Variants of Lehmer’s Conjecture

J. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai
Variants of Lehmer’s Conjecture
1. Ramanujan’s Tau-function

“On certain arithmetical functions” (1916)

Srinivasa Ramanujan
Ramanujan defined the tau-function with the infinite product

\[
\sum_{n=1}^{\infty} \tau(n)q^n : = q \left( (1 - q^1)(1 - q^2)(1 - q^3)(1 - q^4)(1 - q^5) \cdots \right)^{24}
\]

\[
= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - \ldots.
\]
**The Prototype**

**Fact**

The function $\Delta(z) := \sum_{n=1}^{\infty} \tau(n)e^{2\pi inz}$ is a **weight 12 modular (cusp)** form for $\text{SL}_2(\mathbb{Z})$.
The Prototype

**Fact**

The function \( \Delta(z) := \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n z} \)

is a **weight 12** modular (cusp) form for \( SL_2(\mathbb{Z}) \).

For \( \text{Im}(z) > 0 \) and \((a \ b \ c \ d) \in SL_2(\mathbb{Z})\), this means that

\[
\Delta \left( \frac{az + b}{cz + d} \right) = (cz + d)^{12} \Delta(z).
\]
THE PROTOTYPE

FACT

The function $\Delta(z) := \sum_{n=1}^{\infty} \tau(n)e^{2\pi inz}$ is a weight 12 modular (cusp) form for $SL_2(\mathbb{Z})$.

For $\text{Im}(z) > 0$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, this means that

$$\Delta \left( \frac{az + b}{cz + d} \right) = (cz + d)^{12} \Delta(z).$$

UBIQUITY OF FUNCTIONS LIKE $\Delta(z)$

- Arithmetic Geometry: Elliptic curves, BSD Conjecture, ...
- Number Theory: Partitions, Quad. forms, ...
- Mathematical Physics: Mirror symmetry, ...
- Representation Theory: Moonshine, symmetric groups, ...
1. Ramanujan’s Tau-function

**Theorem (Mordell (1917))**

The following are true:

1. If \( \gcd(n, m) = 1 \), then \( \tau(nm) = \tau(n)\tau(m) \).
**Testing ground (Hecke operators)**

**Theorem (Mordell (1917))**

The following are true:

1. If $\gcd(n, m) = 1$, then $\tau(nm) = \tau(n)\tau(m)$.

2. If $p$ is prime, then $\tau(p^m) = \tau(p)\tau(p^{m-1}) - p^{11}\tau(p^{m-2})$.
Testing ground (Hecke operators)

Theorem (Mordell (1917))

The following are true:

1. If $\text{gcd}(n, m) = 1$, then $\tau(nm) = \tau(n)\tau(m)$.
2. If $p$ is prime, then $\tau(p^m) = \tau(p)\tau(p^{m-1}) - p^{11}\tau(p^{m-2})$.

Structure of Modular form spaces

- (30s) Theory of Hecke operators (linear endomorphisms)
Testing ground (Hecke operators)

Theorem (Mordell (1917))

The following are true:

1. If \( \gcd(n, m) = 1 \), then \( \tau(nm) = \tau(n)\tau(m) \).
2. If \( p \) is prime, then \( \tau(p^m) = \tau(p)\tau(p^{m-1}) - p^{11}\tau(p^{m-2}) \).

Structure of Modular form spaces

- (30s) Theory of Hecke operators (linear endomorphisms)
- (70s) Atkin-Lehner Theory of newforms (i.e. eigenforms)
Theorem (Ramanujan (1916))

If we let \( \sigma_\nu(n) := \sum_{d \mid n} d^\nu \), then

\[
\tau(n) \equiv \begin{cases} 
  n^2 \sigma_1(n) & \text{mod 3} \\
  n \sigma_1(n) & \text{mod 5} \\
  n \sigma_3(n) & \text{mod 7} \\
  \sigma_{11}(n) & \text{mod 691}
\end{cases}
\]
Theorem (Ramanujan (1916))

If we let \( \sigma_\nu(n) := \sum_{d|n} d^\nu \), then

\[
\tau(n) \equiv \begin{cases} 
  n^2 \sigma_1(n) & \text{(mod 3)} \\
  n \sigma_1(n) & \text{(mod 5)} \\
  n \sigma_3(n) & \text{(mod 7)} \\
  \sigma_{11}(n) & \text{(mod 691)}. 
\end{cases}
\]
Testing ground (Galois representations)

Theorem (Ramanujan (1916))

If we let \( \sigma_\nu(n) := \sum_{d|n} d^\nu \), then

\[ \tau(n) \equiv \begin{cases} 
  n^2 \sigma_1(n) \pmod{3} \\
  n \sigma_1(n) \pmod{5} \\
  n \sigma_3(n) \pmod{7} \\
  \sigma_{11}(n) \pmod{691}.
\end{cases} \]

Dawn of Galois Representations

- (Serre & Deligne, 70s) Reformulated using representations

\[ \rho_{\Delta, \ell} : \text{Gal}(\overline{Q}/Q) \to \text{GL}_2(F_\ell). \]
Variants of Lehmer’s Conjecture
1. Ramanujan’s Tau-function

**Theorem (Ramanujan (1916))**

If we let $\sigma_\nu(n) := \sum_{d|n} d^\nu$, then

$$\tau(n) \equiv \begin{cases} n^2 \sigma_1(n) & \text{(mod 3)} \\ n \sigma_1(n) & \text{(mod 5)} \\ n \sigma_3(n) & \text{(mod 7)} \\ \sigma_{11}(n) & \text{(mod 691)} \end{cases}.$$ 

**Dawn of Galois Representations**

- (Serre & Deligne, 70s) Reformulated using representations $\rho_{\Delta, \ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F}_\ell)$.
- (Wiles, 90s) Used to prove Fermat’s Last Theorem.
Testing ground (Ramanujan’s Conjecture)

**Conjecture (Ramanujan (1916))**

For primes $p$ we have $|\tau(p)| \leq 2p^{\frac{11}{2}}$. 


**Testing ground (Ramanujan’s Conjecture)**

**Conjecture (Ramanujan (1916))**

For primes $p$ we have $|\tau(p)| \leq 2p^{\frac{11}{2}}$.

**Dawn of Ramanujan-Petersson**

- (Deligne’s Fields Medal (1978))

  Proof of the Weil Conjectures $\implies$ Ramanujan’s Conjecture.
Testing ground (Ramanujan’s Conjecture)

Conjecture (Ramanujan (1916))

For primes $p$ we have $|\tau(p)| \leq 2p^{\frac{11}{2}}$.

Dawn of Ramanujan-Petersson

- (Deligne’s Fields Medal (1978))
  
  Proof of the Weil Conjectures $\Rightarrow$ Ramanujan’s Conjecture.

- (Ramanujan-Petersson)
  
  Generalized to newforms and generic automorphic forms.
Lehmer’s Conjecture

For every \( n \geq 1 \) we have \( \tau(n) \neq 0 \).
Lehmer’s Conjecture

Conjecture (Lehmer (1947))

For every $n \geq 1$ we have $\tau(n) \neq 0$. 

D. H. Lehmer
Theorem (Lehmer (1947))

If $\tau(n) = 0$, then $n$ is prime.
Theorem (Lehmer (1947))

If \( \tau(n) = 0 \), then \( n \) is prime.

