Elliptic Curves and Moonshine

Maryam Khaqan

Emory University

Vanderbilt Number Theory Seminar
September 1st, 2020

Main Idea

Can moonshine help answer number theoretic questions?

Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $E(\mathbb{Q})$ denote the set of $\mathbb{Q}$-rational points of E.

Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $E(\mathbb{Q})$ denote the set of $\mathbb{Q}$-rational points of E.

Theorem 1 (Mordell).

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}.$$

Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $E(\mathbb{Q})$ denote the set of $\mathbb{Q}$-rational points of E.

Theorem 1 (Mordell).

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tor}}.$$

Computing the rank r of a general elliptic curve is considered a hard problem in number theory.

Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $E(\mathbb{Q})$ denote the set of $\mathbb{Q}$-rational points of E.

Theorem 1 (Mordell).

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}.$$

Computing the rank r of a general elliptic curve is considered a hard problem in number theory.

Conjecture (Birch and Swinnerton–Dyer).

The rank of an elliptic curve equals the order of vanishing of its L-function $L_E(s)$ at $s = 1$.

Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $E(\mathbb{Q})$ denote the set of $\mathbb{Q}$-rational points of E.

Theorem 1 (Mordell).

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}.$$

Computing the rank r of a general elliptic curve is considered a hard problem in number theory.

Conjecture (Birch and Swinnerton–Dyer).

The rank of an elliptic curve equals the order of vanishing of its L-function $L_E(s)$ at $s = 1$.

It is known that if $L_E(1) \neq 0$, then $r = 0$.

An Elliptic Curve

Let E be the following elliptic curve over $\mathbb{Q}$,

$$y^2 = x^3 + 864x - 432$$

An Elliptic Curve

Let E be the following elliptic curve over $\mathbb{Q}$,

$$y^2 = x^3 + 864x - 432$$

For $d < 0$ a fundamental discriminant, let E^d be the quadratic twist,

$$E^d:\ y^2 = x^3 + 864d^2x - 432d^3$$

An Elliptic Curve

Let E be the following elliptic curve over $\mathbb{Q}$,

$$y^2 = x^3 + 864x - 432$$

For $d < 0$ a fundamental discriminant, let E^d be the quadratic twist,

$$E^d: \; y^2 = x^3 + 864d^2x - 432d^3$$

Question: How does rank(E^d) vary with d?

Some Data

We will restrict to discriminants such that $\left(\frac{d}{19}\right) = -1$.

$\lvert d \rvert$	$\mathrm{rank}(E^d)$
4	0
7	0
11	0
20	0
23	2
24	0
$\vdots$	$\vdots$
83	2
87	2
104	2
111	0

Modular Form

Let $F(\tau)$ denote the unique (weakly holomorphic) modular form in $M^{+,!}_{\frac{3}{2}}(\Gamma_0(4))$ such that

$$F(q) = q^{-5} + O(q)$$

Modular Form

Let $F(\tau)$ denote the unique (weakly holomorphic) modular form in $M^{+,!}_{\frac{3}{2}}(\Gamma_0(4))$ such that

$$F(q) = q^{-5} + O(q)$$

Let $c(d)$ denote the coefficient of q^{-d} in the q-expansion for F.

More Data

$\lvert d \rvert$	$c(d)$	$\operatorname{rank}(E^d)$
4	- 565760	0
7	52756480	0
11	5874905295	0
20	- 19691491018752	0
23	19134687173120	2
24	- 39491997576192 0	0
$\vdots$	$\vdots$	$\vdots$
83	2785957292415739748496579900	2
87	12789100785793929041912463360	2
104	-5795391541224855221729145169920	2
111	6209987264585911490401602404352 0	0

More Data

$\lvert d\rvert$	$c(d) \mod 19$	$\mathrm{rank}(E^d)$
4	3	0
7	16	0
11	16	0
20	3	0
23	0	2
24	13	0
$\vdots$	$\vdots$	$\vdots$
83	0	2
87	0	2
104	0	2
111	13	0

Theorem

Let Th denote *Thompson's group*, the sporadic simple group of order $2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

Theorem

Let Th denote *Thompson's group*, the sporadic simple group of order $2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

Theorem 2.

