Local origin congruences for elliptic modular forms.

Dan Fretwell
University of Bristol
(daniel.fretwell@bristol.ac.uk)

Outline of talk

Let $q = e^{2\pi iz}$ for $z \in \mathcal{H}$. Recall the discriminant function:

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

Ramanujan

$\tau(n) \equiv \sigma_{11}(n) \bmod 691$ (here $\sigma_k(n) = \sum_{d|n} d^k$).

Alternatively, we have $\Delta \equiv E_{12} \bmod 691$, where:

$$E_{12}(z) = -\frac{B_{12}}{24} + \sum_{n=1}^{\infty} \sigma_{11}(n) q^n.$$

Let $q = e^{2\pi i z}$ for $z \in \mathcal{H}$. Recall the discriminant function:

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

Ramanujan

$\tau(n) \equiv \sigma_{11}(n) \bmod 691$ (here $\sigma_k(n) = \sum_{d|n} d^k$).

Alternatively, we have $\Delta \equiv E_{12} \bmod 691$, where:

$$E_{12}(z) = -\frac{B_{12}}{24} + \sum_{n=1}^{\infty} \sigma_{11}(n) q^n.$$

Let $q = e^{2\pi i z}$ for $z \in \mathcal{H}$. Recall the discriminant function:

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

Ramanujan

$\tau(n) \equiv \sigma_{11}(n) \bmod 691$ (here $\sigma_k(n) = \sum_{d|n} d^k$).

Alternatively, we have $\Delta \equiv E_{12} \bmod 691$, where:

$$E_{12}(z) = -\frac{B_{12}}{24} + \sum_{n=1}^{\infty} \sigma_{11}(n) q^n.$$

What's the point?

- **Computation** - Gives us arithmetic information about $\tau(n)$. For example it gives us lots of evidence for the following open conjecture of Lehmer:

Conjecture

$\tau(n) \neq 0$ for all n.

- **Bloch-Kato** - a mysterious and open conjecture generalising BSD and the Analytic Class Number formula.

What's the point?

- **Computation** - Gives us arithmetic information about $\tau(n)$. For example it gives us lots of evidence for the following open conjecture of Lehmer:

Conjecture

$\tau(n) \neq 0$ for all n.

- **Bloch-Kato** - a mysterious and open conjecture generalising BSD and the Analytic Class Number formula.

- **Galois representations** - Assigned to Δ is a two dimensional Galois representation:

$$\rho_\Delta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_{691}).$$

The congruence is equivalent to:

$$\mathrm{tr}(\rho_\Delta(\mathrm{Frob}_p)) \equiv 1 + p^{11} = \mathrm{tr}((1 \oplus \chi^{11})(\mathrm{Frob}_p)),$$

which tells us that:

$$\rho_\Delta \sim \begin{pmatrix} 1 & \star \\ 0 & \chi^{11} \end{pmatrix}$$

with $\star$ non-trivial mod 691. Ribet shows how knowing this is equivalent to knowing that 691 divides $|\mathrm{Cl}_{\mathbb{Q}(\zeta_{691})}|$.

Other weights

Theorem

Let $k \geq 4$ be even. Suppose $\mathrm{ord}_l\left(\frac{B_k}{2k}\right) > 0$ for l prime. Then there exists a normalized eigenform $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ with Fourier coefficients satisfying:

$$a_n \equiv \sigma_{k-1}(n) \bmod \lambda,$$

for some prime $\lambda \mid l$ of the coefficient field $\mathbb{Q}_f$.

Outline of talk

1. Ramanujan's congruence
2. Level p congruences
3. A sketch proof
4. A cute infinite family of examples

Can we find Eisenstein congruences at level p?

Well $S_k(\mathrm{SL}_2(\mathbb{Z})) \hookrightarrow S_k(\Gamma_0(p))$ and so all level 1 congruences transfer over. However we get new ones!

