On the arithmetic of modular forms

Gabor Wiese

28 June 2017

Number Theory

Is -1 a square?

Is -1 a square modulo a prime p?

Is -1 a square mod p?

3	squares modulo 3: $\{0, 1\} \not\ni -1$
5	
7	
11	
13	
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	
7	
11	
13	
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 = 2 \cdot 2 - 5$
7	
11	
13	
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	
11	
13	
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	squares modulo 7: $\{0, 1, 2, 4\} \not\ni -1$
11	
13	
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	
13	
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	squares modulo 11: $\{0, 1, 3, 4, 5, 9\} \not\ni -1$
13	
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 = 5 \cdot 5 - 2 \cdot 13$
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	squares modulo 19: $\{0, 1, 4, 5, 6, 7, 9, 11, 16, 17\} \not\ni -1$
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	squares modulo 23: $\{0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \not\ni -1$
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	-1 no square mod 23
29	
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	-1 no square mod 23
29	$-1 = 12 \cdot 12 - 5 \cdot 29$
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	-1 no square mod 23
29	$-1 \equiv 12^2 \mod 29$
31	
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	-1 no square mod 23
29	$-1 \equiv 12^2 \mod 29$
31	squares modulo 31: $\{0, 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\} \not\ni -1$
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	-1 no square mod 23
29	$-1 \equiv 12^2 \mod 29$
31	-1 no square mod 31
37	

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	-1 no square mod 23
29	$-1 \equiv 12^2 \mod 29$
31	-1 no square mod 31
37	$-1 = 31 \cdot 31 - 26 \cdot 37$

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	-1 no square mod 23
29	$-1 \equiv 12^2 \mod 29$
31	-1 no square mod 31
37	$-1 \equiv 31^2 \mod 37$

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	-1 no square mod 23
29	$-1 \equiv 12^2 \mod 29$
31	-1 no square mod 31
37	$-1 \equiv 31^2 \mod 37$

-1 is a square modulo p

$$\Leftrightarrow$$

$p = 2$ or $p \equiv 1 \mod 4$.

Is -1 a square mod p?

3	-1 no square mod 3
5	$-1 \equiv 2^2 \mod 5$
7	-1 no square mod 7
11	-1 no square mod 11
13	$-1 \equiv 5^2 \mod 13$
19	-1 no square mod 19
23	-1 no square mod 23
29	$-1 \equiv 12^2 \mod 29$
31	-1 no square mod 31
37	$-1 \equiv 31^2 \mod 37$

$$-1 \text{ is a square modulo } p \iff p = 2 \text{ or } p \equiv 1 \mod 4.$$

Proof. $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$.
It contains an element of order $4 \Leftrightarrow 4 \mid p-1$.

Is -1 a square mod p?

Reformulation:
Does $X^2 + 1$ factor into linear polynomials modulo p?

Is -1 a square mod p?

Reformulation:
Does $X^2 + 1$ factor into linear polynomials modulo p?

Examples.
$-1 \equiv 5^2 \mod 13 \Rightarrow X^2 + 1 \equiv (X - 5) \cdot (X + 5) \mod 13.$

Is -1 a square mod p?

Reformulation:
Does $X^2 + 1$ factor into linear polynomials modulo p?

Examples.
$-1 \equiv 5^2 \mod 13 \Rightarrow X^2 + 1 \equiv (X - 5) \cdot (X + 5) \mod 13.$
$X^2 + 1$ is irreducible modulo 3.

Is -1 a square mod p?

Reformulation:
Does $X^2 + 1$ factor into linear polynomials modulo p?

Examples.
$-1 \equiv 5^2 \mod 13 \Rightarrow X^2 + 1 \equiv (X - 5) \cdot (X + 5) \mod 13.$
$X^2 + 1$ is irreducible modulo 3.

Proposition.
$X^2 + 1 \equiv (X - *) \cdot (X + *) = ()() \mod p \Leftrightarrow p \equiv 1, 2 \mod 4.$

Is -1 a square mod p?

Generalisation:

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

Is -1 a square mod p?

Generalisation:

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

p	factorisation
5	$(X^2+3)(X^2+X+1)(X^2+4X+1)$
13	$(X^3+10X+4)(X^3+10X+9)$
17	$(X^2+3)(X^2+2X+6)(X^2+15X+6)$
19	$(X^2+9)(X^2+X+12)(X^2+18X+12)$
31	$(X^3+28X+15)(X^3+28X+16)$
47	$(X^3+44X+20)(X^3+44X+27)$
53	$(X^2+22)(X^2+5X+25)(X^2+48X+25)$
59	$(X+9)(X+21)(X+29)(X+30)(X+38)(X+50)$
73	$(X^3+70X+14)(X^3+70X+59)$
97	$(X^2+39)(X^2+41X+42)(X^2+56X+42)$
101	$(X+4)(X+28)(X+32)(X+69)(X+73)(X+97)$

Is -1 a square mod p?

Generalisation:

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

p	factorisation
5	()()()
13	()()
17	()()()
19	()()()
31	()()
47	()()
53	()()()
59	()()()()()()
73	()()
97	()()()
101	()()()()()()

Is -1 a square mod p?