Theorem (Serre (81), Thorner-Zaman (2018))

We have that

\[
\#\{\text{prime } p \leq X : \tau(p) = 0\} \ll \pi(X) \cdot \frac{(\log \log X)^2}{\log(X)}.
\]
Results on Lehmer’s Conjecture

**Theorem (Lehmer (1947))**

If \( \tau(n) = 0 \), then \( n \) is prime.

**Theorem (Serre (81), Thorner-Zaman (2018))**

We have that

\[
\#\{\text{prime } p \leq X : \tau(p) = 0\} \ll \pi(X) \cdot \frac{(\log \log X)^2}{\log(X)}.
\]

Namely, the set of \( p \) for which \( \tau(p) = 0 \) has density zero.
## Numerical Investigations

<table>
<thead>
<tr>
<th>N</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>3316799</td>
<td>Lehmer (1947)</td>
</tr>
<tr>
<td>214928639999</td>
<td>Lehmer (1949)</td>
</tr>
<tr>
<td>$10^{15}$</td>
<td>Serre (1973, p. 98), Serre (1985)</td>
</tr>
<tr>
<td>1213229187071998</td>
<td>Jennings (1993)</td>
</tr>
<tr>
<td>22689242781695999</td>
<td>Jordan and Kelly (1999)</td>
</tr>
<tr>
<td>22798241520242687999</td>
<td>Bosman (2007)</td>
</tr>
<tr>
<td>982149821766199295999</td>
<td>Zeng and Yin (2013)</td>
</tr>
<tr>
<td>816212624008487344127999</td>
<td>Derickx, van Hoeij, and Zeng (2013)</td>
</tr>
</tbody>
</table>

Lehmer’s Conjecture confirmed for $n \leq N$
Variants of Lehmer’s Conjecture

2. Lehmer’s Conjecture

**Variant: Varying newforms and fixing \( p \)**

Theorem (Calegari, Sardari (2020))

Fix a prime \( p \) and level \( N \) coprime to \( p \).

At most finitely many non-CM level \( N \) newforms \( f = q + \sum_{n=2}^{\infty} a_f(n)q^n \) have \( a_f(p) = 0 \).
**Variant: Varying newforms and fixing $p$**

**Theorem (Calegari, Sardari (2020))**

Fix a prime $p$ and level $N$ coprime to $p$. 

**Fix a prime $p$ and level $N$ coprime to $p$.**
**Theorem (Calegari, Sardari (2020))**

Fix a prime $p$ and level $N$ coprime to $p$.

At most finitely many non-CM level $N$ newforms

$$f = q + \sum_{n=2}^{\infty} a_f(n) q^n$$

have $a_f(p) = 0$. 
2. Lehmer’s Conjecture

**Variant: Can** \( \tau(n) = \alpha \)?
**Variant:** Can $\tau(n) = \alpha$?

**Theorem (Murty, Murty, Shorey (1987))**

For odd integers $\alpha$, there are at most finitely many $n$ for which

$$\tau(n) = \alpha.$$
**Variant:** Can $\tau(n) = \alpha$?

**Theorem (Murty, Murty, Shorey (1987))**

For odd integers $\alpha$, there are at most finitely many $n$ for which $\tau(n) = \alpha$.

**Remarks**

1. Computationally prohibitive (i.e. “linear forms in logs”).
**Variant: Can $\tau(n) = \alpha$?**

**Theorem (Murty, Murty, Shorey (1987))**

For odd integers $\alpha$, there are at most finitely many $n$ for which

$$\tau(n) = \alpha.$$ 

**Remarks**

(1) Computationally prohibitive (i.e. “linear forms in logs”).

(2) (Lygeros and Rozier, 2013) If $n > 1$, then $\tau(n) \neq \pm 1$. 

**Variants of Lehmer’s Conjecture**

2. Lehmer’s Conjecture

**Variant: Can $\tau(n) = \alpha?$**

**Theorem (Murty, Murty, Shorey (1987))**

For **odd** integers $\alpha$, there are at most finitely many $n$ for which $\tau(n) = \alpha$.

**Remarks**

1. Computationally prohibitive (i.e. “linear forms in logs”).
2. (Lygeros and Rozier, 2013) If $n > 1$, then $\tau(n) \neq \pm 1$.
3. Classifying soln’s to $\tau(n) = \alpha$ not done in any other cases.
Can $|\tau(n)| = \ell^m$, a power of an odd prime?

**Theorem (B-C-O-T)**

If $|\tau(n)| = \ell^m$, then $n = p^{d-1}$, with $p$ and $d | \ell(\ell^2 - 1)$ are odd primes.
Can $|\tau(n)| = \ell^m$, a power of an odd prime?

**Theorem (B-C-O-T)**

If $|\tau(n)| = \ell^m$, then $n = p^{d-1}$, with $p$ and $d | \ell(\ell^2 - 1)$ are odd primes.

**Algorithm for solving $\tau(n) = \pm \ell^m$.**
Can $|\tau(n)| = \ell^m$, a power of an odd prime?

**Theorem (B-C-O-T)**

If $|\tau(n)| = \ell^m$, then $n = p^{d-1}$, with $p$ and $d \mid \ell(\ell^2 - 1)$ are odd primes.

**Algorithm for solving $\tau(n) = \pm \ell^m$.**

1. List the finitely many odd primes $d \mid \ell(\ell^2 - 1)$. 
3. Our Results

CAN $|\tau(n)| = \ell^m$, A POWER OF AN ODD PRIME?

**Theorem (B-C-O-T)**

If $|\tau(n)| = \ell^m$, then $n = p^{d-1}$, with $p$ and $d \mid \ell(\ell^2 - 1)$ are odd primes.

**Algorithm for solving $\tau(n) = \pm \ell^m$.**

1. List the finitely many odd primes $d \mid \ell(\ell^2 - 1)$.
2. For each $d$, **simply** solve $\tau(p^{d-1}) = \pm \ell^m$ for primes $p$. 
A satisfying result

Theorem (B-C-O-T + UVA REU)

For $n > 1$ we have

$$\tau(n) \not\in \{\pm 1, \pm 691\} \cup \{\pm \ell : 3 \leq \ell < 100 \text{ prime}\}.$$
A SATISFYING RESULT

**Theorem (B-C-O-T + UVA REU)**

For $n > 1$ we have

$$\tau(n) \not\in \{\pm 1, \pm 691\} \cup \{\pm \ell : 3 \leq \ell < 100 \text{ prime}\}.$$  

**Remark (UVA REU)**

These results have been extended to $|\tau(n)| = \alpha$ odd.
3. Our Results

**General Results**

**Our Setting**

Let \( f \in S_{2k}(N) \) be a level \( N \) weight \( 2k \) newform with

\[
    f(z) = q + \sum_{n=2}^{\infty} a_f(n)q^n \cap \mathbb{Z}[[q]] \quad (q := e^{2\pi i z})
\]

and trivial mod 2 residual Galois representation.
Variants of Lehmer’s Conjecture
3. Our Results

**General Results**

**Our Setting**

Let \( f \in S_{2k}(N) \) be a level \( N \) weight \( 2k \) newform with

\[
f(z) = q + \sum_{n=2}^{\infty} a_f(n)q^n \cap \mathbb{Z}[[q]] \quad (q := e^{2\pi i z})
\]

and trivial mod 2 residual Galois representation.

