On the arithmetic of modular forms

Gabor Wiese

15 June 2017

Modular forms

There are five fundamental operations: addition, subtraction, multiplication, division, and modular forms.

Martin Eichler (1912-1992)

Modular forms

There are five fundamental operations: addition, subtraction, multiplication, division, and modular forms.

Martin Eichler (1912-1992)

J'aime bien les formes modulaires. [...] C'est un sujet sur lequel on n'a jamais de mauvaises surprises: si l'on devine un énoncé, c'est un énoncé encore plus beau qui est vrai !

Jean-Pierre Serre (*1926)

Arithmetic significance of coefficients of modular forms

Examples (19th century):

Gotthold Eisenstein (1823-1852)

Carl Jacobi (1804-1851)

Arithmetic significance of coefficients of modular forms

Examples (19th century):

Gotthold Eisenstein (1823-1852)

Carl Jacobi (1804-1851)

Eisenstein series

Arithmetic significance of coefficients of modular forms

Examples (19th century):

Gotthold Eisenstein (1823-1852)

Carl Jacobi (1804-1851)

Eisenstein series

$$E_k = * \sum_{(n,m)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(m\tau+n)^k}$$

Arithmetic significance of coefficients of modular forms

Examples (19th century):

Gotthold Eisenstein (1823-1852) Carl Jacobi (1804-1851)

Eisenstein series

$$E_k = \frac{(k-1)!}{(2\pi i)^k} \cdot \zeta(k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n, \quad q = e^{2\pi i \tau},$$

where $\sigma_{k-1}(n) = \sum_{0<d|n} d^{k-1}$.

Arithmetic significance of coefficients of modular forms

Examples (19th century):

Gotthold Eisenstein (1823-1852)

Carl Jacobi (1804-1851)

Eisenstein series

$$E_k = \frac{(k-1)!}{(2\pi i)^k} \cdot \zeta(k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n, \quad q = e^{2\pi i \tau},$$

where $\sigma_{k-1}(n) = \sum_{0<d|n} d^{k-1}$.

Coefficients: Special zeta-value and divisor function.

Arithmetic significance of coefficients of modular forms

Examples (19th century):

Gotthold Eisenstein (1823-1852)   Carl Jacobi (1804-1851)

Eisenstein series

$$E_k = \frac{(k-1)!}{(2\pi i)^k} \cdot \zeta(k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n, \quad q = e^{2\pi i \tau},$$

where $\sigma_{k-1}(n) = \sum_{0<d|n} d^{k-1}$.

Coefficients: Special zeta-value and divisor function.

Matching Jacobi's Theta-series with Eisenstein series, one gets:

$$\#\{x \in \mathbb{Z}^4 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 = n\} = 8 \sum_{4\nmid d|n, 1\le d\le n} d.$$

Arithmetic significance of coefficients of modular forms

Another view on Eisenstein series.

Recall: $E_k = \frac{(k-1)!}{(2\pi i)^k} \cdot \zeta(k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n$.

Arithmetic significance of coefficients of modular forms

Another view on Eisenstein series.

Recall: $E_k = \frac{(k-1)!}{(2\pi i)^k} \cdot \zeta(k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n$.

Fix a prime ℓ.

ℓ-adic cyclotomic character: $\chi(\mathrm{Frob}_p) = p$.

Arithmetic significance of coefficients of modular forms

Another view on Eisenstein series.

Recall: $E_k = \frac{(k-1)!}{(2\pi i)^k} \cdot \zeta(k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n$.

Fix a prime ℓ.

ℓ-adic cyclotomic character: $\chi(\mathrm{Frob}_p) = p$.

$$\chi : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n} | n \in \mathbb{N}) \to \mathbb{Z}_\ell^\times$$

given by the action on the p-power roots of unity:

$$\sigma(\zeta_{\ell^n}) = \zeta_{\ell^n}^{\chi(\sigma)}.$$

Particularly, $\mathrm{Frob}_p(\zeta_{\ell^n}) = \zeta_{\ell^n}^{p} = \zeta_{\ell^n}^{\chi(\mathrm{Frob}_p)}$, whence $\chi(\mathrm{Frob}_p) = p$.