Generalisation:

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

p	factorisation
5	()()()
13	()()
17	()()()
19	()()()
31	()()
47	()()
53	()()()
59	()()()()()()
73	()()
97	()()()
101	()()()()()()

Rule ????

The answer is given by a modular form...

What is a modular form?

Es gibt fünf Grundoperationen: Addition, Subtraktion, Multiplikation, Division und Modulformen.

Martin Eichler (1912-1992)

What is a modular form?

Es gibt fünf Grundoperationen: Addition, Subtraktion, Multiplikation, Division und Modulformen.

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)

What is a modular form?

A modular form is an object from

geometry and/or (harmonic) analysis

(according to taste...)

What is a modular form?

A modular form is an object from

geometry and/or (harmonic) analysis

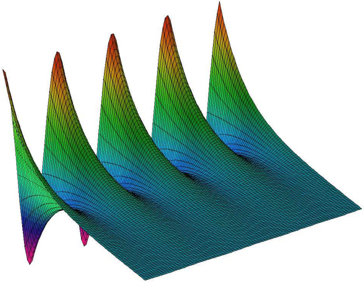
(according to taste...)

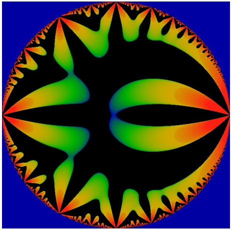
Their coefficients are

arithmetically significant.

What is a modular form?

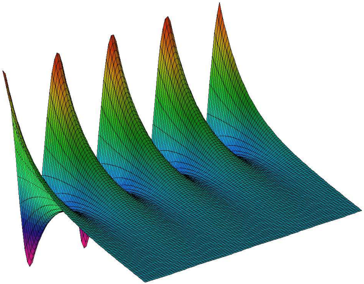
Modular forms are highly symmetric functions.

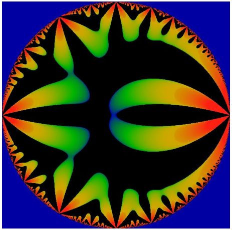




What is a modular form?

Modular forms are highly symmetric functions.

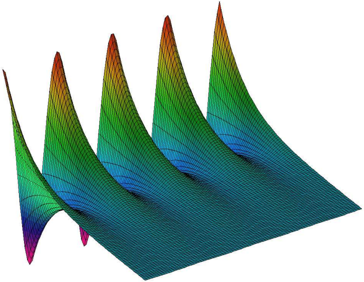


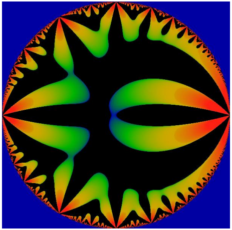


- Complex Analysis: Fourier series with certain transformation properties.

What is a modular form?

Modular forms are highly symmetric functions.





- Complex Analysis: Fourier series with certain transformation properties.
- Geometry: Differential forms on modular curves.
  Modular curves are curves parametrising elliptic curves.

What is a modular form?

A modular form is an object from geometry and/or analysis.

Definition. *A modular form of weight k is a holomorphic function*

$$f : \mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\} \to \mathbb{C}$$

such that

- $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ *for all* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$

What is a modular form?

A modular form is an object from geometry and/or analysis.

Definition. *A modular form of weight k is a holomorphic function*

$$f : \mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\} \to \mathbb{C}$$

such that

- $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ *for all* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$
- *(special case)* $f(z+1) = f(z)$ *for* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$

What is a modular form?

A modular form is an object from geometry and/or analysis.

Definition. *A modular form of weight k is a holomorphic function*

$$f : \mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\} \to \mathbb{C}$$

such that

- $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ *for all* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$
- *(special case)* $f(z+1) = f(z)$ *for* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$
- $f(z) = \sum_{n=0}^{\infty} a_n q^n$ *where* $q = e^{2\pi i z}$.

What is a modular form?

A modular form is an object from geometry and/or analysis.

Definition. *A modular form of weight k is a holomorphic function*

$$f : \mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\} \to \mathbb{C}$$

such that

- $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ *for all* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$
- *(special case)* $f(z+1) = f(z)$ *for* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$
- $f(z) = \sum_{n=0}^{\infty} a_n q^n$ *where* $q = e^{2\pi i z}$.

This is the definition for **level** 1. More generally, level $N \in \mathbb{N}$.

What is a modular form?

Hecke eigenforms are modular forms with special arithmetic.

Erich Hecke (1887-1947)

What is a modular form?

Hecke eigenforms are modular forms with special arithmetic.

Erich Hecke (1887-1947)

The Fourier coefficients of a Hecke eigenform satisfy

$$a_n a_m = a_{nm} \qquad \text{if } \gcd(n, m) = 1.$$

What is a modular form?

Hecke eigenforms are modular forms with special arithmetic.

Erich Hecke (1887-1947)

The Fourier coefficients of a Hecke eigenform satisfy

$$a_n a_m = a_{nm} \qquad \text{if } \gcd(n, m) = 1.$$

The Fourier coefficients of Hecke eigenforms a_n are algebraic integers.

