# Newform Eisenstein congruences of local origin

Jenny Roberts
(joint work with Dan Fretwell)

University of Bristol

24 May 2023

# Ramanujan's congruence

**Recall:** the discriminant function $\Delta \in S_{12}(SL_2(\mathbb{Z}))$ has $q$-expansion

$$\Delta(z) = q \prod_{n \geq 1} (1 - q^n)^{24}$$

# Ramanujan's congruence

**Recall:** the discriminant function $\Delta \in S_{12}(SL_2(\mathbb{Z}))$ has $q$-expansion

$$\Delta(z) = q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n$$
$$= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \cdots$$

# Ramanujan's congruence

**Recall:** the discriminant function $\Delta \in S_{12}(SL_2(\mathbb{Z}))$ has $q$-expansion

$$\begin{aligned}\Delta(z) &= q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n \\ &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \cdots\end{aligned}$$

and the Eisenstein series $E_{12} \in M_{12}(SL_2(\mathbb{Z}))$ has $q$-expansion

$$\begin{aligned}E_{12}(z) &= -\frac{B_{12}}{24} + \sum_{n \geq 1} \sigma_{11}(n) q^n \in M_{12}(SL_2(\mathbb{Z})) \\ &= \frac{691}{65520} + q + 2049q^2 + 177148q^3 + 4196353q^4 \\ &\quad + 48828126q^5 + 362976252q^6 + \cdots\end{aligned}$$

# Ramanujan's congruence

If we were to compare the Fourier coefficients of these two series...

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\tau(n)$ | 1 | $-24$ | 252 | $-1472$ | 4830 | $-6048$ |
| $\sigma_{11}(n)$ | 1 | 2049 | 177148 | 4196353 | 48828126 | 362976252 |

# Ramanujan's congruence

If we were to compare the Fourier coefficients of these two series...

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\tau(n) \mod 691$ | 1 | 667 | 252 | 601 | 684 | 171 |
| $\sigma_{11}(n) \mod 691$ | 1 | 667 | 252 | 601 | 684 | 171 |

# Ramanujan's congruence

If we were to compare the Fourier coefficients of these two series...

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\tau(n)$ mod 691 | 1 | 667 | 252 | 601 | 684 | 171 |
| $\sigma_{11}(n)$ mod 691 | 1 | 667 | 252 | 601 | 684 | 171 |

## Ramanujan's congruence

$\tau(n) \equiv \sigma_{11}(n)$ mod 691

# Ramanujan's congruence

Why does this congruence hold?

# Ramanujan's congruence

Why does this congruence hold?

## Proof (Sketch)

We have

$$E_{12}(z) = -\frac{B_{12}}{24} + \sum_{n\geq 1} \sigma_{11}(n)q^n \in M_{12}(SL_2(\mathbb{Z}))$$

and

$$\Delta(z) = \sum_{n\geq 1} \tau(n)q^n \in S_{12}(SL_2(\mathbb{Z})).$$

- Since $\mathrm{ord}_{691}(B_{12}) > 0$ we see that $E_{12}$ reduces to an eigenform $\overline{E}_{12} \in S_{12}(SL_2(\mathbb{Z}), \overline{\mathbb{F}}_{691})$.

# Ramanujan's congruence

Why does this congruence hold?

## Proof (Sketch)

We have

$$E_{12}(z) = -\frac{B_{12}}{24} + \sum_{n\geq 1} \sigma_{11}(n)q^n \in M_{12}(SL_2(\mathbb{Z}))$$

and

$$\Delta(z) = \sum_{n\geq 1} \tau(n)q^n \in S_{12}(SL_2(\mathbb{Z})).$$

- Since $\mathrm{ord}_{691}(B_{12}) > 0$ we see that $E_{12}$ reduces to an eigenform $\overline{E}_{12} \in S_{12}(SL_2(\mathbb{Z}), \overline{\mathbb{F}}_{691})$.
- This space is spanned by the reductions of eigenforms in $S_{12}(SL_2(\mathbb{Z}), \mathbb{Z}_{691})$, which is 1-dimensional spanned by $\Delta$.

# Ramanujan's congruence

Why does this congruence hold?

## Proof (Sketch)

We have

$$E_{12}(z) = -\frac{B_{12}}{24} + \sum_{n\geq 1} \sigma_{11}(n)q^n \in M_{12}(SL_2(\mathbb{Z}))$$

and

$$\Delta(z) = \sum_{n\geq 1} \tau(n)q^n \in S_{12}(SL_2(\mathbb{Z})).$$

- Since $\mathrm{ord}_{691}(B_{12}) > 0$ we see that $E_{12}$ reduces to an eigenform $\overline{E}_{12} \in S_{12}(SL_2(\mathbb{Z}), \overline{\mathbb{F}}_{691})$.
- This space is spanned by the reductions of eigenforms in $S_{12}(SL_2(\mathbb{Z}), \mathbb{Z}_{691})$, which is 1-dimensional spanned by $\Delta$.
- Then $\overline{E}_{12} = \overline{\Delta}$, implying the congruence.

