Elliptic Curves with Missing Frobenius Trace

Kevin Vissuet

Department of Mathematics
University of Illinois at Chicago

January 14, 2021

Outline

Basic Definitions

Notation

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N_E.

Basic Definitions

Notation

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N_E.

Definition

The Frobenius trace, $a_p(E) \in \mathbb{Z}$ associated to $p \nmid N_E$:

$$a_p(E) := p + 1 - \#E(\mathbb{F}_p).$$

Basic Definitions

Notation

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N_E.

Definition

The Frobenius trace, $a_p(E) \in \mathbb{Z}$ associated to $p \nmid N_E$:

$$a_p(E) := p + 1 - \#E(\mathbb{F}_p).$$

Definition

$$\pi_{E,r}(X) := \#\{p \leq X : p \nmid N_E,\, a_p(E) = r\}.$$

Lang-Trotter Conjecture [1976]

$$\pi_{E,r}(X) := \#\{p \leq X : p \nmid N_E,\ a_p(E) = r\}.$$

Conjecture (Lang-Trotter, 1976)

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and $r \in \mathbb{Z}$. Then $\exists\, C_{E,r} \geq 0$ so that, as $X \to \infty$,

$$\pi_{E,r}(X) \sim C_{E,r} \frac{\sqrt{X}}{\log X}.$$

Lang-Trotter Conjecture [1976]

$$\pi_{E,r}(X) := \#\{p \leq X : p \nmid N_E,\ a_p(E) = r\}.$$

Conjecture (Lang-Trotter, 1976)

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and $r \in \mathbb{Z}$. Then $\exists\, C_{E,r} \geq 0$ so that, as $X \to \infty$,

$$\pi_{E,r}(X) \sim C_{E,r} \frac{\sqrt{X}}{\log X}.$$

If $C_{E,r} = 0$: $\quad \begin{array}{c} \pi_{E,r}(X) \sim 0 \\ \text{as } X \to \infty \end{array} \overset{\text{def}}{\iff} \forall X \geq 0,\ \pi_{E,r}(X) = 0.$

Lang-Trotter Conjecture [1976]

$$\pi_{E,r}(X) := \#\{p \leq X : p \nmid N_E,\ a_p(E) = r\}.$$

Conjecture (Lang-Trotter, 1976)

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and $r \in \mathbb{Z}$. Then $\exists\, C_{E,r} \geq 0$ so that, as $X \to \infty$,

$$\pi_{E,r}(X) \sim C_{E,r} \frac{\sqrt{X}}{\log X}.$$

If $C_{E,r} = 0$: $\quad \begin{array}{c} \pi_{E,r}(X) \sim 0 \\ \text{as } X \to \infty \end{array} \overset{\text{def}}{\iff} \forall X \geq 0,\ \pi_{E,r}(X) = 0.$

Definition

When $C_{E,r} = 0$, we will call r a **missing Frobenius trace for** E.

Definition

When $C_{E,r} = 0$, we will call r a **missing Frobenius trace for** E.

Definition

When $C_{E,r} = 0$, we will call r a **missing Frobenius trace for** E.

Example

Consider

$$E_3 : \; y^2 + xy + y = x^3 - x^2 - 56x + 163.$$

Definition

When $C_{E,r} = 0$, we will call r a **missing Frobenius trace for** E.

Example

Consider

$$E_3 : \; y^2 + xy + y = x^3 - x^2 - 56x + 163.$$

The sequence $(a_p(E_3) \mod 3 : p \nmid N_{E_3} \text{ and } p \leq 100)$ is

$$(0, 2, 0, 2, 0, 2, 0, 0, 2, 2, 0, 2, 0, 0, 0, 2, 2, 0, 2, 2, 0, 0, 2).$$

Definition

When $C_{E,r} = 0$, we will call r a **missing Frobenius trace for** E.

Example

Consider

$$E_3 : \; y^2 + xy + y = x^3 - x^2 - 56x + 163.$$

The sequence $(a_p(E_3) \mod 3 : p \nmid N_{E_3} \text{ and } p \leq 100)$ is

$$(0, 2, 0, 2, 0, 2, 0, 0, 2, 2, 0, 2, 0, 0, 0, 2, 2, 0, 2, 2, 0, 0, 2).$$

See: the residue class $1 \mod 3$ is missing.

Definition

When $C_{E,r} = 0$, we will call r a **missing Frobenius trace for** E.

Example

Consider

$$E_3 : \ y^2 + xy + y = x^3 - x^2 - 56x + 163.$$

The sequence $(a_p(E_3) \mod 3 : p \nmid N_{E_3} \text{ and } p \leq 100)$ is

$$(0, 2, 0, 2, 0, 2, 0, 0, 2, 2, 0, 2, 0, 0, 0, 2, 2, 0, 2, 2, 0, 0, 2).$$

See: the residue class $1 \mod 3$ is missing.

This is caused by the rational point $P := (7, 5) \in E_3[3]$, which affects the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E_3[3]$.

Definition

When $C_{E,r} = 0$, we will call r a **missing Frobenius trace for** E.

Example

Consider

$$E_3 : \; y^2 + xy + y = x^3 - x^2 - 56x + 163.$$

The sequence $(a_p(E_3) \mod 3 : p \nmid N_{E_3} \text{ and } p \leq 100)$ is

$$(0, 2, 0, 2, 0, 2, 0, 0, 2, 2, 0, 2, 0, 0, 0, 2, 2, 0, 2, 2, 0, 0, 2).$$

See: the residue class $1 \mod 3$ is missing.

This is caused by the rational point $P := (7, 5) \in E_3[3]$, which affects the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E_3[3]$. It follows that every $r \equiv 1 \mod 3$ is a missing Frobenius trace for E_3.