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

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

Arithmetic significance of coefficients of modular forms

Examples (19th century):

Gotthold Eisenstein (1823-1852)

Carl Jacobi (1804-1851)

Eisenstein series

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

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

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

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

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

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:

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

Symmetries of equations

Evariste Galois (1811-1832)

Idea (Galois): Equations satisfy symmetries.

Symmetries of equations

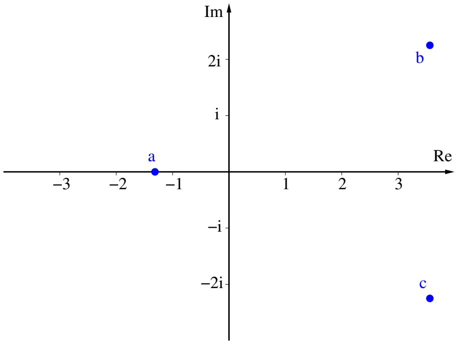
Evariste Galois (1811-1832)

Idea (Galois): Equations satisfy symmetries.

Algebraically speaking: a symmetry is a field automorphism.

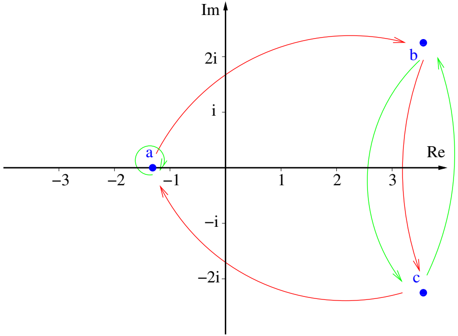
Symmetries of equations

Consider $X^3 - 6X^2 + 9X + 23 = 0$. Three solutions $a, b, c \in \mathbb{C}$:



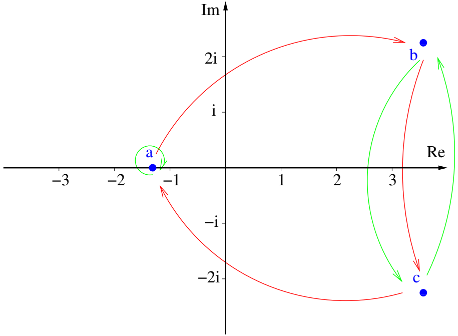
Symmetries of equations

Consider $X^3 - 6X^2 + 9X + 23 = 0$. Three solutions $a, b, c \in \mathbb{C}$:



Symmetries of equations

Consider $X^3 - 6X^2 + 9X + 23 = 0$. Three solutions $a, b, c \in \mathbb{C}$:



There are 6 symmetries in this example.

The symmetry group is called the Galois group.

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: $\chi(\mathrm{Frob}_p) = p$.

$$\chi : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^\times$$

given by the action on the ℓ-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

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

In particular,

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

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

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

In particular,

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

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

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

Arithmetic significance of coefficients of modular forms

Another view on Eisenstein series.

Fix a prime ℓ.

We constructed a Galois representation

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

such that
the trace of Frobenius at any prime $p \neq \ell$ is the p-th coefficient of the Eisenstein series of weight k:

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

Arithmetic significance of coefficients of modular forms

Another view on Eisenstein series.

Fix a prime ℓ.

We constructed a Galois representation

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

such that
the trace of Frobenius at any prime $p \neq \ell$ is the p-th coefficient of the Eisenstein series of weight k:

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

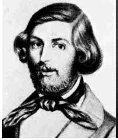
In a sense, the modular form is the character of the Galois representation.

One says that ρ is attached to the Eisenstein series.

From Geometry to Number Theory

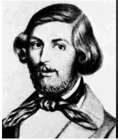
Geometry/Analysis	**Number Theory**
Modular Forms	**Galois Representations**

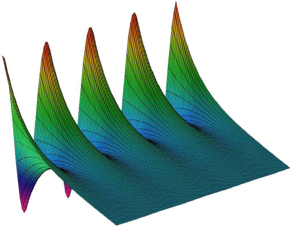
From Geometry to Number Theory

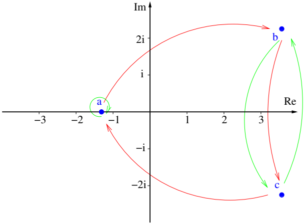
Geometry/Analysis **Modular Forms**	**Number Theory** **Galois Representations**
 	

From Geometry to Number Theory

Geometry/Analysis **Modular Forms**	**Number Theory** **Galois Representations**

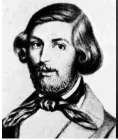






From Geometry to Number Theory

Geometry/Analysis
Modular Forms

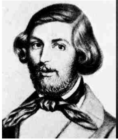



Hecke eigenforms
$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$
with $a_1 = 1$

Number Theory
Galois Representations

Galois repres.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Z}}_\ell)$
s.t. $\det(\rho(\text{compl. conj.})) = -1$

From Geometry to Number Theory

Geometry/Analysis **Modular Forms**		**Number Theory** **Galois Representations**
 		
Hecke eigenforms $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$ with $a_1 = 1$	$\longrightarrow$	Galois repres. $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Z}}_\ell)$ s.t. $\det(\rho(\text{compl. conj.})) = -1$
f level N	$\mapsto$	ρ_f unramified outside $N\ell$ $\mathrm{Tr}(\rho_f(\mathrm{Frob}_p)) = a_p$

Shimura, Deligne, Serre.

