sx + w)$ where $u, s, r, w \in K$.

Remark Notice that r and w translate the elliptic curve, s scales the y value, and u scales both the x and y values.

Proposition

Let K be a field, and E and E' be elliptic curves defined by a Weierstrass model. If $\phi : E \to E'$ is a K-isomorphism such that $\phi(\mathcal{O}_E) = \phi(\mathcal{O}_{E'})$, then $\phi(x, y) = (u^2x + r, u^3y + u^2sx + w)$ where $u, s, r, w \in K$.

Remark Notice that r and w translate the elliptic curve, s scales the y value, and u scales both the x and y values.

The Admissible Change of Variables

Proposition

Let K be a field, and E and E' be elliptic curves defined by a Weierstrass model. If $\phi : E \to E'$ is a K-isomorphism such that $\phi(\mathcal{O}_E) = \phi(\mathcal{O}_{E'})$, then $\phi(x, y) = (u^2x + r, u^3y + u^2sx + w)$ where $u, s, r, w \in K$.

Remark Notice that r and w translate the elliptic curve, s scales the y value, and u scales both the x and y values.

Remark If Δ, c_4, c_6 are associated to E and Δ', c_4', c_6' are associated to E', then we have the relations:

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

Applications

Example

Let E_1 and E_2 be elliptic curves defined over the rational numbers

$$E_1 : y^2 + xy + y = x^3 + x^2 + x + 1$$

$$E_2 : y^2 + \frac{27}{5}xy + \frac{51}{125}y = x^3 - \frac{157}{25}x^2 - \frac{19}{25}x - \frac{9}{3125}$$

There is an isomorphism $\phi : E_1 \leftrightarrow E_2$ by $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + w)$ where $u = 5, s = 8, r = 13, t = 21$.

Applications

Example

Let E_1 and E_2 be elliptic curves defined over the rational numbers

$$E_1 : y^2 + xy + y = x^3 + x^2 + x + 1$$

$$E_2 : y^2 + \frac{27}{5}xy + \frac{51}{125}y = x^3 - \frac{157}{25}x^2 - \frac{19}{25}x - \frac{9}{3125}$$

There is an isomorphism $\phi : E_1 \leftrightarrow E_2$ by $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + w)$ where $u = 5, s = 8, r = 13, t = 21$.

- Recall that the j-invariant fails for $\mathbb{Q}$-isomorphisms.

Applications

Example

Let E_1 and E_2 be elliptic curves defined over the rational numbers

$$E_1 : y^2 + xy + y = x^3 + x^2 + x + 1$$

$$E_2 : y^2 + \frac{27}{5}xy + \frac{51}{125}y = x^3 - \frac{157}{25}x^2 - \frac{19}{25}x - \frac{9}{3125}$$

There is an isomorphism $\phi : E_1 \leftrightarrow E_2$ by $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + w)$ where $u = 5, s = 8, r = 13, t = 21.$

- Recall that the j-invariant fails for $\mathbb{Q}$-isomorphisms.

  The admissible change of variables provides us with a useful way to translate over $\mathbb{Q}$-isomorphic curves.

Global Minimal Model and Minimal Discriminant

Definition

Let E be a rational elliptic curve given by

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

We say E_{min} is a **global minimal model** of E if

- $a_1, a_2, a_3, a_4, a_6, c_4, c_6$, and Δ are integers
- $|\Delta|$ is minimal over all $\mathbb{Q}$-isomorphic elliptic curves of E.

Remark We call Δ the **minimal discriminant** of E_{min} and denote it by Δ_{min}. Moreover, the quantities c_4 and c_6 of a global model are called the associated quantities to a minimal model.

Additive Reduction and Semistable

Let E be a rational elliptic curve and let p be a prime.

Definition (Additive Reduction)

If p divides $\gcd(c_4, \Delta)$ then we say that E has **additive reduction** at p

Definition (Semistable)

If p does not divide $\gcd(c_4, \Delta)$ then we say that E is **semistable** at a point p. We call E semistable if E is semistable at all primes.

Definition (The Conductor)

We define the **conductor** of a rational elliptic curve E to be

$$N_E = \prod_{p \mid \Delta_E^{min}} p^{f_p}$$

Where $f_p = \begin{cases} 1 \text{ if } E \text{ is semistable at } p \\ 2 + \delta_p \text{ if } E \text{ has additive reduction at } p \end{cases}$
and δ is a function that depends on the primes.

For $p \geq 5$, $\delta_p = 0$. For $p = 2$, $\delta_p \leq 6$ and for $p = 3$, $\delta_p \leq 3$.

Definition (The Conductor)

We define the **conductor** of a rational elliptic curve E to be

$$N_E = \prod_{p | \Delta_E^{min}} p^{f_p}$$

Where $f_p = \begin{cases} 1 \text{ if } E \text{ is semistable at } p \\ 2 + \delta_p \text{ if } E \text{ has additive reduction at } p \end{cases}$
and δ is a function that depends on the primes.

For $p \geq 5$, $\delta_p = 0$. For $p = 2$, $\delta_p \leq 6$ and for $p = 3$, $\delta_p \leq 3$.

Definition (The Conductor)

We define the **conductor** of a rational elliptic curve E to be

$$N_E = \prod_{p \mid \Delta_E^{min}} p^{f_p}$$

Where $f_p = \begin{cases} 1 \text{ if } E \text{ is semistable at } p \\ 2 + \delta_p \text{ if } E \text{ has additive reduction at } p \end{cases}$
and δ is a function that depends on the primes.

For $p \geq 5$, $\delta_p = 0$. For $p = 2$, $\delta_p \leq 6$ and for $p = 3$, $\delta_p \leq 3$.

Remark If E is semistable, then $N_E = \mathrm{rad}(\Delta_E^{min})$.

