Elliptic Curves and Moonshine

Maryam Khaqan

Emory University

Vanderbilt Number Theory Seminar
September 1st, 2020
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).**

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

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 $\mathbb{Q}$,

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

$$E^d: \quad y^2 = x^3 + 864d^2x - 432d^3$$
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 $\text{rank}(E^d)$ vary with $d$?
Some Data

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

| \( |d| \) | \( \text{rank}(E^d) \) |
|------|-----------|
| 4    | 0         |
| 7    | 0         |
| 11   | 0         |
| 20   | 0         |
| 23   | 2         |
| 24   | 0         |
| \vdots | \vdots |
| 83   | 2         |
| 87   | 2         |
| 104  | 2         |
| 111  | 0         |
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 $F(\tau)$ 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

<p>| $|d|$ | $c(d)$ | $\text{rank}(E^d)$ |
|---|---|---|
| 4 | -565760 | 0 |
| 7 | 52756480 | 0 |
| 11 | 5874905295 | 0 |
| 20 | -19691491018752 | 0 |
| 23 | 191346871173120 | 2 |
| 24 | -394919975761920 | 0 |
| ... | ... | ... |
| 83 | 2785957292415739748496579900 | 2 |
| 87 | 12789100785793929041912463360 | 2 |
| 104 | -5795391541224855221729145169920 | 2 |
| 111 | 62099872645859114904016024043520 | 0 |</p>
<table>
<thead>
<tr>
<th>$d$</th>
<th>$c(d) \mod 19$</th>
<th>rank($E^d$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>16</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>16</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>24</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>83</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>87</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>104</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>111</td>
<td>13</td>
<td>0</td>
</tr>
</tbody>
</table>
Let $T h$ denote *Thompson’s group*, the sporadic simple group of order $2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
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*

$$\dim(W_{|d|}) \neq 0 \pmod{19},$$

*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.
  • Other results.
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 \( \mathcal{M} \)-irreps = coefficients of \( J \)
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 $M$-irreps $=$ coefficients of $J$

This gets weirder.
Coincidence? I think not.

Dimensions of $\mathcal{M}$-irreps are the entries in the first column of the character table.
Coincidence? I think not.

Dimensions of $\mathbb{M}$-irreps are the entries in the first column of the character table.
Look at the second column 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 column of the character table. Look at the second column 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 $M$-module $V$ whose graded dimension is $J(\tau)$ and each of whose McKay–Thompson series,

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

is a normalized principle modulus for a genus-zero subgroup $\Gamma_g$ 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,

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

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

This conjecture was proven by Borcherds (building on work by Conway–Norton, Frenkel–Lepowsky–Meurmann) in 1992.
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 $g \rightarrow \Gamma_g$ determines each of the traces $\text{trace}(g|V_n)$ for $g \in M$ and $n \in \mathbb{Z}$.
Fact.

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

Thus the assignment $g \rightarrow \Gamma_g$ determines each of the traces $\text{trace}(g|V_n)$ 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.
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 $\mathcal{W} = \bigoplus_{n \in \mathbb{Z}} \mathcal{W}_n$ such that if

$$\dim(\mathcal{W}|_d|) \not\equiv 0 \pmod{19},$$

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.
  - 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 $W = \bigoplus_{n \in \mathbb{Z}} W_n$ such that the graded trace

$$F_g(\tau) = 6q^{-5} + \sum_{n > 0} \text{trace}(g|W_n)q^n$$

for each $g$ is a weakly holomorphic modular form in $M_{3/2}^{+,!}(\Gamma_0(4|g|), \psi_g)$ which has a specific behaviour at the cusps.
The proof of Theorem 2 consists of two distinct parts.

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

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

for each $g$ is a weakly holomorphic modular form in $M_3^{+,!}(\Gamma_0(4|g|), \psi_g)$ which has a specific behaviour at the cusps.