# Why do we care?

It turns out, this congruence has deep consequences...

# Why do we care?

It turns out, this congruence has deep consequences...

There exists a non trivial $[\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Q}(\zeta_{691}))[691]$ satisfying:

$$\sigma \cdot [\mathfrak{a}] = \chi_{691}(\sigma)^{-11}[\mathfrak{a}] \text{ for all } \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}),$$

where $\chi_{691} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_{691}^*$ is the mod 691 cyclotomic character.

# Why do we care?

It turns out, this congruence has deep consequences...

There exists a non trivial $[\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Q}(\zeta_{691}))[691]$ satisfying:

$$\sigma \cdot [\mathfrak{a}] = \chi_{691}(\sigma)^{-11}[\mathfrak{a}] \text{ for all } \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}),$$

where $\chi_{691} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_{691}^*$ is the mod 691 cyclotomic character.

More generally, Eisenstein congruences were used to prove:

## Herbrand-Ribet Theorem

For $2 \leq k \leq p-3$ even:

$$\mathrm{ord}_p(B_k) > 0 \iff \exists \text{ element in the } \chi_p^{1-k} \text{ eigenspace of } \mathrm{Cl}(\mathbb{Q}(\zeta_p))[p].$$

# Next steps

**Q1:** Can we find other congruences like this, but for higher levels and non-trivial character?

# Next steps

**Q1:** Can we find other congruences like this, but for higher levels and non-trivial character?

- Higher levels: Dummigan-Fretwell (2014), Billerey-Menares (2016)
- Non-trivial character: Minimal level - Dummigan (2007), lift by prime level - Spencer (2018)

# Next steps

**Q1:** Can we find other congruences like this, but for higher levels and non-trivial character?

- Higher levels: Dummigan-Fretwell (2014), Billerey-Menares (2016)
- Non-trivial character: Minimal level - Dummigan (2007), lift by prime level - Spencer (2018)

**Q2:** What can we say about how "new" the modular forms that satisfy the congruence are?

# Next steps

**Q1:** Can we find other congruences like this, but for higher levels and non-trivial character?

- Higher levels: Dummigan-Fretwell (2014), Billerey-Menares (2016)
- Non-trivial character: Minimal level - Dummigan (2007), lift by prime level - Spencer (2018)

**Q2:** What can we say about how "new" the modular forms that satisfy the congruence are?

- Trivial character: Dummigan-Fretwell (2014), Billerey-Menares (2016)

# Next steps

**Q1:** Can we find other congruences like this, but for higher levels and non-trivial character?

- Higher levels: Dummigan-Fretwell (2014), Billerey-Menares (2016)
- Non-trivial character: Minimal level - Dummigan (2007), lift by prime level - Spencer (2018)

**Q2:** What can we say about how "new" the modular forms that satisfy the congruence are?

- Trivial character: Dummigan-Fretwell (2014), Billerey-Menares (2016)

**Q3:** How do we find them, e.g. modulo what primes?

- Generalise Ribet's converse to Herbrand's theorem

# Next steps

**Q1:** Can we find other congruences like this, but for higher levels and non-trivial character?

- Higher levels: Dummigan-Fretwell (2014), Billerey-Menares (2016)
- Non-trivial character: Minimal level - Dummigan (2007), lift by prime level - Spencer (2018)

**Q2:** What can we say about how "new" the modular forms that satisfy the congruence are?

- Trivial character: Dummigan-Fretwell (2014), Billerey-Menares (2016)

**Q3:** How do we find them, e.g. modulo what primes?

- Generalise Ribet's converse to Herbrand's theorem

**Goal:** Generalise to newform congruences with non-trivial character and lift by squarefree level.

# Definitions - Congruence subgroups

Define the congruence subgroups of $SL_2(\mathbb{Z})$:

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

# Definitions - Modular forms of level N

Let $M_k(\Gamma_0(N), \chi)$ be the space of modular forms of weight $k \geq 2$, level $N$ and Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ with modulus $N$.

# Definitions - Modular forms of level N

Let $M_k(\Gamma_0(N),\chi)$ be the space of modular forms of weight $k \geq 2$, level $N$ and Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ with modulus $N$.

## Definition (Modular form)

$f \in M_k(\Gamma_0(N),\chi)$ if:

- $f$ is holomorphic on the complex upper half plane
- $f$ satisfies:

$$f[\gamma]_k := (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) = \chi(d) f(z)$$

  for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

- $f[\alpha]_k$ must be holomorphic at $\infty$ for all $\alpha \in SL_2(\mathbb{Z})$, i.e. at all cusps.