Isogeny

Definition

A $\mathbb{Q}$**-isogeny** between two elliptic curves E_1 and E_2 is a morphism $\varphi : E_1 \to E_2$ where φ is defined over $\mathbb{Q}$. E_1 and E_2 are said to be isogenous

Isogeny

Definition

A $\mathbb{Q}$**-isogeny** between two elliptic curves E_1 and E_2 is a morphism $\varphi : E_1 \to E_2$ where φ is defined over $\mathbb{Q}$. E_1 and E_2 are said to be isogenous

Definition

If two elliptic curves, E_1 and E_2, are **isogenous** then $N_{E_1} = N_{E_2}$

Isogeny

Definition

A $\mathbb{Q}$**-isogeny** between two elliptic curves E_1 and E_2 is a morphism $\varphi : E_1 \to E_2$ where φ is defined over $\mathbb{Q}$. E_1 and E_2 are said to be isogenous

Definition

If two elliptic curves, E_1 and E_2, are **isogenous** then $N_{E_1} = N_{E_2}$

Isogeny

Definition

A $\mathbb{Q}$**-isogeny** between two elliptic curves E_1 and E_2 is a morphism $\varphi : E_1 \to E_2$ where φ is defined over $\mathbb{Q}$. E_1 and E_2 are said to be isogenous

Definition

If two elliptic curves, E_1 and E_2, are **isogenous** then $N_{E_1} = N_{E_2}$

Proposition

*We say two curves are in the same **isogeny class** if they are isogenous.*

Definition (Reduced minimal model)

Let E be a rational elliptic curve. The reduced minimal model of E is given by a Weierstrass model

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

which is a global minimal model of E such that $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$

Note: The reduced minimal model of a rational elliptic curve is unique!

Definition (p-adic valuation)

Let p be a prime. The ***p*-adic valuation**

$$v_p : \mathbb{Z} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$$

is defined as

$$v_p(n) = \begin{cases} \max\{v \in \mathbb{Z}_{\geq 0} \,:\, p^v \mid n\} & \text{if } n \neq 0 \\ \infty & \text{if } n = 0. \end{cases}$$

The p-adic valuation of an integer n can be thought of intuitively as the highest power of p occurring within the prime power decomposition of n.

Example ($v_p(24)$ for $p = 2, 3,$ and 5)

$$v_2(24) = v_2(2^3 \cdot 3^1) = 3$$

$$v_3(24) = v_3(2^3 \cdot 3^1) = 1$$

$$v_5(24) = v_5(2^3 \cdot 3^1) = ?$$

Example ($v_p(24)$ for $p = 2, 3,$ and 5)

$$v_2(24) = v_2(2^3 \cdot 3^1) \\ = 3$$

$$v_3(24) = v_3(2^3 \cdot 3^1) \\ = 1$$

$$v_5(24) = v_5(2^3 \cdot 3^1) \\ = ?$$

There are no powers of 5 contained in 24, therefore we have that $v_5(24) = 0$.

Example ($v_p(24)$ for $p = 2, 3$, and 5)

$$v_2(24) = v_2(2^3 \cdot 3^1) \\ = 3$$

$$v_3(24) = v_3(2^3 \cdot 3^1) \\ = 1$$

$$v_5(24) = v_5(2^3 \cdot 3^1) \\ = ?$$

There are no powers of 5 contained in 24, therefore we have that $v_5(24) = 0$.

Example ($v_p(24)$ for $p = 2, 3$, and 5)

$$v_2(24) = v_2(2^3 \cdot 3^1) \\ = 3$$

$$v_3(24) = v_3(2^3 \cdot 3^1) \\ = 1$$

$$v_5(24) = v_5(2^3 \cdot 3^1) \\ = ?$$

There are no powers of 5 contained in 24, therefore we have that $v_5(24) = 0$.

Remark We have the identity $v_p(ab) = v_p(a) + v_p(b)$, where a, b are integers (or, integral-valued functions).

Kraus' Theorem

Theorem (Kraus)

Let α, β, and γ be integers such that $\alpha^3 - \beta^2 = 1728\gamma$, with $\gamma \neq 0$. Then there exists a rational elliptic curve E given by an integral Weierstrass equation having invariants $c_4 = \alpha$ and $c_6 = \beta$ if and only if the following hold:

(i) $v_3(\beta) \neq 2$
(ii) either $\beta \equiv -1 \mod 4$ *or both* $v_2(\alpha) \geq 4$ *and* $\beta \equiv 0$ *or* $8 \mod 32$

Quadratic Twists

Definition

We say two elliptic curves E and E' are twists of each other if $j(E) = j(E')$

We use the quadratic twist in order to truly classify the minimal discriminants of rational elliptic curves, as they give the full picture of the equivalence classes in $X_0(N)$

Visualizing the Twist

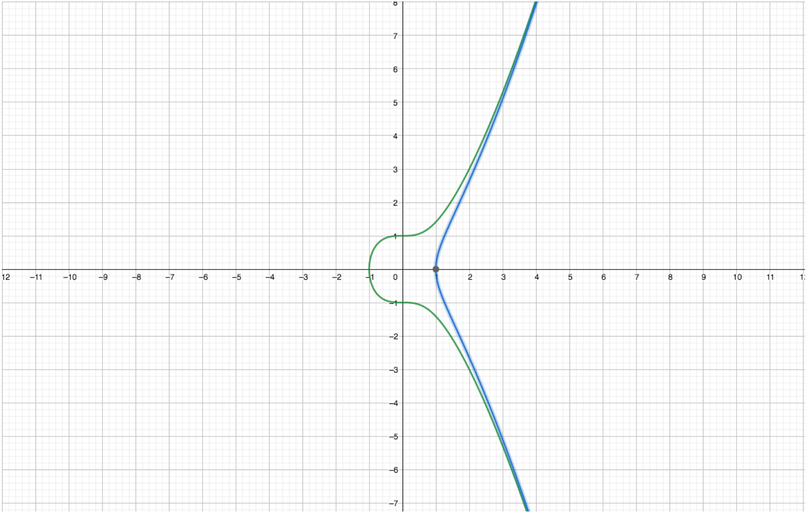

Figure: Two Quadratic Twists,
$y^2 = x^3 + 1$ and $y^2 = x^3 - 1$.

Definition (The Modular Curve $X_0(N)$)

The Modular Curve $X_0(N)$ for $N \geq 2$ parameterizes isomorphism classes of triples (E, E', π) where $\pi : E \to E'$ is an isogeny with $\ker(\pi) \cong C_N$.