**Remark (mod 2 condition?)**

- The condition “essentially” means that
  \( a_f(n) \) is odd \( \iff \) \( n \) is an odd square.
**GENERAL RESULTS**

**OUR SETTING**

Let \( f \in S_{2k}(N) \) be a level \( N \) weight \( 2k \) newform with

\[
  f(z) = q + \sum_{n=2}^{\infty} a_f(n) q^n \cap \mathbb{Z}[[q]]
\]

\( q := e^{2\pi i z} \)

and trivial mod 2 residual Galois representation.

**REMARK (mod 2 condition?)**

- The condition “essentially” means that \( a_f(n) \) is odd \(\iff\) \( n \) is an odd square.
- Elliptic curves \( E/\mathbb{Q} \) with a rational 2-torsion point.
GENERAL RESULTS

Our Setting

Let $f \in S_{2k}(N)$ be a level $N$ weight $2k$ newform with

$$f(z) = q + \sum_{n=2}^{\infty} a_f(n) q^n \cap \mathbb{Z}[[q]] \quad (q := e^{2\pi i z})$$

and trivial mod 2 residual Galois representation.

Remark (mod 2 condition?)

- The condition “essentially” means that $a_f(n)$ is odd $\iff$ $n$ is an odd square.
- Elliptic curves $E/\mathbb{Q}$ with a rational 2-torsion point.
- All forms of level $2^a M$ with $a \geq 0$ and $M \in \{1, 3, 5, 15, 17\}$.
**General Results** \((\ell \text{ an odd prime})\)

**Theorem (B-C-O-T)**

Suppose that \(2k \geq 4\) and \(a_f(2)\) is even. If \(|a_f(n)| = \ell^m\), then \(n = p^{d-1}\), with \(p\) and \(d | \ell(\ell^2 - 1)\) odd primes.
## General Results (\( \ell \) an odd prime)

**Theorem (B-C-O-T)**

Suppose that \( 2k \geq 4 \) and \( a_f(2) \) is even.
If \( |a_f(n)| = \ell^m \), then \( n = p^{d-1} \), with \( p \) and \( d | \ell(\ell^2 - 1) \) odd primes.

**Corollary (B-C-O-T)**

If \( \gcd(3 \cdot 5, 2k - 1) \neq 1 \) and \( 2k \geq 12 \), then
\[
a_f(n) \notin \{ \pm 1 \} \cup \{ \pm \ell : 3 \leq \ell < 37 \text{ prime} \} \cup \{-37\}.
\]
3. Our Results

**GENERAL RESULTS** (*ℓ* an odd prime)

**Theorem (B-C-O-T)**

Suppose that $2k \geq 4$ and $a_f(2)$ is even.

If $|a_f(n)| = \ell^m$, then $n = p^{d-1}$, with $p$ and $d | \ell(\ell^2 - 1)$ odd primes.

**Corollary (B-C-O-T)**

If $\gcd(3 \cdot 5, 2k - 1) \neq 1$ and $2k \geq 12$, then

$a_f(n) \not\in \{\pm 1\} \cup \{\pm \ell : 3 \leq \ell < 37 \text{ prime}\} \cup \{-37\}$.

**Assuming GRH, we have**

$a_f(n) \not\in \{\pm 1\} \cup \{\pm \ell : 3 \leq \ell \leq 97 \text{ prime with } \ell \neq 37\} \cup \{-37\}$. 
Remarks and an Example

Remarks

1. Analogous conclusions probably don’t hold for $2k = 2$. 

2. The method actually locates possible Fourier coefficients. For $2k = 4$, the only potential counterexamples are: 
   
   \[ a_f(3^2) = 37, \quad a_f(5^2) = 19, \quad a_f(7^2) = -19, \quad a_f(17^2) = -13, \quad a_f(43^2) = 17. \]

3. For $2k = 16$, we have $a_f(3^2) = 37$ is the only possible exception.

UVA REU will study odd weight, Nebentypus, and general $\alpha$. 

J. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai
Remarks and an Example

Remarks

1. Analogous conclusions probably don’t hold for $2k = 2$.

2. The method actually locates possible Fourier coefficients.
3. Our Results

Remarks and an Example

Remarks

1. Analogous conclusions probably don’t hold for $2k = 2$.

2. The method actually locates possible Fourier coefficients.
   
   For $2k = 4$ the only potential counterexamples are:

   \[
   \begin{align*}
   a_f(3^2) &= 37, \\
   a_f(3^4) &= 19, \\
   a_f(7^4) &= 11,
   \end{align*}
   \]

   \[
   \begin{align*}
   a_f(3^2) &= -11, \\
   a_f(5^2) &= 19, \\
   a_f(7^2) &= -19, \\
   a_f(17^2) &= -13, \\
   a_f(43^2) &= 17.
   \end{align*}
   \]
Remarks and an Example

Remarks

1. Analogous conclusions probably don’t hold for $2k = 2$.

2. The method actually locates possible Fourier coefficients. For $2k = 4$ the only potential counterexamples are:

$$a_f(3^2) = 37, \quad a_f(3^2) = -11, \quad a_f(3^2) = -23,$$
$$a_f(3^4) = 19, \quad a_f(5^2) = 19, a_f(7^2) = -19,$$
$$a_f(7^4) = 11, \quad a_f(17^2) = -13, \quad a_f(43^2) = 17.$$  

For $2k = 16$ we have $a_f(3^2) = 37$ is the only possible exception.
3. Our Results

Remarks and an Example

Remarks

1. Analogous conclusions probably don’t hold for $2k = 2$.

2. The method actually locates possible Fourier coefficients. For $2k = 4$ the only potential counterexamples are:

\[
\begin{align*}
af(3^2) &= 37, \quad af(3^2) = -11, \quad af(3^2) = -23, \\
af(3^4) &= 19, \quad af(5^2) = 19, \quad af(7^2) = -19, \\
af(7^4) &= 11, \quad af(17^2) = -13, \quad af(43^2) = 17.
\end{align*}
\]

For $2k = 16$ we have $af(3^2) = 37$ is the only possible exception.

3. UVA REU will study odd wt, Nebentypus, and general $\alpha$. 

J. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai
Example: The weight 16 Hecke eigenform

\[ E_4(z) \Delta(z) := \left(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \right) \cdot \Delta(z) \]

has no coefficients with absolute value \(3 \leq \ell \leq 37\) (GRH \(\Rightarrow \ell \leq 97\).)
Example: The weight 16 Hecke eigenform

The Hecke eigenform $E_4 \Delta$

$$E_4(z) \Delta(z) := \left( 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \right) \cdot \Delta(z)$$

has no coefficients with absolute value $3 \leq \ell \leq 37$ (GRH $\implies \ell \leq 97$.)
3. Our Results

\textbf{Can $\alpha$ be a coefficient for large weights?}

\textbf{Theorem (B-C-O-T)}

For prime powers $\ell^m$, if $f$ has weight $2^k > M \pm (\ell, m) = O_\ell(m)$, then $a_f(n) \neq \pm \ell^m$.