There exists an infinite-dimensional graded Th-module $W = \bigoplus_{n \in \mathbb{Z}} W_n$ such that if

$$\dim(W_{|d|}) \not\equiv 0 \pmod{19},$$

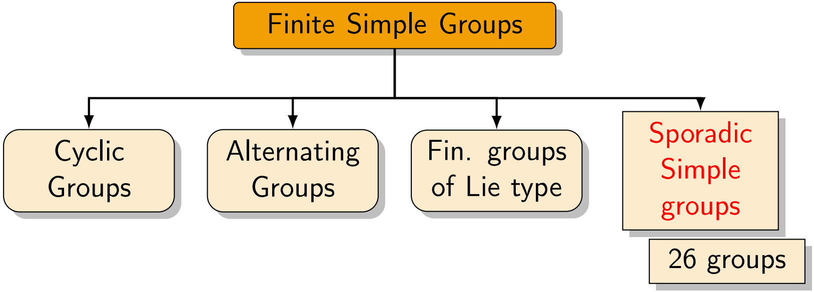
then the Mordell–Weil group $E^d(\mathbb{Q})$ is finite for each elliptic curve E of conductor 19, and each $d < 0$ as above.

Plan for the rest of the talk

- ✓ Motivation+Statement of Theorem 2.
- What is moonshine?
- (Sketch of) Proof of Theorem 2.
  1. Step 1: Existence of module.
  2. Step 2: Elliptic Curves.
- Other results.

Finite Simple Groups

The complete classification of finite simple groups is one of the greatest achievements of 20th-century mathematics.



The Monster is born

- The Monster group is the largest of the sporadic simple groups.

$$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

The Monster is born

- The Monster group is the largest of the sporadic simple groups.

  $$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

- Fischer and Griess first conjectured the existence of the Monster group in 1973, and Griess announced a construction in 1981.

The Monster is born

- The Monster group is the largest of the sporadic simple groups.

$$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

- Fischer and Griess first conjectured the existence of the Monster group in 1973, and Griess announced a construction in 1981.
- In the interim, Conway and Norton conjectured that that the smallest non-trivial $\mathbb{M}$-irrep is 196883-dimensional, and Fischer, Livingstone, and Thorne computed the character table for the Monster based on this assumption (1978).

The Monster is born

- The Monster group is the largest of the sporadic simple groups.

$$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

- Fischer and Griess first conjectured the existence of the Monster group in 1973, and Griess announced a construction in 1981.
- In the interim, Conway and Norton conjectured that that the smallest non-trivial $\mathbb{M}$-irrep is 196883-dimensional, and Fischer, Livingstone, and Thorne computed the character table for the Monster based on this assumption (1978).

Coincidence?

John McKay: Consider the normalized elliptic modular invariant

$$J(\tau) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + O(q^4),$$

$$1 + 196883 = 196884$$

Coincidence?

John McKay: Consider the normalized elliptic modular invariant

$$J(\tau) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + O(q^4),$$

$$1 + 196883 = 196884$$

John Thompson:

$$1 + 196883 + 21296876 = 21493760$$
$$2 \cdot 1 + 2 \cdot 196883 + 21296876 + 842609326 = 864299970.$$

dimensions of $\mathbb{M}$-irreps = coefficients of J

Coincidence?

John McKay: Consider the normalized elliptic modular invariant

$$J(\tau) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + O(q^4),$$

$$1 + 196883 = 196884$$

John Thompson:

$$1 + 196883 + 21296876 = 21493760$$
$$2 \cdot 1 + 2 \cdot 196883 + 21296876 + 842609326 = 864299970.$$
$$\text{dimensions of } \mathbb{M}\text{-irreps} = \text{coefficients of J}$$

This gets weirder.

Coincidence? I think not.

Dimensions of $\mathbb{M}$-irreps are the entries in the first coloumn of the character table.

Coincidence? I think not.

Dimensions of $\mathbb{M}$-irreps are the entries in the first coloumn of the character table.
Look at the second coloumn instead:

$$1 + 4371 = 4372$$
$$1 + 4371 + 91884 = 96256$$
$$2 \cdot 1 + 2 \cdot 4371 + 91884 + 1139374 = 1240002$$

Traces of element of order 2 on $\mathbb{M}$-irreps $= ?$

Coincidence? I think not.