Definition

By an isomorphism class of triples we mean that $(E_1, E_1', \pi_1) \sim (E_2, E_2', \pi_2)$ if and only if there are isomorphisms $\varphi : E_1 \to E_2$, $\varphi' : E_1' \to E_2'$ such that $\pi_2 \circ \varphi = \varphi' \circ \pi_1$

Remark This definition is not the one found in the literature, these have been translated into the ones above

Parametrizing Elliptic Curves

- We have that the modular curve $X_0(N)$ is genus 0 if and only if $N = 1, 2, \cdots, 10, 12, 13, 16, 18, 25$.

Theorem

Let $X_0(N)$ be a genus 0 modular curve. Then there is 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 $\pi_t : E_1(t) \to E_2(t)$ as a $\mathbb{Q}$-isogeny with $\ker \pi_t \cong C_N$

- Recall that intuitively we have $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\mathcal{O}\}$

Five Students Performed Math Research One Summer, Not Even COLLEGE Professors Expected What Happened Next!

The Results!

Theorem

Let a and b be relatively prime integers $E_{N,j}$ be as defined above and suppose that

$$\begin{array}{lll} f_5 = 125a^2 + 22ab + b^2 & \textit{is fourth-power free} & \textit{if } N = 5 \\ f_7 = 49a^2 + 13ab + b^2 & \textit{is sixth-power free} & \textit{if } N = 7 \\ f_{13} = \left(13a^2 + 5ab + b^2\right)\left(13a^2 + 6ab + b^2\right) & \textit{is sixth-power free} & \textit{if } N = 13 \end{array}$$

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

Theorem

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

(N,j)			Conditions on $u_{N,j}$
$(5,1)$	$u_{N,j}=50$	$\Longleftrightarrow$	$v_5(b)\geq 3$ with a odd
	$u_{N,j}=25$	$\Longleftrightarrow$	$v_5(b)\geq 3$ with a even
	$u_{N,j}=5$	$\Longleftrightarrow$	$v_5(b)=2$
	$u_{N,j}=2$	$\Longleftrightarrow$	$v_5(b)=1$ with a odd
	$u_{N,j}=1$	$\Longleftrightarrow$	$v_5(b)=1$ with a even or $v_5(b)=0$
$(5,2)$	$u_{N,j}=10$	$\Longleftrightarrow$	$v_5(b)\geq 3$ with a odd
	$u_{N,j}=5$	$\Longleftrightarrow$	$v_5(b)\geq 3$ with a even
	$u_{N,j}=2$	$\Longleftrightarrow$	$v_5(b)\leq 2$ with a odd
	$u_{N,j}=1$	$\Longleftrightarrow$	$v_5(b)\leq 2$ with a even
$(6,1)$	$u_{N,j}=6$	$\Longleftrightarrow$	b is even and $v_3(b)=1$ with $\frac{ab}{3}\equiv 2 \mod 3$
	$u_{N,j}=3$	$\Longleftrightarrow$	b is odd and $v_3(b)=1$ with $\frac{ab}{3}\equiv 2 \mod 3$
	$u_{N,j}=2$	$\Longleftrightarrow$	b is even and either $v_3(b)\neq 1$ or $v_3(b)=1$ with $\frac{ab}{3}\equiv 1 \mod 3$
	$u_{N,j}=1$	$\Longleftrightarrow$	b is odd and either $v_3(b)\neq 1$ or $v_3(b)=1$ with $\frac{ab}{3}\equiv 1 \mod 3$
$(6,2)$	$u_{N,j}=4$	$\Longleftrightarrow$	$v_2(b)=1$
	$u_{N,j}=2$	$\Longleftrightarrow$	$v_2(b)\geq 2$
	$u_{N,j}=1$	$\Longleftrightarrow$	$v_2(b)=0$
$(7,1)$	$u_{N,j}=98$	$\Longleftrightarrow$	$v_7(b)=2, v_7(f_7)=5$, and $ab\equiv 1,2 \bmod 4$
	$u_{N,j}=49$	$\Longleftrightarrow$	$v_7(b)=2, v_7(f_7)=5$, and $ab\equiv 0,3 \bmod 4$
	$u_{N,j}=14$	$\Longleftrightarrow$	$v_7(b)\geq 3$ and $ab\equiv 1,2 \bmod 4$
	$u_{N,j}=7$	$\Longleftrightarrow$	$v_7(b)\geq 3$ and $ab\equiv 0,3 \bmod 4$
	$u_{N,j}=2$	$\Longleftrightarrow$	$4\nmid ab$ and the above conditions do not hold.
	$u_{N,j}=1$	$\Longleftrightarrow$	the above conditions do not hold.

Theorem

$(7,2)$	$u_{N,j}=14$	$\Longleftrightarrow$	$v_7(b)=2, v_7(f_7)=5$, and $ab\equiv 1,2 \bmod 4$
	$u_{N,j}=7$	$\Longleftrightarrow$	$v_7(b)=2, v_7(f_7)=5$, and $ab\equiv 0,3 \bmod 4$
	$u_{N,j}=2$	$\Longleftrightarrow$	$ab\equiv 1,2 \bmod 4$ and the above conditions do not hold
	$u_{N,j}=1$	$\Longleftrightarrow$	the above conditions do not hold
$(8,1)$	$u_{N,j}=6$	$\Longleftrightarrow$	$v_2(a-b)\geq 3$
	$u_{N,j}=3$	$\Longleftrightarrow$	$v_2(a-b)=2$
	$u_{N,j}=2$	$\Longleftrightarrow$	$v_2(a-b)=1$
	$u_{N,j}=1$	$\Longleftrightarrow$	$v_2(a-b)=0$
$(8,2)$	$u_{N,j}=2$	$\Longleftrightarrow$	$v_2(a)\geq 1$ or $v_2(a)\geq 4$
	$u_{N,j}=1$	$\Longleftrightarrow$	otherwise
$(9,1)$	$u_{N,j}=9$	$\Longleftrightarrow$	$v_2(b-a)\geq 2$
	$u_{N,j}=3$	$\Longleftrightarrow$	$v_2(b-a)=1$
	$u_{N,j}=1$	$\Longleftrightarrow$	$v_2(b-a)=0$
$(9,2)$	$u_{N,j}=3$	$\Longleftrightarrow$	$v_2(b-a)\geq 2$ or $3\mid a$
	$u_{N,j}=1$	$\Longleftrightarrow$	$v_2(b-a)\leq 1$ and $3\nmid a$
$(13,j)$	$u_{N,j}=26$	$\Longleftrightarrow$	$v_{13}(b)\geq 1$ and either $b\equiv 2 \bmod 4$ or $v_2(a)\geq 2$
	$u_{N,j}=13$	$\Longleftrightarrow$	$v_{13}(b)\geq 1$ and either $b\not\equiv 2 \bmod 4$ or $v_2(a)\leq 1$
	$u_{N,j}=2$	$\Longleftrightarrow$	$v_{13}(b)=0$ and either $b\equiv 2 \bmod 4$ or $v_2(a)\geq 2$
	$u_{N,j}=1$	$\Longleftrightarrow$	$v_{13}(b)\leq 0$ and either $b\not\equiv 2 \bmod 4$ or $v_2(a)\leq 1$