Example

Consider

$$E_{28}: \; y^2 = x^3 - 7138223372x + 232131092574192.$$

The sequence $(a_p(E_{28}) \mod 28 : p \leq 580 \text{ and } p \nmid N_{E_{28}})$ is

$$(0, 1, 2, 26, 25, 22, 24, 19, 10, 9, 26, 22, 2, 24, 1, 10, 6, 10, 10, 16, 21, 21, 25, 22, 18, 23, 6, 20, 0, 19, 16, 11, 4, 17, 6, 16, 21, 16, 5, 24, 19, 15, 10, 26, 0, 14, 1, 3, 6, 14, 14, 21, 4, 18, 14, 3, 27, 14, 5, 14, 18, 21, 27, 20, 27, 16, 9, 25, 24, 0, 11, 22, 6, 3, 13, 10, 25, 2, 19, 18, 21, 20, 4, 6, 3, 2, 6, 20, 4, 12, 26, 18, 26, 21, 14, 8, 11, 26, 23, 4, 3, 16, 18).$$

Example

Consider

$$E_{28}: \; y^2 = x^3 - 7138223372x + 232131092574192.$$

The sequence $(a_p(E_{28}) \mod 28 : p \leq 580 \text{ and } p \nmid N_{E_{28}})$ is

$$(0, 1, 2, 26, 25, 22, 24, 19, 10, 9, 26, 22, 2, 24, 1, 10, 6, 10, 10, 16, 21, 21, 25, 22, 18, 23, 6, 20, 0, 19, 16, 11, 4, 17, 6, 16, 21, 16, 5, 24, 19, 15, 10, 26, 0, 14, 1, 3, 6, 14, 14, 21, 4, 18, 14, 3, 27, 14, 5, 14, 18, 21, 27, 20, 27, 16, 9, 25, 24, 0, 11, 22, 6, 3, 13, 10, 25, 2, 19, 18, 21, 20, 4, 6, 3, 2, 6, 20, 4, 12, 26, 18, 26, 21, 14, 8, 11, 26, 23, 4, 3, 16, 18).$$

See: the residue class $7 \mod 28$ is missing.

Example

Consider

$$E_{28}: \; y^2 = x^3 - 7138223372x + 232131092574192.$$

The sequence $(a_p(E_{28}) \mod 28 : p \leq 580 \text{ and } p \nmid N_{E_{28}})$ is

$(0, 1, 2, 26, 25, 22, 24, 19, 10, 9, 26, 22, 2, 24, 1, 10, 6, 10, 10, 16, 21, 21, 25, 22, 18, 23, 6, 20, 0, 19, 16, 11, 4, 17, 6, 16, 21, 16, 5, 24, 19, 15, 10, 26, 0, 14, 1, 3, 6, 14, 14, 21, 4, 18, 14, 3, 27, 14, 5, 14, 18, 21, 27, 20, 27, 16, 9, 25, 24, 0, 11, 22, 6, 3, 13, 10, 25, 2, 19, 18, 21, 20, 4, 6, 3, 2, 6, 20, 4, 12, 26, 18, 26, 21, 14, 8, 11, 26, 23, 4, 3, 16, 18).$

See: the residue class $7 \mod 28$ is missing.

Due to the nature of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E_{28}[28]$, every $r \equiv 7 \mod 28$ is a missing Frobenius trace for E_{28}.

Example

Consider

$$E_{28}: \ y^2 = x^3 - 7138223372x + 232131092574192.$$

The sequence $(a_p(E_{28}) \mod 28 : p \leq 580 \text{ and } p \nmid N_{E_{28}})$ is

$$(0, 1, 2, 26, 25, 22, 24, 19, 10, 9, 26, 22, 2, 24, 1, 10, 6, 10, 10, 16, 21, 21, 25, 22, 18, 23, 6, 20, 0, 19, 16, 11, 4, 17, 6, 16, 21, 16, 5, 24, 19, 15, 10, 26, 0, 14, 1, 3, 6, 14, 14, 21, 4, 18, 14, 3, 27, 14, 5, 14, 18, 21, 27, 20, 27, 16, 9, 25, 24, 0, 11, 22, 6, 3, 13, 10, 25, 2, 19, 18, 21, 20, 4, 6, 3, 2, 6, 20, 4, 12, 26, 18, 26, 21, 14, 8, 11, 26, 23, 4, 3, 16, 18).$$

See: the residue class $7 \mod 28$ is missing.

Due to the nature of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E_{28}[28]$, every $r \equiv 7 \mod 28$ is a missing Frobenius trace for E_{28}. ($m = 28$ is the smallest level for which E_{28} has a missing trace modulo m.)

Goal: to describe $C_{E,r}$.

Goal: to describe $C_{E,r}$.

Notation

We let $GL_2(\hat{\mathbb{Z}})$ *denotes the inverse limit of the projective system* $\{GL_2(\mathbb{Z}/m\mathbb{Z}) : m \in \mathbb{N}\}$ *with respect to the canonical projection maps. We have*

$$GL_2(\hat{\mathbb{Z}}) = \varprojlim GL_2(\mathbb{Z}/m\mathbb{Z}) \simeq \prod_{\ell \text{ prime}} GL_2(\mathbb{Z}_\ell),$$

Goal: to describe $C_{E,r}$.

Notation

We let $GL_2(\hat{\mathbb{Z}})$ denotes the inverse limit of the projective system $\{GL_2(\mathbb{Z}/m\mathbb{Z}) : m \in \mathbb{N}\}$ with respect to the canonical projection maps. We have

$$GL_2(\hat{\mathbb{Z}}) = \lim_{\leftarrow} GL_2(\mathbb{Z}/m\mathbb{Z}) \simeq \prod_{\ell \text{ prime}} GL_2(\mathbb{Z}_\ell),$$

Notation

Let ρ_E be defined by letting $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act on $E_{\text{tors}} := \bigcup_{m=1}^{\infty} E[m]$ and fixing compatible $\mathbb{Z}/m\mathbb{Z}$-bases of each $E[m]$:

$$\rho_E : \ G_{\mathbb{Q}} \longrightarrow GL_2(\hat{\mathbb{Z}}).$$

Serre's Open Image Theorem

Theorem (Serre, 1972)

If E has no complex multiplication, then $\rho_E(G_{\mathbb{Q}}) \subseteq GL_2(\hat{\mathbb{Z}})$ is an open subgroup, or, equivalently, that the index of $\rho_E(G_{\mathbb{Q}})$ in $GL_2(\hat{\mathbb{Z}})$ is finite. Consequently, there is a positive integer m for which

$$\ker\left(GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/m\mathbb{Z})\right) \subseteq \rho_E(G_{\mathbb{Q}}).$$

Serre's Open Image Theorem

Theorem (Serre, 1972)

If E has no complex multiplication, then $\rho_E(G_{\mathbb{Q}}) \subseteq GL_2(\hat{\mathbb{Z}})$ is an open subgroup, or, equivalently, that the index of $\rho_E(G_{\mathbb{Q}})$ in $GL_2(\hat{\mathbb{Z}})$ is finite. Consequently, there is a positive integer m for which

$$\ker\left(GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/m\mathbb{Z})\right) \subseteq \rho_E(G_{\mathbb{Q}}).$$

Definition

For any open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we denote by m_G its **level**, i.e. the smallest $m \in \mathbb{N}$ for which $\ker\left(\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})\right) \subseteq G$, and for any $m \in \mathbb{N}$ we define

$$G(m) := G \mod m \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Lang-Trotter Conjecture [1976] cont

Let $G_E := \rho_E(G_{\mathbb{Q}})$

Lang-Trotter Conjecture [1976] cont

Let $G_E := \rho_E(G_{\mathbb{Q}})$ and let m_E be the level of G_E.