\textbf{Example}

We have $M \pm (3, m) = 2^m + \sqrt{m} \cdot 10^32$. 
3. Our Results

**CAN α BE A COEFFICIENT FOR LARGE WEIGHTS?**

**Theorem (B-C-O-T)**

For prime powers $\ell^m$, if $f$ has weight $2k > M^\pm(\ell, m) = O_\ell(m)$, then

$$a_f(n) \neq \pm \ell^m.$$
Can $\alpha$ be a coefficient for large weights?

**Theorem (B-C-O-T)**

For prime powers $\ell^m$, if $f$ has weight $2k > M^\pm(\ell, m) = O_\ell(m)$, then $a_f(n) \neq \pm \ell^m$.

**Example**

We have $M^\pm(3, m) = 2m + \sqrt{m} \cdot 10^{32}$. 
PRIMALITY OF $\tau(n)$

**Theorem (Lehmer (1965))**

There are prime values of $\tau(n)$. 

Namely, we have that $\tau(251^2) = 80561663527802406257321747$. 

Remark In 2013 Lygeros and Rozier found further prime values of $\tau(n)$. 

J. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai
Primality of $\tau(n)$

**Theorem (Lehmer (1965))**

There are prime values of $\tau(n)$. Namely, we have that

$$\tau(251^2) = 80561663527802406257321747.$$
**Primality of $\tau(n)$**

**Theorem (Lehmer (1965))**

There are prime values of $\tau(n)$. Namely, we have that

$$\tau(251^2) = 80561663527802406257321747.$$ 

**Remark**

In 2013 Lygeros and Rozier found further prime values of $\tau(n)$. 
3. Our Results

**Number of Prime Divisors of \( \tau(n) \)**

**Notation**

\[ \Omega(n) := \text{number of prime divisors of } n \text{ with multiplicity} \]
\[ \omega(n) := \text{number of distinct prime divisors of } n \]
**Number of Prime Divisors of $\tau(n)$**

**Notation**

- $\Omega(n) :=$ number of prime divisors of $n$ with multiplicity
- $\omega(n) :=$ number of distinct prime divisors of $n$

**Theorem (B-C-O-T)**

If $n > 1$ is an integer, then

$$\Omega(\tau(n)) \geq \sum_{p|n \text{ prime}} \left( \sigma_0(\text{ord}_p(n) + 1) - 1 \right) \geq \omega(n).$$
Remarks

Lehmer’s prime example shows that this bound is sharp as

$$\Omega(\tau(251^2)) = \sigma_0(2 + 1) - 1 = 1.$$
Variants of Lehmer’s Conjecture

3. Our Results

Remarks

1. Lehmer’s prime example shows that this bound is sharp as

\[ \Omega(\tau(251^2)) = \sigma_0(2 + 1) - 1 = 1. \]

Solving $|\tau(n)| = \ell$ an odd prime
SOLVING $|\tau(n)| = \ell$ AN ODD PRIME

(1) By Jacobi’s identity (or trivial mod 2 Galois rep’n), we have:

$$\sum_{n=1}^{\infty} \tau(n)q^n \equiv q \prod_{n=1}^{\infty} (1 - q^{8n})^3 = \sum_{k=0}^{\infty} q^{(2k+1)^2} \pmod{2}.$$
SOLVING $|\tau(n)| = \ell$ AN ODD PRIME

(1) By Jacobi’s identity (or trivial mod 2 Galois rep’n), we have:

$$\sum_{n=1}^{\infty} \tau(n)q^n \equiv q \prod_{n=1}^{\infty} (1 - q^{8n})^3 = \sum_{k=0}^{\infty} q^{(2k+1)^2} \pmod{2}.$$ 

$$\implies n = (2k + 1)^2$$
SOLVING $|\tau(n)| = \ell$ AN ODD PRIME

(1) By Jacobi’s identity (or trivial mod 2 Galois rep’n), we have:

$$\sum_{n=1}^{\infty} \tau(n)q^n \equiv q \prod_{n=1}^{\infty} (1 - q^{8n})^3 = \sum_{k=0}^{\infty} q^{(2k+1)^2} \pmod{2}.$$ 

$$\implies n = (2k+1)^2 \text{ and by Hecke multiplicativity } \implies n = p^{2t}.$$
SOLVING $|\tau(n)| = \ell$ AN ODD PRIME

(1) By Jacobi’s identity (or trivial mod 2 Galois rep’n), we have:

$$\sum_{n=1}^{\infty} \tau(n)q^n \equiv q \prod_{n=1}^{\infty} (1 - q^{8n})^3 = \sum_{k=0}^{\infty} q^{(2k+1)^2} \pmod{2}.$$

$$\implies n = (2k + 1)^2$$ and by Hecke multiplicativity $$\implies n = p^{2t}.$$

(2) Hecke-Mordell gives the recurrence in $m$:

$$\tau(p^{m+1}) = \tau(p)\tau(p^m) - p^{11} \tau(p^{m-2}).$$
SOLVING $|\tau(n)| = \ell$ AN ODD PRIME

(1) By Jacobi’s identity (or trivial mod 2 Galois rep’n), we have:

$$\sum_{n=1}^{\infty} \tau(n)q^n \equiv q \prod_{n=1}^{\infty} (1 - q^{8n})^3 = \sum_{k=0}^{\infty} q^{(2k+1)^2} \pmod{2}.$$ 

$$\implies n = (2k + 1)^2$$ and by Hecke multiplicativity $\implies n = p^{2t}$.

(2) Hecke-Mordell gives the recurrence in $m$:

$$\tau(p^{m+1}) = \tau(p)\tau(p^m) - p^{11}\tau(p^{m-2}).$$

$$\implies \{1 = \tau(p^0), \tau(p), \tau(p^2), \tau(p^3), \ldots \} \text{ is periodic modulo } \ell.$$
SOLVING $|\tau(n)| = \ell$ AN ODD PRIME

(1) By Jacobi's identity (or trivial mod 2 Galois rep'n), we have:

$$\sum_{n=1}^{\infty} \tau(n)q^n \equiv q \prod_{n=1}^{\infty} (1 - q^{8n})^3 = \sum_{k=0}^{\infty} q^{(2k+1)^2} \pmod{2}.$$  

$$\Rightarrow n = (2k+1)^2$$  

and by Hecke multiplicativity $\Rightarrow n = p^{2t}$.  

(2) Hecke-Mordell gives the recurrence in $m$:  

$$\tau(p^{m+1}) = \tau(p)\tau(p^m) - p^{11}\tau(p^{m-2}).$$  

$$\Rightarrow \{1 = \tau(p^0), \tau(p), \tau(p^2), \tau(p^3), \ldots \}$$  

is periodic modulo $\ell$.  

(3) The first time $\ell \mid \tau(p^{d-1})$ has $d \mid \ell(\ell^2 - 1)$.
Strategy continued...

(4) **Big Claim.** Every term in \( \{ \tau(p), \tau(p^2), \ldots \} \) is divisible by a prime that **does not divide** any previous term.
(4) **Big Claim. Every term** in \{\tau(p), \tau(p^2), \ldots \} is divisible by a prime that **does not divide** any previous term.