We Found the Minimal Discriminant of $X_0(8)$ Using THESE Crazy Techniques! You Won't Believe How We Got $\Delta_{E_2}^{\min}$!

Parameterization of E_1 and E_2 in $X_0(8)$

- Define $E_1(t)$ as the following:

$$E_1 : y^2 = x^3 - 27a_4^1(t)x - 54a_6^1(t)$$

Where $a_4^1 = t^4 + 60\,t^3 + 134\,t^2 + 60\,t + 1$ and
$a_6^1 = \left(t^4 - 132\,t^3 - 250\,t^2 - 132\,t + 1\right)\left(t^2 + 6\,t + 1\right)$

- Similarly define $E_2(t)$ as:

$$E_2 : y^2 = x^3 - 27a_4^2(t)x - 54a_6^2(t)$$

where $a_4^2 = 16\,t^4 - 16\,t^2 + 1$ and $a_6^2 = \left(32\,t^4 - 32\,t^2 - 1\right)\left(2\,t^2 - 1\right)$

E_2 in $X_0(8)$ as an Example

Take $(E_1, E_2, \pi) \in X_0(8)$. We have that E_2 can be parameterized by rational point $t = \frac{b}{a}$ (where a, b are coprime) as the following:

$$y^2 = x^3 + \left(\frac{-27a^4 + 432a^2b^2 - 432b^4}{a^4}\right)x + \frac{-54a^6 - 1620a^4b^2 + 5184a^2b^4 - 3456b^6}{a^6}$$

Theorem

The minimal discriminant of E_2 is $u^{-12}\Delta$ with $u \mid 2$. Moreover,

$$u = \begin{cases} 2 \text{ if and only if } v_2(a) \geq 1 \text{ or } v_2(b^2 - a^2) \geq 4 \\ 1 \iff v_2(a) = 0 \text{ and } v_2(b^2 - a^2) < 4 \end{cases}$$

Finding the possible GCD's between invariants

Before beginning this proof we will take a small detour into explaining the process of finding the GCD's

Definition (The Euclidean Algorithm)

Let R be an integral domain (recall an integral domain has no zero-divisors), and let $a, b \in R$ with $b \neq 0$. Then R is a Euclidean Domain if there exists some $q, r \in R$ such that:

$$a = qb + r$$

Before beginning this proof we will take a small detour into explaining the process of finding the GCD's

Definition (The Euclidean Algorithm)

Let R be an integral domain (recall an integral domain has no zero-divisors), and let $a, b \in R$ with $b \neq 0$. Then R is a Euclidean Domain if there exists some $q, r \in R$ such that:

$$a = qb + r$$

Remark There is prime factorization in a Euclidean Domain

Finding the possible GCD's between invariants

Before beginning this proof we will take a small detour into explaining the process of finding the GCD's

Definition (The Euclidean Algorithm)

Let R be an integral domain (recall an integral domain has no zero-divisors), and let $a, b \in R$ with $b \neq 0$. Then R is a Euclidean Domain if there exists some $q, r \in R$ such that:

$$a = qb + r$$

Remark There is prime factorization in a Euclidean Domain

Finding the possible GCD's between invariants

Before beginning this proof we will take a small detour into explaining the process of finding the GCD's

Definition (The Euclidean Algorithm)

Let R be an integral domain (recall an integral domain has no zero-divisors), and let $a, b \in R$ with $b \neq 0$. Then R is a Euclidean Domain if there exists some $q, r \in R$ such that:

$$a = qb + r$$

Remark There is prime factorization in a Euclidean Domain

Theorem (Bezout's Identity)

Let R be a Euclidean domain, a, b be non-zero elements of R, and $d = r_n$, the last nonzero prime factor for a and b. Then d is the greatest common divisor of a and b and there are elements $x, y \in R$ such that $d = ax + by$

Finding the possible GCD's between invariants

Before beginning this proof we will take a small detour into explaining the process of finding the GCD's

Definition (The Euclidean Algorithm)

Let R be an integral domain (recall an integral domain has no zero-divisors), and let $a, b \in R$ with $b \neq 0$. Then R is a Euclidean Domain if there exists some $q, r \in R$ such that:

$$a = qb + r$$

Remark There is prime factorization in a Euclidean Domain

Theorem (Bezout's Identity)

Let R be a Euclidean domain, a, b be non-zero elements of R, and $d = r_n$, the last nonzero prime factor for a and b. Then d is the greatest common divisor of a and b and there are elements $x, y \in R$ such that $d = ax + by$

Using the Euclidean Algorithm and Wolfram Mathematica, we obtained the greatest common denominators for invariants of various curves and $X_0(8)$.

Proof

Proposition

For E isomorphic to E', u^4 divides the greatest common divisor of the invariants associated with E. Since u^4 divides the gcd's between the invariants we find that $u \mid 8$

- We apply the change of variables with $(x, y) \mapsto ((\frac{3}{a})^2 x, (\frac{3}{a})^3 y)$. There is an integral Weierstrass Model F isomorphic to E_2 having

$$c_4 = 2^4(a^4 - 16a^2b^2 + 16b^4)$$
$$c_6 = 2^6(a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4)$$
$$\Delta_{8,2} = 2^8(-a + b)(a + b)b^2a^8$$

as its invariants c_4, c_6, and Δ respectively.

