

Modular forms and an explicit Chebotarev variant  
of the Brun-Titchmarsh theorem  
Comparative Prime Number Theory Symposium

Hari Iyer (joint work with Daniel Hu and Alexander Shashkov)

June 17, 2024

# 1. Modular forms

- **Modular forms.** Highly symmetric, holomorphic functions on the upper half plane which are ubiquitous in number theory.

# 1. Modular forms

- **Modular forms.** Highly symmetric, holomorphic functions on the upper half plane which are ubiquitous in number theory.
- The first example of a modular form was written down in 1916 by Ramanujan:

$$\begin{aligned}\Delta(q) &= q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n \\ &= q - 24q^2 + 252q^3 - 1472q^4 + \dots\end{aligned}$$

# 1. Modular forms

- **Modular forms.** Highly symmetric, holomorphic functions on the upper half plane which are ubiquitous in number theory.
- The first example of a modular form was written down in 1916 by Ramanujan:

$$\begin{aligned}\Delta(q) &= q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n \\ &= q - 24q^2 + 252q^3 - 1472q^4 + \dots\end{aligned}$$

- **Properties.** Weight 12, normalized, cuspidal newform for the full modular group  $SL_2(\mathbb{Z})$ . The Fourier coefficients  $\tau(n)$  are **Ramanujan's tau function**.

$n$	1	2	3	4	5	6	...
$\tau(n)$	1	-24	252	-1472	4830	-6048	...

- **Lehmer's conjecture.** Lehmer (1947) asked whether  $\tau(n) \neq 0$  for all  $n \geq 1$ .

- **Lehmer's conjecture.** Lehmer (1947) asked whether  $\tau(n) \neq 0$  for all  $n \geq 1$ .
- This is unsolved, but what can we say about the proportion of integers  $n \geq 1$  such that  $\tau(n) \neq 0$ ? Let

$$D_{\Delta} := \lim_{x \rightarrow \infty} \frac{\#\{n \leq x : \tau(n) \neq 0\}}{x}.$$

# Reduction to a prime-counting problem

- **Idea.** To bound  $D_\Delta$  below, express it in terms of a prime-counting function.

# Reduction to a prime-counting problem

- **Idea.** To bound  $D_\Delta$  below, express it in terms of a prime-counting function.
- Let

$$\pi_\Delta(x) := \#\{p \leq x \text{ prime} \mid \tau(p) = 0\}.$$



# Reduction to a prime-counting problem

- **Idea.** To bound  $D_\Delta$  below, express it in terms of a prime-counting function.
- Let

$$\pi_\Delta(x) := \#\{p \leq x \text{ prime} \mid \tau(p) = 0\}.$$

- Serre (1981) shows that

$$\begin{aligned} D_\Delta &= \prod_{\substack{p \text{ prime} \\ \tau(p)=0}} \left(1 - \frac{1}{p+1}\right) \\ &= \prod_{\substack{p \leq X_0 \\ \tau(p)=0}} \left(1 - \frac{1}{p+1}\right) \exp\left(-\int_{X_0}^{\infty} \frac{\pi_\Delta(x)}{x(x+1)} dx\right). \end{aligned}$$

# Reduction to a prime-counting problem

- **Idea.** To bound  $D_\Delta$  below, express it in terms of a prime-counting function.
- Let

$$\pi_\Delta(x) := \#\{p \leq x \text{ prime} \mid \tau(p) = 0\}.$$

- Serre (1981) shows that

$$\begin{aligned} D_\Delta &= \prod_{\substack{p \text{ prime} \\ \tau(p)=0}} \left(1 - \frac{1}{p+1}\right) \\ &= \prod_{\substack{p \leq X_0 \\ \tau(p)=0}} \left(1 - \frac{1}{p+1}\right) \exp\left(-\int_{X_0}^{\infty} \frac{\pi_\Delta(x)}{x(x+1)} dx\right). \end{aligned}$$

- In order to bound  $D_\Delta$  below, it suffices to:

# Reduction to a prime-counting problem

- **Idea.** To bound  $D_\Delta$  below, express it in terms of a prime-counting function.
- Let

$$\pi_\Delta(x) := \#\{p \leq x \text{ prime} \mid \tau(p) = 0\}.$$

- Serre (1981) shows that

$$\begin{aligned} D_\Delta &= \prod_{\substack{p \text{ prime} \\ \tau(p)=0}} \left(1 - \frac{1}{p+1}\right) \\ &= \prod_{\substack{p \leq X_0 \\ \tau(p)=0}} \left(1 - \frac{1}{p+1}\right) \exp\left(-\int_{X_0}^{\infty} \frac{\pi_\Delta(x)}{x(x+1)} dx\right). \end{aligned}$$

- In order to bound  $D_\Delta$  below, it suffices to:
  - Choose  $X_0$  sufficiently large.

# Reduction to a prime-counting problem

- **Idea.** To bound  $D_\Delta$  below, express it in terms of a prime-counting function.
- Let

$$\pi_\Delta(x) := \#\{p \leq x \text{ prime} \mid \tau(p) = 0\}.$$

- Serre (1981) shows that

$$\begin{aligned} D_\Delta &= \prod_{\substack{p \text{ prime} \\ \tau(p)=0}} \left(1 - \frac{1}{p+1}\right) \\ &= \prod_{\substack{p \leq X_0 \\ \tau(p)=0}} \left(1 - \frac{1}{p+1}\right) \exp\left(-\int_{X_0}^{\infty} \frac{\pi_\Delta(x)}{x(x+1)} dx\right). \end{aligned}$$

- In order to bound  $D_\Delta$  below, it suffices to:
  - Choose  $X_0$  sufficiently large.
  - Bound  $\pi_\Delta(x)$  above,  $x \geq X_0$ .

- **Very small** ( $2 \leq x \leq 10^{19}$ ).  $\tau(p) \neq 0$  for  $p \leq 10^{19}$  (Bosman).

- **Very small** ( $2 \leq x \leq 10^{19}$ ).  $\tau(p) \neq 0$  for  $p \leq 10^{19}$  (Bosman).
- **Small** ( $10^{19} < x \leq 10^{23}$ ). Computer search bounds the product for  $p \leq 10^{23}$  (Rouse–Thorner).

- **Very small** ( $2 \leq x \leq 10^{19}$ ).  $\tau(p) \neq 0$  for  $p \leq 10^{19}$  (Bosman).
- **Small** ( $10^{19} < x \leq 10^{23}$ ). Computer search bounds the product for  $p \leq 10^{23}$  (Rouse–Thorner).
- **Pretty large** ( $10^{23} < x \leq X_0$ ). Serre, Swinnerton-Dyer, Lehmer and others show that:

$\tau(p) = 0 \implies p$  lies in one of 33 residue classes mod 3488033912832000,

so the classical Brun–Titchmarsh theorem (Montgomery–Vaughan) bounds primes in progressions.

- **Very small** ( $2 \leq x \leq 10^{19}$ ).  $\tau(p) \neq 0$  for  $p \leq 10^{19}$  (Bosman).
- **Small** ( $10^{19} < x \leq 10^{23}$ ). Computer search bounds the product for  $p \leq 10^{23}$  (Rouse–Thorner).
- **Pretty large** ( $10^{23} < x \leq X_0$ ). Serre, Swinnerton-Dyer, Lehmer and others show that:

$\tau(p) = 0 \implies p$  lies in one of 33 residue classes mod 3488033912832000,

so the classical Brun–Titchmarsh theorem (Montgomery–Vaughan) bounds primes in progressions.

- **Very large** ( $x > X_0$ ). **We need an explicit upper bound for  $\pi_\Delta(x)$  in this range.**



- Produce an **explicit** bound on  $\pi_{\Delta}(x)$  for sufficiently large  $x \geq X_0$ , and with the cutoff  $X_0$  made small.

- Produce an **explicit** bound on  $\pi_{\Delta}(x)$  for sufficiently large  $x \geq X_0$ , and with the cutoff  $X_0$  made small.
- **Idea.** Relate  $\pi_{\Delta}(x)$  to algebraic number theory using connections between modular forms and Galois representations.