Example

$$q - 36q^2 - 81q^3 + 784q^4 + \ldots \in S_{10}^{\mathrm{new}}(\Gamma_0(3))$$

is a normalized eigenform satisfying $a_p \equiv \sigma_9(p) \bmod 61$ for all $p \neq 3$ prime.

However $\mathrm{ord}_{61}\left(\frac{B_{10}}{20}\right) = 0$.

Can we find Eisenstein congruences at level p?

Well $S_k(\mathrm{SL}_2(\mathbb{Z})) \hookrightarrow S_k(\Gamma_0(p))$ and so all level 1 congruences transfer over. However we get new ones!

Example

$$q - 36q^2 - 81q^3 + 784q^4 + ... \in S_{10}^{\text{new}}(\Gamma_0(3))$$

is a normalized eigenform satisfying $a_p \equiv \sigma_9(p) \bmod 61$ for all $p \neq 3$ prime.

However $\mathrm{ord}_{61}\left(\frac{B_{10}}{20}\right) = 0$.

Can we find Eisenstein congruences at level p?

Well $S_k(\mathrm{SL}_2(\mathbb{Z})) \hookrightarrow S_k(\Gamma_0(p))$ and so all level 1 congruences transfer over. However we get new ones!

Example

$$q - 36q^2 - 81q^3 + 784q^4 + \ldots \in S_{10}^{\mathrm{new}}(\Gamma_0(3))$$

is a normalized eigenform satisfying $a_p \equiv \sigma_9(p) \bmod 61$ for all $p \neq 3$ prime.

However $\mathrm{ord}_{61}\left(\frac{B_{10}}{20}\right) = 0$.

How can we explain this congruence?

Ramanujan's congruence comes from the fact that $\mathrm{ord}_l\left(\frac{B_k}{2k}\right) > 0$. Equivalently $\mathrm{ord}_l\left(\frac{\zeta(k)}{\pi^k}\right) > 0$.

Define:

$$\zeta_{\{p\}}(k) = \prod_{q \neq p}\left(1 - \frac{1}{q^k}\right)^{-1}.$$

Then:

$$\frac{\zeta_{\{p\}}(k)}{\pi^k} = \left(1 - \frac{1}{p^k}\right)\frac{\zeta(k)}{\pi^k} = \frac{(p^k - 1)\zeta(k)}{(p\pi)^k}.$$

So we might expect congruences at level p when $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$. Note that $3^{10} - 1 = 61 \times 2^3 \times 11^2$.

How can we explain this congruence?

Ramanujan's congruence comes from the fact that $\mathrm{ord}_l\left(\frac{B_k}{2k}\right) > 0$. Equivalently $\mathrm{ord}_l\left(\frac{\zeta(k)}{\pi^k}\right) > 0$.

Define:

$$\zeta_{\{p\}}(k) = \prod_{q \neq p} \left(1 - \frac{1}{q^k}\right)^{-1}.$$

Then:

$$\frac{\zeta_{\{p\}}(k)}{\pi^k} = \left(1 - \frac{1}{p^k}\right)\frac{\zeta(k)}{\pi^k} = \frac{(p^k-1)\zeta(k)}{(p\pi)^k}.$$

So we might expect congruences at level p when $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$. Note that $3^{10} - 1 = 61 \times 2^3 \times 11^2$.

How can we explain this congruence?

Ramanujan's congruence comes from the fact that $\mathrm{ord}_l\left(\frac{B_k}{2k}\right) > 0$. Equivalently $\mathrm{ord}_l\left(\frac{\zeta(k)}{\pi^k}\right) > 0$.

Define:

$$\zeta_{\{p\}}(k) = \prod_{q \neq p}\left(1 - \frac{1}{q^k}\right)^{-1}.$$

Then:

$$\frac{\zeta_{\{p\}}(k)}{\pi^k} = \left(1 - \frac{1}{p^k}\right)\frac{\zeta(k)}{\pi^k} = \frac{(p^k - 1)\zeta(k)}{(p\pi)^k}.$$

So we might expect congruences at level p when $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$. Note that $3^{10} - 1 = 61 \times 2^3 \times 11^2$.