Recall Kraus' Theorem

Theorem (Kraus)

Let α, β, and γ be integers such that $\alpha^3 - \beta^2 = 1728\gamma$, with $\gamma \neq 0$. Then there exists a rational elliptic curve E given by an integral Weierstrass equation having invariants $c_4 = \alpha$ and $c_6 = \beta$ if and only if the following hold:

(i) $v_3(\beta) \neq 2$
(ii) either $\beta \equiv -1 \mod 4$ or both $v_2(\alpha) \geq 4$ and $\beta \equiv 0$ or $8 \mod 32$

Proof

- Suppose $v_2(a) \geq 1$ or $v_2(b^2 - a^2) \geq 4$. This yield the quantities

$$c_4' = 2^{-4}c_4 = (a^4 - 16a^2b^2 + 16b^4)$$
$$c_6' = 2^{-6}c_6 = (a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4)$$
$$\Delta' = 2^{-12}\Delta = 2^{-4}(-a + b)(a + b)b^2a^8$$

Proof

- Suppose $v_2(a) \geq 1$ or $v_2(b^2 - a^2) \geq 4$. This yield the quantities

$$c_4' = 2^{-4}c_4 = (a^4 - 16a^2b^2 + 16b^4)$$
$$c_6' = 2^{-6}c_6 = (a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4)$$
$$\Delta' = 2^{-12}\Delta = 2^{-4}(-a + b)(a + b)b^2a^8$$

- Notice that $v_2((-a + b)(a + b)b^2a^8) = v_2(b^2 - a^2) + 2v_2(b) + 8v_2(a) \geq 4$. So $2^{-12}\Delta \in \mathbb{Z}$

Proof

- Suppose $v_2(a) \geq 1$ or $v_2(b^2 - a^2) \geq 4$. This yield the quantities

$$c_4' = 2^{-4}c_4 = (a^4 - 16a^2b^2 + 16b^4)$$
$$c_6' = 2^{-6}c_6 = (a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4)$$
$$\Delta' = 2^{-12}\Delta = 2^{-4}(-a + b)(a + b)b^2a^8$$

- Notice that $v_2((-a + b)(a + b)b^2a^8) = v_2(b^2 - a^2) + 2v_2(b) + 8v_2(a) \geq 4$. So $2^{-12}\Delta \in \mathbb{Z}$
- We will now verify Kraus' theorem to check that an integral Weierstrass

Checking Part i) of Krauss' Theorem

- We want to show that $v_3(2^{-6}c_6) \neq 2$

Checking Part i) of Krauss' Theorem

- We want to show that $v_3(2^{-6}c_6) \neq 2$
- Consider $2^{-6}c_6 \mod 3$. We find that

$$\begin{aligned} 2^{-6}c_6 &= (a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) \\ &\equiv a^6 + b^6 \mod 3 \end{aligned}$$

Since a, b are relatively prime and any integer not divisible by 3 to the 6th power is 1, we have that $c_6 \mod 3 \equiv 1 \text{ or } 2 \mod 3$. Thus $v_3(2^{-6}c_6) = 0 \neq 2$.

Checking Part ii) of Krauss' Theorem

- Suppose $v_2(a) \geq 1$, then we have $a = 2k$ for some $k \in \mathbb{Z}$

Checking Part ii) of Krauss' Theorem

- Suppose $v_2(a) \geq 1$, then we have $a = 2k$ for some $k \in \mathbb{Z}$
- We want to show that $v_2(2^{-4}c_4) \geq 4$ and $2^{-6}c_6 \equiv 0$ or $8 \mod 32$.

Checking Part ii) of Krauss' Theorem

- Suppose $v_2(a) \geq 1$, then we have $a = 2k$ for some $k \in \mathbb{Z}$
- We want to show that $v_2(2^{-4}c_4) \geq 4$ and $2^{-6}c_6 \equiv 0$ or $8 \mod 32$.
- We have that

$$\begin{aligned} v_2(2^{-4}c_4) &= v_2(a^4 - 16a^2b^2 + 16b^4) \\ &= v_2(2^4k^4 - 2^6k^2b^2 + 2^4b^4) \\ &= 4 + v_2(k^4 - 2^2k^2b^2 + b^4) \geq 4 \end{aligned}$$

Checking Part ii) of Krauss' Theorem

- Suppose $v_2(a) \geq 1$, then we have $a = 2k$ for some $k \in \mathbb{Z}$
- We want to show that $v_2(2^{-4}c_4) \geq 4$ and $2^{-6}c_6 \equiv 0 \text{ or } 8 \mod 32$.
- We have that

$$\begin{aligned} v_2(2^{-4}c_4) &= v_2(a^4 - 16a^2b^2 + 16b^4) \\ &= v_2(2^4k^4 - 2^6k^2b^2 + 2^4b^4) \\ &= 4 + v_2(k^4 - 2^2k^2b^2 + b^4) \geq 4 \end{aligned}$$

- Now consider $2^{-6}c_6 \mod 32$. This is congruent to

$$\begin{aligned} (a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) &\equiv 2^5(2k - b^2)(k^4 + 4k^2b^2 - 2b^4) \mod 32 \\ &\equiv 0 \mod 32 \end{aligned}$$

Checking Part ii) of Krauss' Theorem

- Suppose $v_2(a) \geq 1$, then we have $a = 2k$ for some $k \in \mathbb{Z}$
- We want to show that $v_2(2^{-4}c_4) \geq 4$ and $2^{-6}c_6 \equiv 0$ or $8 \mod 32$.
- We have that

$$\begin{aligned} v_2(2^{-4}c_4) &= v_2(a^4 - 16a^2b^2 + 16b^4) \\ &= v_2(2^4k^4 - 2^6k^2b^2 + 2^4b^4) \\ &= 4 + v_2(k^4 - 2^2k^2b^2 + b^4) \geq 4 \end{aligned}$$

- Now consider $2^{-6}c_6 \mod 32$. This is congruent to

$$\begin{aligned} (a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) &\equiv 2^5(2k - b^2)(k^4 + 4k^2b^2 - 2b^4) \mod 32 \\ &\equiv 0 \mod 32 \end{aligned}$$