# Definitions - Generalised Eisenstein series

We can decompose $M_k(\Gamma_0(N),\chi)$ as

$$M_k(\Gamma_0(N),\chi) = S_k(\Gamma_0(N),\chi) \oplus E_k(\Gamma_0(N),\chi)$$

If $k > 2$, the Eisenstein subspace $E_k(\Gamma_0(N),\chi)$ is spanned by the normalised Eisenstein series $E_k^{\psi,\phi}(tz)$ for all ordered pairs of Dirichlet characters $\phi,\psi$ of conductors $u,v$ satisfying $\psi\phi = \chi$ and $tuv \mid N$. $E_k^{\psi,\phi}$ has Fourier expansion:

$$E_k^{\psi,\phi}(z) = \frac{1}{2}\delta(\psi)L(1-k,\psi^{-1}\phi) + \sum_{n=1}^{\infty} \sigma_{k-1}^{\psi,\phi}(n)q^n,$$

$\delta(\psi) = 1$ if $\psi$ is the trivial mod 1 character, 0 otherwise and

$$\sigma_{k-1}^{\psi,\phi}(n) = \sum_{d|n, d>0} \psi(n/d)\phi(d)d^{k-1}$$

is the generalised power divisor series.

# Definitions - Newforms

The cuspidal subspace has an orthogonal decomposition with respect to the Petersson inner product:

$$S_k(\Gamma_0(N),\chi) = S_k^{\text{old}}(\Gamma_0(N),\chi) \oplus S_k^{\text{new}}(\Gamma_0(N),\chi)$$

with $S_k^{\text{old}}(\Gamma_0(N),\chi)$ as usual being spanned by lifts of modular forms in $S_k(\Gamma_0(N/d),\chi)$ with $d \cdot \text{cond}(\chi) \mid N$.

- A modular form is **new** at level $N$ if it lies in the new subspace.

# Definitions - Newforms

The cuspidal subspace has an orthogonal decomposition with respect to the Petersson inner product:

$$S_k(\Gamma_0(N), \chi) = S_k^{\mathsf{old}}(\Gamma_0(N), \chi) \oplus S_k^{\mathsf{new}}(\Gamma_0(N), \chi)$$

with $S_k^{\mathsf{old}}(\Gamma_0(N), \chi)$ as usual being spanned by lifts of modular forms in $S_k(\Gamma_0(N/d), \chi)$ with $d \cdot \mathsf{cond}(\chi) \mid N$.

- A modular form is **new** at level $N$ if it lies in the new subspace.

# Definitions - Newforms

The cuspidal subspace has an orthogonal decomposition with respect to the Petersson inner product:

$$S_k(\Gamma_0(N),\chi) = S_k^{\text{old}}(\Gamma_0(N),\chi) \oplus S_k^{\text{new}}(\Gamma_0(N),\chi)$$

with $S_k^{\text{old}}(\Gamma_0(N),\chi)$ as usual being spanned by lifts of modular forms in $S_k(\Gamma_0(N/d),\chi)$ with $d \cdot \text{cond}(\chi) \mid N$.

- A modular form is **new** at level $N$ if it lies in the new subspace.
- An **eigenform** is an eigenvector for all the Hecke operators, $T_p$, with $p \nmid N$.

# Definitions - Newforms

The cuspidal subspace has an orthogonal decomposition with respect to the Petersson inner product:

$$S_k(\Gamma_0(N),\chi) = S_k^{\text{old}}(\Gamma_0(N),\chi) \oplus S_k^{\text{new}}(\Gamma_0(N),\chi)$$

with $S_k^{\text{old}}(\Gamma_0(N),\chi)$ as usual being spanned by lifts of modular forms in $S_k(\Gamma_0(N/d),\chi)$ with $d \cdot \text{cond}(\chi) \mid N$.

- A modular form is **new** at level $N$ if it lies in the new subspace.
- An **eigenform** is an eigenvector for all the Hecke operators, $T_p$, with $p \nmid N$.
- $f = \sum_{n \geq 0} a_n(f) q^n \in M_k(\Gamma_0(N),\chi)$ is **normalised** if $a_1(f) = 1$.

# Definitions - Newforms

The cuspidal subspace has an orthogonal decomposition with respect to the Petersson inner product:

$$S_k(\Gamma_0(N), \chi) = S_k^{\text{old}}(\Gamma_0(N), \chi) \oplus S_k^{\text{new}}(\Gamma_0(N), \chi)$$

with $S_k^{\text{old}}(\Gamma_0(N), \chi)$ as usual being spanned by lifts of modular forms in $S_k(\Gamma_0(N/d), \chi)$ with $d \cdot \text{cond}(\chi) \mid N$.

- A modular form is **new** at level $N$ if it lies in the new subspace.
- An **eigenform** is an eigenvector for all the Hecke operators, $T_p$, with $p \nmid N$.
- $f = \sum_{n \geq 0} a_n(f) q^n \in M_k(\Gamma_0(N), \chi)$ is **normalised** if $a_1(f) = 1$.
- We say $f \in M_k(\Gamma_0(N), \chi)$ is a **newform** if $f$ is a normalised eigenform which is new at level N.