Inverse Galois Problem

Hilbert

Given a finite group G.
Is there a number field $K/\mathbb{Q}$ such that its Galois group is G?

Inverse Galois Problem

Hilbert

Given a finite group G.
Is there a number field $K/\mathbb{Q}$ such that its Galois group is G?

Approach: Use the map from Hecke eigenforms to Galois representations and look for suitable modular forms f.

Inverse Galois Problem

Hilbert

Given a finite group G.
Is there a number field $K/\mathbb{Q}$ such that its Galois group is G?

Approach: Use the map from Hecke eigenforms to Galois representations and look for suitable modular forms f.

Example theorem (Dieulefait-W., W.). *Fix $d \in \mathbb{N}$ even. The set of primes*

$$\{\ell \mid \mathrm{PSL}_2(\mathbb{F}_{\ell^d}) \text{ is a Galois group over } \mathbb{Q}\}$$

has positive density.

Inverse Galois Problem

Hilbert

Given a finite group G.
Is there a number field $K/\mathbb{Q}$ such that its Galois group is G?

Approach: Use the map from Hecke eigenforms to Galois representations and look for suitable modular forms f.

Example theorem (Dieulefait-W., W.). *Fix $d \in \mathbb{N}$ even. The set of primes*

$$\{\ell \mid \mathrm{PSL}_2(\mathbb{F}_{\ell^d}) \text{ is a Galois group over } \mathbb{Q}\}$$

has positive density.

For $d = 2$, the density is > 0.99 (computed by Master student).

Inverse Galois Problem

Hilbert

Given a finite group G.
Is there a number field $K/\mathbb{Q}$ such that its Galois group is G?

Approach: Use the map from Hecke eigenforms to Galois representations and look for suitable modular forms f.

Example theorem (Dieulefait-W., W.). *Fix $d \in \mathbb{N}$ even. The set of primes*

$$\{\ell \mid \mathrm{PSL}_2(\mathbb{F}_{\ell^d}) \text{ is a Galois group over } \mathbb{Q}\}$$

has positive density.

For $d = 2$, the density is > 0.99 (computed by Master student).

Under the assumption of Maeda's Conjecture, the density is 1.

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

p	factorisation
5	$(X^2+3)(X^2+X+1)(X^2+4X+1)$
13	$(X^3+10X+4)(X^3+10X+9)$
17	$(X^2+3)(X^2+2X+6)(X^2+15X+6)$
19	$(X^2+9)(X^2+X+12)(X^2+18X+12)$
31	$(X^3+28X+15)(X^3+28X+16)$
47	$(X^3+44X+20)(X^3+44X+27)$
53	$(X^2+22)(X^2+5X+25)(X^2+48X+25)$
59	$(X+9)(X+21)(X+29)(X+30)(X+38)(X+50)$
73	$(X^3+70X+14)(X^3+70X+59)$
97	$(X^2+39)(X^2+41X+42)(X^2+56X+42)$
101	$(X+4)(X+28)(X+32)(X+69)(X+73)(X+97)$

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

p	factorisation
5	()()()
13	()()
17	()()()
19	()()()
31	()()
47	()()
53	()()()
59	()()()()()()
73	()()
97	()()()
101	()()()()()()

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

p	factorisation	a_p
5	()()()	0
13	()()	-1
17	()()()	0
19	()()()	0
31	()()	-1
47	()()	-1
53	()()()	0
59	()()()()()()	2
73	()()	-1
97	()()()	0
101	()()()()()()	2

Proposition.

There is a modular form (of weight 1 and level 23) $f = \sum_{n=1}^{\infty} a_n q^n$ s.t.
3 factors $\Leftrightarrow a_p = 0$,
2 factors $\Leftrightarrow a_p = -1$,
6 factors $\Leftrightarrow a_p = 2$.

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

p	factorisation	a_p
5	()()()	0
13	()()	-1
17	()()()	0
19	()()()	0
31	()()	-1
47	()()	-1
53	()()()	0
59	()()()()()()	2
73	()()	-1
97	()()()	0
101	()()()()()()	2

Proposition.

There is a modular form (of weight 1 and level 23) $f = \sum_{n=1}^{\infty} a_n q^n$ s.t. 3 factors $\Leftrightarrow a_p = 0$, 2 factors $\Leftrightarrow a_p = -1$, 6 factors $\Leftrightarrow a_p = 2$.

Proof. The absolute Galois group of the splitting field of $P(X)$ is the kernel of ρ_f.

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

p	factorisation	a_p
5	()()()	0
13	()()	-1
17	()()()	0
19	()()()	0
31	()()	-1
47	()()	-1
53	()()()	0
59	()()()()()()	2
73	()()	-1
97	()()()	0
101	()()()()()()	2

Proposition.

There is a modular form (of weight 1 and level 23) $f = \sum_{n=1}^{\infty} a_n q^n$ s.t.
3 factors $\Leftrightarrow a_p = 0$,
2 factors $\Leftrightarrow a_p = -1$,
6 factors $\Leftrightarrow a_p = 2$.