Lang-Trotter Conjecture [1976] cont

Let $G_E := \rho_E(G_{\mathbb{Q}})$ and let m_E be the level of G_E.

$$C_{E,r} = \frac{2}{\pi} \cdot \frac{m_E |G_E(m_E)_r|}{|G_E(m_E)|} \prod_{\substack{\ell \text{ prime} \\ \ell \nmid m_E}} \frac{\ell |\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})_r|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|},$$

where, for any subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$,

$$H_r := \{g \in H : \operatorname{tr} g \equiv r \mod m\}.$$

Lang-Trotter Conjecture [1976] cont

Let $G_E := \rho_E(G_\mathbb{Q})$ and let m_E be the level of G_E.

$$C_{E,r} = \frac{2}{\pi} \cdot \frac{m_E |G_E(m_E)_r|}{|G_E(m_E)|} \prod_{\substack{\ell \text{ prime} \\ \ell \nmid m_E}} \frac{\ell |\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})_r|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|},$$

where, for any subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$,

$$H_r := \{g \in H : \operatorname{tr} g \equiv r \mod m\}.$$

The infinite product over primes $\ell \nmid m_E$ is *convergent*, and each ℓ-th factor is nonzero.

Lang-Trotter Conjecture [1976] cont

Let $G_E := \rho_E(G_{\mathbb{Q}})$ and let m_E be the level of G_E.

$$C_{E,r} = \frac{2}{\pi} \cdot \frac{m_E |G_E(m_E)_r|}{|G_E(m_E)|} \prod_{\substack{\ell \text{ prime} \\ \ell \nmid m_E}} \frac{\ell |\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})_r|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|},$$

where, for any subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$,

$$H_r := \{g \in H : \operatorname{tr} g \equiv r \mod m\}.$$

The infinite product over primes $\ell \nmid m_E$ is *convergent*, and each ℓ-th factor is nonzero.

It follows that

$$C_{E,r} = 0 \iff \exists m \mid m_E \text{ for which } G_E(m)_r = \emptyset.$$

Modular Curves Preliminaries

Definition

An open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ satisfying

$$\exists r \in \mathbb{Z} \text{ for which } \{g \in G : \operatorname{tr} g \equiv r \mod m_G\} = \emptyset$$

is called a **missing trace group**.

Modular Curves Preliminaries

Definition

An open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ satisfying

$$\exists r \in \mathbb{Z} \text{ for which } \{g \in G : \operatorname{tr} g \equiv r \mod m_G\} = \emptyset$$

is called a **missing trace group**.

Notation

For any open subgroup $G \subseteq GL_2(\hat{\mathbb{Z}})$, let $\tilde{G} := \langle G, -I \rangle$, and consider the modular curve $X_{\tilde{G}}$, whose non-CM rational points correspond to non-CM elliptic curves E with $\rho_E(G_{\mathbb{Q}}) \subseteq \tilde{G}$, up to conjugation inside $GL_2(\hat{\mathbb{Z}})$.

Modular Curves Preliminaries

Definition

An open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ satisfying

$$\exists r \in \mathbb{Z} \;\text{ for which }\; \{g \in G : \operatorname{tr} g \equiv r \mod m_G\} = \emptyset$$

is called a **missing trace group**.

Notation

For any open subgroup $G \subseteq GL_2(\hat{\mathbb{Z}})$, let $\tilde{G} := \langle G, -I \rangle$, and consider the modular curve $X_{\tilde{G}}$, whose non-CM rational points correspond to non-CM elliptic curves E with $\rho_E(G_{\mathbb{Q}}) \subseteq \tilde{G}$, up to conjugation inside $GL_2(\hat{\mathbb{Z}})$.

Our interest: modular curves $X_{\tilde{G}}$ of genus zero, where G is a missing trace group.

Theorem (Main Thesis Result)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. We have that $\rho_E(G_{\mathbb{Q}})$ is contained in a missing trace group $G \subseteq GL_2(\hat{\mathbb{Z}})$ whose associated modular curve $X_{\tilde{G}}$ has genus zero if and only if there is a 3-tuple (m, i, k) as listed in the shared table and $t_0, D_0 \in \mathbb{Q}$ so that either E is isomorphic over $\mathbb{Q}$ to one of the following two elliptic curves:

$$D_0 y^2 = x^3 + a_{4;m,i}(t_0)x + a_{6;m,i}(t_0) \quad (-I \in G)$$
$$d_{m,i,k}(t_0) y^2 = x^3 + a_{4;m,i}(t_0)x + a_{6;m,i}(t_0) \quad (-I \notin G),$$

where the j-invariant and twist parameter $j_{m,i}(t), d_{m,i,k}(t) \in \mathbb{Q}(t)$ are as listed in the shared tables and the coefficients $a_{4;m,i}(t), a_{6,m,i}(t) \in \mathbb{Q}(t)$ are defined by

$$a_{4;m,i}(t) := \frac{108 j_{m,i}(t)}{1728 - j_{m,i}(t)}, \qquad a_{6;m,i}(t) := \frac{432 j_{m,i}(t)}{1728 - j_{m,i}(t)}.$$

Notation

For open $G_1, G_2 \subseteq GL_2(\hat{\mathbb{Z}})$:

$$G_1 \doteq G_2 \overset{\text{def}}{\iff} \exists g \in GL_2(\hat{\mathbb{Z}}) \textit{ with } G_1 = gG_2g^{-1},$$
$$G_1 \dot{\subseteq} G_2 \overset{\text{def}}{\iff} \exists g \in GL_2(\hat{\mathbb{Z}}) \textit{ with } G_1 \subseteq gG_2g^{-1}.$$

Notation

For open $G_1, G_2 \subseteq GL_2(\hat{\mathbb{Z}})$:

$$G_1 \doteq G_2 \overset{\text{def}}{\iff} \exists g \in GL_2(\hat{\mathbb{Z}}) \text{ with } G_1 = gG_2g^{-1},$$
$$G_1 \dot{\subseteq} G_2 \overset{\text{def}}{\iff} \exists g \in GL_2(\hat{\mathbb{Z}}) \text{ with } G_1 \subseteq gG_2g^{-1}.$$