**Big Claim** \implies |\tau(p^{2t})| = \ell requires that \(2t = d - 1\).
Strategy continued...

(4) **Big Claim.** *Every term* in \( \{\tau(p), \tau(p^2), \ldots \} \) *is divisible by a prime that does not divide* any previous term.

**Big Claim** \( \implies |\tau(p^{2t})| = \ell \) requires that \( 2t = d - 1 \).

(5) EZ divisibility properties + **Big Claim** \( \implies d \) is prime.
(4) Big Claim. **Every term** in \{\tau(p), \tau(p^2), \ldots\} is divisible by a prime that **does not divide** any previous term.

**Big Claim** \implies |\tau(p^{2t})| = \ell requires that \(2t = d - 1\).

(5) EZ divisibility properties + **Big Claim** \implies d is prime.

(6) For the **finitely many** odd primes \(d | \ell(\ell^2 - 1)\), solve for \(p\)

\[\tau(p^{d-1}) = \pm \ell.\]
Strategy continued...

(4) **Big Claim.** Every term in \( \{ \tau(p), \tau(p^2), \ldots \} \) is divisible by a prime that **does not divide** any previous term.

**Big Claim** \( \implies |\tau(p^{2t})| = \ell \) requires that \( 2t = d - 1 \).

(5) EZ divisibility properties + **Big Claim** \( \implies d \) is prime.

(6) For the **finitely many** odd primes \( d | \ell(\ell^2 - 1) \), solve for \( p \)

\[
\tau(p^{d-1}) = \pm \ell.
\]

(7) Any soln gives an integer point on a genus \( g \geq 1 \) algebraic curve, which by Siegel has **finitely many** (if any) integer points.
**Definition**

A term \(a(n)\) in an integer sequence \(\{a(1), a(2), \ldots\}\) has a **primitive prime divisor** if there is a prime \(\ell\) for which TFAT:

1. \(\ell \mid a(n)\)
2. \(\ell \nmid a(1) a(2) \cdots a(n-1)\)

Otherwise, \(a(n)\) is said to be defective.

**Example (Carmichael 1913)**

The Fibonacci numbers in red are defective: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, ...

\(F_{12} = 144\) is the last defective one!
Definition

A term $a(n)$ in an integer sequence $\{a(1), a(2), \ldots \}$ has a \textbf{primitive prime divisor} if there is a prime $\ell$ for which TFAT:

1. We have $\ell \mid a(n)$.
2. We have $\ell \nmid a(1)a(2) \cdots a(n - 1)$.
PRIMITIVE PRIME DIVISORS

**Definition**

A term $a(n)$ in an integer sequence $\{a(1), a(2), \ldots\}$ has a **primitive prime divisor** if there is a prime $\ell$ for which TFAT:

1. We have $\ell \mid a(n)$.
2. We have $\ell \nmid a(1)a(2) \cdots a(n - 1)$.

Otherwise, $a(n)$ is said to be **defective**.
**Definition**

A term $a(n)$ in an integer sequence $\{a(1), a(2), \ldots \}$ has a **primitive prime divisor** if there is a prime $\ell$ for which TFAT:

1. We have $\ell \mid a(n)$.
2. We have $\ell \nmid a(1)a(2) \cdots a(n-1)$.

Otherwise, $a(n)$ is said to be **defective**.

**Example (Carmichael 1913)**

The Fibonacci numbers in red are defective:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots$$

$F_{12} = 144$ is the last defective one!
Lucas sequences

**Definition**
Suppose that $\alpha$ and $\beta$ are algebraic integers for which TFAT:

1. $\alpha + \beta$ and $\alpha \beta$ are relatively prime non-zero integers.
Lucas sequences

**Definition**

Suppose that $\alpha$ and $\beta$ are algebraic integers for which TFAT:

1. $\alpha + \beta$ and $\alpha \beta$ are relatively prime non-zero integers.
2. We have that $\alpha/\beta$ is not a root of unity.
Lucas Sequences

Definition

Suppose that $\alpha$ and $\beta$ are algebraic integers for which TFAT:

1. $\alpha + \beta$ and $\alpha \beta$ are relatively prime non-zero integers.
2. We have that $\alpha/\beta$ is not a root of unity.

Their Lucas numbers $\{u_n(\alpha, \beta)\} = \{u_1 = 1, u_2 = \alpha + \beta, \ldots \}$ are:

$$u_n(\alpha, \beta) := \frac{\alpha^n - \beta^n}{\alpha - \beta} \in \mathbb{Z}.$$
Primitve Prime Divisors

Theorem (Bilu, Hanrot, Voutier (2001))

Lucas numbers $u_n(\alpha, \beta)$, with $n > 30$, have primitive prime divisors.
5. Primitive Prime Divisors of Lucas Sequences

**Primitive Prime Divisors**

**Theorem (Bilu, Hanrot, Voutier (2001))**

Lucas numbers $u_n(\alpha, \beta)$, with $n > 30$, have primitive prime divisors.

**Theorem (B-H-V (2001), Abouzaid (2006))**

A classification of defective Lucas numbers is obtained:
Primitive Prime Divisors

**Theorem (Bilu, Hanrot, Voutier (2001))**

Lucas numbers $u_n(\alpha, \beta)$, with $n > 30$, have primitive prime divisors.

**Theorem (B-H-V (2001), Abouzaid (2006))**

A classification of defective Lucas numbers is obtained:

- Finitely many sporadic sequences
- Explicit parameterized infinite families.
A Lucas sequence $u_n(\alpha, \beta)$ is potentially weight $2k$ modular at a prime $p$ if TFAT:
Relevant Lucas Sequences

Definition

A Lucas sequence $u_n(\alpha, \beta)$ is potentially weight $2k$ modular at a prime $p$ if TFAT:

1. We have $B := \alpha \beta = p^{2k-1}$.

2. We have that $A := \alpha + \beta$ satisfies $|A| \leq 2p^{2k-1}$. 
5. Primitive Prime Divisors of Lucas Sequences

Relevant Lucas Sequences

Definition

A Lucas sequence $u_n(\alpha, \beta)$ is potentially weight $2k$ modular at a prime $p$ if TFAT:

1. We have $B := \alpha \beta = p^{2k-1}$.

2. We have that $A := \alpha + \beta$ satisfies $|A| \leq 2p^{\frac{2k-1}{2}}$.

Corollary (Brute Force)

The potentially modular defective Lucas numbers have been classified.
### Table 1. Sporadic examples of defective $u_n(\alpha, \beta)$ satisfying (2.2)

<table>
<thead>
<tr>
<th>$(A, B)$</th>
<th>Defective $u_n(\alpha, \beta)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(\pm 1, 2^1)$</td>
<td>$u_5 = -1, u_7 = 7, u_8 = \pm 3, u_{12} = \pm 45,$ $u_{13} = -1, u_{18} = \pm 85, u_{30} = \mp 24475$</td>
</tr>
<tr>
<td>$(\pm 1, 3^1)$</td>
<td>$u_5 = 1, u_{12} = \pm 160$</td>
</tr>
<tr>
<td>$(\pm 1, 5^1)$</td>
<td>$u_7 = 1, u_{12} = \mp 3024$</td>
</tr>
<tr>
<td>$(\pm 2, 3^1)$</td>
<td>$u_3 = 1, u_{10} = \mp 22$</td>
</tr>
<tr>
<td>$(\pm 2, 7^1)$</td>
<td>$u_8 = \mp 40$</td>
</tr>
<tr>
<td>$(\pm 2, 11^1)$</td>
<td>$u_5 = 5$</td>
</tr>
<tr>
<td>$(\pm 5, 7^1)$</td>
<td>$u_{10} = \mp 3725$</td>
</tr>
<tr>
<td>$(\pm 3, 2^3)$</td>
<td>$u_3 = 1$</td>
</tr>
<tr>
<td>$(\pm 5, 2^3)$</td>
<td>$u_6 = \pm 85$</td>
</tr>
</tbody>
</table>
Remark

Since $(A, B) = (A, p^{2k-1})$, there are only two with weight $2k \geq 4$. 