Proof. The absolute Galois group of the splitting field of $P(X)$ 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

How does $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p?

p	factorisation	a_p
5	()()()	0
13	()()	-1
17	()()()	0
19	()()()	0
31	()()	-1
47	()()	-1
53	()()()	0
59	()()()()()()	2
73	()()	-1
97	()()()	0
101	()()()()()()	2

Proposition.

There is a modular form (of weight 1 and level 23) $f = \sum_{n=1}^{\infty} a_n q^n$ s.t.
3 factors $\Leftrightarrow a_p = 0$,
2 factors $\Leftrightarrow a_p = -1$,
6 factors $\Leftrightarrow a_p = 2$.

Proof. The absolute Galois group of the splitting field of $P(X)$ is the kernel of ρ_f.

P mod p	Frob_p	$\rho(\mathrm{Frob}_p)$	trace	a_p
()()()()()()	identity	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	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	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \begin{pmatrix} 0 & \zeta \\ \zeta^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^2 \\ \zeta & 0 \end{pmatrix}$	0	0

What can one compute explicitly?

Coefficients of modular forms of weight ≥ 2 can be computed using (co)homological methods ('modular symbols').

'Standard' implementations in Magma, Sage. 'Easy'!!

What can one compute explicitly?

Coefficients of modular forms of weight ≥ 2 can be computed using (co)homological methods ('modular symbols').

'Standard' implementations in Magma, Sage. 'Easy'!!

Galois representations are very hard to compute explicitly!!

What can one compute explicitly?

Coefficients of modular forms of weight ≥ 2 can be computed using (co)homological methods ('modular symbols').

'Standard' implementations in Magma, Sage. 'Easy'!!

Galois representations are very hard to compute explicitly!!

$\Rightarrow$ Compute modular forms to learn about number theory.

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 $f = \sum_{n=1}^{\infty} a_n q^n$.

Distribution of coefficients

Fix a Hecke eigenform $f = \sum_{n=1}^{\infty} a_n q^n$.

(1) Distribution modulo ℓ^m.

For fixed $b \in \mathbb{Z}$, what is the density of the set

$$\{p \mid a_p \equiv b \mod \ell^m\}?$$

Distribution of coefficients

Fix a Hecke eigenform $f = \sum_{n=1}^{\infty} a_n q^n$.

(1) Distribution modulo ℓ^m.

For fixed $b \in \mathbb{Z}$, what is the density of the set

$$\{p \mid a_p \equiv b \mod \ell^m\}?$$

(2) 'Real distribution'.

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

How are the b_p distributed over $[-2, 2]$?

Distribution of coefficients

Fix a Hecke eigenform $f = \sum_{n=1}^{\infty} a_n q^n$.

(1) Distribution modulo ℓ^m.

Answer is given by the Theorem of Chebotarev (1922).

Distribution of coefficients

Fix a Hecke eigenform $f = \sum_{n=1}^{\infty} a_n q^n$.

(1) Distribution modulo ℓ^m.

Answer is given by the Theorem of Chebotarev (1922).

Example: Let f be the Hecke eigenform in our example.

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

Distribution of coefficients

Fix a Hecke eigenform $f = \sum_{n=1}^{\infty} a_n q^n$.

(1) Distribution modulo ℓ^m.

Answer is given by the Theorem of Chebotarev (1922).

Example: Let f be the Hecke eigenform in our example.

P mod p	Frob_p	$\rho(\mathrm{Frob}_p)$	trace	a_p
()()()()()()	identity	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	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	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \begin{pmatrix} 0 & \zeta \\ \zeta^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^2 \\ \zeta & 0 \end{pmatrix}$	0	0

The density of the set $\{p \mid a_p \equiv b \mod 7\}$ equals

b	0	1	2	3	4	5	6
density	$\frac{1}{2}$	0	$\frac{1}{6}$	0	0	0	$\frac{1}{3}$

Distribution of coefficients

Fix a Hecke eigenform $f = \sum_{n=1}^{\infty} a_n q^n$.

(2) 'Real distribution'.

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

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

Distribution of coefficients

Fix a Hecke eigenform $f = \sum_{n=1}^{\infty} a_n q^n$.

(2) 'Real distribution'.

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

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

Nice illustration by Andrew Sutherland.

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?

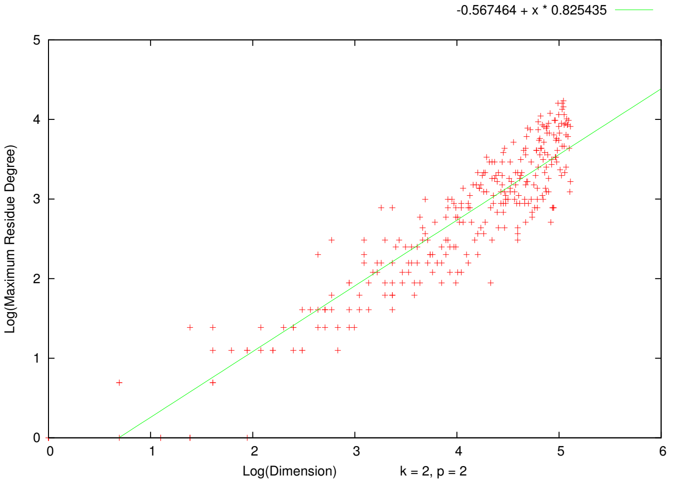
Related: Let f run through all Hecke eigenforms of weight 2 and all prime levels. Are the mod ℓ reductions of all the coefficients of all these forms contained in a finite extension of $\mathbb{F}_\ell$?