Dimensions of $\mathbb{M}$-irreps are the entries in the first coloumn of the character table.
Look at the second coloumn instead:

$$1 + 4371 = 4372$$
$$1 + 4371 + 91884 = 96256$$
$$2 \cdot 1 + 2 \cdot 4371 + 91884 + 1139374 = 1240002$$

Traces of element of order 2 on $\mathbb{M}$-irreps = ?

$$T_{2A}(\tau) = q^{-1} + 4372q + 96256q^2 + 1240002q^3 + O(q^4).$$

Monstrous Moonshine

Conjecture (Thompson 1979).

There exists an infinite-dimensional $\mathbb{M}$-module V whose graded dimension is $J(\tau)$ and each of whose McKay–Thompson series,

$$T_g(\tau) := \sum_{n \geq -1} \mathrm{trace}(g|V_n)q^n$$

is a normalized principle modulus for a genus-zero subgroup Γ_g of $SL_2(\mathbb{R})$.

This conjecture was proven by Borcherds (building on work by Conway–Norton, Frenkel–Lepowsky–Meurmann) in 1992.

Monstrous Moonshine

Conjecture (Thompson 1979).

There exists an infinite-dimensional $\mathbb{M}$-module V whose graded dimension is $J(\tau)$ and each of whose McKay–Thompson series,

$$T_g(\tau) := \sum_{n \geq -1} \operatorname{trace}(g|V_n)q^n$$

is a normalized principle modulus for a genus-zero subgroup Γ_g of $SL_2(\mathbb{R})$.

This conjecture was proven by Borcherds (building on work by Conway–Norton, Frenkel–Lepowsky–Meurmann) in 1992.

Genus-Zero Property

Fact.

A normalized principle modulus is uniquely determined by its invariance group.

Genus-Zero Property

Fact.

A normalized principle modulus is uniquely determined by its invariance group.

Thus the assignment $g \to \Gamma_g$ determines each of the traces $\mathrm{trace}(g|V_n)$ for $g \in \mathbb{M}$ and $n \in \mathbb{Z}$.

Genus-Zero Property

Fact.

A normalized principle modulus is uniquely determined by its invariance group.

Thus the assignment $g \to \Gamma_g$ determines each of the traces $\mathrm{trace}(g|V_n)$ for $g \in \mathbb{M}$ and $n \in \mathbb{Z}$.
In particular, this allows us to compute the structure of V as an $\mathbb{M}$-module *without doing any computations with the Monster itself.*

Theorem

Let Th denote the *Thompson's group,* the sporadic simple group of order $2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

Theorem.

There exists an infinite-dimensional graded Th-module $W = \bigoplus_{n \in \mathbb{Z}} W_n$ such that if

$$\dim(W_{|d|}) \not\equiv 0 \pmod{19},$$

then the Mordell–Weil group $E^d(\mathbb{Q})$ is finite for each elliptic curve E of conductor 19, and each $d < 0$ as above.

Plan for the rest of the talk

- ✓ Motivation+Statement of Theorem 2.
- ✓ What is moonshine?
- (Sketch of) Proof of Theorem 2.
  1. Step 1: Existence of module.
  2. Step 2: Elliptic Curves.
- Other results.

Sketch of proof

The proof of Theorem 2 consists of two distinct parts.

1) **Existence of module.** Prove that there exists an infinite-dimensional, graded Th-module $W = \oplus_{n\in\mathbb{Z}} W_n$ such that the graded trace

$$\mathcal{F}_g(\tau) = 6q^{-5} + \sum_{n>0} \mathrm{trace}(g|W_n)q^n$$

for each g is a weakly holomorphic modular form in $M^{+,!}_{\frac{3}{2}}(\Gamma_0(4|g|), \psi_g)$ which has a specific behaviour at the cusps.

Sketch of proof

The proof of Theorem 2 consists of two distinct parts.

1) **Existence of module.** Prove that there exists an infinite-dimensional, graded Th-module $W = \oplus_{n\in\mathbb{Z}} W_n$ such that the graded trace

$$\mathcal{F}_g(\tau) = 6q^{-5} + \sum_{n>0} \mathrm{trace}(g|W_n)q^n$$

for each g is a weakly holomorphic modular form in $M^{+,!}_{\frac{3}{2}}(\Gamma_0(4|g|), \psi_g)$ which has a specific behaviour at the cusps.