Table 1. Sporadic examples of defective $u_n(\alpha, \beta)$ satisfying (2.2)
Variants of Lehmer’s Conjecture

5. Primitive Prime Divisors of Lucas Sequences

\[ B_{1,k}^{r,\pm} : Y^2 = X^{2k-1} \pm 3^r, \quad B_{2,k} : Y^2 = 2X^{2k-1} - 1, \quad B_{3,k}^{\pm} : Y^2 = 2X^{2k-1} \pm 2, \]
\[ B_{4,k}^r : Y^2 = 3X^{2k-1} + (-2)^{r+2}, \quad B_{5,k}^{\pm} : Y^2 = 3X^{2k-1} \pm 3, \quad B_{6,k}^{r,\pm} : Y^2 = 3X^{2k-1} \pm 3 \cdot 2^r. \]

<table>
<thead>
<tr>
<th>((A, B))</th>
<th>(\text{Defective } u_n(\alpha, \beta))</th>
<th>(\text{Constraints on parameters})</th>
</tr>
</thead>
<tbody>
<tr>
<td>((\pm m, p))</td>
<td>(u_3 = -1)</td>
<td>(m &gt; 1 \text{ and } p = m^2 + 1)</td>
</tr>
<tr>
<td>((\pm m, p^{2k-1}))</td>
<td>(u_3 = \varepsilon 3^r)</td>
<td>((p, \pm m) \in B_{1,k}^{r,\varepsilon} \text{ with } 3 \nmid m, \varepsilon, r, m \neq (1, 1, 2), \text{ and } m^2 \geq 4\varepsilon 3^{r-1})</td>
</tr>
<tr>
<td>((\pm m, p^{2k-1}))</td>
<td>(u_4 = \mp m)</td>
<td>((p, \pm m) \in B_{2,k}^r \text{ with } m &gt; 1 \text{ odd})</td>
</tr>
<tr>
<td>((\pm m, p^{2k-1}))</td>
<td>(u_4 = \pm 2\varepsilon m)</td>
<td>((p, \pm m) \in B_{3,k}^\varepsilon \text{ with } (\varepsilon, m) \neq (1, 2) \text{ and } m &gt; 2 \text{ even})</td>
</tr>
<tr>
<td>((\pm m, p^{2k-1}))</td>
<td>(u_6 = \pm(-2)^r m(2m^2 + (-2)^r)/3)</td>
<td>((p, \pm m) \in B_{4,k}^r \text{ with } \gcd(m, 6) = 1, (r, m) \neq (1, 1), \text{ and } m^2 \geq (-2)^{r+2})</td>
</tr>
<tr>
<td>((\pm m, p^{2k-1}))</td>
<td>(u_6 = \pm\varepsilon m(2m^2 + 3\varepsilon))</td>
<td>((p, \pm m) \in B_{5,k}^\varepsilon \text{ with } 3 \mid m \text{ and } m &gt; 3)</td>
</tr>
<tr>
<td>((\pm m, p^{2k-1}))</td>
<td>(u_6 = \pm 2^{r+1}\varepsilon m(m^2 + 3\varepsilon \cdot 2^{r-1}))</td>
<td>((p, \pm m) \in B_{6,k}^{r,\varepsilon} \text{ with } m \equiv 3 \text{ mod } 6 \text{ and } m^2 \geq 3\varepsilon \cdot 2^{r+2})</td>
</tr>
</tbody>
</table>

**Table 2.** Parameterized families of defective \(u_n(\alpha, \beta)\) satisfying (2.2)

*Notation: \(m, k, r \in \mathbb{Z}^+, \varepsilon = \pm 1, p \text{ is a prime number.})*
Variants of Lehmer’s Conjecture
5. Primitive Prime Divisors of Lucas Sequences

**KEY LEMMAS**

**Lemma (Relative Divisibility)**

*If* \( d | n \), *then* \( u_d(\alpha, \beta) | u_n(\alpha, \beta) \).
Key Lemmas

**Lemma (Relative Divisibility)**

If \( d \mid n \), then \( u_d(\alpha, \beta) \mid u_n(\alpha, \beta) \).

**Lemma (First \( \ell \)-divisibility)**

We let \( m_\ell(\alpha, \beta) \) be the smallest \( n \geq 2 \) for which \( \ell \mid u_n(\alpha, \beta) \).
Key Lemmas

Lemma (Relative Divisibility)

If \( d \mid n \), then \( u_d(\alpha, \beta) \mid u_n(\alpha, \beta) \).

Lemma (First \( \ell \)-divisibility)

We let \( m_\ell(\alpha, \beta) \) be the smallest \( n \geq 2 \) for which \( \ell \mid u_n(\alpha, \beta) \).

If \( \ell \nmid \alpha \beta \) is an odd prime with \( m_\ell(\alpha, \beta) > 2 \), then \( m_\ell(\alpha, \beta) \mid \ell(\ell^2 - 1) \).
Variants of Lehmer’s Conjecture
6. Lucas sequences arising from newforms

**Properties of Newforms**

**Theorem (Atkin-Lehner, Deligne)**

If \( f(z) = q + \sum_{n=2}^{\infty} a_f(n) q^n \in S_{2k}(N) \cap \mathbb{Z}[[q]] \) is a newform, then TFAT.
Properties of Newforms

Theorem (Atkin-Lehner, Deligne)

If \( f(z) = q + \sum_{n=2}^{\infty} a_f(n)q^n \in S_{2k}(N) \cap \mathbb{Z}[[q]] \) is a newform, then TFAT.

1. If \( \gcd(n_1, n_2) = 1 \), then \( a_f(n_1 n_2) = a_f(n_1) a_f(n_2) \).
Properties of Newforms

**Theorem (Atkin-Lehner, Deligne)**

If \( f(z) = q + \sum_{n=2}^{\infty} a_f(n) q^n \in S_{2k}(N) \cap \mathbb{Z}[[q]] \) is a newform, then TFAT.

1. If \( \gcd(n_1, n_2) = 1 \), then \( a_f(n_1 n_2) = a_f(n_1) a_f(n_2) \).

2. If \( p \nmid N \) is prime and \( m \geq 2 \), then
   \[ a_f(p^m) = a_f(p) a_f(p^{m-1}) - p^{2k-1} a_f(p^{m-2}) \].
Properties of Newforms

Theorem (Atkin-Lehner, Deligne)

If $f(z) = q + \sum_{n=2}^{\infty} a_f(n)q^n \in S_{2k}(N) \cap \mathbb{Z}[[q]]$ is a newform, then TFAT.