How can we explain this congruence?

Ramanujan's congruence comes from the fact that $\mathrm{ord}_l\left(\frac{B_k}{2k}\right) > 0$. Equivalently $\mathrm{ord}_l\left(\frac{\zeta(k)}{\pi^k}\right) > 0$.

Define:

$$\zeta_{\{p\}}(k) = \prod_{q \neq p} \left(1 - \frac{1}{q^k}\right)^{-1}.$$

Then:

$$\frac{\zeta_{\{p\}}(k)}{\pi^k} = \left(1 - \frac{1}{p^k}\right) \frac{\zeta(k)}{\pi^k} = \frac{(p^k - 1)\zeta(k)}{(p\pi)^k}.$$

So we might expect congruences at level p when $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$. Note that $3^{10} - 1 = 61 \times 2^3 \times 11^2$.

Theorem (Dummigan, F.)

Let $k \geq 4$ be even and $l > 3$ be a prime such that $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$. Then there exists a normalized eigenform $f \in S_k(\Gamma_0(p))$ such that (for $q \neq p$):

$$a_q \equiv 1 + q^{k-1} \bmod \lambda$$

with $\lambda | l$ in $\mathbb{Q}_f$.

The result is actually true in much greater generality, e.g. forms with character, Γ_1, higher level.

Theorem (Dummigan, F.)

Let $k \geq 4$ be even and $l > 3$ be a prime such that $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$. Then there exists a normalized eigenform $f \in S_k(\Gamma_0(p))$ such that (for $q \neq p$):

$$a_q \equiv 1 + q^{k-1} \bmod \lambda$$

with $\lambda | l$ in $\mathbb{Q}_f$.

The result is actually true in much greater generality, e.g. forms with character, Γ_1, higher level.

Outline of talk

Some preliminary stuff

- **Cusps**
  $\Gamma_0(p)\backslash\mathcal{H}$ has two cusps represented by $[0], [\infty]$. So to be a cusp form you must vanish at both.
- **Eisenstein series**

$$M_k(\Gamma_0(p)) = S_k(\Gamma_0(p)) \oplus \mathbb{C}E_k \oplus \mathbb{C}E'_k,$$

  where $E'_k(z) = E_k(pz)$.
- **Fricke involution**
  Let $A_p = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$. There is an endomorphism W_p on $M_k(\Gamma_0(p))$ given by:

$$(W_p(f))(z) = z^{-k} f(A_p z) = z^{-k} f\left(-\frac{1}{pz}\right).$$

  Note A_p swaps the two cusps $[0], [\infty]$.

Some preliminary stuff

- **Cusps**
  $\Gamma_0(p)\backslash\mathcal{H}$ has two cusps represented by $[0], [\infty]$. So to be a cusp form you must vanish at both.
- **Eisenstein series**

$$M_k(\Gamma_0(p)) = S_k(\Gamma_0(p)) \oplus \mathbb{C}E_k \oplus \mathbb{C}E'_k,$$

  where $E'_k(z) = E_k(pz)$.
- **Fricke involution**
  Let $A_p = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$. There is an endomorphism W_p on $M_k(\Gamma_0(p))$ given by:

$$(W_p(f))(z) = z^{-k} f(A_p z) = z^{-k} f\left(-\frac{1}{pz}\right).$$

  Note A_p swaps the two cusps $[0], [\infty]$.