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

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

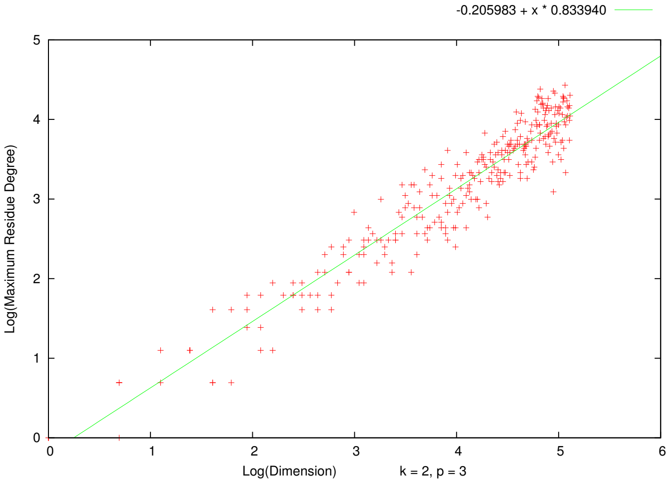
Distribution of coefficients

Degrees of residual coefficient fields mod ℓ for $k = 2$ in prime levels.



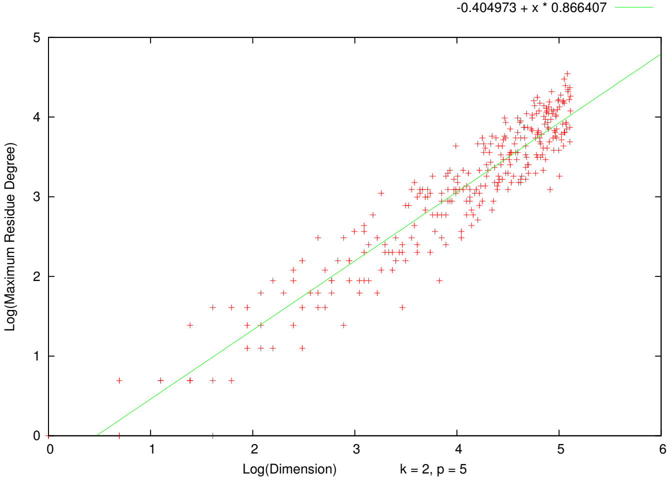
Distribution of coefficients

Degrees of residual coefficient fields mod ℓ for $k = 2$ in prime levels.



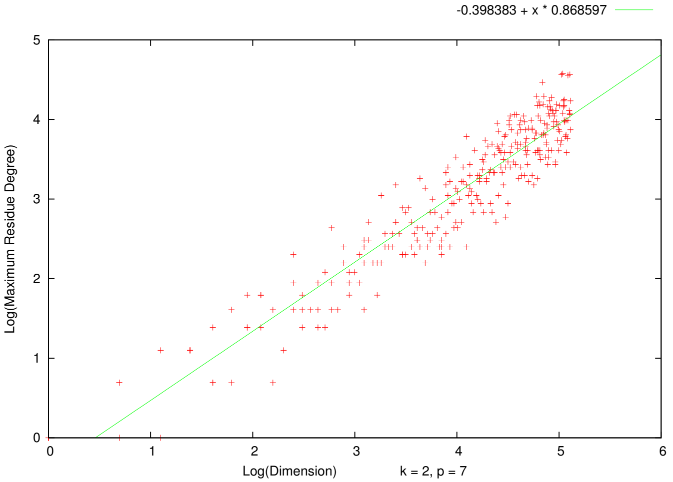
Distribution of coefficients

Degrees of residual coefficient fields mod ℓ for $k = 2$ in prime levels.



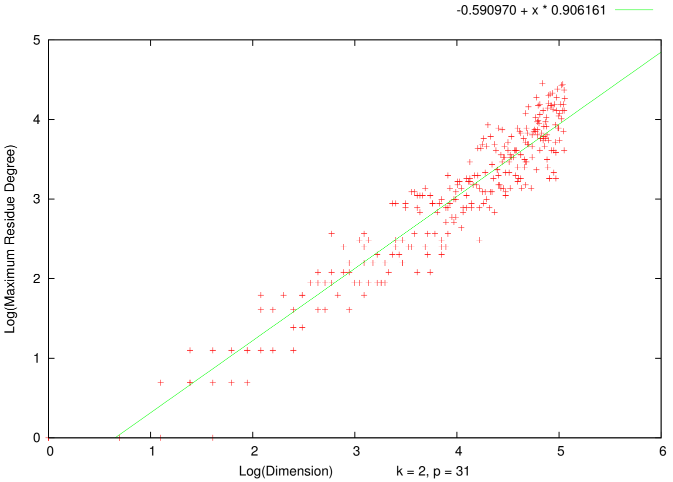
Distribution of coefficients

Degrees of residual coefficient fields mod ℓ for $k = 2$ in prime levels.



