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?

| 3 | squares modulo 3: $\{0,1\} ot \ni -1$ |
|----|---------------------------------------|
| 5 | |
| 7 | |
| 11 | |
| 13 | |
| 19 | |
| 23 | |
| 29 | |
| 31 | |
| 37 | |
| | |

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

$$\begin{array}{c|c|c} 3 & -1 & \text{no square mod } 3 \\ 5 & -1 &= 2 \cdot 2 - 5 \\ 7 & 11 & 13 \\ 19 & 23 & \\ 29 & 31 & \\ 37 & \end{array}$$

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

```
\begin{vmatrix} -1 \text{ no square mod } 3 \\ -1 \equiv 2^2 \mod 5 \\ \text{squares modulo } 7: \{0, 1, 2, 4\} \not\supseteq -1 \\ \end{vmatrix}
```



| $\begin{vmatrix} -1 & \text{no square mod } 3 \\ -1 &\equiv 2^2 & \text{mod } 5 \\ 1 & \text{no square mod } 7 \end{vmatrix}$ | , |
|---|---|
| -1 no square mod <i>i</i> | |
| | |
| | |

```
-1 no square mod 3

-1 \equiv 2^2 \mod 5

-1 no square mod 7

squares modulo 11: {0, 1, 3, 4, 5, 9} ₹ -1
```

| 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 | |

 $\begin{array}{c} -1 \text{ no square mod } 3 \\ -1 \equiv 2^2 \mod 5 \\ -1 \text{ no square mod } 7 \\ -1 \text{ no square mod } 11 \\ -1 = 5 \cdot 5 - 2 \cdot 13 \end{array}$

| 3 |
|----|
| 5 |
| 7 |
| 11 |
| 13 |
| 19 |
| 23 |
| 29 |
| 31 |
| 37 |

| -1 no square mod 3 | |
|-------------------------|---|
| $-1 \equiv 2^2 \mod 5$ | |
| -1 no square mod 7 | |
| -1 no square mod 1 | 1 |
| $-1 \equiv 5^2 \mod 13$ | |
| | |
| | |
| | |
| | |
| | |

 $\begin{array}{l} -1 \text{ no square mod } 3 \\ -1 \equiv 2^2 \mod 5 \\ -1 \text{ no square mod } 7 \\ -1 \text{ no square mod } 11 \\ -1 \equiv 5^2 \mod 13 \\ \text{ squares modulo } 19: \ \{0, 1, 4, 5, 6, 7, 9, 11, 16, 17\} \not\supseteq -1 \end{array}$

| 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 | |

| 5 |
|----|
| 5 |
| 7 |
| 11 |
| 13 |
| 19 |
| 23 |
| 29 |
| 31 |
| 37 |
| |

| 3 | -1 no square mod 3 |
|----|------------------------|
| 5 | $-1 \equiv 2 \mod 5$ |
| 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 | |

| 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 | |
| | |

| 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 | |

| 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 | |

| 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 | |

| 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 | $-1 = 31 \cdot 31 - 26 \cdot 37$ |
| | |

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



-1 is a square modulo p \Leftrightarrow p = 2 or $p \equiv 1 \mod 4$.

| 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 $p \equiv 1 \mod 4$.

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

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

Examples. $-1 \equiv 5^2 \mod 13 \Rightarrow X^2 + 1 \equiv (X - 5) \cdot (X + 5) \mod 13.$ 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. 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. $X^2 + 1 \equiv (X - *) \cdot (X + *) = ()() \mod p \Leftrightarrow p \equiv 1, 2 \mod 4.$

Generalisation:

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

Generalisation:

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

| р | 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) |

Generalisation:

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

| р | factorisation |
|-----|---------------|
| 5 | ()()() |
| 13 | ()() |
| 17 | 000 |
| 19 | ()()() |
| 31 | ()() |
| 47 | ()() |
| 53 | ()()() |
| 59 | ()()()()()() |
| 73 | ()() |
| 97 | 000 |
| 101 | ()()()()()() |
| | |

Generalisation:

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

| р | 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)

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)
A modular form is an object from geometry and/or (harmonic) analysis

(according to taste...)