# A general conjecture

Assume we have

- $N, M$ - coprime, squarefree integers, $k > 2$ - integer.
- $E_k^{\psi,\phi}$ - new at level $N$ (cond($\psi$)·cond($\phi$) $= N$) with $\psi\phi = \chi$, $\tilde{\chi}$ is a lift of $\chi$ to modulus $NM$.
- $l > k + 1$, $l \nmid NM$ - prime of $\mathbb{Z}[\psi, \phi]$.
- $\lambda$ - prime above $l$ in the ring of integers of the extension of $\mathbb{Q}(\psi, \phi)$ generated by the Fourier coefficients of $f$.

# A general conjecture

Assume we have

- $N, M$ - coprime, squarefree integers, $k > 2$ - integer.
- $E_k^{\psi,\phi}$ - new at level $N$ (cond($\psi$)·cond($\phi$) $= N$) with $\psi\phi = \chi$, $\tilde{\chi}$ is a lift of $\chi$ to modulus $NM$.
- $l > k+1$, $l \nmid NM$ - prime of $\mathbb{Z}[\psi, \phi]$.
- $\lambda$ - prime above $l$ in the ring of integers of the extension of $\mathbb{Q}(\psi, \phi)$ generated by the Fourier coefficients of $f$.

## Conjecture (Fretwell, R.)

There exists a newform $f \in S_k(\Gamma_1(NM), \tilde{\chi})$ such that

$$a_q(f) \equiv a_q(E_k^{\psi,\phi}) \pmod{\lambda}$$

for all primes $q \nmid NMl$, if and only if both of the following hold:

1. $\mathrm{ord}_l(L(1-k, \psi^{-1}\phi)\prod_{p\in\mathcal{P}_M}(\psi(p) - \phi(p)p^k)) > 0$.
2. $l \mid (\psi(p) - \phi(p)p^k)(\psi(p) - \phi(p)p^{k-2}) \ \forall \ p \in \mathcal{P}_M$.

# A general conjecture

Assume we have

- $N, M$ - coprime, squarefree integers, $k > 2$ - integer.
- $E_k^{\psi,\phi}$ - new at level $N$ (cond($\psi$)·cond($\phi$) $= N$) with $\psi\phi = \chi$, $\tilde{\chi}$ is a lift of $\chi$ to modulus $NM$.
- $l > k+1$, $l \nmid NM$ - prime of $\mathbb{Z}[\psi, \phi]$.
- $\lambda$ - prime above $l$ in the ring of integers of the extension of $\mathbb{Q}(\psi, \phi)$ generated by the Fourier coefficients of $f$.

## Conjecture (Fretwell, R.)

There exists a newform $f \in S_k(\Gamma_1(NM), \tilde{\chi})$ such that

$$a_q(f) \equiv a_q(E_k^{\psi,\phi}) \pmod{\lambda}$$

for all primes $q \nmid NMl$, if and only if both of the following hold:

1. $\mathrm{ord}_l(L(1-k, \psi^{-1}\phi) \prod_{p \in \mathcal{P}_M} (\psi(p) - \phi(p)p^k)) > 0$.
2. $l \mid (\psi(p) - \phi(p)p^k)(\psi(p) - \phi(p)p^{k-2}) \ \forall \ p \in \mathcal{P}_M$.

1. Tells us that we will get a congruence modulo prime $l$ with some eigenform $f$
2. Gives us information about how "new" $f$ is

# A general conjecture (simplified)

How does the generalisation compare to Ramanujan's result?

# A general conjecture (simplified)

How does the generalisation compare to Ramanujan's result?

- We had a congruence between a cuspform $\Delta$ and Eisenstein series $E_{12}$.

# A general conjecture (simplified)

How does the generalisation compare to Ramanujan's result?

- We had a congruence between a cuspform $\Delta$ and Eisenstein series $E_{12}$.
- We can find a congruence between a cuspform $f = \sum_{n \geq 1} a_n q^n$ (new at level $NM$) and an Eisenstein series $E_k^{\psi,\phi}$, (new at level $N$).

# A general conjecture (simplified)

How does the generalisation compare to Ramanujan's result?

- We had a congruence between a cuspform $\Delta$ and Eisenstein series $E_{12}$.
- We can find a congruence between a cuspform $f = \sum_{n \geq 1} a_n q^n$ (new at level $NM$) and an Eisenstein series $E_k^{\psi,\phi}$, (new at level $N$).
- The congruence held modulo 691, this worked because 691 divided $B_{12}$ (the constant coefficient of $E_{12}$).

# A general conjecture (simplified)

How does the generalisation compare to Ramanujan's result?

- We had a congruence between a cuspform $\Delta$ and Eisenstein series $E_{12}$.
- We can find a congruence between a cuspform $f = \sum_{n\geq 1} a_n q^n$ (new at level $NM$) and an Eisenstein series $E_k^{\psi,\phi}$, (new at level $N$).
- The congruence held modulo 691, this worked because 691 divided $B_{12}$ (the constant coefficient of $E_{12}$).
- The congruence holds modulo prime $l$, where $l$ divides either the constant term of the Eisenstein series or an Euler product (with Euler factors at primes dividing $M$).
- To ensure $f$ is new, $l$ also has to divide another quantity at each prime dividing $M$.