Some preliminary stuff

- **Cusps**
  $\Gamma_0(p)\backslash\mathcal{H}$ has two cusps represented by $[0], [\infty]$. So to be a cusp form you must vanish at both.
- **Eisenstein series**

$$M_k(\Gamma_0(p)) = S_k(\Gamma_0(p)) \oplus \mathbb{C}E_k \oplus \mathbb{C}E'_k,$$

  where $E'_k(z) = E_k(pz)$.
- **Fricke involution**
  Let $A_p = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$. There is an endomorphism W_p on $M_k(\Gamma_0(p))$ given by:

$$(W_p(f))(z) = z^{-k} f(A_p z) = z^{-k} f\left(-\frac{1}{pz}\right).$$

  Note A_p swaps the two cusps $[0], [\infty]$.

Proof sketch

Let $F_k = E_k - E_k'$. Then $F_k \in M_k(\Gamma_0(p))$ has no constant term, hence satisfies $F_k([\infty]) = 0$.

However, we do not know the value $F_k([0])$ so cannot conclude that F_k is a cusp form.

Idea - use the Fricke involution to swap the cusps. Then we know $W_p(F_k)([0]) = 0$ and left with finding $W_p(F_k)([\infty])$.

Proof sketch

Let $F_k = E_k - E_k'$. Then $F_k \in M_k(\Gamma_0(p))$ has no constant term, hence satisfies $F_k([\infty]) = 0$.

However, we do not know the value $F_k([0])$ so cannot conclude that F_k is a cusp form.

Idea - use the Fricke involution to swap the cusps. Then we know $W_p(F_k)([0]) = 0$ and left with finding $W_p(F_k)([\infty])$.

Proof sketch

Let $F_k = E_k - E'_k$. Then $F_k \in M_k(\Gamma_0(p))$ has no constant term, hence satisfies $F_k([\infty]) = 0$.

However, we do not know the value $F_k([0])$ so cannot conclude that F_k is a cusp form.

Idea - use the Fricke involution to swap the cusps. Then we know $W_p(F_k)([0]) = 0$ and left with finding $W_p(F_k)([\infty])$.

But:

$$W_p(F_k)(z) = p^k E_k'(z) - E_k(z),$$

which has constant term $-\frac{(p^k-1)B_k}{2k}$.

However $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$ by assumption, hence $W_p(F_k)$ is a "cusp form mod l".

By some magic (Deligne-Serre lemma) we can then lift to a genuine normalized eigenform $f \in S_k(\Gamma_0(p))$ (with coefficients in some number field $K = \mathbb{Q}_f$) such that $f \equiv W_p(F_k) \bmod \lambda$ for some prime $\lambda | l$ in K.

Note that the Fourier coefficients of $W_p(F_k)$ at $q \neq p$ are $1 + q^{k-1}$ and so we are done.

But:

$$W_p(F_k)(z) = p^k E_k'(z) - E_k(z),$$

which has constant term $-\frac{(p^k-1)B_k}{2k}$.

However $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$ by assumption, hence $W_p(F_k)$ is a "cusp form mod l".

By some magic (Deligne-Serre lemma) we can then lift to a genuine normalized eigenform $f \in S_k(\Gamma_0(p))$ (with coefficients in some number field $K = \mathbb{Q}_f$) such that $f \equiv W_p(F_k) \bmod \lambda$ for some prime $\lambda | l$ in K.

Note that the Fourier coefficients of $W_p(F_k)$ at $q \neq p$ are $1 + q^{k-1}$ and so we are done.

But:

$$W_p(F_k)(z) = p^k E_k'(z) - E_k(z),$$

which has constant term $-\frac{(p^k-1)B_k}{2k}$.

However $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$ by assumption, hence $W_p(F_k)$ is a "cusp form mod l".

By some magic (Deligne-Serre lemma) we can then lift to a genuine normalized eigenform $f \in S_k(\Gamma_0(p))$ (with coefficients in some number field $K = \mathbb{Q}_f$) such that $f \equiv W_p(F_k) \bmod \lambda$ for some prime $\lambda | l$ in K.

Note that the Fourier coefficients of $W_p(F_k)$ at $q \neq p$ are $1 + q^{k-1}$ and so we are done.

But:

$$W_p(F_k)(z) = p^k E_k'(z) - E_k(z),$$

which has constant term $-\frac{(p^k-1)B_k}{2k}$.