Notation

$$\begin{aligned}
\mathfrak{G} &:= \{G \subseteq GL_2(\hat{\mathbb{Z}}) : \ G \text{ is open and } \det G = \hat{\mathbb{Z}}^{\times}\},\\
\mathfrak{G}(g) &:= \{G \in \mathfrak{G} : X_{\tilde{G}} \text{ has genus } g\},\\
\mathfrak{G}_{MT} &:= \{G \in \mathfrak{G} : \exists r \in \mathbb{Z} \text{ with } G_r = \emptyset\},\\
\mathfrak{G}_{MT}^{\max} &:= \{G \in \mathfrak{G}_{MT} : \ G \text{ is maximal with respect to } \dot{\subseteq}\},\\
\mathfrak{G}_{MT}(g) &:= \mathfrak{G}_{MT} \cap \mathfrak{G}(g), \qquad \mathfrak{G}_{MT}^{\max}(g) := \mathfrak{G}_{MT}^{\max} \cap \mathfrak{G}(g).
\end{aligned}$$

Notation

For open $G_1, G_2 \subseteq GL_2(\hat{\mathbb{Z}})$*:*

$$G_1 \doteq G_2 \overset{\text{def}}{\iff} \exists g \in GL_2(\hat{\mathbb{Z}}) \text{ with } G_1 = gG_2g^{-1},$$
$$G_1 \dot{\subseteq} G_2 \overset{\text{def}}{\iff} \exists g \in GL_2(\hat{\mathbb{Z}}) \text{ with } G_1 \subseteq gG_2g^{-1}.$$

Notation

$$\begin{aligned}
\mathfrak{G} &:= \{G \subseteq GL_2(\hat{\mathbb{Z}}) : \ G \text{ is open and } \det G = \hat{\mathbb{Z}}^\times\}, \\
\mathfrak{G}(g) &:= \{G \in \mathfrak{G} : X_{\tilde{G}} \text{ has genus } g\}, \\
\mathfrak{G}_{MT} &:= \{G \in \mathfrak{G} : \exists r \in \mathbb{Z} \text{ with } G_r = \emptyset\}, \\
\mathfrak{G}_{MT}^{\max} &:= \{G \in \mathfrak{G}_{MT} : \ G \text{ is maximal with respect to } \dot{\subseteq}\}, \\
\mathfrak{G}_{MT}(g) &:= \mathfrak{G}_{MT} \cap \mathfrak{G}(g), \qquad \mathfrak{G}_{MT}^{\max}(g) := \mathfrak{G}_{MT}^{\max} \cap \mathfrak{G}(g).
\end{aligned}$$

$$\exists r \text{ with } C_{E,r} = 0 \iff \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G, \text{ some } G \in \mathfrak{G}_{MT}^{\max}$$

$$\exists r \text{ with } C_{E,r} = 0 \iff \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G, \text{ some } G \in \mathfrak{G}_{MT}^{\max}$$

$$\exists r \text{ with } C_{E,r} = 0 \iff \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G, \text{ some } G \in \mathfrak{G}_{MT}^{\max}$$

Main theorem $\iff$ explicit models / twist families for $X_{\tilde{G}}$, $\forall G \in \mathfrak{G}_{MT}^{\max}(0)$.

$$\exists r \text{ with } C_{E,r} = 0 \iff \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G, \text{ some } G \in \mathfrak{G}_{MT}^{\max}$$

Main theorem $\iff$ explicit models / twist families for $X_{\tilde{G}}$, $\forall G \in \mathfrak{G}_{MT}^{\max}(0)$.

Proof in four steps:

1. Bound m_G for each $G \in \mathfrak{G}_{MT}^{\max}(0)$,

$$\exists r \text{ with } C_{E,r} = 0 \iff \rho_E(G_{\mathbb{Q}}) \mathrel{\dot{\subseteq}} G, \text{ some } G \in \mathfrak{G}_{MT}^{\max}$$

Main theorem $\iff$ explicit models / twist families for $X_{\tilde{G}}$, $\forall G \in \mathfrak{G}_{MT}^{\max}(0)$.

Proof in four steps:

1. Bound m_G for each $G \in \mathfrak{G}_{MT}^{\max}(0)$,
2. Find all $G \in \mathfrak{G}_{MT}^{\max}(0)/\doteq$,

$$\exists r \text{ with } C_{E,r} = 0 \iff \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G, \text{ some } G \in \mathfrak{G}_{MT}^{\max}$$

Main theorem $\iff$ explicit models / twist families for $X_{\tilde{G}}$, $\forall G \in \mathfrak{G}_{MT}^{\max}(0)$.

Proof in four steps:

1. Bound m_G for each $G \in \mathfrak{G}_{MT}^{\max}(0)$,
2. Find all $G \in \mathfrak{G}_{MT}^{\max}(0)/\doteq$,
3. For each such G, exhibit $j_{\tilde{G}} : X_{\tilde{G}} \to X(1)$,

$$\exists r \text{ with } C_{E,r} = 0 \iff \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G, \text{ some } G \in \mathfrak{G}_{MT}^{\max}$$

Main theorem $\iff$ explicit models / twist families for $X_{\tilde{G}}$, $\forall G \in \mathfrak{G}_{MT}^{\max}(0)$.

Proof in four steps:

1. Bound m_G for each $G \in \mathfrak{G}_{MT}^{\max}(0)$,
2. Find all $G \in \mathfrak{G}_{MT}^{\max}(0)/ \doteq$,
3. For each such G, exhibit $j_{\tilde{G}} : X_{\tilde{G}} \to X(1)$,
4. In case $-I \notin G$, find the twist family $\mathcal{E}/\mathbb{Q}(t)$ satisfying $\rho_{\mathcal{E}}(G_{\mathbb{Q}(t)}) \subseteq G$.

$$\exists r \text{ with } C_{E,r} = 0 \iff \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G, \text{ some } G \in \mathfrak{G}_{MT}^{\max}$$

Main theorem $\iff$ explicit models / twist families for $X_{\tilde{G}}$, $\forall G \in \mathfrak{G}_{MT}^{\max}(0)$.

Proof in four steps:

1. Bound m_G for each $G \in \mathfrak{G}_{MT}^{\max}(0)$,
2. Find all $G \in \mathfrak{G}_{MT}^{\max}(0)/\doteq$,
3. For each such G, exhibit $j_{\tilde{G}} : X_{\tilde{G}} \to X(1)$,
4. In case $-I \notin G$, find the twist family $\mathcal{E}/\mathbb{Q}(t)$ satisfying $\rho_{\mathcal{E}}(G_{\mathbb{Q}(t)}) \subseteq G$.