- Now suppose $v_2(b^2 - a^2) \geq 4$, we have that a and b must both be odd. This means that $2^{-6}c_6$ is odd and so it suffices to verify $2^{-6}c_6 \equiv 3 \mod 4$. Notice that

$$\begin{aligned} 2^{-6}c_6 &\equiv (a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) \mod 4 \\ &\equiv (1 - 2)(1 + 32 - 32) \equiv 3 \mod 4 \end{aligned}$$

Checking Part ii) of Krauss' Theorem

- Suppose $v_2(a) \geq 1$, then we have $a = 2k$ for some $k \in \mathbb{Z}$
- We want to show that $v_2(2^{-4}c_4) \geq 4$ and $2^{-6}c_6 \equiv 0$ or $8 \mod 32$.
- We have that

$$\begin{aligned} v_2(2^{-4}c_4) &= v_2(a^4 - 16a^2b^2 + 16b^4) \\ &= v_2(2^4k^4 - 2^6k^2b^2 + 2^4b^4) \\ &= 4 + v_2(k^4 - 2^2k^2b^2 + b^4) \geq 4 \end{aligned}$$

- Now consider $2^{-6}c_6 \mod 32$. This is congruent to

$$\begin{aligned} (a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) &\equiv 2^5(2k - b^2)(k^4 + 4k^2b^2 - 2b^4) \mod 32 \\ &\equiv 0 \mod 32 \end{aligned}$$

- Now suppose $v_2(b^2 - a^2) \geq 4$, we have that a and b must both be odd. This means that $2^{-6}c_6$ is odd and so it suffices to verify $2^{-6}c_6 \equiv 3 \mod 4$. Notice that

$$\begin{aligned} 2^{-6}c_6 &\equiv (a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) \mod 4 \\ &\equiv (1-2)(1+32-32) \equiv 3 \mod 4 \end{aligned}$$

- So Kraus' Theorem holds under the conditions $v_2(a) \geq 1$ or $v_2(b^2 - a^2) \geq 4$, so there exists an integral Weierstrass Model having discriminant $2^{-12}\Delta$.

No Other Admissible Change of Variables

- We will now prove we cannot have an integral Weierstrass model having discriminant $2^{-12}\Delta'$ by doing another admissible change of variables.

No Other Admissible Change of Variables

- We will now prove we cannot have an integral Weierstrass model having discriminant $2^{-12}\Delta'$ by doing another admissible change of variables.
- We have $a = 2^2\hat{a}$ where $\hat{a} \in \mathbb{Z}$ (not automatic).

No Other Admissible Change of Variables

- We will now prove we cannot have an integral Weierstrass model having discriminant $2^{-12}\Delta'$ by doing another admissible change of variables.
- We have $a = 2^2\hat{a}$ where $\hat{a} \in \mathbb{Z}$ (not automatic).
- So we have the following:

$$2^{-4}c_4' = 2^{-4}(a^4 - 16a^2b^2 + 16b^4) = (16\hat{a}^4 - 16\hat{a}^2b^2 + b^4)$$
$$2^{-6}c_6' = 2^{-6}(a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) = (8\hat{a}^2 - b^2)(8\hat{a}^4 + 16\hat{a}^2b^2 - b^4)$$
$$2^{-12}\Delta' = 2^{-16}3(-a + b)(a + b)b^2a^8 = (-4\hat{a} + b)(4\hat{a} + b)b^2\hat{a}^8$$

No Other Admissible Change of Variables

- We will now prove we cannot have an integral Weierstrass model having discriminant $2^{-12}\Delta'$ by doing another admissible change of variables.
- We have $a = 2^2\hat{a}$ where $\hat{a} \in \mathbb{Z}$ (not automatic).
- So we have the following:

$$\begin{aligned} 2^{-4}c_4' &= 2^{-4}(a^4 - 16a^2b^2 + 16b^4) = (16\hat{a}^4 - 16\hat{a}^2b^2 + b^4) \\ 2^{-6}c_6' &= 2^{-6}(a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) = (8\hat{a}^2 - b^2)(8\hat{a}^4 + 16\hat{a}^2b^2 - b^4) \\ 2^{-12}\Delta' &= 2^{-16}3(-a+b)(a+b)b^2a^8 = (-4\hat{a}+b)(4\hat{a}+b)b^2\hat{a}^8 \end{aligned}$$

- We have that $2^{-6}c_6' = (8\hat{a}^2 - b^2)(8\hat{a}^4 + 16\hat{a}^2b^2 - b^4)$ is odd. To check Kraus' Theorem, we must verify that $2^{-6}c_6' \equiv 3 \mod 4$.

No Other Admissible Change of Variables

- We will now prove we cannot have an integral Weierstrass model having discriminant $2^{-12}\Delta'$ by doing another admissible change of variables.
- We have $a = 2^2\hat{a}$ where $\hat{a} \in \mathbb{Z}$ (not automatic).
- So we have the following:

$$2^{-4}c_4' = 2^{-4}(a^4 - 16a^2b^2 + 16b^4) = (16\hat{a}^4 - 16\hat{a}^2b^2 + b^4)$$
$$2^{-6}c_6' = 2^{-6}(a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) = (8\hat{a}^2 - b^2)(8\hat{a}^4 + 16\hat{a}^2b^2 - b^4)$$
$$2^{-12}\Delta' = 2^{-16}3(-a+b)(a+b)b^2a^8 = (-4\hat{a}+b)(4\hat{a}+b)b^2\hat{a}^8$$

- We have that $2^{-6}c_6' = (8\hat{a}^2 - b^2)(8\hat{a}^4 + 16\hat{a}^2b^2 - b^4)$ is odd. To check Kraus' Theorem, we must verify that $2^{-6}c_6' \equiv 3 \mod 4$.
- Notice that,

$$2^{-6}c_6' = (8\hat{a}^2 - b^2)(8\hat{a}^4 + 16\hat{a}^2b^2 - b^4) \equiv (-b^2)(-b^4) \equiv 1 \mod 4 \not\equiv 3 \mod 4$$