Arithmetic significance of coefficients of modular forms

Another view on Eisenstein series.

Recall: $E_k = \frac{(k-1)!}{(2\pi i)^k} \cdot \zeta(k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n$.

Fix a prime ℓ.

ℓ-adic cyclotomic character: $\chi(\mathrm{Frob}_p) = p$.

Consider the reducible semi-simple Galois representation

$$\rho := 1 \oplus \chi^{k-1} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p), \quad \rho(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & \chi^{k-1}(\sigma) \end{pmatrix}.$$

In particular,

$$\rho(\mathrm{Frob}_p) = \begin{pmatrix} 1 & 0 \\ 0 & \chi^{k-1}(\mathrm{Frob}_p) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p^{k-1} \end{pmatrix}.$$

Then $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 1 + p^{k-1} = \sigma_{k-1}(p)$.

This is the p-th coefficient of the Eisenstein series of weight k.

Arithmetic significance of coefficients of modular forms

Eisenstein series: $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 1 + p^{k-1} = \sigma_{k-1}(p)$.

The Eisenstein series example is a very special case of a general theorem of Shimura and Deligne:

Arithmetic significance of coefficients of modular forms

Eisenstein series: $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 1 + p^{k-1} = \sigma_{k-1}(p)$.

The Eisenstein series example is a very special case of a general theorem of Shimura and Deligne:

Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a Hecke eigenform (of level N, Dirichlet character ψ and weight k) with $a_1 = 1$. Let ℓ be a prime. Then there exists a Galois representation

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Z}}_\ell)$$

which is unramified outside $N\ell$ and satisfies for all primes $p \nmid N\ell$

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = a_p \text{ and } \det(\rho(\mathrm{Frob}_p)) = \psi(p)p^{k-1}.$$

Arithmetic significance of coefficients of modular forms

A concrete (baby) example.

- Let $f = \sum_{n=1}^{\infty} a_n q^n$ a particular modular form with Galois representation $\rho = \rho_f$.

Arithmetic significance of coefficients of modular forms

A concrete (baby) example.

- Let $f = \sum_{n=1}^{\infty} a_n q^n$ a particular modular form with Galois representation $\rho = \rho_f$.
- Let $P(X) = X^6 - 6X^4 + 9X^2 + 23$. The absolute Galois group of its splitting field is the kernel of ρ_f.

Arithmetic significance of coefficients of modular forms

A concrete (baby) example.

- Let $f = \sum_{n=1}^{\infty} a_n q^n$ a particular modular form with Galois representation $\rho = \rho_f$.
- Let $P(X) = X^6 - 6X^4 + 9X^2 + 23$. The absolute Galois group of its splitting field is the kernel of ρ_f.

P mod p	Frob_p	$\rho(\mathrm{Frob}_p)$
()()()()()()	identity	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
()()	2 3-cycles	$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}, \begin{pmatrix} \zeta^2 & 0 \\ 0 & \zeta \end{pmatrix}, \zeta = e^{2\pi i/3}$
()()()	3 2-cycles	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta \\ \zeta^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^2 \\ \zeta & 0 \end{pmatrix}$

Arithmetic significance of coefficients of modular forms

A concrete (baby) example.

- Let $f = \sum_{n=1}^{\infty} a_n q^n$ a particular modular form with Galois representation $\rho = \rho_f$.
- Let $P(X) = X^6 - 6X^4 + 9X^2 + 23$. The absolute Galois group of its splitting field is the kernel of ρ_f.

P mod p	Frob_p	$\rho(\mathrm{Frob}_p)$	trace
()()()()()()	identity	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	2
()()	2 3-cycles	$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}, \begin{pmatrix} \zeta^2 & 0 \\ 0 & \zeta \end{pmatrix}, \zeta = e^{2\pi i/3}$	-1
()()()	3 2-cycles	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta \\ \zeta^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^2 \\ \zeta & 0 \end{pmatrix}$	0

Arithmetic significance of coefficients of modular forms

A concrete (baby) example.