Notation

For step 1:

$$\mathfrak{G}_{MT}^{\max}(g, m) := \{G \in \mathfrak{G}_{MT}^{\max}(g) : m_G = m\}$$

Step 1: Bounding m_G for $G \in \mathfrak{G}_{MT}^{\max}(0)$

Step 1: Bounding m_G for $G \in \mathfrak{G}_{MT}^{\max}(0)$

$$\mathfrak{G}_{MT}^{\max}(g, m) := \{G \in \mathfrak{G}_{MT}^{\max}(g) : m_G = m\}$$

Step 1: Bounding m_G for $G \in \mathfrak{G}_{MT}^{\max}(0)$

$$\mathfrak{G}_{MT}^{\max}(g,m) := \{G \in \mathfrak{G}_{MT}^{\max}(g) : m_G = m\}$$

Theorem (Step 1 Thm)

$$\mathfrak{G}_{MT}^{\max}(0) = \bigcup_{m \in \left\{ \substack{2,3,4,5,6,7,8, \\ 9,10,12,14,28} \right\}} \mathfrak{G}_{MT}^{\max}(0,m),$$

Step 1: Bounding m_G for $G \in \mathfrak{G}_{MT}^{\max}(0)$

$$\mathfrak{G}_{MT}^{\max}(g,m) := \{G \in \mathfrak{G}_{MT}^{\max}(g) : m_G = m\}$$

Theorem (Step 1 Thm)

$$\mathfrak{G}_{MT}^{\max}(0) = \bigcup_{m \in \left\{ \substack{2,3,4,5,6,7,8, \\ 9,10,12,14,28} \right\}} \mathfrak{G}_{MT}^{\max}(0,m),$$

Proof sketch of Step 1 Thm:

1. Work of Cummins-Pauli $\rightsquigarrow$ $\forall G \in \mathfrak{G}(0)$, the SL_2-level of G is ≤ 96

Step 1: Bounding m_G for $G \in \mathfrak{G}_{MT}^{\max}(0)$

$$\mathfrak{G}_{MT}^{\max}(g, m) := \{G \in \mathfrak{G}_{MT}^{\max}(g) : m_G = m\}$$

Theorem (Step 1 Thm)

$$\mathfrak{G}_{MT}^{\max}(0) = \bigcup_{m \in \left\{ \substack{2,3,4,5,6,7,8,\\ 9,10,12,14,28} \right\}} \mathfrak{G}_{MT}^{\max}(0, m),$$

Proof sketch of Step 1 Thm:

1. Work of Cummins-Pauli $\rightsquigarrow$ $\forall G \in \mathfrak{G}(0)$, the SL_2-level of G is ≤ 96
2. Group theory $\rightsquigarrow$ upper bound for m_G for any $G \in \mathfrak{G}_{MT}^{\max}(0)$

Step 1: Bounding m_G for $G \in \mathfrak{G}_{MT}^{\max}(0)$

$$\mathfrak{G}_{MT}^{\max}(g, m) := \{G \in \mathfrak{G}_{MT}^{\max}(g) : m_G = m\}$$

Theorem (Step 1 Thm)

$$\mathfrak{G}_{MT}^{\max}(0) = \bigcup_{m \in \left\{ \substack{2,3,4,5,6,7,8,\\ 9,10,12,14,28} \right\}} \mathfrak{G}_{MT}^{\max}(0, m),$$

Proof sketch of Step 1 Thm:

1. Work of Cummins-Pauli $\rightsquigarrow$ $\forall G \in \mathfrak{G}(0)$, the SL_2-level of G is ≤ 96
2. Group theory $\rightsquigarrow$ upper bound for m_G for any $G \in \mathfrak{G}_{MT}^{\max}(0)$
3. A MAGMA computation then finishes Step 1 Thm.

Bounding the level

Bounding the level

Proposition (Jones, McMurdy)

Let $G \subseteq GL_2(\hat{\mathbb{Z}})$ be an open subgroup. We then have

$$\frac{level_{\mathrm{SL}_2}(G)}{level_{\mathrm{SL}_2}(\tilde{G})} \in \{1, 2\},$$

Bounding the level

Proposition (Jones, McMurdy)

Let $G \subseteq GL_2(\hat{\mathbb{Z}})$ be an open subgroup. We then have

$$\frac{level_{\mathrm{SL}_2}(G)}{level_{\mathrm{SL}_2}(\tilde{G})} \in \{1, 2\},$$

Proposition (Cummins,Pauli)

$$\left\{ level_{\mathrm{SL}_2}(\tilde{G}) : G \in \mathfrak{G}(0) \right\} = \left\{ \begin{matrix} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 \\ 18, 20, 21, 24, 25, 26, 27, 28, 30, 32, 36, 48 \end{matrix} \right\}.$$

Bounding the level

Proposition (Jones, McMurdy)

Let $G \subseteq GL_2(\hat{\mathbb{Z}})$ be an open subgroup. We then have

$$\frac{level_{\mathrm{SL}_2}(G)}{level_{\mathrm{SL}_2}(\tilde{G})} \in \{1, 2\},$$

Proposition (Cummins,Pauli)

$$\left\{ level_{\mathrm{SL}_2}(\tilde{G}) : G \in \mathfrak{G}(0) \right\} = \left\{ \begin{matrix} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 \\ 18, 20, 21, 24, 25, 26, 27, 28, 30, 32, 36, 48 \end{matrix} \right\}.$$

Thus,

$$G \in \mathfrak{G}(0) \implies \mathrm{level}_{\mathrm{SL}_2}(G) \in \left\{ \begin{matrix} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \\ 13, 14, 15, 16, 18, 20, 21, 22, 24, \\ 25, 26, 27, 28, 30, 32, 36, 40, \\ 42, 48, 50, 52, 54, 56, 60, 64, 72, 96 \end{matrix} \right\},$$

Notation

$$m_G := level_{GL_2}(G)$$
$$m_S := level_{\mathrm{SL}_2}(G),$$

For an open subgroup $G \subseteq GL_2(\hat{\mathbb{Z}})$, we set

$$d_G := \gcd\left(m_S^\infty, \left|\frac{G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]}\right|\right),$$

i.e. d_G is the largest factor of $\left|\frac{G(m_S)\cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S),G(m_S)]}\right|$ supported on primes dividing m_S.

Notation

$$m_G := level_{GL_2}(G)$$
$$m_S := level_{\mathrm{SL}_2}(G),$$

For an open subgroup $G \subseteq GL_2(\hat{\mathbb{Z}})$, we set

$$d_G := \gcd\left(m_S^{\infty}, \left| \frac{G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]} \right| \right),$$

i.e. d_G is the largest factor of $\left| \frac{G(m_S)\cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S),G(m_S)]} \right|$ supported on primes dividing m_S.