- Produce an **explicit** bound on  $\pi_{\Delta}(x)$  for sufficiently large  $x \geq X_0$ , and with the cutoff  $X_0$  made small.
- **Idea.** Relate  $\pi_{\Delta}(x)$  to algebraic number theory using connections between modular forms and Galois representations.
- We make explicit an effective Lang-Trotter bound proved in work of Thorner-Zaman (2018).

- Let  $\ell \neq p$  be a prime. By Deligne (1969), there exists a representation

$$\rho_{\Delta, \ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$$

such that  $\rho_{\Delta, \ell}(\text{Frob}_p)$  has characteristic polynomial

$$x^2 - \tau(p)x + p^{11} \in \mathbb{F}_\ell[x].$$

- Let  $\ell \neq p$  be a prime. By Deligne (1969), there exists a representation

$$\rho_{\Delta, \ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$$

such that  $\rho_{\Delta, \ell}(\text{Frob}_p)$  has characteristic polynomial

$$x^2 - \tau(p)x + p^{11} \in \mathbb{F}_\ell[x].$$

- When surjective,  $\rho_{\Delta, \ell}$  factors through some finite Galois extension  $L_\ell/\mathbb{Q}$ :

$$\rho_{\Delta, \ell} : \text{Gal}(L_\ell/\mathbb{Q}) \xrightarrow{\sim} \text{GL}_2(\mathbb{F}_\ell).$$

- Let  $\ell \neq p$  be a prime. By Deligne (1969), there exists a representation

$$\rho_{\Delta, \ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$$

such that  $\rho_{\Delta, \ell}(\text{Frob}_p)$  has characteristic polynomial

$$x^2 - \tau(p)x + p^{11} \in \mathbb{F}_\ell[x].$$

- When surjective,  $\rho_{\Delta, \ell}$  factors through some finite Galois extension  $L_\ell/\mathbb{Q}$ :

$$\rho_{\Delta, \ell} : \text{Gal}(L_\ell/\mathbb{Q}) \xrightarrow{\sim} \text{GL}_2(\mathbb{F}_\ell).$$

(By Serre and Swinnerton-Dyer (1972),  $\rho_{\Delta, \ell}$  is surjective for  $\ell > 691$ .)

# Reduction to a Chebotarev problem

- For  $\ell$  a prime, define

$$\pi_{\Delta}(x, \ell) := \# \left\{ p \leq x \mid \tau(p) \equiv 0 \pmod{\ell}, \left( \frac{\tau(p)^2 - 4p^{11}}{\ell} \right) = 1 \right\}.$$

# Reduction to a Chebotarev problem

- For  $\ell$  a prime, define

$$\pi_{\Delta}(x, \ell) := \# \left\{ p \leq x \mid \tau(p) \equiv 0 \pmod{\ell}, \left( \frac{\tau(p)^2 - 4p^{11}}{\ell} \right) = 1 \right\}.$$

- By a sieving argument of Wan (1990), we can choose primes  $\ell_1, \dots, \ell_t$  such that

$$\pi_{\Delta}(x) \leq \sum_{j=1}^t \pi_{\Delta}(x, \ell_j) + \text{small}$$

so it suffices to bound  $\pi_{\Delta}(x, \ell)$ .



# Reduction to a Chebotarev problem

- For  $\ell$  a prime, define

$$\pi_{\Delta}(x, \ell) := \# \left\{ p \leq x \mid \tau(p) \equiv 0 \pmod{\ell}, \left( \frac{\tau(p)^2 - 4p^{11}}{\ell} \right) = 1 \right\}.$$

- By a sieving argument of Wan (1990), we can choose primes  $\ell_1, \dots, \ell_t$  such that

$$\pi_{\Delta}(x) \leq \sum_{j=1}^t \pi_{\Delta}(x, \ell_j) + \text{small}$$

so it suffices to bound  $\pi_{\Delta}(x, \ell)$ .