No Other Admissible Change of Variables

- We will now prove we cannot have an integral Weierstrass model having discriminant $2^{-12}\Delta'$ by doing another admissible change of variables.
- We have $a = 2^2\hat{a}$ where $\hat{a} \in \mathbb{Z}$ (not automatic).
- So we have the following:

$$2^{-4}c_4' = 2^{-4}(a^4 - 16a^2b^2 + 16b^4) = (16\hat{a}^4 - 16\hat{a}^2b^2 + b^4)$$
$$2^{-6}c_6' = 2^{-6}(a^2 - 2b^2)(a^4 + 32a^2b^2 - 32b^4) = (8\hat{a}^2 - b^2)(8\hat{a}^4 + 16\hat{a}^2b^2 - b^4)$$
$$2^{-12}\Delta' = 2^{-16}3(-a+b)(a+b)b^2a^8 = (-4\hat{a}+b)(4\hat{a}+b)b^2\hat{a}^8$$

- We have that $2^{-6}c_6' = (8\hat{a}^2 - b^2)(8\hat{a}^4 + 16\hat{a}^2b^2 - b^4)$ is odd. To check Kraus' Theorem, we must verify that $2^{-6}c_6' \equiv 3 \mod 4$.
- Notice that,

$$2^{-6}c_6' = (8\hat{a}^2 - b^2)(8\hat{a}^4 + 16\hat{a}^2b^2 - b^4) \equiv (-b^2)(-b^4) \equiv 1 \mod 4 \not\equiv 3 \mod 4$$

- So Kraus' Theorem does not hold. So we have that $2^{-12}\Delta$ is the minimal discriminant under these conditions.

Concluding Steps

- We do a similar process with the conditions a is odd and $v_2(b^2 - a^2) \leq 3$ to show that $1^{-12}\Delta$ is the minimal discriminant.

Concluding Steps

- We do a similar process with the conditions a is odd and $v_2(b^2 - a^2) \leq 3$ to show that $1^{-12}\Delta$ is the minimal discriminant.
- The minimal discriminant of E_2 is $u^{-12}\Delta$ with $u \mid 2$. Moreover,

$$u = \begin{cases} 2 \leftarrow v_2(a) \geq 1 \text{ or } v_2(b^2 - a^2) \geq 4 \\ 1 \leftarrow v_2(a) = 0 \text{ (i.e a is odd) and } v_2(b^2 - a^2) < 4 \end{cases}$$

Concluding Steps

- We do a similar process with the conditions a is odd and $v_2(b^2 - a^2) \leq 3$ to show that $1^{-12}\Delta$ is the minimal discriminant.
- The minimal discriminant of E_2 is $u^{-12}\Delta$ with $u \mid 2$. Moreover,

$$u = \begin{cases} 2 \leftarrow v_2(a) \geq 1 \text{ or } v_2(b^2 - a^2) \geq 4 \\ 1 \leftarrow v_2(a) = 0 \text{ (i.e a is odd) and } v_2(b^2 - a^2) < 4 \end{cases}$$

- As we have exhausted all possibilities on a and b, we have an if and only if,

$$u = \begin{cases} 2 \iff v_2(a) \geq 1 \text{ or } v_2(b^2 - a^2) \geq 4 \\ 1 \iff v_2(a) = 0 \text{ and } v_2(b^2 - a^2) < 4 \end{cases}$$

These 2 Simple Ratios May Solve One of the World's Hardest Math Problems!

The *ABC* Conjecture

Definition (*ABC* Triple)

Denoted $P = (a, b, c)$, is a triple of integers a, b, c such that a, b, c are relatively prime non-zero integers and $a + b = c$.

The *ABC* Conjecture

Definition (*ABC* Triple)

Denoted $P = (a, b, c)$, is a triple of integers a, b, c such that a, b, c are relatively prime non-zero integers and $a + b = c$.

Definition (Quality)

The quality of an *ABC* triple $P = (a, b, c)$ is the quantity

$$q(P) = \frac{\log \max\{|a|, |b|, |c|\}}{\log rad(abc)}$$

Definition (*ABC* Triple)

Denoted $P = (a, b, c)$, is a triple of integers a, b, c such that a, b, c are relatively prime non-zero integers and $a + b = c$.

Definition (Quality)

The quality of an *ABC* triple $P = (a, b, c)$ is the quantity

$$q(P) = \frac{log\ max\{|a|, |b|, |c|\}}{log\ rad(abc)}$$

Definition (*ABC* Triple)

Denoted $P = (a, b, c)$, is a triple of integers a, b, c such that a, b, c are relatively prime non-zero integers and $a + b = c$.

Definition (Quality)

The quality of an *ABC* triple $P = (a, b, c)$ is the quantity

$$q(P) = \frac{log\, max\{|a|, |b|, |c|\}}{log\, rad(abc)}$$

Remark We say an *ABC* triple is good if $q(P) > 1$ and if a, b, c are positive

The *ABC* Conjecture

Definition (*ABC* Triple)

Denoted $P = (a, b, c)$, is a triple of integers a, b, c such that a, b, c are relatively prime non-zero integers and $a + b = c$.

Definition (Quality)

The quality of an *ABC* triple $P = (a, b, c)$ is the quantity

$$q(P) = \frac{log\ max\{|a|, |b|, |c|\}}{log\ rad(abc)}$$

Remark We say an *ABC* triple is good if $q(P) > 1$ and if a, b, c are positive

The *ABC* Conjecture

Definition (*ABC* Triple)

Denoted $P = (a, b, c)$, is a triple of integers a, b, c such that a, b, c are relatively prime non-zero integers and $a + b = c$.