Proposition

Let $G \in \mathfrak{G}_{MT}^{\max}$ be a maximal missing trace group of GL_2-level m_G and SL_2*-level m_S satisfying* $\det G = \hat{\mathbb{Z}}^{\times}$*. Then m_G divides $d_G m_S$.*

Proof

WLOG: we may assume that $m_G > m_S$;

Let p be any prime for which $v_p(m_G) > v_p(m_S)$

$m'_G := m_G / p^{v_p(m_G) - v_p(m_S)}$.

Note that, for any prime ℓ, we have

$$v_\ell(m'_G) = \begin{cases} v_\ell(m_G) & \text{if } \ell \neq p \\ v_\ell(m_S) & \text{if } \ell = p. \end{cases} \tag{1}$$

Proof

WLOG: we may assume that $m_G > m_S$;

Let p be any prime for which $v_p(m_G) > v_p(m_S)$

$m'_G := m_G / p^{v_p(m_G) - v_p(m_S)}$.

Note that, for any prime ℓ, we have

$$v_\ell(m'_G) = \begin{cases} v_\ell(m_G) & \text{if } \ell \neq p \\ v_\ell(m_S) & \text{if } \ell = p. \end{cases} \tag{1}$$

Since m_S divides m'_G, we have

$$\ker\left(\mathrm{SL}_2(\mathbb{Z}/m_G\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m'_G\mathbb{Z})\right) \subseteq G(m_G). \tag{2}$$

Proof

WLOG: we may assume that $m_G > m_S$;

Let p be any prime for which $v_p(m_G) > v_p(m_S)$

$m'_G := m_G / p^{v_p(m_G) - v_p(m_S)}$.

Note that, for any prime ℓ, we have

$$v_\ell(m'_G) = \begin{cases} v_\ell(m_G) & \text{if } \ell \neq p \\ v_\ell(m_S) & \text{if } \ell = p. \end{cases} \tag{1}$$

Since m_S divides m'_G, we have

$$\ker\left(\mathrm{SL}_2(\mathbb{Z}/m_G\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m'_G\mathbb{Z})\right) \subseteq G(m_G). \tag{2}$$

And since G is maximal among missing trace groups, it follows that

$$\mathrm{tr}\left(G(m'_G)\right) = \mathbb{Z}/m'_G\mathbb{Z}. \tag{3}$$

Claim: $p|m'_G$

Suppose for contradiction:
$p \nmid m'_G$, and define $\alpha := v_p(m_G) - v_p(m_S)$.

Claim: $p | m'_G$

Suppose for contradiction:
$p \nmid m'_G$, and define $\alpha := v_p(m_G) - v_p(m_S)$.

$$\mathbb{Z}/m_G\mathbb{Z} \simeq \mathbb{Z}/m'_G\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z},$$

$$\ker\left(\mathrm{SL}_2(\mathbb{Z}/m_G\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m'_G\mathbb{Z})\right) \subseteq G(m_G) \Rightarrow \{I\} \times \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq G(m_G).$$

By $\det G(m_G) = (\mathbb{Z}/m_G\mathbb{Z})^\times$, By $\det G(m_G) = (\mathbb{Z}/m_G\mathbb{Z})^\times$, $\{I\} \times \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq G(m_G)$

By $\det G(m_G) = (\mathbb{Z}/m_G\mathbb{Z})^\times$, $\{I\} \times \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq G(m_G)$ and Goursat's Lemma, we have

By $\det G(m_G) = (\mathbb{Z}/m_G\mathbb{Z})^\times$, $\{I\} \times \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq G(m_G)$ and Goursat's Lemma, we have

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}), \tag{4}$$

where $\psi_{m'_G} : G(m'_G) \longrightarrow \Gamma$ and $\psi_p : \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \longrightarrow \Gamma$ denote surjective group homomorphisms onto the common quotient group Γ implicit in the fibered product.

By $\det G(m_G) = (\mathbb{Z}/m_G\mathbb{Z})^\times$, $\{I\} \times \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq G(m_G)$ and Goursat's Lemma, we have

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}), \tag{4}$$

where $\psi_{m'_G} : G(m'_G) \longrightarrow \Gamma$ and $\psi_p : \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \longrightarrow \Gamma$ denote surjective group homomorphisms onto the common quotient group Γ implicit in the fibered product.

Furthermore,

$$\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \ker \psi_p.$$

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}),$$
$$\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \ker \psi_p,$$

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}),$$

$$\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \ker \psi_p,$$

Thus, for every $\gamma \in \Gamma$, there exists $d \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ for which

$$\{g \in \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \det g = d\} \subseteq \psi_p^{-1}(\gamma).$$

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}),$$

$$\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \ker \psi_p,$$

Thus, for every $\gamma \in \Gamma$, there exists $d \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ for which

$$\{g \in \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \det g = d\} \subseteq \psi_p^{-1}(\gamma).$$

Since $\mathrm{tr}\left(\{g \in \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \det g = d\}\right) = \mathbb{Z}/p^\alpha\mathbb{Z}$, it is then easy to deduce that $\mathrm{tr}\left(G(m_G)\right) = \mathbb{Z}/m_G\mathbb{Z}$, a contradiction.

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}),$$

$$\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \ker \psi_p,$$

Thus, for every $\gamma \in \Gamma$, there exists $d \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ for which

$$\{g \in \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \det g = d\} \subseteq \psi_p^{-1}(\gamma).$$

Since $\operatorname{tr}(\{g \in \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \det g = d\}) = \mathbb{Z}/p^\alpha\mathbb{Z}$, it is then easy to deduce that $\operatorname{tr}(G(m_G)) = \mathbb{Z}/m_G\mathbb{Z}$, a contradiction.

Therefore $p \mid m'_G$.

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}),$$
$$\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \ker \psi_p,$$

Thus, for every $\gamma \in \Gamma$, there exists $d \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ for which

$$\{g \in \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \det g = d\} \subseteq \psi_p^{-1}(\gamma).$$

Since $\mathrm{tr}\left(\{g \in \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \det g = d\}\right) = \mathbb{Z}/p^\alpha\mathbb{Z}$, it is then easy to deduce that $\mathrm{tr}\left(G(m_G)\right) = \mathbb{Z}/m_G\mathbb{Z}$, a contradiction.

Therefore $p \mid m'_G$.

Since $v_p(m'_G) = v_p(m_S)$, we see that $p \mid m_S$.