- But  $\tau(p) \equiv 0 \pmod{\ell}, \tau(p)^2 - 4p^{11} \in (\mathbb{F}_{\ell}^{\times})^2$  is equivalent to  $\text{tr}(\rho_{\Delta, \ell}(\text{Frob}_p)) = 0, \text{tr}(\rho_{\Delta, \ell}(\text{Frob}_p))^2 - 4 \cdot \det(\rho_{\Delta, \ell}(\text{Frob}_p)) \in (\mathbb{F}_{\ell}^{\times})^2$ ,

# Reduction to a Chebotarev problem

- For  $\ell$  a prime, define

$$\pi_{\Delta}(x, \ell) := \# \left\{ p \leq x \mid \tau(p) \equiv 0 \pmod{\ell}, \left( \frac{\tau(p)^2 - 4p^{11}}{\ell} \right) = 1 \right\}.$$

- By a sieving argument of Wan (1990), we can choose primes  $\ell_1, \dots, \ell_t$  such that

$$\pi_{\Delta}(x) \leq \sum_{j=1}^t \pi_{\Delta}(x, \ell_j) + \text{small}$$

so it suffices to bound  $\pi_{\Delta}(x, \ell)$ .

- But  $\tau(p) \equiv 0 \pmod{\ell}, \tau(p)^2 - 4p^{11} \in (\mathbb{F}_{\ell}^{\times})^2$  is equivalent to  $\text{tr}(\rho_{\Delta, \ell}(\text{Frob}_p)) = 0, \text{tr}(\rho_{\Delta, \ell}(\text{Frob}_p))^2 - 4 \cdot \det(\rho_{\Delta, \ell}(\text{Frob}_p)) \in (\mathbb{F}_{\ell}^{\times})^2$ ,  
i.e.  $\text{Frob}_p \in C$ , so

$$\pi_{\Delta}(x, \ell) = \#\{p \leq x \mid \text{Frob}_p \in C\}$$

where  $C \subset \text{Gal}(L_{\ell}/\mathbb{Q})$  is the union of conjugacy classes of traceless matrices with distinct eigenvalues in  $\mathbb{F}_{\ell}$ . **This is a Chebotarev problem!**

# The Chebotarev density theorem

- Let  $L/K$  a Galois extension of number fields,  $C \subset \text{Gal}(L/K)$  a conjugacy class. Let

$$\pi_C(x, L/K) := \# \{ \mathfrak{p} \subset \mathcal{O}_K \text{ prime} \mid N\mathfrak{p} \leq x, \text{Frob}_{\mathfrak{p}} = C \}.$$

# The Chebotarev density theorem

- Let  $L/K$  a Galois extension of number fields,  $C \subset \text{Gal}(L/K)$  a conjugacy class. Let

$$\pi_C(x, L/K) := \# \{ \mathfrak{p} \subset \mathcal{O}_K \text{ prime} \mid N\mathfrak{p} \leq x, \text{Frob}_{\mathfrak{p}} = C \}.$$

- **Chebotarev density theorem.** We have

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|} \frac{x}{\log x} \text{ as } x \rightarrow \infty.$$

# The Chebotarev density theorem

- Let  $L/K$  a Galois extension of number fields,  $C \subset \text{Gal}(L/K)$  a conjugacy class. Let

$$\pi_C(x, L/K) := \# \{ \mathfrak{p} \subset \mathcal{O}_K \text{ prime} \mid N\mathfrak{p} \leq x, \text{Frob}_{\mathfrak{p}} = C \}.$$

- **Chebotarev density theorem.** We have

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|} \frac{x}{\log x} \text{ as } x \rightarrow \infty.$$

- **Our Chebotarev variant of the Brun-Titchmarsh theorem.** If  $x \gg_{L/K} X_1$ , then

$$\pi_C(x, L/K) \leq 2023 \frac{|C|}{|G|} \frac{x}{\log x}.$$

# The Chebotarev density theorem

- Let  $L/K$  a Galois extension of number fields,  $C \subset \text{Gal}(L/K)$  a conjugacy class. Let

$$\pi_C(x, L/K) := \# \{ \mathfrak{p} \subset \mathcal{O}_K \text{ prime} \mid N\mathfrak{p} \leq x, \text{Frob}_{\mathfrak{p}} = C \}.$$

- **Chebotarev density theorem.** We have

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|} \frac{x}{\log x} \text{ as } x \rightarrow \infty.$$

- **Our Chebotarev variant of the Brun-Titchmarsh theorem.** If  $x \gg_{L/K} X_1$ , then

$$\pi_C(x, L/K) \leq 2023 \frac{|C|}{|G|} \frac{x}{\log x}.$$

**A small range  $X_1$  is crucial for applications.**

- Work of Murty-Murty-Saradha (1988) allows comparison of  $\pi_C(x, L/K)$  with  $\pi_{C'}(x, L/F)$  for an intermediate extension  $F$  with abelian  $L/F$ .