2) **Connection to elliptic curves.** For $g \in 19A$, and d as above,

$$\dim(W_{|d|}) = \mathrm{trace}(g|W_{|d|}) \pmod{19}.$$

Existence of Th-module

For each rational conjugacy class $g \notin \{21A, 30AB\}$, define

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{\frac{3}{2},4|g|,\psi_g}(\tau)$$

Existence of Th-module

For each rational conjugacy class $g \notin \{21A, 30AB\}$, define

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{\frac{3}{2},4|g|,\psi_g}(\tau) = \lim_{K\to\infty} \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_K(4|g|)} q^{-5}|_{\frac{3}{2},\psi_g}\gamma$$

where $\Gamma_\infty := \{\pm\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right) : n \in \mathbb{Z}\}$ is the stabilizer of ∞ in $\Gamma_0(N)$, and

$$\Gamma_K(N) := \left\{\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma_0(N) : |c| < K \text{ and } |d| < K^2\right\}$$

Rademacher Sum

For each rational conjugacy class $g \notin \{21A, 30AB\}$, define

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{\frac{3}{2},4|g|,\psi_g}(\tau)$$

Rademacher Sum

For each rational conjugacy class $g \notin \{21A, 30AB\}$, define

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{\frac{3}{2},4|g|,\psi_g}(\tau)$$

Then, $f_g^{wh}(\tau)$ converges,

Rademacher Sum

For each rational conjugacy class $g \notin \{21A, 30AB\}$, define

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{\frac{3}{2},4|g|,\psi_g}(\tau)$$

Then, $f_g^{wh}(\tau)$ converges, has vanishing shadow,

Rademacher Sum

For each rational conjugacy class $g \notin \{21A, 30AB\}$, define

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{\frac{3}{2},4|g|,\psi_g}(\tau)$$

Then, $f_g^{wh}(\tau)$ converges, has vanishing shadow, and

$$\mathscr{F}_g(\tau) - f_g^{wh}(\tau) \in S_g := S^+_{3/2}(\Gamma_0(4|g|), \psi_g)$$

Rademacher Sum

For each rational conjugacy class $g \notin \{21A, 30AB\}$, define

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{\frac{3}{2},4|g|,\psi_g}(\tau)$$

Then, $f_g^{wh}(\tau)$ converges, has vanishing shadow, and

$$\mathcal{F}_g(\tau) - f_g^{wh}(\tau) \in S_g := S^+_{3/2}(\Gamma_0(4|g|), \psi_g)$$

Which (if any) cusp forms $f_g \in S_g$ are "allowed"?

Criteria for Existence of a Module

W is a Th-module iff there exist $m_1, m_2, \ldots, m_{39}(n) \in \mathbb{Z}$ such that

$$\mathrm{trace}(g|W_n) = \sum_{j=1}^{39} m_j(n)\chi_j(g)$$

where χ_j are the irreducible rational characters of Th.

Criteria for Existence of a Module

W is a Th-module iff there exist $m_1, m_2, \ldots, m_{39}(n) \in \mathbb{Z}$ such that

$$\mathrm{trace}(g|W_n) = \sum_{j=1}^{39} m_j(n)\chi_j(g)$$

where χ_j are the irreducible rational characters of Th.
Thus, the cusp forms that work are the ones that make these multiplicities integral.

2) Connection to elliptic curves

From the proof of the first part, we have,

$$\begin{aligned}\mathcal{F}_{19A}(\tau) &= 6R^{[-5],+}_{\frac{3}{2},76}(\tau) + 18f^{cusp}_{19A}(\tau)\\ &= 6q^{-5} + \sum_{n>0}\left(6r(n) + 18b_{19A}(n)\right)q^n\end{aligned}$$

where f^{cusp}_{19A} is the unique normalized cusp form in $S^{+}_{\frac{3}{2}}\left(\Gamma_0(76)\right)$.

2) Connection to elliptic curves

From the proof of the first part, we have,

$$\begin{aligned}\mathcal{F}_{19A}(\tau) &= 6R^{[-5],+}_{\frac{3}{2},76}(\tau) + 18f^{cusp}_{19A}(\tau) \\ &= 6q^{-5} + \sum_{n>0} \left(6r(n) + 18b_{19A}(n)\right) q^n\end{aligned}$$

where f^{cusp}_{19A} is the unique normalized cusp form in $S^{+}_{\frac{3}{2}}(\Gamma_0(76))$. Furthermore,

