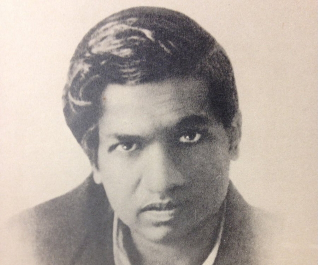
VARIANTS OF LEHMER'S CONJECTURE

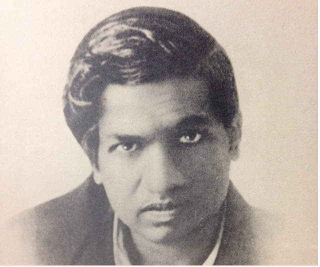
J. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai

"ON CERTAIN ARITHMETICAL FUNCTIONS" (1916)



Srinivasa Ramanujan

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

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** $\mathrm{SL}_2(\mathbb{Z})$.

For $\mathrm{Im}(z) > 0$ *and* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, *this means that*

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

THE PROTOTYPE

FACT

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

For $\mathrm{Im}(z) > 0$ *and* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, *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,...*

TESTING GROUND (HECKE OPERATORS)

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* $\gcd(n, m) = 1$, *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)*

TESTING GROUND (GALOIS REPRESENTATIONS)

THEOREM (RAMANUJAN (1916))

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

TESTING GROUND (GALOIS REPRESENTATIONS)

THEOREM (RAMANUJAN (1916))

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

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

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*
$$\rho_{\Delta,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell).$$

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*
$$\rho_{\Delta,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell).$$
- (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 $\Longrightarrow$ *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 $\Longrightarrow$ *Ramanujan's Conjecture.*

- (Ramanujan-Petersson)
  Generalized to newforms and generic automorphic forms.

LEHMER'S CONJECTURE

D. H. Lehmer

LEHMER'S CONJECTURE

D. H. Lehmer

CONJECTURE (LEHMER (1947))

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

RESULTS ON LEHMER'S CONJECTURE

THEOREM (LEHMER (1947))

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

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

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

RESULTS ON LEHMER'S CONJECTURE

THEOREM (LEHMER (1947))

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

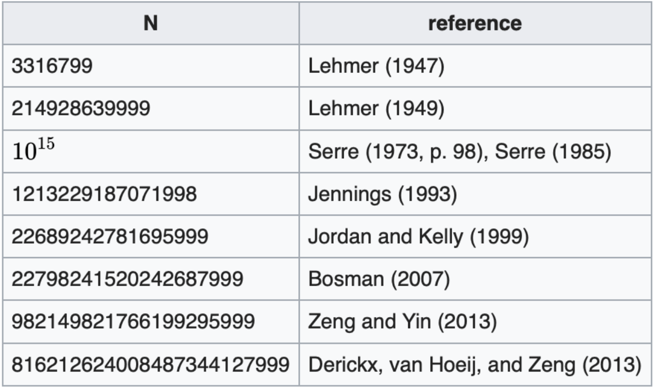
THEOREM (SERRE (81), THORNER-ZAMAN (2018))

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



N	reference
3316799	Lehmer (1947)
214928639999	Lehmer (1949)
10^{15}	Serre (1973, p. 98), Serre (1985)
1213229187071998	Jennings (1993)
22689242781695999	Jordan and Kelly (1999)
22798241520242687999	Bosman (2007)
982149821766199295999	Zeng and Yin (2013)
816212624008487344127999	Derickx, van Hoeij, and Zeng (2013)

Lehmer's Conjecture confirmed for $n \leq N$

VARIANT: VARYING NEWFORMS AND FIXING p

VARIANT: VARYING NEWFORMS AND FIXING p

THEOREM (CALEGARI, SARDARI (2020))

Fix a prime p and level N coprime to p.

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: CAN $\tau(n) = \alpha$?

VARIANT: CAN $\tau(n) = \alpha$?

THEOREM (MURTY, MURTY, SHOREY (1987))

For odd integers α, 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 α, 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 α, 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 $\tau(n) \neq \pm 1$.

VARIANT: CAN $\tau(n) = \alpha$?

THEOREM (MURTY, MURTY, SHOREY (1987))

For odd integers α, 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* $d \mid \ell(\ell^2 - 1)$ *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* $d \mid \ell(\ell^2-1)$ *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* $d \mid \ell(\ell^2-1)$.

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

$$\tau(n) \notin \{\pm 1, \pm 691\} \cup \{\pm \ell \;:\; 3 \leq \ell < 100 \text{ prime}\}.$$

A SATISFYING RESULT

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

For $n > 1$ we have

$$\tau(n) \notin \{\pm 1, \pm 691\} \cup \{\pm \ell \ : \ 3 \leq \ell < 100 \text{ prime}\}.$$

REMARK (UVA REU)

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

GENERAL RESULTS

OUR SETTING

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

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

and **trivial mod 2 residual Galois representation**.