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

$$\dim(W_{|d|}) = \text{trace}(g|W_{|d|}) \pmod{19}.$$
Existence of $Th$-module

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

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{3,4\abs{g},\psi_g}(\tau)$$
Existence of $Th$-module

For each rational conjugacy class $g \not\in \{21A, 30AB\}$, define

$$f^\text{wh}_g(\tau) = 6R_{\frac{3}{2}, 4|g|, \psi_g}(\tau) = \lim_{K \to \infty} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_K(4|g|)} q^{-5\left|\frac{3}{2}, \psi_g \gamma\right|}$$

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

$$\Gamma_K(N) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : |c| < K \ \text{and} \ |d| < K^2 \}$$
For each rational conjugacy class $g \not\in \{21A, 30AB\}$, define

$$f_g^{wh}(\tau) = 6R_{\frac{3}{2}, 4|g|, \psi_g}^{[-5], +}(\tau)$$
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 \( g \not\in \{21A, 30AB\} \), define

\[
f_{g}^{wh}(\tau) = 6R_{\frac{3}{2}, 4|g|, \psi_{g}}[\frac{-5}{g}, +]\]

Then, \( f_{g}^{wh}(\tau) \) converges, has vanishing shadow,
Rademacher Sum

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

\[
f_g^{\text{wh}}(\tau) = 6R_{\frac{3}{2}, 4|g|, \psi_g}(\tau)
\]

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

\[
\mathcal{F}_g(\tau) - f_g^{\text{wh}}(\tau) \in S_g := S_{3/2}^+(\Gamma_0(4|g|), \psi_g)
\]
For each rational conjugacy class $g \notin \{21A, 30AB\}$, define

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

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

$$F_g(\tau) - f_g^{wh}(\tau) \in S_g := S_{3/2}^+ (\Gamma_0(4|g|), \psi_g)$$

**Which (if any) cusp forms $f_g \in S_g$ are “allowed”?**
$\mathcal{W}$ is a $Th$-module iff there exist $m_1, m_2, \ldots, m_{39}(n) \in \mathbb{Z}$ such that

$$\text{trace}(g|\mathcal{W}_n) = \sum_{j=1}^{39} m_j(n)\chi_j(g)$$

where $\chi_j$ are the irreducible rational characters of $Th$.
Criteria for Existence of a Module

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

\[
\text{trace}(g|W_n) = \sum_{j=1}^{39} m_j(n)\chi_j(g)
\]

where \( \chi_j \) are the irreducible rational characters of \( T_h \).
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,

\[
F_{19A}(\tau) = 6R_{\frac{3}{2},76}^{\tau,-5,\tau} + 18f_{19A}^{cusp}(\tau) = 6q^{-5} + \sum_{n>0} (6r(n) + 18b_{19A}(n)) q^n
\]

where \(f_{19A}^{cusp}\) is the unique normalized cusp form in \(S_{\frac{3}{2}}^+(\Gamma_0(76))\).
2) Connection to elliptic curves

From the proof of the first part, we have,

\[ \mathcal{F}_{19A}(\tau) = 6R_{\frac{3}{2},76}^{[-5],+} (\tau) + 18f_{19A}^{cusp}(\tau) \]

\[ = 6q^{-5} + \sum_{n > 0} (6r(n) + 18b_{19A}(n)) q^n \]

where \( f_{19A}^{cusp} \) 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,

$$\mathcal{F}_{19A}(\tau) = 6R^{[-5],+}_{3,76}(\tau) + 18f_{19A}^{cusp}(\tau)$$

$$= 6q^{-5} + \sum_{n>0} (6r(n) + 18b_{19A}(n)) q^n$$

where $f_{19A}^{cusp}$ is the unique normalized cusp form in $S_{3/2}^+(\Gamma_0(76))$. Furthermore,

$$\dim(W_n) \equiv 6r(n) + 18b_{19A}(n) \mod 19$$
For $g \in 19A$ and $d$ as above,

**Lemma 3.**

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

"Proof."