# Direct implication

Assume $a_q(f) \equiv \psi(q) + \phi(q)q^{k-1} \pmod{\lambda}$ for some newform $f \in S_k(\Gamma_1(NM), \tilde{\chi})$, $\lambda$ a prime above $l$.

There is an $l$-adic Galois representation attached to $f$:

$$\rho_{f,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Z}_l})$$

with mod $l$ reduction given by:

$$\overline{\rho}_{f,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_l}).$$

By the congruence condition, we then have:

$$\mathrm{Tr}(\overline{\rho}_{f,l}) = \overline{\psi} + \overline{\phi}\chi_l^{k-1},$$

i.e. $\overline{\rho}_{f,l}$ has composition factors $\{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\}$, where $\chi_l$ is the mod $l$ cyclotomic character.

# Direct implication

Assume $a_q(f) \equiv \psi(q) + \phi(q)q^{k-1} \pmod{\lambda}$ for some newform $f \in S_k(\Gamma_1(NM), \tilde{\chi})$, $\lambda$ a prime above $l$.

There is an $l$-adic Galois representation attached to $f$:

$$\rho_{f,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Z}_l})$$

with mod $l$ reduction given by:

$$\overline{\rho}_{f,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_l}).$$

By the congruence condition, we then have:

$$\mathrm{Tr}(\overline{\rho}_{f,l}) = \overline{\psi} + \overline{\phi}\chi_l^{k-1},$$

i.e. $\overline{\rho}_{f,l}$ has composition factors $\{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\}$, where $\chi_l$ is the mod $l$ cyclotomic character.

# Direct implication

Assume $a_q(f) \equiv \psi(q) + \phi(q)q^{k-1} \pmod{\lambda}$ for some newform $f \in S_k(\Gamma_1(NM), \tilde{\chi})$, $\lambda$ a prime above $l$.

There is an $l$-adic Galois representation attached to $f$:

$$\rho_{f,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Z}_l})$$

with mod $l$ reduction given by:

$$\overline{\rho}_{f,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_l}).$$

By the congruence condition, we then have:

$$\mathrm{Tr}(\overline{\rho}_{f,l}) = \overline{\psi} + \overline{\phi}\chi_l^{k-1},$$

i.e. $\overline{\rho}_{f,l}$ has composition factors $\{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\}$, where $\chi_l$ is the mod $l$ cyclotomic character.

# Direct implication

Assume $a_q(f) \equiv \psi(q) + \phi(q)q^{k-1} \pmod{\lambda}$ for some newform $f \in S_k(\Gamma_1(NM), \tilde{\chi})$, $\lambda$ a prime above $l$.

There is an $l$-adic Galois representation attached to $f$:

$$\rho_{f,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Z}_l})$$

with mod $l$ reduction given by:

$$\overline{\rho}_{f,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_l}).$$

By the congruence condition, we then have:

$$\mathrm{Tr}(\overline{\rho}_{f,l}) = \overline{\psi} + \overline{\phi}\chi_l^{k-1},$$

i.e. $\overline{\rho}_{f,l}$ has composition factors $\{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\}$, where $\chi_l$ is the mod $l$ cyclotomic character.

Let $p$ be a prime dividing $M$. Then the composition factors of $\overline{\rho}_{f,l}$ "locally at $p$" are:

$$\{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\}$$

where $\mu$ is the unramified character mapping the Frobenius at $p$ to $a_p(f)/p^{k/2-1}$ (mod $\lambda$).

Equating the two sets of composition factors locally at $p$:

$$\{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\} = \{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\},$$

which leaves us with two cases:

(A) $\overline{\psi} = \mu\chi_l^{k/2}$, $\overline{\phi}\chi_l^{k-1} = \mu\chi_l^{k/2-1}$.

(B) $\overline{\psi} = \mu\chi_l^{k/2-1}$, $\overline{\phi}\chi_l^{k-1} = \mu\chi_l^{k/2}$.

Let $p$ be a prime dividing $M$. Then the composition factors of $\overline{\rho}_{f,l}$ "locally at $p$" are:

$$\{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\}$$

where $\mu$ is the unramified character mapping the Frobenius at $p$ to $a_p(f)/p^{k/2-1}$ (mod $\lambda$).

Equating the two sets of composition factors locally at $p$:

$$\{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\} = \{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\},$$

which leaves us with two cases:

(A) $\overline{\psi} = \mu\chi_l^{k/2}$, $\overline{\phi}\chi_l^{k-1} = \mu\chi_l^{k/2-1}$.

(B) $\overline{\psi} = \mu\chi_l^{k/2-1}$, $\overline{\phi}\chi_l^{k-1} = \mu\chi_l^{k/2}$.

Let $p$ be a prime dividing $M$. Then the composition factors of $\overline{\rho}_{f,l}$ "locally at $p$" are:

$$\{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\}$$

where $\mu$ is the unramified character mapping the Frobenius at $p$ to $a_p(f)/p^{k/2-1}$ (mod $\lambda$).