GENERAL RESULTS

OUR SETTING

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

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

and **trivial mod 2 residual Galois representation**.

REMARK (MOD 2 CONDITION?)

- *The condition "essentially" means that*

$$a_f(n) \text{ is odd} \quad \Longleftrightarrow \quad n \text{ is an odd square.}$$

GENERAL RESULTS

OUR SETTING

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

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

and **trivial mod 2 residual Galois representation**.

REMARK (MOD 2 CONDITION?)

- *The condition "essentially" means that*
  $$a_f(n) \text{ is odd} \quad \Longleftrightarrow \quad n \text{ is an odd square.}$$
- *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*

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

and **trivial mod 2 residual Galois representation**.

Remark (mod 2 condition?)

- *The condition "essentially" means that*
  $$a_f(n) \text{ is odd } \iff n \text{ is an odd square.}$$
- *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 (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* $d \mid \ell(\ell^2 - 1)$ *odd primes.*

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* $d \mid \ell(\ell^2-1)$ *odd primes.*

COROLLARY (B-C-O-T)

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

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

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* $d \mid \ell(\ell^2 - 1)$ *odd primes.*

COROLLARY (B-C-O-T)

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

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

Assuming GRH, we have

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

REMARKS AND AN EXAMPLE

REMARKS

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

REMARKS AND AN EXAMPLE

REMARKS

1. *Analogous conclusions probably don't hold for* $2k = 2$.
2. *The method actually* **locates** *possible Fourier coefficients.*

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:*

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

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:*

$$\begin{aligned} &a_f(3^2) = 37, \quad a_f(3^2) = -11, \quad a_f(3^2) = -23, \\ &a_f(3^4) = 19, \quad a_f(5^2) = 19, a_f(7^2) = -19, \\ &a_f(7^4) = 11, \quad a_f(17^2) = -13, \quad a_f(43^2) = 17. \end{aligned}$$

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

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. UVA REU *will study odd wt, Nebentypus, and general* α.

EXAMPLE: THE WEIGHT 16 HECKE EIGENFORM

EXAMPLE: THE WEIGHT 16 HECKE EIGENFORM

EXAMPLE

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 $\Longrightarrow \ell \leq 97$.)

CAN α BE A COEFFICIENT FOR LARGE WEIGHTS?

CAN α BE A COEFFICIENT FOR LARGE WEIGHTS?

THEOREM (B-C-O-T)

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

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

CAN α BE A COEFFICIENT FOR LARGE WEIGHTS?

THEOREM (B-C-O-T)

For prime powers ℓ^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 $\tau(n)$.

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 $\tau(n)$.

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

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

$$\Omega(\tau(n)) \geq \sum_{\substack{p \mid n \\ prime}} (\sigma_0(\mathrm{ord}_p(n)+1)-1) \geq \omega(n).$$

REMARKS

REMARKS

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

$$\Omega(\tau(251^{2})) = \sigma_0(2+1) - 1 = 1.$$

REMARKS

REMARKS

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

$$\Omega(\tau(251^{2})) = \sigma_0(2+1) - 1 = 1.$$

2. *A generalization exists for newforms with integer coefficients and trivial residual mod 2 Galois representation.*

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:

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

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

SOLVING $|\tau(n)| = \ell$ AN ODD PRIME

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

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

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

SOLVING $|\tau(n)| = \ell$ AN ODD PRIME

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

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

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

(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:

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

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

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

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

$\Longrightarrow \quad \{1 = \tau(p^0), \tau(p), \tau(p^2), \tau(p^3), \dots\}$ is **periodic** modulo ℓ.

SOLVING $|\tau(n)| = \ell$ AN ODD PRIME

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

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

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

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

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

$$\implies \quad \{1 = \tau(p^0), \tau(p), \tau(p^2), \tau(p^3), \dots\} \text{ is } \textbf{periodic} \text{ modulo } \ell.$$

(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.

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.

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

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**.

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 $d \mid \ell(\ell^2 - 1)$, solve for p

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

STRATEGY CONTINUED...

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

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

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

(6) For the **finitely many** odd primes $d \mid \ell(\ell^2 - 1)$, 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.