- Let $f = \sum_{n=1}^{\infty} a_n q^n$ a particular modular form with Galois representation $\rho = \rho_f$.
- Let $P(X) = X^6 - 6X^4 + 9X^2 + 23$. The absolute Galois group of its splitting field is the kernel of ρ_f.

P mod p	Frob_p	$\rho(\mathrm{Frob}_p)$	trace	a_p
()()()()()()	identity	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	2	2
()()	2 3-cycles	$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}, \begin{pmatrix} \zeta^2 & 0 \\ 0 & \zeta \end{pmatrix}, \zeta = e^{2\pi i/3}$	-1	-1
()()()	3 2-cycles	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta \\ \zeta^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^2 \\ \zeta & 0 \end{pmatrix}$	0	0

Arithmetic significance of coefficients of modular forms

Natural questions:

(I) How are the a_p distributed?

Arithmetic significance of coefficients of modular forms

Natural questions:

(I) How are the a_p distributed?

(II) What information is contained in the Galois representation?

Arithmetic significance of coefficients of modular forms

Natural questions:

(I) How are the a_p distributed?

(II) What information is contained in the Galois representation?

(III) In how far are Galois representations governed by modular forms?

Distribution of coefficients

Fix a Hecke eigenform f of weight k (say, $\psi = 1$).

Distribution of coefficients

Fix a Hecke eigenform f of weight k (say, $\psi = 1$).

(1) Distribution modulo ℓ^m.

Chebotarev: The proportion of $\rho_f(\mathrm{Frob}_p) \mod \ell^m$ falling into a given conjugacy class C equals $\frac{\#C}{\#G}$, where G is the image of the Galois representation ρ_f modulo ℓ^m (a finite group).

Distribution of coefficients

Fix a Hecke eigenform f of weight k (say, $\psi = 1$).

(1) Distribution modulo ℓ^m.

Chebotarev: The proportion of $\rho_f(\mathrm{Frob}_p) \mod \ell^m$ falling into a given conjugacy class C equals $\frac{\#C}{\#G}$, where G is the image of the Galois representation ρ_f modulo ℓ^m (a finite group).

(2) 'Real distribution'.

Normalise the coefficients $b_p = \frac{a_p}{p^{(k-1)/2}} \in [-2, 2]$.

The normalised coefficients are equidistributed with respect to the Sato-Tate measure. Proved very recently by Taylor, etc. (Hard).

Distribution of coefficients

Fix a Hecke eigenform f of weight k (say, $\psi = 1$).

(3) Lang-Trotter.

Say f comes from a non-CM elliptic curve.

The set $\{p \mid a_p = 0\}$ has density 0 and behaves asymptotically like $c\frac{\sqrt{x}}{\log(x)}$ for some constant $c > 0$.

Distribution of coefficients

Fix a Hecke eigenform f of weight k (say, $\psi = 1$).

(3) Lang-Trotter.

Say f comes from a non-CM elliptic curve.

The set $\{p \mid a_p = 0\}$ has density 0 and behaves asymptotically like $c\frac{\sqrt{x}}{\log(x)}$ for some constant $c > 0$.

(4) Lang-Trotter-like question.

Say f is of weight 2 (without inner twists) with coefficients in a quadratic field $\mathbb{Q}(\sqrt{D})$. The set $\{p \mid a_p \in \mathbb{Q}\}$ has density 0.

How does it behave asymptotically?

Distribution of coefficients

Fix a prime number p and consider a sequence of Hecke eigenforms f_n such that weight+level tend to infinity.

Distribution of coefficients

Fix a prime number p and consider a sequence of Hecke eigenforms f_n such that weight+level tend to infinity.

(2) 'Real distribution'.

The normalised coefficients $b_p(f_n)$ (p fixed and n running!) are equidistributed.
This is a theorem of Serre (1997)

Distribution of coefficients

Fix a prime number p and consider a sequence of Hecke eigenforms f_n such that weight+level tend to infinity.

(2) 'Real distribution'.