However $\mathrm{ord}_l\left(\frac{(p^k-1)B_k}{2k}\right) > 0$ by assumption, hence $W_p(F_k)$ is a "cusp form mod l".

By some magic (Deligne-Serre lemma) we can then lift to a genuine normalized eigenform $f \in S_k(\Gamma_0(p))$ (with coefficients in some number field $K = \mathbb{Q}_f$) such that $f \equiv W_p(F_k) \bmod \lambda$ for some prime $\lambda | l$ in K.

Note that the Fourier coefficients of $W_p(F_k)$ at $q \neq p$ are $1 + q^{k-1}$ and so we are done.

Outline of talk

1. Ramanujan's congruence
2. Level p congruences
3. A sketch proof
4. A cute infinite family of examples

Note that if $l \mid p^k - 1$ then $l \mid p^{mk} - 1$ for any $m \geq 1$.

Also if $p = 2$ we can **force** $p^k - 1$ to itself be prime. So we expect there to be Eisenstein congruences for cusp forms of level 2, weights $2np_0$ and with Mersenne prime modulus $M_{p_0} = 2^{p_0} - 1$...

...as long as M_{p_0} doesn't divide the denominator of $\frac{B_{2np_0}}{4np_0}$. But by Von Staudt-Clausen this happens if and only if $M_{p_0} - 1 \nmid 2np_0$, i.e. if and only if $\frac{M_{p_0}-1}{2p_0} \nmid n$.

Note that if $l \mid p^k - 1$ then $l \mid p^{mk} - 1$ for any $m \geq 1$.

Also if $p = 2$ we can **force** $p^k - 1$ to itself be prime. So we expect there to be Eisenstein congruences for cusp forms of level 2, weights $2np_0$ and with Mersenne prime modulus $M_{p_0} = 2^{p_0} - 1$...

...as long as M_{p_0} doesn't divide the denominator of $\frac{B_{2np_0}}{4np_0}$. But by Von Staudt-Clausen this happens if and only if $M_{p_0} - 1 \nmid 2np_0$, i.e. if and only if $\frac{M_{p_0}-1}{2p_0} \nmid n$.

Note that if $l \mid p^k - 1$ then $l \mid p^{mk} - 1$ for any $m \geq 1$.

Also if $p = 2$ we can **force** $p^k - 1$ to itself be prime. So we expect there to be Eisenstein congruences for cusp forms of level 2, weights $2np_0$ and with Mersenne prime modulus $M_{p_0} = 2^{p_0} - 1$...

...as long as M_{p_0} doesn't divide the denominator of $\frac{B_{2np_0}}{4np_0}$. But by Von Staudt-Clausen this happens if and only if $M_{p_0} - 1 \nmid 2np_0$, i.e. if and only if $\frac{M_{p_0}-1}{2p_0} \nmid n$.

Note that if $l \mid p^k - 1$ then $l \mid p^{mk} - 1$ for any $m \geq 1$.

Also if $p = 2$ we can **force** $p^k - 1$ to itself be prime. So we expect there to be Eisenstein congruences for cusp forms of level 2, weights $2np_0$ and with Mersenne prime modulus $M_{p_0} = 2^{p_0} - 1$...

...as long as M_{p_0} doesn't divide the denominator of $\frac{B_{2np_0}}{4np_0}$. But by Von Staudt-Clausen this happens if and only if $M_{p_0} - 1 \nmid 2np_0$, i.e. if and only if $\frac{M_{p_0}-1}{2p_0} \nmid n$.

Corollary (F.)

Let $p_0 \geq 3$ be prime and $n \geq 1$. Then $\frac{M_{p_0}-1}{2p_0} \nmid n$ if and only if there exists a normalized eigenform $f \in S_{2np_0}(\Gamma_0(2))$ such that:

$$a_q \equiv 1 + q^{2np_0 - 1} \bmod \lambda,$$

for all $q \neq 2$, where $\lambda \mid M_{p_0}$ in $\mathbb{Q}_f$.