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 ℓ for which TFAT:

PRIMITIVE PRIME DIVISORS

DEFINITION

A term $a(n)$ in an integer sequence $\{a(1), a(2), \dots\}$ has a **primitive prime divisor** if there is a prime ℓ 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 ℓ 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.**

PRIMITIVE PRIME DIVISORS

DEFINITION

A term $a(n)$ in an integer sequence $\{a(1), a(2), \dots\}$ has a **primitive prime divisor** if there is a prime ℓ 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:

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

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

LUCAS SEQUENCES

DEFINITION

Suppose that α and β are algebraic integers for which TFAT:

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

LUCAS SEQUENCES

DEFINITION

Suppose that α and β are algebraic integers for which TFAT:

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

LUCAS SEQUENCES

DEFINITION

Suppose that α and β are algebraic integers for which TFAT:

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

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

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

PRIMITIVE PRIME DIVISORS

THEOREM (BILU, HANROT, VOUTIER (2001))

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

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.**

RELEVANT LUCAS SEQUENCES

DEFINITION

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 $|A| \leq 2p^{\frac{2k-1}{2}}$.

RELEVANT LUCAS SEQUENCES

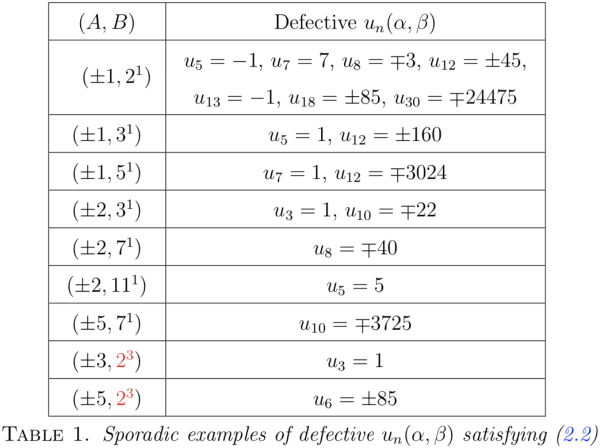
DEFINITION

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 $|A| \leq 2p^{\frac{2k-1}{2}}$.

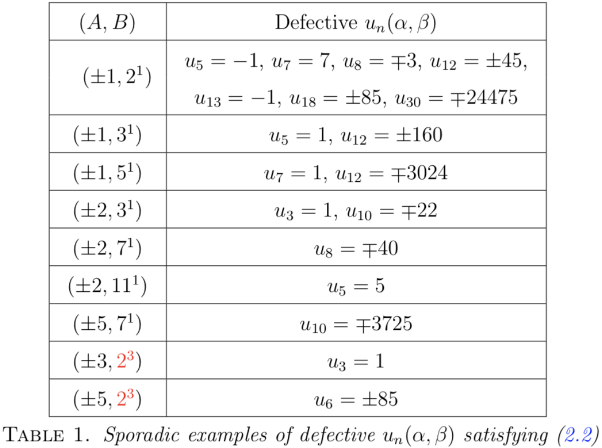
COROLLARY (BRUTE FORCE)

The potentially modular defective Lucas numbers have been classified.



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

TABLE 1. *Sporadic examples of defective $u_n(\alpha, \beta)$ satisfying (2.2)*



(A, B)	Defective $u_n(\alpha, \beta)$
$(\pm1, 2^1)$	$u_5 = -1$, $u_7 = 7$, $u_8 = \mp3$, $u_{12} = \pm45$, $u_{13} = -1$, $u_{18} = \pm85$, $u_{30} = \mp24475$
$(\pm1, 3^1)$	$u_5 = 1$, $u_{12} = \pm160$
$(\pm1, 5^1)$	$u_7 = 1$, $u_{12} = \mp3024$
$(\pm2, 3^1)$	$u_3 = 1$, $u_{10} = \mp22$
$(\pm2, 7^1)$	$u_8 = \mp40$
$(\pm2, 11^1)$	$u_5 = 5$
$(\pm5, 7^1)$	$u_{10} = \mp3725$
$(\pm3, 2^3)$	$u_3 = 1$
$(\pm5, 2^3)$	$u_6 = \pm85$