1. If $\gcd(n_1, n_2) = 1$, then $a_f(n_1n_2) = a_f(n_1)a_f(n_2)$.

2. If $p \nmid N$ is prime and $m \geq 2$, then
   $$a_f(p^m) = a_f(p)a_f(p^{m-1}) - p^{2k-1}a_f(p^{m-2}).$$

3. If $p \nmid N$ is prime and $\alpha_p$ and $\beta_p$ are roots of $F_p(x) := x^2 - a_f(p)x + p^{2k-1}$, then
   $$a_f(p^m) = u_{m+1}(\alpha_p, \beta_p) = \frac{\alpha_p^{m+1} - \beta_p^{m+1}}{\alpha_p - \beta_p}.$$
Properties of Newforms

**Theorem (Atkin-Lehner, Deligne)**

If \( f(z) = q + \sum_{n=2}^{\infty} a_f(n)q^n \in S_{2k}(N) \cap \mathbb{Z}[[q]] \) is a newform, then TFAT.

1. If \( \gcd(n_1, n_2) = 1 \), then \( a_f(n_1 n_2) = a_f(n_1) a_f(n_2) \).

2. If \( p \nmid N \) is prime and \( m \geq 2 \), then
   \[
   a_f(p^m) = a_f(p) a_f(p^{m-1}) - p^{2k-1} a_f(p^{m-2}).
   \]

3. If \( p \nmid N \) is prime and \( \alpha_p \) and \( \beta_p \) are roots of \( F_p(x) := x^2 - a_f(p)x + p^{2k-1} \), then
   \[
   a_f(p^m) = u_{m+1}(\alpha_p, \beta_p) = \frac{\alpha_p^{m+1} - \beta_p^{m+1}}{\alpha_p - \beta_p}.
   \]

4. We have \( |a_f(p)| \leq 2p^{\frac{2k-1}{2}} \).
“Strategy for Lehmer Variants Revisited”
Variants of Lehmer’s Conjecture
6. Lucas sequences arising from newforms

“Strategy for Lehmer Variants Revisited”

(1) Suppose that $|a_f(n)| = \ell$.

(2) Hecke multiplicativity $\implies n = p^t$ a prime power.

(3) Trivial mod 2 Galois + Hecke $a_f(p^m)$ recursion $\implies n = p^{2m}$.
“Strategy for Lehmer Variants Revisited”

1. Suppose that $|a_f(n)| = \ell$.
2. Hecke multiplicativity $\implies n = p^t$ a prime power.
3. Trivial mod 2 Galois + Hecke $a_f(p^m)$ recursion $\implies n = p^{2m}$.
4. Note that $a_f(p^{2m}) = u_{2m+1}(\alpha_p, \beta_p)$.

5. Rule out defective Lucas numbers using the classification.
6. “Relative divisibility” and “First $\ell$-divisibility” of $u_n(\alpha_p, \beta_p) = \implies 2m + 1 = d$ odd prime with $d | \ell (\ell^2 - 1)$.
7. For each $d | \ell (\ell^2 - 1)$ classify integer points for the “curve” $a_f(p^d - 1) = \pm \ell$. 
“Strategy for Lehmer Variants Revisited”

(1) Suppose that $|a_f(n)| = \ell$.

(2) Hecke multiplicativity $\implies n = p^t$ a prime power.

(3) Trivial mod 2 Galois + Hecke $a_f(p^m)$ recursion $\implies n = p^{2m}$.

(4) Note that $a_f(p^{2m}) = u_{2m+1}(\alpha_p, \beta_p)$.

(5) Rule out defective Lucas numbers using the classification.

(6) “Relative divisibility” and “First $\ell$-divisibility” of $u_n(\alpha_p, \beta_p)$ $\implies 2m + 1 = d$ odd prime with $d \mid \ell(\ell^2 - 1)$.
"Strategy for Lehmer Variants Revisited"

(1) Suppose that $|a_f(n)| = \ell$.
(2) Hecke multiplicativity $\implies n = p^t$ a prime power.
(3) Trivial mod 2 Galois + Hecke $a_f(p^m)$ recursion $\implies n = p^{2m}$.
(4) Note that $a_f(p^{2m}) = u_{2m+1}(\alpha_p, \beta_p)$.
(5) Rule out defective Lucas numbers using the classification.
(6) “Relative divisibility” and “First $\ell$-divisibility” of $u_n(\alpha_p, \beta_p)$ $\implies 2m + 1 = d$ odd prime with $d | \ell(\ell^2 - 1)$.
(7) For each $d | \ell(\ell^2 - 1)$ classify integer points for the “curve” $a_f(p^{d-1}) = \pm \ell$. 

☐
FORMULAS FOR $a_f(p^2)$ AND $a_f(p^4)$

**Lemma**

*TFAT.*

1. If $a_f(p^2) = \alpha$, then $(p, a_f(p))$ is an integer point on

$$Y^2 = X^{2k-1} + \alpha.$$
FORMULAS FOR $a_f(p^2)$ AND $a_f(p^4)$

**Lemma**

*TFAT.*

1. If $a_f(p^2) = \alpha$, then $(p, a_f(p))$ is an integer point on

$$Y^2 = X^{2k-1} + \alpha.$$ 

2. If $a_f(p^4) = \alpha$, then $(p, 2a_f(p)^2 - 3p^{2k-1})$ is an integer point on

$$Y^2 = 5X^{2(2k-1)} + 4\alpha.$$
FORMULAS FOR $a_f(p^{2m})$ FOR $m \geq 3$

**Definition**

In terms of the generating function

$$\frac{1}{1 - \sqrt{YT} + XT^2} =: \sum_{m=0}^{\infty} F_m(X,Y) \cdot T^m = 1 + \sqrt{Y} \cdot T + \ldots$$
FORMULAS FOR $a_f(p^{2m})$ FOR $m \geq 3$

**Definition**

In terms of the generating function

$$\frac{1}{1 - \sqrt{YT} + XT^2} =: \sum_{m=0}^{\infty} F_m(X,Y) \cdot T^m = 1 + \sqrt{Y} \cdot T + \ldots$$

we have the special cyclotomic Thue polynomials

$$F_{2m}(X,Y) = \prod_{k=1}^{m} \left( Y - 4X \cos^2 \left( \frac{\pi k}{2m+1} \right) \right).$$
FORMULAS FOR $a_f(p^{2m})$ FOR $m \geq 3$

**Definition**

In terms of the generating function

$$\frac{1}{1 - \sqrt{YT} + XT^2} =: \sum_{m=0}^{\infty} F_m(X, Y) \cdot T^m = 1 + \sqrt{Y} \cdot T + \ldots$$

we have the special cyclotomic Thue polynomials

$$F_{2m}(X, Y) = \prod_{k=1}^{m} \left( Y - 4X \cos^2 \left( \frac{\pi k}{2m + 1} \right) \right).$$

**Lemma**

*If $f$ is a newform, then*

$$a_f(p^{2m}) = F_{2m}(p^{2k-1}, a_f(p)^2).$$
Explicit Example

**Theorem (B-C-O-T + UVA REU)**

For $n > 1$ we have

$$\tau(n) \not\in \{\pm 1, \pm 691\} \cup \{\pm \ell \mid 3 \leq \ell < 100 \text{ prime}\}.$$
Sketch of the Proof

1. For each prime $\ell$, list odd primes $d \mid \ell^2 - 1$.

2. We must rule out $\tau(p^d - 1) = \pm \ell$.

3. Otherwise, there is a special integer point on:

   Elliptic and hyperelliptic curves (for $a_f(p^2)$ & $a_f(p^4)$).