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}),$$
$$\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \ker \psi_p,$$

Thus, for every $\gamma \in \Gamma$, there exists $d \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ for which

$$\{g \in \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \det g = d\} \subseteq \psi_p^{-1}(\gamma).$$

Since $\mathrm{tr}\left(\{g \in \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \det g = d\}\right) = \mathbb{Z}/p^\alpha\mathbb{Z}$, it is then easy to deduce that $\mathrm{tr}\left(G(m_G)\right) = \mathbb{Z}/m_G\mathbb{Z}$, a contradiction.

Therefore $p \mid m'_G$.

Since $v_p(m'_G) = v_p(m_S)$, we see that $p \mid m_S$. Since the prime p was arbitrary, it follows that

$$m_G \mid m_S^\infty.$$

Quick Lemma

Notation

Let $G \subseteq GL_2(\hat{\mathbb{Z}})$ be an open subgroup of GL_2-level m_G and SL_2*-level m_S, and $m \in \mathbb{N}$ with $m_S \mid m \mid m_G$, we let π_{GL_2} and $\pi_{\mathbb{G}_m}$ denote the canonical projection maps*

$$\pi_{GL_2} : GL_2(\mathbb{Z}/m_G\mathbb{Z}) \longrightarrow GL_2(\mathbb{Z}/m\mathbb{Z}),$$
$$\pi_{\mathbb{G}_m} : (\mathbb{Z}/m_G\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times.$$

Quick Lemma Continued

$$\pi_{\mathrm{GL}_2} : \mathrm{GL}_2(\mathbb{Z}/m_G\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$
$$\pi_{\mathbb{G}_m} : (\mathbb{Z}/m_G\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times.$$

Lemma

Let $G \subseteq GL_2(\hat{\mathbb{Z}})$ be an open subgroup satisfying $m_G \mid m_S^\infty$ and let m be any positive integer satisfying $m_S \mid m$ and $m \mid m_G$. Then there exists a unique group homomorphism

$$\delta : G(m) \longrightarrow (\mathbb{Z}/m_G\mathbb{Z})^\times$$

satisfying $\pi_{\mathbb{G}_m} \circ \delta = \det$, *and such that*

$$G(m_G) = \left\{ g \in \pi_{GL_2}^{-1}\left(G(m)\right) : \delta\left(\pi_{GL_2}(g)\right) = \det g \right\}.$$

If $\det G = \hat{\mathbb{Z}}^\times$, *then* δ *is surjective and* $\delta\left(G(m) \cap \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})\right) = \ker \pi_{\mathbb{G}_m}$.

Bounding The Computation Proof Continued

$$m_G/m_S = \left|\ker\left((\mathbb{Z}/m_G\mathbb{Z})^\times \to (\mathbb{Z}/m_S\mathbb{Z})^\times\right)\right| = \left|\delta\left(G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})\right)\right|,$$

which in turn divides

$$\left|\frac{G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]}\right|.$$

Since $m_G \mid m_S^\infty$, m_G/m_S also divides m_S^∞, and thus,

$$\frac{m_G}{m_S} \text{ divides } \gcd\left(m_S^\infty, \left|\frac{G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]}\right|\right),$$

Bounding The Computation Proof Continued

$$m_G/m_S = \left|\ker\left((\mathbb{Z}/m_G\mathbb{Z})^\times \to (\mathbb{Z}/m_S\mathbb{Z})^\times\right)\right| = \left|\delta\left(G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})\right)\right|,$$

which in turn divides

$$\left|\frac{G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]}\right|.$$

Since $m_G \mid m_S^\infty$, m_G/m_S also divides m_S^∞, and thus,

$$\frac{m_G}{m_S} \text{ divides } \gcd\left(m_S^\infty, \left|\frac{G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]}\right|\right),$$

so m_G divides $m_S d_G$, as claimed.

Examples

Level 2 curves

Magma

$$\frac{\mathfrak{G}_{MT}^{\max}(0,2)}{\doteq} = \{G_{2,1}\}$$

$$G_{2,1}(2) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

$$G_{2,1} = \tilde{G}_{2,1}$$

Level 2 curves

Magma

$$\frac{\mathfrak{G}_{MT}^{\max}(0,2)}{\doteq} = \{G_{2,1}\}$$

$$G_{2,1}(2) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

$$G_{2,1} = \tilde{G}_{2,1}$$

Reference (Zywina)

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{2,1} \iff \exists t_0 \in \mathbb{Q} \textit{ for which } j_E = j_{2,1}(t_0).$$

where

$$j_{2,1}(t) := 256\frac{(t+1)^3}{t}.$$

Level 2 curves continued

$$\mathcal{E}_{2,1,1}: \; Dy^2 = x^3 + a_{4;2,1}(t)x + a_{6;2,1}(t)$$

$$a_{4;2,1}(t) = \frac{108 * 256\frac{(t+1)^3}{t}}{1728 - 256\frac{(t+1)^3}{t}}$$

$$a_{6;2,1}(t) = \frac{432 * 256\frac{(t+1)^3}{t}}{1728 - 256\frac{(t+1)^3}{t}}$$

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{2,1} \iff \exists t_0, D_0 \in \mathbb{Q}$$

for which E is isomorphic over $\mathbb{Q}$ to $\mathcal{E}_{2,1,1}(t_0, D_0)$.

Level 12 Curves

Magma

$$\frac{\mathfrak{G}_{MT}^{\max}(0,12)}{\doteq} = \{G_{12,1,1}, G_{12,2,1}, G_{12,3,1}, G_{12,4,1}, G_{12,4,2}\}$$

$$G_{12,1,1}(12) = \left\langle \begin{pmatrix} 7 & 7 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 7 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 9 \\ 9 & 8 \end{pmatrix} \right\rangle \simeq GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_{\psi^{(1,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{12,2,1}(12) = \left\langle \begin{pmatrix} 5 & 8 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 11 \\ 0 & 11 \end{pmatrix}, \begin{pmatrix} 7 & 6 \\ 3 & 7 \end{pmatrix} \right\rangle \simeq GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_{\psi^{(2,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{12,3,1}(12) = \left\langle \begin{pmatrix} 5 & 11 \\ 0 & 11 \end{pmatrix}, \begin{pmatrix} 5 & 11 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 9 & 11 \end{pmatrix} \right\rangle \simeq GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_{\psi^{(3,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{12,4,1}(12) = \left\langle \begin{pmatrix} 5 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 7 & 6 \\ 0 & 11 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \right\rangle \simeq \pi_{GL_2}^{-1}\left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times_{\psi^{(4,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{12,4,2}(12) = \left\langle \begin{pmatrix} 5 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 11 & 6 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \right\rangle \simeq \pi_{GL_2}^{-1}\left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times_{\psi^{(4,2)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$$