Definition (Quality)

The quality of an *ABC* triple $P = (a, b, c)$ is the quantity

$$q(P) = \frac{\log \max\{|a|, |b|, |c|\}}{\log rad(abc)}$$

Remark We say an *ABC* triple is good if $q(P) > 1$ and if a, b, c are positive

Conjecture (*ABC* Conjecture)

For every $\epsilon > 0$ there are finitely many ABC triples $P = (a, b, c)$ satisfying $q(P) > 1 + \epsilon$

Szpiro Ratio

Conjecture (Szpiro Conjecture)

For every $\epsilon > 0$ there exists a positive constant κ_ϵ such that for all rational elliptic curves E,

$$|\Delta_E^{min}| \leq \kappa_\epsilon N_E^{6+\epsilon}$$

Definition (Szpiro Ratio)

Let E be a rational elliptic curve with minimal discriminant Δ_E^{min} and associated invariants c_4 and c_6.

$$\sigma(E) = \frac{log|\Delta_E^{min}|}{log\ N_E}$$

Modified Szpiro Ratio

Conjecture (Modified Szpiro Conjecture)

For every $\epsilon > 0$ *there are finitely many rational elliptic curves E satisfying*

$$\sigma_m(E) > 6 + \epsilon$$

Modified Szpiro Ratio

Conjecture (Modified Szpiro Conjecture)

For every $\epsilon > 0$ there are finitely many rational elliptic curves E satisfying

$$\sigma_m(E) > 6 + \epsilon$$

Definition (Modified Szpiro Ratio)

Let E be a rational elliptic curve with minimal discriminant Δ_E^{min} and associated invariants c_4 and c_6.

$$\sigma_m(E) = \frac{log\ \max\{|c_4^3|, c_6^2\}}{log\ N_E}$$

Modified Szpiro Ratio

Conjecture (Modified Szpiro Conjecture)

For every $\epsilon > 0$ there are finitely many rational elliptic curves E satisfying

$$\sigma_m(E) > 6 + \epsilon$$

Definition (Modified Szpiro Ratio)

Let E be a rational elliptic curve with minimal discriminant Δ_E^{min} and associated invariants c_4 and c_6.

$$\sigma_m(E) = \frac{\log \max\{|c_4^3|, c_6^2\}}{\log N_E}$$

Modified Szpiro Ratio

Conjecture (Modified Szpiro Conjecture)

For every $\epsilon > 0$ there are finitely many rational elliptic curves E satisfying

$$\sigma_m(E) > 6 + \epsilon$$

Definition (Modified Szpiro Ratio)

Let E be a rational elliptic curve with minimal discriminant Δ_E^{min} and associated invariants c_4 and c_6.

$$\sigma_m(E) = \frac{log\ \max\{|c_4^3|, c_6^2\}}{log\ N_E}$$

Remark We say that E is good if $\sigma_m(E) > 6$

Modified Szpiro Ratio

Conjecture (Modified Szpiro Conjecture)

For every $\epsilon > 0$ there are finitely many rational elliptic curves E satisfying

$$\sigma_m(E) > 6 + \epsilon$$

Definition (Modified Szpiro Ratio)

Let E be a rational elliptic curve with minimal discriminant Δ_E^{min} and associated invariants c_4 and c_6.

$$\sigma_m(E) = \frac{log\ \max\{|c_4^3|, c_6^2\}}{log\ N_E}$$

Remark We say that E is good if $\sigma_m(E) > 6$

Modified Szpiro Ratio

Conjecture (Modified Szpiro Conjecture)

For every $\epsilon > 0$ there are finitely many rational elliptic curves E satisfying

$$\sigma_m(E) > 6 + \epsilon$$

Definition (Modified Szpiro Ratio)

Let E be a rational elliptic curve with minimal discriminant Δ_E^{min} and associated invariants c_4 and c_6.

$$\sigma_m(E) = \frac{\log\ \max\{|c_4^3|, c_6^2\}}{\log N_E}$$

Remark We say that E is good if $\sigma_m(E) > 6$

Remark The Modified Szpiro Conjecture is equivalent to the *ABC* Conjecture

Definition (Naive Height)

The naive height of E is:

$$h_{naive}(E) = \frac{1}{12} log\ max|c_4^3|, c_6^2$$

- Like mentioned before, we define the equivalence classes as

$$[(E_1(t), E_2(t), \pi(t)] \in X_0(N)(\mathbb{Q})$$

- We define S as

$$S = \left\{ \frac{b}{a} \;\middle|\; \gcd(a, b) = 1, 1 \leq a, b \leq 650 \right\}$$

Remark Important to note that $t \in S$

Szpiro Ratio Table

Table 1: Szpiro Conjecture Database

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	

Looking at Szpiro Ratios

Naive Height

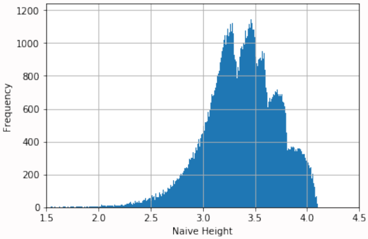

Figure: $X_0(8)$

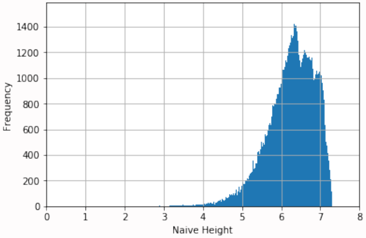

Figure: $X_0(12)$

Szpiro Ratio

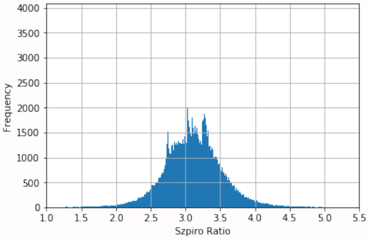

Figure: $X_0(8)$

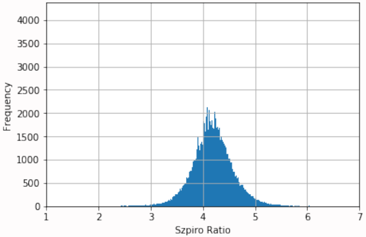

Figure: $X_0(12)$

Modified Szpiro Ratio

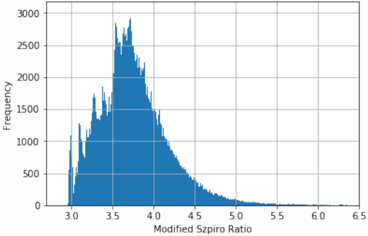

Figure: $X_0(8)$

assets/Histograms/12MSR.png

Figure: $X_0(12)$

Thanks

This research was conducted at Pomona College in Claremont, California, and this project was supported by the National Science Foundation (DMS-1659203), Pomona College, and viewers like you. Thank you.

References I

[1] A. Barrios.
Modular curves and the modified szpiro conjecture.

[2] S. Lang.
Old and new conjectured diophantine inequalities.
Bulletin of The American Mathematical Society, (1):37–75, July 1990.

[3] T. Weston.
The modular curves $x_0(11)$ and $x_1(11)$.