For example, take $p_0 = 5$, then $M_5 = 31$ and $\frac{M_5 - 1}{10} = 3$. So for any $n \not\equiv 0 \bmod 3$ we expect a congruence for $f \in S_{10n}(\Gamma_0(2))$.

$n = 1$

$$f(z) = q + 16q^2 - 156q^3 + 256q^4 + 870q^5 + ...$$

satisfies $a_q \equiv 1 + q^9 \bmod 31$ for all $q \neq 2$.

$n = 2$

$$f(z) = q + 512q^2 - 53028q^3 + 262144q^4 - 5556930q^5 + ...$$

satisfies $a_q \equiv 1 + q^{19} \bmod 31$ for all $q \neq 2$.

$n = 3$

None of the 6 normalized eigenforms in $S_{30}(\Gamma_0(2))$ satisfy the congruence $a_q \equiv 1 + q^{29} \bmod 31$ for all $q \neq 2$.

For example, take $p_0 = 5$, then $M_5 = 31$ and $\frac{M_5 - 1}{10} = 3$. So for any $n \not\equiv 0 \bmod 3$ we expect a congruence for $f \in S_{10n}(\Gamma_0(2))$.

$n = 1$

$$f(z) = q + 16q^2 - 156q^3 + 256q^4 + 870q^5 + \ldots$$

satisfies $a_q \equiv 1 + q^9 \bmod 31$ for all $q \neq 2$.

$n = 2$

$$f(z) = q + 512q^2 - 53028q^3 + 262144q^4 - 5556930q^5 + \ldots$$

satisfies $a_q \equiv 1 + q^{19} \bmod 31$ for all $q \neq 2$.

$n = 3$

None of the 6 normalized eigenforms in $S_{30}(\Gamma_0(2))$ satisfy the congruence $a_q \equiv 1 + q^{29} \bmod 31$ for all $q \neq 2$.

For example, take $p_0 = 5$, then $M_5 = 31$ and $\frac{M_5 - 1}{10} = 3$. So for any $n \not\equiv 0 \bmod 3$ we expect a congruence for $f \in S_{10n}(\Gamma_0(2))$.

$n = 1$

$$f(z) = q + 16q^2 - 156q^3 + 256q^4 + 870q^5 + ...$$

satisfies $a_q \equiv 1 + q^9 \bmod 31$ for all $q \neq 2$.

$n = 2$

$$f(z) = q + 512q^2 - 53028q^3 + 262144q^4 - 5556930q^5 + ...$$

satisfies $a_q \equiv 1 + q^{19} \bmod 31$ for all $q \neq 2$.

$n = 3$

None of the 6 normalized eigenforms in $S_{30}(\Gamma_0(2))$ satisfy the congruence $a_q \equiv 1 + q^{29} \bmod 31$ for all $q \neq 2$.

For example, take $p_0 = 5$, then $M_5 = 31$ and $\frac{M_5 - 1}{10} = 3$. So for any $n \not\equiv 0 \bmod 3$ we expect a congruence for $f \in S_{10n}(\Gamma_0(2))$.

$n = 1$

$$f(z) = q + 16q^2 - 156q^3 + 256q^4 + 870q^5 + \ldots$$

satisfies $a_q \equiv 1 + q^9 \bmod 31$ for all $q \neq 2$.

$n = 2$

$$f(z) = q + 512q^2 - 53028q^3 + 262144q^4 - 5556930q^5 + \ldots$$

satisfies $a_q \equiv 1 + q^{19} \bmod 31$ for all $q \neq 2$.

$n = 3$

None of the 6 normalized eigenforms in $S_{30}(\Gamma_0(2))$ satisfy the congruence $a_q \equiv 1 + q^{29} \bmod 31$ for all $q \neq 2$.

Thank you for listening!