Level 12 continued

$$G_{12,1,1}(12) = \left\langle \begin{pmatrix} 7 & 7 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 7 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 9 \\ 9 & 8 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_\psi \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$$

$$\begin{aligned} \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} &:= \{ g \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) : \chi_4(\det g) = \varepsilon(g \mod 2) \} \\ &= \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 0 \end{pmatrix} \right\rangle, \end{aligned} \tag{5}$$

where $\chi_4 : (\mathbb{Z}/4\mathbb{Z})^\times \to \{\pm 1\}$ is the unique nontrivial multiplicative character and

$$\varepsilon : \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\simeq} S_3 \longrightarrow \frac{S_3}{A_3} \xrightarrow{\simeq} \{\pm 1\}. \tag{6}$$

$$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_\psi \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} := \{(g_4, g_3) : \psi_4(g_4) = \psi_3(g_3)\}$$

$$\begin{tikzcd}
\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_\psi \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \arrow[dr, dashed] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
& \mathrm{GL}_2(\mathbb{Z}/12\mathbb{Z}) \arrow[r] \arrow[d] & \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \arrow[d, two heads, "\psi_3"] \\
& \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \arrow[r, two heads, "\psi_4"] & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}$$

Reference (Sutherland, Zywina)

$$\rho_{E,4}(G_{\mathbb{Q}}) \subseteq GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \iff \exists t_0 \in \mathbb{Q} \;\; \textit{with} \;\; j_E = j_4(t_0)$$

where

$$j_4(t) := -t^2 + 1728.$$

$$\rho_{E,3}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \iff \exists t_0 \in \mathbb{Q} \; \textit{with} \;\; j_E = j_3(t_0)$$

where

$$j_3(t) = 27\frac{(t+1)(t+9)^3}{t^3}.$$

Magma (Resolving the Singularities)

$$-t^2 + 1728 = 27\frac{(s+1)(s+9)^3}{s^3}$$

$$s = -\frac{27}{u^2} \quad t = \frac{u^4 - 18u^2 - 27}{u}$$

$$j_{12}(u) := -\frac{(u^2-27)(u^2-3)^3}{u^2}$$

$$\rho_{E,12}(G_{\mathbb{Q}}) \dot{\subseteq} \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \iff \exists u_0 \in \mathbb{Q} \text{ with } j_E = j_{12}(u_0)$$

$$a_{4;12,1}(u) := a_{4;3,1}\left(-\frac{27}{u^2}\right) \quad a_{6;12,1} := a_{6;3,1}\left(-\frac{27}{u^2}\right)$$

$$\mathcal{E}_{12} : \; Dy^2 = x^3 + a_{4;12,1}(u)x + a_{6;12,1}(u)$$

$$\mathcal{E}_{12,1}:\ Dy^2 = x^3 + a_{4;12,i}(u)x + a_{6;12,i}(u)$$

$$\mathcal{E}_{12,1}: \; Dy^2 = x^3 + a_{4;12,i}(u)x + a_{6;12,i}(u)$$

$$\mathbb{Q}(\mathcal{E}_{12,1}[4])^{\ker \psi_4} = \mathbb{Q}\left(\sqrt{\frac{Du(u^2-27)(u^2-3)}{u^4-18u^2-27}}\right),$$
$$\mathbb{Q}(\mathcal{E}_{12,1}[3])^{\ker \psi_3} = \mathbb{Q}(\sqrt{-3}).$$

$$\mathcal{E}_{12,1} : \; Dy^2 = x^3 + a_{4;12,i}(u)x + a_{6;12,i}(u)$$

$$\mathbb{Q}(\mathcal{E}_{12,1}[4])^{\ker \psi_4} = \mathbb{Q}\left(\sqrt{\frac{Du(u^2-27)(u^2-3)}{u^4-18u^2-27}}\right),$$
$$\mathbb{Q}(\mathcal{E}_{12,1}[3])^{\ker \psi_3} = \mathbb{Q}(\sqrt{-3}).$$

Thus,

$$\rho_{\mathcal{E}_{12,1}}(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,1,1} \iff \mathbb{Q}\left(\sqrt{\frac{Du(u^2-27)(u^2-3)}{u^4-18u^2-27}}\right) = \mathbb{Q}\left(\sqrt{-3}\right)$$
$$\iff D \in -\frac{3u(u^2-27)(u^2-3)}{u^4-18u^2-27}(\mathbb{Q}(u)^{\times})^2.$$

$$\rho_{\mathcal{E}_{12,1}}(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,1,1} \iff \mathbb{Q}\left(\sqrt{\frac{Du(u^2-27)(u^2-3)}{u^4-18u^2-27}}\right) = \mathbb{Q}\left(\sqrt{-3}\right)$$

$$\iff D \in -\frac{3u(u^2-27)(u^2-3)}{u^4-18u^2-27}(\mathbb{Q}(u)^\times)^2.$$

$$\rho_{\mathcal{E}_{12,1}}(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,1,1} \iff \mathbb{Q}\left(\sqrt{\frac{Du(u^2-27)(u^2-3)}{u^4-18u^2-27}}\right) = \mathbb{Q}\left(\sqrt{-3}\right)$$

$$\iff D \in -\frac{3u(u^2-27)(u^2-3)}{u^4-18u^2-27}(\mathbb{Q}(u)^{\times})^2.$$

$$d_{12,1,1}(u) := -\frac{3u(u^2-27)(u^2-3)}{u^4-18u^2-27}$$

$$\mathcal{E}_{12,1,1}:\ d_{12,1,1}(u)y^2 = x^3 + a_{4;12,1}(u)x + a_{6;12,1}(u).$$

$$\rho_{\mathcal{E}_{12,1}}(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,1,1} \iff \mathbb{Q}\left(\sqrt{\frac{Du(u^2-27)(u^2-3)}{u^4-18u^2-27}}\right) = \mathbb{Q}\left(\sqrt{-3}\right)$$

$$\iff D \in -\frac{3u(u^2-27)(u^2-3)}{u^4-18u^2-27}(\mathbb{Q}(u)^{\times})^2.$$

$$d_{12,1,1}(u) := -\frac{3u(u^2-27)(u^2-3)}{u^4-18u^2-27}$$

$$\mathcal{E}_{12,1,1}: \ d_{12,1,1}(u)y^2 = x^3 + a_{4;12,1}(u)x + a_{6;12,1}(u).$$

$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,1,1} \iff \exists u_0 \in \mathbb{Q}$ for which E is isomorphic over $\mathbb{Q}$ to $\mathcal{E}_{12,1,1}(u_0)$