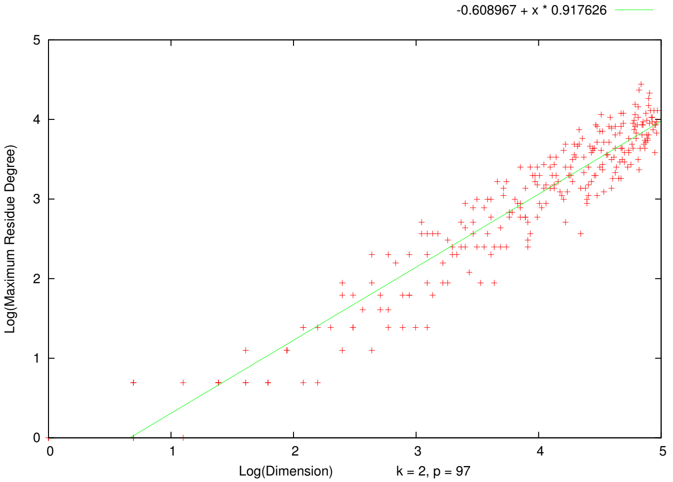
Distribution of coefficients

Degrees of residual coefficient fields mod ℓ for $k = 2$ in prime levels.



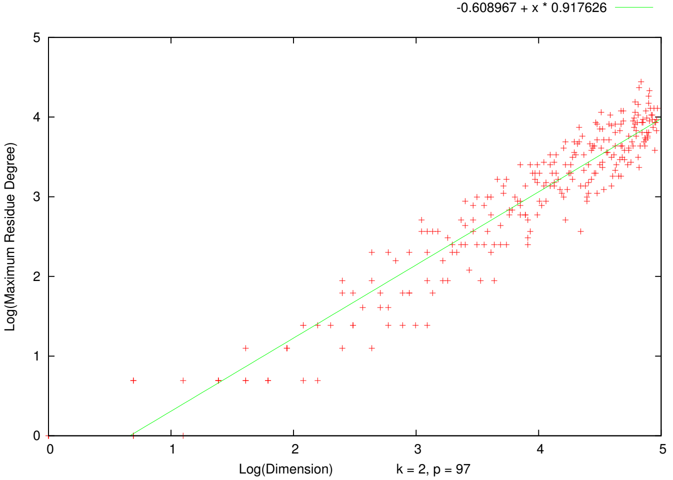
Distribution of coefficients

Degrees of residual coefficient fields mod ℓ for $k = 2$ in prime levels.



Distribution of coefficients

Degrees of residual coefficient fields mod ℓ for $k = 2$ in prime levels.



Any idea?

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?

The ramification of the Galois representation can be (partially) read off from the modular form.

Arithmetic information in ρ_f

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

The ramification of the Galois representation can be (partially) read off from the modular form.

Theorem (Gross, Coleman-Voloch, W.) *If f is of weight one, prime-to-ℓ level and geometrically defined over $\overline{\mathbb{F}}_\ell$, then the attached Galois representation $\overline{\rho}_f$ is unramified at ℓ.*

Moreover, this characterises weight one among all weights (at least if $\ell > 2$).

Arithmetic information in ρ_f

Modular forms have various generalisations. The simplest one are Hilbert modular forms.

Arithmetic information in ρ_f

Modular forms have various generalisations. The simplest one are Hilbert modular forms.

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

Modular forms have various generalisations. The simplest one are Hilbert modular forms.

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.

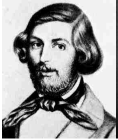
It is believed and partially proved that this characterises parallel weight one forms among all Hilbert Hecke eigenforms.

From Geometry to Number Theory and Back

Geometry/Analysis	Number Theory
Modular Forms	Galois Representations

From Geometry to Number Theory and Back

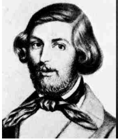
Geometry/Analysis
Modular Forms

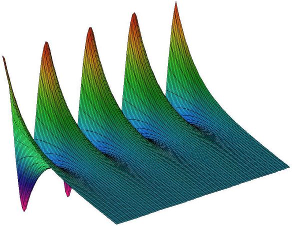


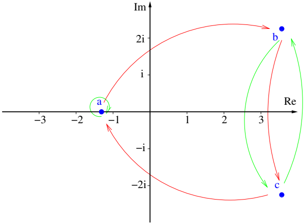
Number Theory
Galois Representations

From Geometry to Number Theory and Back

Geometry/Analysis	Number Theory
Modular Forms	Galois Representations

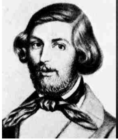




From Geometry to Number Theory and Back

Geometry/Analysis	**Number Theory**
Modular Forms	**Galois Representations**

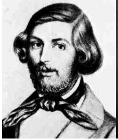



Hecke eigenforms
$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$
with $a_1 = 1$

Galois repres.
$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$
s.t. $\det(\overline{\rho}(\text{compl. conj.})) = -1$

From Geometry to Number Theory and Back

Geometry/Analysis		**Number Theory**
Modular Forms		**Galois Representations**

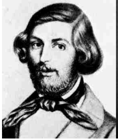



Hecke eigenforms	$\longrightarrow$	Galois repres.
$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$		$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$
with $a_1 = 1$		s.t. $\det(\overline{\rho}(\text{compl. conj.})) = -1$
f	$\mapsto$	$\overline{\rho}_f$
level N		unramified outside $N\ell$
		$\mathrm{Tr}(\overline{\rho}_f(\mathrm{Frob}_p)) = a_p$

Shimura, Deligne, Serre.