$$\dim(W_n) \equiv 6r(n) + 18b_{19A}(n) \mod 19$$

2) Connection to elliptic curves

From the proof of the first part, we have,

$$\begin{aligned}\mathcal{F}_{19A}(\tau) &= 6R^{[-5],+}_{\frac{3}{2},76}(\tau) + 18f^{cusp}_{19A}(\tau) \\ &= 6q^{-5} + \sum_{n>0} \left(6r(n) + 18b_{19A}(n)\right) q^n\end{aligned}$$

where f^{cusp}_{19A} is the unique normalized cusp form in $S^{+}_{\frac{3}{2}}(\Gamma_0(76))$.
Furthermore,

$$\dim(W_n) \equiv 6r(n) + 18b_{19A}(n) \mod 19$$

The Rademacher Sum part

For $g \in 19A$ and d as above,

Lemma 3.

$$r(|d|) = 0$$

"Proof:"

$$r(n) = \text{const.}^* \sum_{Q \in \mathcal{Q}_{5n}^{(19)}/\Gamma_0(19)} \chi_5(Q) \frac{J_{19}^{+}(\tau_Q)}{\omega^{(19)}(Q)}$$

where $\mathcal{Q}_D^{(N)}$ is the set of positive definite quadratic forms $Q = ax^2 + bxy + cy^2$ of discriminant $-D = b^2 - 4ac < 0$ such that $N|a$.

The Rademacher Sum part

For $g \in 19A$ and d as above,

Lemma 3.

$$r(|d|) = 0$$

"Proof:"

$$r(n) = \text{const.}^* \sum_{Q \in \mathcal{Q}_{5n}^{(19)}/\Gamma_0(19)} \chi_5(Q) \frac{J_{19}^{+}(\tau_Q)}{\omega^{(19)}(Q)}$$

where $\mathcal{Q}_D^{(N)}$ is the set of positive definite quadratic forms $Q = ax^2 + bxy + cy^2$ of discriminant $-D = b^2 - 4ac < 0$ such that $N|a$. For $n = |d|$, $\left(\frac{5d}{19}\right) = -1$, so this set is empty.

Final Steps

Thus,

$$\dim(W_{|d|}) \equiv 18b_{19A}(|d|) \mod 19$$

i.e., if $\dim(W_{|d|}) \not\equiv 0 \pmod{19}$ then $19 \nmid b_{19A}(|d|)$.

Final Steps

Thus,

$$\dim(W_{|d|}) \equiv 18 b_{19A}(|d|) \mod 19$$

i.e., if $\dim(W_{|d|}) \not\equiv 0 \pmod{19}$ then $19 \nmid b_{19A}(|d|)$.

We will show that this means that $19 \nmid L_{E^d}(1)$, for each elliptic curve E of order 19.

Final Steps

Thus,

$$\dim(W_{|d|}) \equiv 18 b_{19A}(|d|) \mod 19$$

i.e., if $\dim(W_{|d|}) \not\equiv 0 \pmod{19}$ then $19 \nmid b_{19A}(|d|)$.

We will show that this means that $19 \nmid L_{E^d}(1)$, for each elliptic curve E of order 19.

In particular, $L_{E^d}(1) \neq 0$ and thus, $r = 0$.

$19 \nmid L_{E^d}(1)$

By the modularity theorem, for each E of conductor 19, there exists a unique weight 2 newform $\mathcal{G}_E = \sum_{n=1}^{\infty} a_E(n)q^n$ of level 19 such that,

$$L_E(s) = \sum_{n=1}^{\infty} a_E(n)n^{-s}.$$

$19 \nmid L_{E^d}(1)$

By the modularity theorem, for each E of conductor 19, there exists a unique weight 2 newform $\mathcal{G}_E = \sum_{n=1}^{\infty} a_E(n) q^n$ of level 19 such that,

$$L_E(s) = \sum_{n=1}^{\infty} a_E(n) n^{-s}.$$

We let $g_E(\tau) = \sum_{n=3}^{\infty} b_E(n) q^n \in S^{+}_{\frac{3}{2}}(\Gamma_0(76))$ be the weight $\frac{3}{2}$ cusp form associated to $\mathcal{G}_E$ under the Shintani lift.