TABLE 1. *Sporadic examples of defective $u_n(\alpha, \beta)$ satisfying (2.2)*

REMARK

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

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

(A, B)	Defective $u_n(\alpha, \beta)$	Constraints on parameters
$(\pm m, p)$	$u_3 = -1$	$m > 1$ and $p = m^2 + 1$
$(\pm m, p^{2k-1})$	$u_3 = \varepsilon 3^r$	$(p, \pm m) \in B_{1,k}^{r,\varepsilon}$ with $3 \nmid m$, $(\varepsilon, r, m) \neq (1, 1, 2)$, and $m^2 \geq 4\varepsilon 3^{r-1}$
$(\pm m, p^{2k-1})$	$u_4 = \mp m$	$(p, \pm m) \in B_{2,k}$ with $m > 1$ odd
$(\pm m, p^{2k-1})$	$u_4 = \pm 2\varepsilon m$	$(p, \pm m) \in B_{3,k}^{\varepsilon}$ with $(\varepsilon, m) \neq (1, 2)$ and $m > 2$ even
$(\pm m, p^{2k-1})$	$u_6 = \pm(-2)^r m(2m^2 + (-2)^r)/3$	$(p, \pm m) \in B_{4,k}^{r}$ with $\gcd(m, 6) = 1$, $(r, m) \neq (1, 1)$, and $m^2 \geq (-2)^{r+2}$
$(\pm m, p^{2k-1})$	$u_6 = \pm \varepsilon m(2m^2 + 3\varepsilon)$	$(p, \pm m) \in B_{5,k}^{\varepsilon}$ with $3 \mid m$ and $m > 3$
$(\pm m, p^{2k-1})$	$u_6 = \pm 2^{r+1} \varepsilon m(m^2 + 3\varepsilon \cdot 2^{r-1})$	$(p, \pm m) \in B_{6,k}^{r,\varepsilon}$ with $m \equiv 3 \bmod 6$ and $m^2 \geq 3\varepsilon \cdot 2^{r+2}$

TABLE 2. Parameterized families of defective $u_n(\alpha, \beta)$ satisfying (2.2)
Notation: $m, k, r \in \mathbb{Z}^+$, $\varepsilon = \pm 1$, p *is a prime number.*

KEY LEMMAS

LEMMA (RELATIVE DIVISIBILITY)

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

KEY LEMMAS

LEMMA (RELATIVE DIVISIBILITY)

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

LEMMA (FIRST ℓ-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 ℓ-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* $m_\ell(\alpha, \beta) \mid \ell(\ell^2 - 1)$.

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* $a_f(n_1n_2) = a_f(n_1)a_f(n_2)$.

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* $a_f(n_1n_2) = a_f(n_1)a_f(n_2)$*.*
2. *If* $p \nmid N$ *is prime and* $m \geq 2$*, then*
$$a_f(p^m) = a_f(p)a_f(p^{m-1}) - p^{2k-1}a_f(p^{m-2}).$$

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* α_p *and* β_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* $a_f(n_1n_2) = a_f(n_1)a_f(n_2)$.
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* α_p *and* β_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"

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

"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 ℓ-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 ℓ-divisbility” of $u_n(\alpha_p, \beta_p)$
$\implies 2m + 1 = d$ odd prime with $d \mid \ell(\ell^2 - 1)$.

(7) For each $d \mid \ell(\ell^2 - 1)$ 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

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

FORMULAS FOR $a_f(p^{2m})$ FOR $m \geq 3$

DEFINITION

In terms of the generating function

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

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

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

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

$$\tau(n) \notin \{\pm 1, \pm 691\} \cup \{\pm \ell \ : \ 3 \leq \ell < 100 \text{ prime}\}.$$

Sketch of the Proof

SKETCH OF THE PROOF

PROOF.

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

SKETCH OF THE PROOF

PROOF.

1. For each prime ℓ list odd primes $d \mid \ell(\ell^2-1)$.
2. We must rule out $\tau(p^{d-1}) = \pm\ell$.

SKETCH OF THE PROOF

PROOF.

1. For each prime ℓ 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 $m \geq 3$).

SKETCH OF THE PROOF

PROOF.

1. For each prime ℓ 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**).

☐

SUMMARY: NUMBER OF PRIME DIVISORS

THEOREM (B-C-O-T)

If $n > 1$ is an integer, then

$$\Omega(\tau(n)) \geq \sum_{\substack{p \mid n \\ prime}} (\sigma_0(\mathrm{ord}_p(n)+1)-1) \geq \omega(n).$$

SUMMARY: NUMBER OF PRIME DIVISORS

THEOREM (B-C-O-T)

If $n > 1$ is an integer, then

$$\Omega(\tau(n)) \geq \sum_{\substack{p \mid n \\ prime}} (\sigma_0(\mathrm{ord}_p(n)+1)-1) \geq \omega(n).$$

REMARKS

1. *This lower bound is sharp.*

SUMMARY: NUMBER OF PRIME DIVISORS

THEOREM (B-C-O-T)

If $n > 1$ is an integer, then

$$\Omega(\tau(n)) \geq \sum_{\substack{p \mid n \\ \textit{prime}}} (\sigma_0(\operatorname{ord}_p(n) + 1) - 1) \geq \omega(n).$$

REMARKS

1. *This lower bound is sharp.*
2. *"Same" result when the mod 2 Galois rep'n is trivial.*

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:*

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* $d \mid \ell(\ell^2-1)$ *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* $d \mid \ell(\ell^2-1)$ *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* $d \mid \ell(\ell^2 - 1)$ *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

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

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* $d \mid \ell(\ell^2-1)$ *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

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

THEOREM (B-C-O-T)

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

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