- Work of Murty-Murty-Saradha (1988) allows comparison of  $\pi_C(x, L/K)$  with  $\pi_{C'}(x, L/F)$  for an intermediate extension  $F$  with abelian  $L/F$ .
- For our  $GL_2(\mathbb{F}_\ell)$  extension, work of Zywina (2015) allows comparison of  $\pi_C(x, L/\mathbb{Q})$  with  $\pi_{C'}(x, L^H/L^B)$  for  $B$  the Borel (upper triangular) and  $H$  the subspace of matrices with equal eigenvalues.  $B/H$  is abelian.



# Bounding $\pi_C(x, L/K)$

- Work of Murty-Murty-Saradha (1988) allows comparison of  $\pi_C(x, L/K)$  with  $\pi_{C'}(x, L/F)$  for an intermediate extension  $F$  with abelian  $L/F$ .
- For our  $GL_2(\mathbb{F}_\ell)$  extension, work of Zywina (2015) allows comparison of  $\pi_C(x, L/\mathbb{Q})$  with  $\pi_{C'}(x, L^H/L^B)$  for  $B$  the Borel (upper triangular) and  $H$  the subspace of matrices with equal eigenvalues.  $B/H$  is abelian.
- **Class field theory.** Assume  $L/K$  is abelian. Let  $\mathfrak{f} = \mathfrak{f}_{L/K}$  be the Artin conductor of  $L/K$  and  $I_{\mathfrak{f}}/P_{\mathfrak{f}}$  the ray class group mod  $\mathfrak{f}$ . By Artin reciprocity  $I_{\mathfrak{f}}/P_{\mathfrak{f}} \simeq \text{Gal}(L/K)$  sending  $\mathfrak{p}$  to  $\text{Frob}_{\mathfrak{p}}$ , so it suffices to bound

$$\pi_C(x, L/K) = \#\{\text{prime ideal } \mathfrak{p} \in \text{coset of ray class group} \mid N\mathfrak{p} \leq x\}.$$

- **Selberg sieve.** Compares a prime ideal counting problem to an integral ideal counting problem via inclusion-exclusion. It then suffices to fix an integral ideal  $\mathfrak{d}$  of  $K$  and bound

$$\#\{\text{integral ideal } \mathfrak{n} \in \text{coset}, N\mathfrak{n} \leq x, \mathfrak{d} \mid \mathfrak{n}\}.$$

- **Selberg sieve.** Compares a prime ideal counting problem to an integral ideal counting problem via inclusion-exclusion. It then suffices to fix an integral ideal  $\mathfrak{d}$  of  $K$  and bound

$$\#\{\text{integral ideal } \mathfrak{n} \in \text{coset}, N\mathfrak{n} \leq x, \mathfrak{d} \mid \mathfrak{n}\}.$$

- **Character orthogonality.** We can filter out ideals in a given coset:

$$\mathbb{1}_{\text{coset}} = \frac{1}{[L : K]} \sum_{\chi \in \widehat{\text{Gal}(L/K)}} \bar{\chi}(\text{coset}) \chi.$$

- **Selberg sieve.** Compares a prime ideal counting problem to an integral ideal counting problem via inclusion-exclusion. It then suffices to fix an integral ideal  $\mathfrak{d}$  of  $K$  and bound

$$\#\{\text{integral ideal } \mathfrak{n} \in \text{coset}, N\mathfrak{n} \leq x, \mathfrak{d} \mid \mathfrak{n}\}.$$

- **Character orthogonality.** We can filter out ideals in a given coset:

$$\mathbb{1}_{\text{coset}} = \frac{1}{[L : K]} \sum_{\chi \in \widehat{\text{Gal}(L/K)}} \bar{\chi}(\text{coset}) \chi.$$