$19 \nmid L_{E^d}(1)$

By the modularity theorem, for each E of conductor 19, there exists a unique weight 2 newform $\mathcal{G}_E = \sum_{n=1}^{\infty} a_E(n)q^n$ of level 19 such that,

$$L_E(s) = \sum_{n=1}^{\infty} a_E(n)n^{-s}.$$

We let $g_E(\tau) = \sum_{n=3}^{\infty} b_E(n)q^n \in S^{+}_{\frac{3}{2}}(\Gamma_0(76))$ be the weight $\frac{3}{2}$ cusp form associated to $\mathcal{G}_E$ under the Shintani lift.

Lemma 4 (Agashe, Kohnen, Duncan–Mertens–Ono).

$$\mathrm{ord}_{19}\left(\frac{L_{E^d}(1)}{\Omega(E^d)}\right) = \mathrm{ord}_{19}\left(\frac{L_{E^{d_0}}(1)}{\Omega(E^{d_0})}\right) + \mathrm{ord}_{19}\left(b_E(|d|)^2\right)$$

where $d_0 = -4$ is the smallest possible d and a quick MAGMA calculation shows that $L_{E^{(-4)}}(1) = 0$.

Final Steps

Thus,

$$\mathrm{ord}_{19}\left(\frac{L_{E^d}(1)}{\Omega(E^d)}\right) = \mathrm{ord}_{19}\left(b_E(|d|)^2\right)$$

where $b_E(|d|)$ is the q^d coefficient of $g_E(\tau) \in S^+_{\frac{3}{2}}(\Gamma_0(76))$.

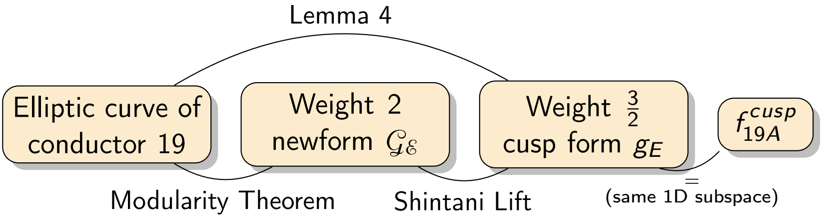
Final Steps

Thus,

$$\operatorname{ord}_{19}\left(\frac{L_{E^d}(1)}{\Omega(E^d)}\right) = \operatorname{ord}_{19}\left(b_E(|d|)^2\right)$$

where $b_E(|d|)$ is the q^d coefficient of $g_E(\tau) \in S^+_{\frac{3}{2}}(\Gamma_0(76))$. Since $S^+_{\frac{3}{2}}(\Gamma_0(76))$ is one-dimensional, $b_E(|d|) = b_{19A}(|d|)$.

(Visual) Summary of Final Steps



Theorem

Let Th denote the *Thompson's group,* the sporadic simple group of order $2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

Theorem.

There exists an infinite-dimensional graded Th-module $W = \bigoplus_{n \in \mathbb{Z}} W_n$ such that if

$$\dim(W_{|d|}) \not\equiv 0 \pmod{19},$$

then the Mordell–Weil group $E^d(\mathbb{Q})$ is finite for each elliptic curve of conductor 19, and each $d < 0$ as above.

A note on the theorem

Each $c(d) = \dim(W_d)$ is given by the finite sum

$$c(d) = \frac{-1}{\sqrt{5}} \sum_{Q \in \mathcal{Q}_{5d}^{(1)}} \chi(Q) j(\tau_Q)$$

where

$$\begin{aligned} \mathcal{Q}_{5d}^{(1)} &:= \text{set of positive definite quadratic forms with discriminant } 5d, \\ \tau_Q &:= \text{the unique root of } Q \text{ in } \mathbb{H}, \end{aligned}$$

and $j(\tau)$ is the usual elliptic modular invariant.

Other results

Now consider $d < 0$ a fundamental discriminant for which $\left(\frac{d}{7}\right) = -1$ and $\left(\frac{d}{2}\right) = 1$.

Other results

Now consider $d < 0$ a fundamental discriminant for which $\left(\frac{d}{7}\right) = -1$ and $\left(\frac{d}{2}\right) = 1$. Let E be an elliptic curve of conductor 14.

Other results

Now consider $d < 0$ a fundamental discriminant for which $\left(\frac{d}{7}\right) = -1$ and $\left(\frac{d}{2}\right) = 1$. Let E be an elliptic curve of conductor 14. Let g denote an element of order 14 in Th.