   Solution to a Thue equation ($F_{2m} = a_f(p^{2m})$ for $m \geq 3$).

4. Use Galois rep’ns + Mordell-Weil + Chabauty-Coleman + facts about Thue eqns to rule these out (a lot here).
Sketch of the Proof

Proof.

1. For each prime $\ell$ list odd primes $d \mid \ell(\ell^2 - 1)$. 
Sketch of the Proof

Proof.

1. For each prime \( \ell \) list odd primes \( d \mid \ell(\ell^2 - 1) \).

2. We must rule out \( \tau(p^{d-1}) = \pm \ell \).
Variants of Lehmer’s Conjecture

7. Integer Points on Special Curves

Sketch of the Proof

Proof.

1. For each prime $\ell$ list odd primes $d | \ell(\ell^2 - 1)$.
2. We must rule out $\tau(p^{d-1}) = \pm \ell$.
3. Otherwise, there is a special integer point on:
   - Elliptic and hyperelliptic curves (for $a_f(p^2)$ & $a_f(p^4)$)
   - Solution to a Thue equation ($F_{2m} = a_f(p^{2m})$ for $m \geq 3$).
Sketch of the Proof

Proof.

1. For each prime $\ell$ list odd primes $d \mid \ell(\ell^2 - 1)$.

2. We must rule out $\tau(p^{d-1}) = \pm \ell$.

3. Otherwise, there is a special integer point on:
   - Elliptic and hyperelliptic curves (for $a_f(p^2) \& a_f(p^4)$)
   - Solution to a Thue equation ($F_{2m} = a_f(p^{2m})$ for $m \geq 3$).

4. Use Galois rep’ns + Mordell-Weil + Chabauty-Coleman + facts about Thue eqns to rule these out (a lot here).
8. Summary

**Summary: Number of Prime Divisors**

**Theorem (B-C-O-T)**

*If* $n > 1$ *is an integer, then*

$$\Omega(\tau(n)) \geq \sum_{p|n} (\sigma_0(\text{ord}_p(n) + 1) - 1) \geq \omega(n).$$
Summary: Number of Prime Divisors

**Theorem (B-C-O-T)**

If $n > 1$ is an integer, then

$$\Omega(\tau(n)) \geq \sum_{p|n, \text{prime}} (\sigma_0(\text{ord}_p(n) + 1) - 1) \geq \omega(n).$$

**Remarks**

1. This lower bound is sharp.
Summary: Number of Prime Divisors

Theorem (B-C-O-T)

If \( n > 1 \) is an integer, then

\[
\Omega(\tau(n)) \geq \sum_{\substack{p|n \text{ prime}}} (\sigma_0(\text{ord}_p(n) + 1) - 1) \geq \omega(n).
\]

Remarks

1. This lower bound is sharp.
2. “Same” result when the mod 2 Galois rep’n is trivial.
8. Summary

**SUMMARY: TRIVIAL MOD 2 NEWFORMS**
### SUMMARY: TRIVIAL MOD 2 NEWFORMS

**Theorem (B-C-O-T)**

> If \(2k \geq 4\) and \(a_f(2)\) is even, then TFAT:

\[
\begin{align*}
1. & \quad |a_f(n)| = \ell^m, \text{ then } n = pd - 1, \text{ with odd primes } d | \ell(\ell^2 - 1) \text{ and } p. \\
2. & \quad \gcd(3 \cdot 5, 2k - 1) \neq 1 \text{ and } n > 1, \text{ then } a_f(n) \not\in \{\pm 1\} \cup \{\pm \ell^m : 3 \leq \ell < 37\} \cup \{-37\}.
\end{align*}
\]

Assuming GRH, we have

\[
\begin{align*}
a_f(n) \not\in \{\pm 1\} \cup \{\pm \ell^m : 3 \leq \ell \leq 97 \text{ prime with } \ell \neq 37\} \cup \{-37\}.
\end{align*}
\]

**Theorem (B-C-O-T)**

For prime powers \(\ell^m\), if \(f\) has weight \(2k > M\pm(\ell,m) = O(\ell^m)\), then

\[
a_f(n) \not= \pm \ell^m.
\]
Summary: Trivial mod 2 newforms

Theorem (B-C-O-T)

If $2k \geq 4$ and $a_f(2)$ is even, then TFAT:
1. If $|a_f(n)| = \ell^m$, then $n = p^{d-1}$, with odd primes $d | \ell(\ell^2 - 1)$ and $p$. 
SUMMARY: TRIVIAL MOD 2 NEWFORMS

THEOREM (B-C-O-T)

If $2k \geq 4$ and $a_f(2)$ is even, then TFAT:

1. If $|a_f(n)| = \ell^m$, then $n = p^{d-1}$, with odd primes $d | \ell(\ell^2 - 1)$ and $p$.

2. If $\gcd(3 \cdot 5, 2k - 1) \neq 1$ and $n > 1$, then

$$a_f(n) \notin \{\pm 1\} \cup \{\pm \ell : 3 \leq \ell < 37\} \cup \{-37\}.$$
Summary: Trivial mod 2 newforms

Theorem (B-C-O-T)

If $2k \geq 4$ and $a_f(2)$ is even, then TFAT:

1. If $|a_f(n)| = \ell^m$, then $n = p^{d-1}$, with odd primes $d | \ell(\ell^2 - 1)$ and $p$.

2. If $\gcd(3 \cdot 5, 2k - 1) \neq 1$ and $n > 1$, then
   
   $$a_f(n) \not\in \{\pm 1\} \cup \{\pm \ell : 3 \leq \ell < 37\} \cup \{-37\}.$$  

Assuming GRH, we have

$$a_f(n) \not\in \{\pm 1\} \cup \{\pm \ell : 3 \leq \ell \leq 97 \text{ prime with } \ell \neq 37\} \cup \{-37\}.$$
Summary: Trivial mod 2 newforms

Theorem (B-C-O-T)

If $2k \geq 4$ and $a_f(2)$ is even, then TFAT:

1. If $|a_f(n)| = \ell^m$, then $n = p^{d-1}$, with odd primes $d | \ell(\ell^2 - 1)$ and $p$.

2. If $\gcd(3 \cdot 5, 2k - 1) \neq 1$ and $n > 1$, then
   
   $a_f(n) \notin \{\pm 1\} \cup \{\pm \ell : 3 \leq \ell < 37\} \cup \{-37\}$.

Assuming GRH, we have

$a_f(n) \notin \{\pm 1\} \cup \{\pm \ell : 3 \leq \ell \leq 97$ prime with $\ell \neq 37\} \cup \{-37\}$.

Theorem (B-C-O-T)

For prime powers $\ell^m$, if $f$ has weight $2k > M^{\pm}(\ell, m) = O_\ell(m)$, then

$a_f(n) \neq \pm \ell^m$. 