Summing over ideals yields the count

$$\sum_{\substack{N\mathfrak{n} \leq x \\ \mathfrak{d} \mid \mathfrak{n}}} \mathbb{1}_{\text{coset}}(\mathfrak{n}) = \frac{1}{[L : K]} \sum_{\chi \in \widehat{\text{Gal}(L/K)}} \bar{\chi}(\text{coset}) \sum_{\substack{N\mathfrak{n} \leq x \\ \mathfrak{d} \mid \mathfrak{n}}} \chi(\mathfrak{n}).$$

- Multiply by a **smooth** test function (Thorner–Zaman), and apply **Mellin inversion** to the Hecke  $L$ -function  $L(s, \chi)$ .

$$\sum_{\substack{N\mathbf{n} \leq x \\ \mathfrak{d}|\mathbf{n}}} \chi(\mathbf{n}) = \int_{2-i\infty}^{2+i\infty} \frac{L(s, \chi) x^s}{N\mathfrak{d}^s} \frac{ds}{s}.$$

- Multiply by a **smooth** test function (Thorner–Zaman), and apply **Mellin inversion** to the Hecke  $L$ -function  $L(s, \chi)$ .

$$\sum_{\substack{N\mathfrak{n} \leq x \\ \mathfrak{d}|\mathfrak{n}}} \chi(\mathfrak{n}) = \int_{2-i\infty}^{2+i\infty} \frac{L(s, \chi) x^s}{N\mathfrak{d}^s} \frac{ds}{s}.$$

- **Shift the contour and bound Hecke  $L$ -functions** in the critical strip by the Phragmén–Lindelöf principle.

Choose  $X_0$ , apply Chebotarev bounds to the extensions  $L_{\ell_i}/\mathbb{Q}$  arising from the  $\ell_1, \dots, \ell_t$ -adic representations to obtain the following.

Choose  $X_0$ , apply Chebotarev bounds to the extensions  $L_{\ell_i}/\mathbb{Q}$  arising from the  $\ell_1, \dots, \ell_t$ -adic representations to obtain the following.

Theorem (Hu–I–Shashkov, 2023)

If  $x \geq e^{e^{16}}$ , then

$$\pi_{\Delta}(x) \leq (3.01 \times 10^{-10}) \frac{x(\log \log x)^2}{(\log x)^2}.$$



Choose  $X_0$ , apply Chebotarev bounds to the extensions  $L_{\ell_i}/\mathbb{Q}$  arising from the  $\ell_1, \dots, \ell_t$ -adic representations to obtain the following.

Theorem (Hu–I–Shashkov, 2023)

If  $x \geq e^{e^{16}}$ , then

$$\pi_{\Delta}(x) \leq (3.01 \times 10^{-10}) \frac{x(\log \log x)^2}{(\log x)^2}.$$

Feed into the integral for  $D_{\Delta}$  to obtain the following.

Theorem (Hu–I–Shashkov, 2023)

**We have  $\tau(n) \neq 0$  for 99.9999999985% of positive integers.**

# Our results

Choose  $X_0$ , apply Chebotarev bounds to the extensions  $L_{\ell_i}/\mathbb{Q}$  arising from the  $\ell_1, \dots, \ell_t$ -adic representations to obtain the following.

Theorem (Hu–I–Shashkov, 2023)

If  $x \geq e^{e^{16}}$ , then

$$\pi_{\Delta}(x) \leq (3.01 \times 10^{-10}) \frac{x(\log \log x)^2}{(\log x)^2}.$$

Feed into the integral for  $D_{\Delta}$  to obtain the following.

Theorem (Hu–I–Shashkov, 2023)

**We have  $\tau(n) \neq 0$  for 99.9999999985% of positive integers.**

This is the first known positive unconditional lower bound for  $D_{\Delta}$ .

# Acknowledgements

We are grateful for the valuable advice of Jesse Thorner and Ken Ono, and for the support of grants from the NSF, the NSA, and the Templeton World Charity Foundation. This research was conducted at the University of Virginia REU.