Other results

Now consider $d < 0$ a fundamental discriminant for which $\left(\frac{d}{7}\right) = -1$ and $\left(\frac{d}{2}\right) = 1$. Let E be an elliptic curve of conductor 14. Let g denote an element of order 14 in Th.

Theorem 5.

If $\mathrm{trace}(g|W_{|d|}) \not\equiv 0 \pmod{49}$, *then the Mordell–Weil group* $E^d(\mathbb{Q})$ *is finite and* $Ш(E^d)[7]$ *is trivial.*

Other results

Now consider $d < 0$ a fundamental discriminant for which $\left(\frac{d}{7}\right) = -1$ and $\left(\frac{d}{2}\right) = 1$. Let E be an elliptic curve of conductor 14. Let g denote an element of order 14 in Th.

Theorem 5.

If $\mathrm{trace}(g|W_{|d|}) \not\equiv 0 \pmod{49}$, *then the Mordell–Weil group* $E^d(\mathbb{Q})$ *is finite and* $\text{Ш}(E^d)[7]$ *is trivial.*
If, on the other hand, $\mathrm{trace}(g|W_{|d|}) \equiv 0 \pmod{49}$ *and* $\mathrm{trace}(g|W_4) \not\equiv 43 \pmod{56}$, *then* $\mathrm{Sel}_7(E^d)$ *is non-trivial, and if* $L_{E^d}(1)$ *is non-zero then so is* $\text{Ш}(E^d)[7]$.

Thank you for your attention.

Details for Lemma 4.

Let $g_E, \mathcal{G}_E$ and d as above.

Lemma 6 (Kohnen+Modularity Theorem).

$$L_{E^d}(1) = \frac{\pi}{2} \frac{\langle \mathcal{G}_E, \mathcal{G}_E \rangle}{|d|^{\frac{1}{2}} \langle g_E, g_E \rangle} \cdot |b_E(|d|)|^2,$$

Details for Lemma 4.

Let $g_E, \mathcal{G}_E$ and d as above.

Lemma 6 (Kohnen+Modularity Theorem).

$$L_{E^d}(1) = \frac{\pi}{2} \frac{\langle \mathcal{G}_E, \mathcal{G}_E \rangle}{|d|^{\frac{1}{2}} \langle g_E, g_E \rangle} \cdot |b_E(|d|)|^2,$$

Lemma 7 (Agashe).

$$\Omega(E^d) = c_E \cdot c_\infty(E^d) \cdot \omega_-(E)/\sqrt{|d|}$$

Details for Lemma 4.

Let $g_E, \mathcal{G}_E$ and d as above.

Lemma 6 (Kohnen+Modularity Theorem).

$$L_{E^d}(1) = \frac{\pi}{2} \frac{\langle \mathcal{G}_E, \mathcal{G}_E \rangle}{|d|^{\frac{1}{2}} \langle g_E, g_E \rangle} \cdot |b_E(|d|)|^2,$$

Lemma 7 (Agashe).

$$\Omega(E^d) = c_E \cdot c_\infty(E^d) \cdot \omega_-(E) / \sqrt{|d|}$$

$$\frac{L_{E^d}(1)}{\Omega(E^d)} = \frac{\pi}{2} \frac{\langle \mathcal{G}_E, \mathcal{G}_E \rangle}{|d|^{\frac{1}{2}} \langle g_E, g_E \rangle c_E \omega_-(E)} \frac{\sqrt{|d|}}{c_\infty(E^d)} \cdot |b_E(|d|)|^2$$

Tate–Shafarevich Group

Definition 6.

For E an elliptic curve over $\mathbb{Q}$, the Tate-Shafarevich group is the subgroup of elements in $H^1(\mathbb{Q}, E)$ which map to zero under every global-to-local restriction map $H^1(\mathbb{Q}, E) \to H^1(\mathbb{Q}_\nu, E)$, one for each place ν of $\mathbb{Q}$.

Conjecture (The Birch and Swinnerton–Dyer conjecture).

The rank r of an elliptic curve E over $\mathbb{Q}$ equals the order of vanishing of $L_E(s)$ at $s = 1$. Moreover, we have

$$\frac{L_E^{(r)}(1)}{r!\Omega(E)} = \#Ш(E)\,\frac{\mathrm{Reg(E)}\prod_\ell c_\ell(\mathrm{E})}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2},$$

where $L_E^{(r)}(s)$ is the r^{th} derivative of $L_E(s)$.