From Geometry to Number Theory and Back

Geometry/Analysis		**Number Theory**
Modular Forms		**Galois Representations**



Hecke eigenforms $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$ with $a_1 = 1$	$\longrightarrow$ $\longleftarrow$	Galois repres. $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ s.t. $\det(\overline{\rho}(\text{compl. conj.})) = -1$
f level N	$\mapsto$	$\overline{\rho}_f$ unramified outside $N\ell$ $\mathrm{Tr}(\overline{\rho}_f(\mathrm{Frob}_p)) = a_p$

Shimura, Deligne, Serre.

Serre's Conjecture (1987).

Khare, Wintenberger, Kisin (2009).

The fabulous world of modular forms

From the front page of the
New York Times of 24 June 1993

At Last, Shout of 'Eureka!' In Age-Old Math Mystery

By GINA KOLATA

More than 350 years ago, a French mathematician wrote a deceptively simple theorem in the margins of a book, adding that he had discovered a marvelous proof of it but lacked space to include it in the margin. He died without ever offering his proof, and mathematicians have been trying ever since to supply it.

Now, after thousands of claims of success that proved untrue, mathematicians say the daunting challenge, perhaps the most famous of unsolved mathematical problems, has at last been surmounted.

The problem is Fermat's last theorem, and its apparent conqueror is Dr. Andrew Wiles, a 40-year-old English mathematician who works at Princeton University. Dr. Wiles announced the result yesterday at the last of three lectures given over three days at Cambridge University in England.

Within a few minutes of the conclusion of his final lecture, computer mail messages were winging around the world as mathematicians alerted each other to the startling and almost wholly unexpected result.

Dr. Leonard Adelman of the University of Southern California said he received a message about an hour after Dr. Wiles's announcement. The frenzy is justified, he said. "It's the most exciting thing that's happened in — geez — maybe ever, in mathematics."

Impossible Is Possible

Mathematicians present at the lecture said they felt "an elation," said Dr. Kenneth Ribet of the University of California at Berkeley, in a telephone interview from Cambridge.

The theorem, an overarching statement about what solutions are possible for certain simple equations, was stated in 1637 by Pierre de Fermat, a 17th-century French mathematician and physicist. Many of the brightest minds in mathematics have struggled to find the proof ever since, and many have concluded that Fermat, contrary to his tantalizing claim, had probably failed to develop one despite his considerable

Continued on Page D22, Column 1

Bettmann Archive

Pierre de Fermat, whose theorem may have been proved.

At Last, a 'Eureka!' in an Age-Old Math Mystery

Dr. Andrew Wiles explaining his proof of Fermat's last theorem yesterday at Cambridge University in England.

The fabulous world of modular forms

From the front page of the
New York Times of 24 June 1993

At Last, Shout of 'Eureka!' In Age-Old Math Mystery

By GINA KOLATA

More than 350 years ago, a French mathematician wrote a deceptively simple theorem in the margins of a book, adding that he had discovered a marvelous proof of it but lacked space to include it in the margin. He died without ever offering his proof, and mathematicians have been trying ever since to supply it.

Now, after thousands of claims of success that proved untrue, mathematicians say the daunting challenge, perhaps the most famous of unsolved mathematical problems, has at last been surmounted.

The problem is Fermat's last theorem, and its apparent conqueror is Dr. Andrew Wiles, a 40-year-old English mathematician who works at Princeton University. Dr. Wiles announced the result yesterday at the last of three lectures given over three days at Cambridge University in England.

Within a few minutes of the conclusion of his final lecture, computer mail messages were winging around the world as mathematicians alerted each other to the startling and almost wholly unexpected result.

Dr. Leonard Adelman of the University of Southern California said he received a message about an hour after Dr. Wiles's announcement. The frenzy is justified, he said. "It's the most exciting thing that's happened in — geez — maybe ever, in mathematics."

Impossible Is Possible

Mathematicians present at the lecture said they felt "an elation," said Dr. Kenneth Ribet of the University of California at Berkeley, in a telephone interview from Cambridge.

The theorem, an overarching statement about what solutions are possible for certain simple equations, was stated in 1637 by Pierre de Fermat, a 17th-century French mathematician and physicist. Many of the brightest minds in mathematics have struggled to find the proof ever since, and many have concluded that Fermat, contrary to his tantalizing claim, had probably failed to develop one despite his considerable

Continued on Page D22, Column 1

Bettmann Archive

Pierre de Fermat, whose theorem may have been proved.

At Last, a 'Eureka!' in an Age-Old Math Mystery

Continued From Page A1

Dr. Andrew Wiles explaining his proof of Fermat's last theorem yesterday at Cambridge University in England.

Fermat's Last Theorem:

$$a^n + b^n = c^n$$

for $n \geq 3$,

$$a, b, c \in \mathbb{Z}_{>0}$$

impossible!!!

Thank you for your attention!