The normalised coefficients $b_p(f_n)$ (p fixed and n running!) are equidistributed.
This is a theorem of Serre (1997)

(1) Distribution modulo ℓ^m.

What can one say about $a_p(f_n) \mod \ell^m$ for p fixed and running n?

Distribution of coefficients

Fix a prime number p and consider a sequence of Hecke eigenforms f_n such that weight+level tend to infinity.

(2) 'Real distribution'.

The normalised coefficients $b_p(f_n)$ (p fixed and n running!) are equidistributed.
This is a theorem of Serre (1997)

(1) Distribution modulo ℓ^m.

What can one say about $a_p(f_n) \mod \ell^m$ for p fixed and running n?

Related: Let f run through all Hecke eigenforms of weight 2 and all prime levels. Are the mod ℓ reductions of all the coefficients of all these forms contained in a finite extension of $\mathbb{F}_\ell$?

Distribution of coefficients

Fix a prime number p and consider a sequence of Hecke eigenforms f_n such that weight+level tend to infinity.

(2) 'Real distribution'.

The normalised coefficients $b_p(f_n)$ (p fixed and n running!) are equidistributed.
This is a theorem of Serre (1997)

(1) Distribution modulo ℓ^m.

What can one say about $a_p(f_n) \mod \ell^m$ for p fixed and running n?

Related: Let f run through all Hecke eigenforms of weight 2 and all prime levels. Are the mod ℓ reductions of all the coefficients of all these forms contained in a finite extension of $\mathbb{F}_\ell$?

I guess 'no', but I cannot prove it.

Distribution of coefficients

Fix a prime number p and consider a sequence of Hecke eigenforms f_n such that weight+level tend to infinity.

(2) 'Real distribution'.

The normalised coefficients $b_p(f_n)$ (p fixed and n running!) are equidistributed.
This is a theorem of Serre (1997)

(1) Distribution modulo ℓ^m.

What can one say about $a_p(f_n) \mod \ell^m$ for p fixed and running n?

Related: Let f run through all Hecke eigenforms of weight 2 and all prime levels. Are the mod ℓ reductions of all the coefficients of all these forms contained in a finite extension of $\mathbb{F}_\ell$?

I guess 'no', but I cannot prove it.

Computations carried out with Marcel Mohyla suggest that the maximum residue degree in level q grows linearly with q.

Arithmetic information in ρ_f

The Galois representation ρ_f attached to f explains arithmetic significance of the coefficients. What else?

Arithmetic information in ρ_f

The Galois representation ρ_f attached to f explains arithmetic significance of the coefficients. What else?

Theorem. *If f is of weight one, prime-to-ℓ level and geometrically defined over $\overline{\mathbb{F}}_\ell$, then ρ_f is unramified at ℓ. Moreover, this characterises weight one among all weights (at least if $\ell > 2$).*

Arithmetic information in ρ_f

The Galois representation ρ_f attached to f explains arithmetic significance of the coefficients. What else?

Theorem. *If f is of weight one, prime-to-ℓ level and geometrically defined over $\overline{\mathbb{F}}_\ell$, then ρ_f is unramified at ℓ. Moreover, this characterises weight one among all weights (at least if $\ell > 2$).*

The theorem is trivial for Hecke eigenforms that are reductions of holomorphic forms (because those have attached Artin representations, and there is not even any 'ℓ').

Arithmetic information in ρ_f

The Galois representation ρ_f attached to f explains arithmetic significance of the coefficients. What else?

Theorem. *If f is of weight one, prime-to-ℓ level and geometrically defined over $\overline{\mathbb{F}}_\ell$, then ρ_f is unramified at ℓ. Moreover, this characterises weight one among all weights (at least if $\ell > 2$).*

The theorem is trivial for Hecke eigenforms that are reductions of holomorphic forms (because those have attached Artin representations, and there is not even any 'ℓ').

However, not all parallel weight one Hecke eigenforms that are geometrically defined over $\overline{\mathbb{F}}_\ell$ lift to holomorphic forms.