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

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

Maryam Khaqan  Elliptic Curves and Moonshine
The Rademacher Sum part

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

**Lemma 3.**

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

“Proof.”

$$r(n) = \text{const.} \sum_{Q \in Q_{5n}^{(19)}/\Gamma_0(19)} \chi_5(Q) \frac{J_1^+(\tau_Q)}{\omega^{(19)}(Q)}$$

where $Q_D^{(N)}$ 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 $n = |d|$, $(\frac{5d}{19}) = -1$, so this set is empty.
Thus, \[ \dim(W_{|d|}) \equiv 18b_{19A}(|d|) \mod 19 \]
i.e., if \( \dim(W_{|d|}) \not\equiv 0 \pmod{19} \) then \( 19 \nmid b_{19A}(|d|) \).
Thus,

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

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

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

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

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

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, \( r = 0 \).
By the modularity theorem, for each $E$ of conductor 19, there exists a unique weight 2 newform $G_E = \sum_{n=1}^{\infty} a_E(n)q^n$ of level 19 such that,

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

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

We let $g_E(\tau) = \sum_{n=3}^{\infty} b_E(n) q^n \in S_{3/2}^{+}(\Gamma_0(76))$ be the weight $3/2$ cusp form associated to $G_E$ under the Shintani lift.
19 \mid L_{E^d}(1)

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

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

We let $g_E(\tau) = \sum_{n=3}^{\infty} b_E(n)q^n \in S_{3/2}^{+}(\Gamma_0(76))$ be the weight $3/2$ cusp form associated to $G_E$ under the Shintani lift.

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

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

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

Maryam Khaqan  Elliptic Curves and Moonshine
Thus,

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

where \( b_E(|d|) \) is the \( q^d \) coefficient of \( g_E(\tau) \in S_{3/2}^{+}(\Gamma_0(76)) \).
Thus,

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

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

Elliptic curve of conductor 19

Weight 2 newform $G_E$

Weight $\frac{3}{2}$ cusp form $g_E$

Modularity Theorem

Shintani Lift

Lemma 4

$f_{cusp}^{19A}$

(same 1D subspace)
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 $\mathcal{W} = \bigoplus_{n \in \mathbb{Z}} \mathcal{W}_n$ such that if

$$\dim(\mathcal{W}_{|d|}) \not\equiv 0 \pmod{19},$$

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

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

where

$\mathcal{Q}^{(1)}_{5d} : = $ set of positive definite quadratic forms with discriminant $5d$,

$\tau_Q : = $ the unique root of $Q$ in $\mathbb{H}$,

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 \( \left( \frac{d}{2} \right) = 1 \).
Now consider $d < 0$ a fundamental discriminant for which $(d/7) = -1$ and $(d/2) = 1$. Let $E$ be an elliptic curve of conductor 14.
Now consider $d < 0$ a fundamental discriminant for which $(d/7) = -1$ and $(d/2) = 1$. Let $E$ be an elliptic curve of conductor 14. Let $g$ denote an element of order 14 in $Th$. 
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* $\text{trace}(g|W_d|) \not\equiv 0 \pmod{49}$, *then the Mordell–Weil group* $E^d(\mathbb{Q})$ *is finite and* $\text{III}(E^d)[7]$ *is trivial.*
Now consider $d < 0$ a fundamental discriminant for which $(\frac{d}{7}) = -1$ and $(\frac{d}{2}) = 1$. Let $E$ be an elliptic curve of conductor 14. Let $g$ denote an element of order 14 in $T h$.

**Theorem 5.**

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

If, on the other hand, $\text{trace}(g|W_d|) \equiv 0 \pmod{49}$ and $\text{trace}(g|W_4) \not\equiv 43 \pmod{56}$, then $\text{Sel}_7(E^d)$ is non-trivial, and if $L_{E^d}(1)$ is non-zero then so is $\text{III}(E^d)[7]$. 
Thank you for your attention.
Let $g_E$, $g_E$ and $d$ as above.

**Lemma 6 (Kohnen+Modularity Theorem).**

$$L_{E^d}(1) = \frac{\pi}{2} \frac{\langle g_E, g_E \rangle}{|d|^{1/2} \langle g_E, g_E \rangle} \cdot |b_E(|d|)|^2,$$
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 $g_E, G_E$ and $d$ as above.

**Lemma 6 (Kohnen+Modularity Theorem).**

$$L_{Ed}(1) = \frac{\pi}{2} \frac{\langle G_E, G_E \rangle}{|d|^\frac{1}{2} \langle g_E, g_E \rangle} \cdot |b_E(|d|)|^2,$$

**Lemma 7 (Agashe).**

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

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

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

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