Equating the two sets of composition factors locally at $p$:

$$\{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\} = \{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\},$$

which leaves us with two cases:

(A) $\overline{\psi} = \mu\chi_l^{k/2}$, $\overline{\phi}\chi_l^{k-1} = \mu\chi_l^{k/2-1}$.

(B) $\overline{\psi} = \mu\chi_l^{k/2-1}$, $\overline{\phi}\chi_l^{k-1} = \mu\chi_l^{k/2}$.

Let $p$ be a prime dividing $M$. Then the composition factors of $\overline{\rho}_{f,l}$ "locally at $p$" are:

$$\{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\}$$

where $\mu$ is the unramified character mapping the Frobenius at $p$ to $a_p(f)/p^{k/2-1}$ (mod $\lambda$).

Equating the two sets of composition factors locally at $p$:

$$\{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\} = \{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\},$$

which leaves us with two cases:

(A) $\overline{\psi} = \mu\chi_l^{k/2}$, $\overline{\phi}\chi_l^{k-1} = \mu\chi_l^{k/2-1}$.

(B) $\overline{\psi} = \mu\chi_l^{k/2-1}$, $\overline{\phi}\chi_l^{k-1} = \mu\chi_l^{k/2}$.

# Direct implication

Evaluating at $p \mid M$ in both cases:

(A) $$\left.\begin{aligned} \psi(p) &\equiv \mu(p)p^{k/2} \pmod{l} \\ \phi(p)p^{k-1} &\equiv \mu(p)p^{k/2-1} \pmod{l} \end{aligned}\right\} \implies \psi(p) - \phi(p)p^k \equiv 0 \pmod{l}.$$

(B) $$\left.\begin{aligned} \psi(p) &\equiv \mu(p)p^{k/2-1} \pmod{l} \\ \phi(p)p^{k-1} &\equiv \mu(p)p^{k/2} \pmod{l} \end{aligned}\right\} \implies \psi(p) - \phi(p)p^{k-2} \equiv 0 \pmod{l}.$$

Also, since $\mu(p) \equiv a_p(f)/p^{k/2-1} \pmod{\lambda}$, we have $a_p(f) \equiv \psi(p) \pmod{\lambda}$ in this case.

To summarise, we have that for all $p$ dividing $M$, we require one of the following:

(A) $\psi(p) - \phi(p)p^k \equiv 0 \pmod{l}$.

(B) $\psi(p) - \phi(p)p^{k-2} \equiv 0 \pmod{l}$ and $a_p(f) \equiv \psi(p) \pmod{\lambda}$.

**Condition 2**

$l \mid (\psi(p) - \phi(p)p^k)(\psi(p) - \phi(p)p^{k-2}) \ \forall\, p \in \mathcal{P}_M$.

This proves the necessity of Condition (2) in the statement of the theorem.

# Direct implication

Evaluating at $p \mid M$ in both cases:

(A) $$\left.\begin{aligned} \psi(p) &\equiv \mu(p)p^{k/2} \pmod{l} \\ \phi(p)p^{k-1} &\equiv \mu(p)p^{k/2-1} \pmod{l} \end{aligned}\right\} \implies \psi(p) - \phi(p)p^{k} \equiv 0 \pmod{l}.$$

(B) $$\left.\begin{aligned} \psi(p) &\equiv \mu(p)p^{k/2-1} \pmod{l} \\ \phi(p)p^{k-1} &\equiv \mu(p)p^{k/2} \pmod{l} \end{aligned}\right\} \implies \psi(p) - \phi(p)p^{k-2} \equiv 0 \pmod{l}.$$

Also, since $\mu(p) \equiv a_p(f)/p^{k/2-1} \pmod{\lambda}$, we have $a_p(f) \equiv \psi(p) \pmod{\lambda}$ in this case.

To summarise, we have that for all $p$ dividing $M$, we require one of the following:

(A) $\psi(p) - \phi(p)p^{k} \equiv 0 \pmod{l}$.

(B) $\psi(p) - \phi(p)p^{k-2} \equiv 0 \pmod{l}$ and $a_p(f) \equiv \psi(p) \pmod{\lambda}$.

**Condition 2**

$l \mid (\psi(p) - \phi(p)p^{k})(\psi(p) - \phi(p)p^{k-2}) \; \forall \, p \in \mathcal{P}_M$.

This proves the necessity of Condition (2) in the statement of the theorem.

# Direct implication

Evaluating at $p \mid M$ in both cases:

(A) $$\left.\begin{aligned} \psi(p) &\equiv \mu(p)p^{k/2} \pmod{l} \\ \phi(p)p^{k-1} &\equiv \mu(p)p^{k/2-1} \pmod{l} \end{aligned}\right\} \implies \psi(p) - \phi(p)p^k \equiv 0 \pmod{l}.$$

(B) $$\left.\begin{aligned} \psi(p) &\equiv \mu(p)p^{k/2-1} \pmod{l} \\ \phi(p)p^{k-1} &\equiv \mu(p)p^{k/2} \pmod{l} \end{aligned}\right\} \implies \psi(p) - \phi(p)p^{k-2} \equiv 0 \pmod{l}.$$

Also, since $\mu(p) \equiv a_p(f)/p^{k/2-1} \pmod{\lambda}$, we have $a_p(f) \equiv \psi(p) \pmod{\lambda}$ in this case.