Arithmetic information in ρ_f

Theorem (Dimitrov, W.). *Let f be a Hilbert modular eigenform (over any totally real field F) of parallel weight one, geometrically defined over $\overline{\mathbb{F}}_\ell$, of level prime to ℓ. Then the attached Galois representation*

$$\rho_f : G_F = \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

is unramified above ℓ.

Arithmetic information in ρ_f

Theorem (Dimitrov, W.). *Let f be a Hilbert modular eigenform (over any totally real field F) of parallel weight one, geometrically defined over $\overline{\mathbb{F}}_\ell$, of level prime to ℓ. Then the attached Galois representation*

$$\rho_f : G_F = \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

is unramified above ℓ.

It is believed and partially proved that this characterises parallel weight one forms among all Hilbert Hecke eigenforms.

Arithmetic information in ρ_f

Theorem (Dimitrov, W.). *Let f be a Hilbert modular eigenform (over any totally real field F) of parallel weight one, geometrically defined over $\overline{\mathbb{F}}_\ell$, of level prime to ℓ. Then the attached Galois representation*

$$\rho_f : G_F = \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

is unramified above ℓ.

It is believed and partially proved that this characterises parallel weight one forms among all Hilbert Hecke eigenforms.

The theorem is again trivial for Hilbert modular forms that are reductions of holomorphic forms (because those have attached Artin representations, and there is not even any 'ℓ').

Arithmetic information in ρ_f

Theorem (Dimitrov, W.). *Let f be a Hilbert modular eigenform (over any totally real field F) of parallel weight one, geometrically defined over $\overline{\mathbb{F}}_\ell$, of level prime to ℓ. Then the attached Galois representation*

$$\rho_f : G_F = \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

is unramified above ℓ.

It is believed and partially proved that this characterises parallel weight one forms among all Hilbert Hecke eigenforms.

The theorem is again trivial for Hilbert modular forms that are reductions of holomorphic forms (because those have attached Artin representations, and there is not even any 'ℓ').

Are there parallel weight one Hilbert eigenforms that are geometrically defined over $\overline{\mathbb{F}}_\ell$ which do not lift to holomorphic forms?

Arithmetic information coming from modular forms

Theorem (Khare, Wintenberger, Deligne, Shimura). We have a correspondence

$$\{f = \sum_{n=0}^{\infty} a_n q^n \mid f \text{ Hecke eigenform } \}$$

$$\updownarrow \; f \mapsto \rho_f$$

$$\{\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \mid \rho \text{ odd, semi-simple } \}.$$

Arithmetic information coming from modular forms

Theorem (Khare, Wintenberger, Deligne, Shimura). We have a correspondence

$$\{f = \textstyle\sum_{n=0}^{\infty} a_n q^n \mid f \text{ Hecke eigenform } \}$$
$$\updownarrow \; f \mapsto \rho_f$$
$$\{\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \mid \rho \text{ odd, semi-simple } \}.$$

For Hilbert modular forms, such a correspondence is conjectured.

Arithmetic information coming from modular forms

Theorem (Khare, Wintenberger, Deligne, Shimura). We have a correspondence

$$\{f = \sum_{n=0}^{\infty} a_n q^n \mid f \text{ Hecke eigenform } \}$$
$$\updownarrow \; f \mapsto \rho_f$$
$$\{\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \mid \rho \text{ odd, semi-simple } \}.$$

For Hilbert modular forms, such a correspondence is conjectured.

Modular forms are explicitly computable. This makes Galois representations computationally accessible.

Arithmetic information coming from modular forms

Theorem (Khare, Wintenberger, Deligne, Shimura). We have a correspondence

$$\{f = \textstyle\sum_{n=0}^{\infty} a_n q^n \mid f \text{ Hecke eigenform } \}$$
$$\updownarrow \; f \mapsto \rho_f$$
$$\{\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \mid \rho \text{ odd, semi-simple } \}.$$

For Hilbert modular forms, such a correspondence is conjectured.

Modular forms are explicitly computable. This makes Galois representations computationally accessible.

Standard methods work for weights ≥ 2. Weight 1 is different!

Thank you for your attention!