To summarise, we have that for all $p$ dividing $M$, we require one of the following:

(A) $\psi(p) - \phi(p)p^k \equiv 0 \pmod{l}$.

(B) $\psi(p) - \phi(p)p^{k-2} \equiv 0 \pmod{l}$ and $a_p(f) \equiv \psi(p) \pmod{\lambda}$.

**Condition 2**

$l \mid (\psi(p) - \phi(p)p^k)(\psi(p) - \phi(p)p^{k-2}) \; \forall \; p \in \mathcal{P}_M$.

This proves the necessity of Condition (2) in the statement of the theorem.

# Direct implication

We can do something similar for primes $p$ dividing $N$, which in this case gives us an equivalence of characters:

$$\{\mu_1\chi_l^{(k-1)/2}, \mu_2\chi_l^{(k-1)/2}\} = \{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\}.$$

We also have $a_p(f) \equiv p^{(k-1)/2}(\mu_1(p) + \mu_2(p)) \pmod{\lambda}$, hence $a_p(f) \equiv \psi(p) + \phi(p)p^{k-1} \pmod{\lambda}$.

Note that if any prime $p \mid M$ satisfies case (A), then Condition (1) follows immediately and we are done. So, assume that for all $p \mid M$, we are in case (B):

$\psi(p) - \phi(p)p^{k-2} \equiv 0 \pmod{l}$,

$a_p(f) \equiv \psi(p) \pmod{\lambda}$.

Need to show:

**Condition 1**

$\mathrm{ord}_l(L(1-k, \psi^{-1}\phi) \prod_{p \in \mathcal{P}_M} (\psi(p) - \phi(p)p^k)) > 0.$

# Direct implication

We can do something similar for primes $p$ dividing $N$, which in this case gives us an equivalence of characters:

$$\{\mu_1\chi_l^{(k-1)/2}, \mu_2\chi_l^{(k-1)/2}\} = \{\overline{\psi}, \overline{\phi}\chi_l^{k-1}\}.$$

We also have $a_p(f) \equiv p^{(k-1)/2}(\mu_1(p) + \mu_2(p)) \pmod{\lambda}$, hence $a_p(f) \equiv \psi(p) + \phi(p)p^{k-1} \pmod{\lambda}$.

Note that if any prime $p \mid M$ satisfies case (A), then Condition (1) follows immediately and we are done. So, assume that for all $p \mid M$, we are in case (B):

$$\psi(p) - \phi(p)p^{k-2} \equiv 0 \pmod{l},$$
$$a_p(f) \equiv \psi(p) \pmod{\lambda}.$$

Need to show:

## Condition 1

$\mathrm{ord}_l(L(1-k, \psi^{-1}\phi)\prod_{p\in\mathcal{P}_M}(\psi(p) - \phi(p)p^k)) > 0.$

# Direct implication

Let

$$E = \left[ \prod_{p \in \mathcal{P}_M} (T_p - \phi(p)p^{k-1}) \right] \alpha_M E_k^{\psi,\phi},$$

where $\alpha_M f(z) := f(Mz)$ and $T_p$ is the $p^{\text{th}}$ Hecke operator.

**Fact 1**

$E$ is a normalised eigenform with Fourier coefficient at prime $p$ given by:

$$a_p(E) = \begin{cases} \psi(p) & \text{if } p \mid M \\ \psi(p) + \phi(p)p^{k-1} & \text{otherwise} \end{cases}$$

With a bit more work, this gives

$$a_n(E) \equiv a_n(f) \pmod{\lambda} \ \forall\ n$$

In particular, since $f$ is a cusp form, this tells us that $E$ must vanish at all cusps.

# Direct implication

Let

$$E = \left[ \prod_{p \in \mathcal{P}_M} (T_p - \phi(p)p^{k-1}) \right] \alpha_M E_k^{\psi,\phi},$$

where $\alpha_M f(z) := f(Mz)$ and $T_p$ is the $p^{\text{th}}$ Hecke operator.

## Fact 1

$E$ is a normalised eigenform with Fourier coefficient at prime $p$ given by:

$$a_p(E) = \begin{cases} \psi(p) & \text{if } p \mid M \\ \psi(p) + \phi(p)p^{k-1} & \text{otherwise} \end{cases}$$

With a bit more work, this gives

$$a_n(E) \equiv a_n(f) \pmod{\lambda} \ \forall\ n$$

In particular, since $f$ is a cusp form, this tells us that $E$ must vanish at all cusps.

# Direct implication

Let

$$E = \left[ \prod_{p \in \mathcal{P}_M} (T_p - \phi(p)p^{k-1}) \right] \alpha_M E_k^{\psi,\phi},$$

where $\alpha_M f(z) := f(Mz)$ and $T_p$ is the $p^{\text{th}}$ Hecke operator.

## Fact 1

$E$ is a normalised eigenform with Fourier coefficient at prime $p$ given by:

$$a_p(E) = \begin{cases} \psi(p) & \text{if } p \mid M \\ \psi(p) + \phi(p)p^{k-1} & \text{otherwise} \end{cases}$$

With a bit more work, this gives

$$a_n(E) \equiv a_n(f) \pmod{\lambda} \ \forall\ n$$

In particular, since $f$ is a cusp form, this tells us that $E$ must vanish at all cusps.

# Direct implication

## Fact 2

We can choose a $\gamma = \left(\begin{smallmatrix} a & \beta \\ b & \delta \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ such that $E[\gamma]_k$ has constant term:

$$-\frac{g(\psi\phi^{-1})}{g(\phi)} \frac{\phi^{-1}(a)\psi\left(\frac{-b}{v}\right)\psi^{-1}(M)}{u^k} L(1-k, \psi^{-1}\phi) \left( \prod_{p \in \mathcal{P}_M} (\psi(p) - \phi(p)p^{k-1}) \right)$$

However, $\frac{g(\psi\phi^{-1})}{g(\phi)}$, $\phi^{-1}(a)$, $\psi\left(\frac{-b}{v}\right)$ and $\psi^{-1}(M)$ are units in $\mathbb{Z}[\psi, \phi]$. Furthermore, $l \nmid u$ since $u \mid N$ and by assumption $l \nmid N$. Hence, $l$ must divide

$$L(1-k, \psi^{-1}\phi) \left( \prod_{p \in \mathcal{P}_M} (\psi(p) - \phi(p)p^{k-1}) \right).$$

Condition (1) follows easily from this, so we are done.

# Direct implication

## Fact 2

We can choose a $\gamma = \left(\begin{smallmatrix} a & \beta \\ b & \delta \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ such that $E[\gamma]_k$ has constant term:

$$-\frac{g(\psi\phi^{-1})}{g(\phi)} \frac{\phi^{-1}(a)\psi\left(\frac{-b}{v}\right)\psi^{-1}(M)}{u^k} L(1-k, \psi^{-1}\phi) \left( \prod_{p \in \mathcal{P}_M} (\psi(p) - \phi(p)p^{k-1}) \right)$$

However, $\frac{g(\psi\phi^{-1})}{g(\phi)}$, $\phi^{-1}(a)$, $\psi\left(\frac{-b}{v}\right)$ and $\psi^{-1}(M)$ are units in $\mathbb{Z}[\psi, \phi]$. Furthermore, $l \nmid u$ since $u \mid N$ and by assumption $l \nmid N$. Hence, $l$ must divide

$$L(1-k, \psi^{-1}\phi) \left( \prod_{p \in \mathcal{P}_M} (\psi(p) - \phi(p)p^{k-1}) \right).$$

Condition (1) follows easily from this, so we are done.

# Reverse implication

- For the reverse implication, we can prove the case where $M = p$ prime.
- A result of Spencer (2018) gives us an eigenform $f$ which satisfies the congruence.
- If this is a newform then we're done, so assume $f$ arises from a modular form $f_0 \in S_k^{new}(\Gamma_0(N), \chi)$.

# Reverse implication

- For the reverse implication, we can prove the case where $M = p$ prime.
- A result of Spencer (2018) gives us an eigenform $f$ which satisfies the congruence.
- If this is a newform then we're done, so assume $f$ arises from a modular form $f_0 \in S_k^{new}(\Gamma_0(N), \chi)$.

To obtain a level $Np$ newform, we use the following:

## Theorem (Diamond 1991)

For $p \nmid N$, the following are equivalent:

1. We have $f_0 \in S_k(\Gamma_0(N), \chi)$ satisfying
$$a_p(f_0)^2 \equiv \chi(p)p^{k-2}(1+p^2) \pmod{\lambda}.$$
2. There is a $p$-newform $f_1 \in S_k(\Gamma_0(Np), \chi)$ satisfying
$$a_q(f_1) \equiv a_q(f_0) \equiv \psi(q) + \phi(q)q^{k-1} \pmod{\lambda'} \ \forall \text{ primes } q \nmid Npl$$

# Consequences/ future work

- Our results provide evidence for a case of the Bloch-Kato conjecture - a conjecture in algebraic number theory relating L-values and arithmetic of Galois modules.

# Consequences/ future work

- Our results provide evidence for a case of the Bloch-Kato conjecture - a conjecture in algebraic number theory relating L-values and arithmetic of Galois modules.
- In particular, our results are expected to produce ‘new’ elements in a Bloch-Kato Selmer group.

# Consequences/ future work

- Our results provide evidence for a case of the Bloch-Kato conjecture - a conjecture in algebraic number theory relating L-values and arithmetic of Galois modules.
- In particular, our results are expected to produce 'new' elements in a Bloch-Kato Selmer group.
- We are also working on generalising our results to Hilbert modular forms.

# Thank you!