A modular form is an object from geometry and/or (harmonic) analysis

(according to taste...)

Their coefficients are

arithmetically significant.

Modular forms are highly symmetric functions.





Modular forms are highly symmetric functions.





 Complex Analysis: Fourier series with certain transformation properties.

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.

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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

• (special case)
$$f(z+1) = f(z)$$
 for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

• (special case)
$$f(z+1) = f(z)$$
 for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

•
$$f(z) = \sum_{n=0}^{\infty} a_n q^n$$
 where $q = e^{2\pi i z}$.

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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

• (special case)
$$f(z+1) = f(z)$$
 for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

•
$$f(z) = \sum_{n=0}^{\infty} a_n q^n$$
 where $q = e^{2\pi i z}$.

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

Hecke eigenforms are modular forms with special arithmetic.



Erich Hecke (1887-1947)

Hecke eigenforms are modular forms with special arithmetic.



Erich Hecke (1887-1947)

The Fourier coefficients of a Hecke eigenform satisfy

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

Hecke eigenforms are modular forms with special arithmetic.



Erich Hecke (1887-1947)

The Fourier coefficients of a Hecke eigenform satisfy $a_n a_m = a_{nm}$ if gcd(n, m) = 1.

The Fourier coefficients of Hecke eigenforms a_n are algebraic integers.





Gotthold Eisenstein (1823-1852)

Carl Jacobi (1804-1851)





Gotthold Eisenstein (1823-1852)

Carl Jacobi (1804-1851)

Eisenstein series





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

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





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





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

Coefficients: Special zeta-value and divisor function.





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:

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



Evariste Galois (1811-1832)

Idea (Galois): Equations satisfy symmetries.



Evariste Galois (1811-1832)

Idea (Galois): Equations satisfy symmetries.

Algebraically speaking: a symmetry is a field automorphism.

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



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



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.

Another view on Eisenstein series.

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

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

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

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

given by the action on the $\ell\text{-power roots}$ of unity:

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

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

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: $\chi(Frob_p) = p$.

Consider the reducible semi-simple Galois representation

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

In particular,

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

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: $\chi(Frob_p) = p$.

Consider the reducible semi-simple Galois representation

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

In particular,

$$\rho(\mathsf{Frob}_p) = \begin{pmatrix} 1 & 0 \\ 0 & \chi^{k-1}(\mathsf{Frob}_p) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p^{k-1} \end{pmatrix}$$
$$\Rightarrow \operatorname{Tr}(\rho(\mathsf{Frob}_p)) = 1 + p^{k-1} = \sigma_{k-1}(p).$$

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

Another view on Eisenstein series.

Fix a prime ℓ .

We constructed a Galois representation

$$ho = 1 \oplus \chi^{k-1} : \mathcal{G}_{\mathbb{Q}} o \operatorname{GL}_2(\mathbb{Z}_{\ell}), \ \
ho(\sigma) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \chi^{k-1}(\sigma) \end{smallmatrix}
ight)$$

such that

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

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

Another view on Eisenstein series.

Fix a prime ℓ .

We constructed a Galois representation

$$ho = 1 \oplus \chi^{k-1} : \mathcal{G}_{\mathbb{Q}} o \operatorname{GL}_2(\mathbb{Z}_{\ell}), \ \
ho(\sigma) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \chi^{k-1}(\sigma) \end{smallmatrix}
ight)$$

such that

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

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

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

One says that ρ is attached to the Eisenstein series.

Geometry/Analysis Modular Forms Number Theory Galois Representations

Geometry/Analysis Modular Forms



Number Theory Galois Representations



Geometry/Analysis Modular Forms



Number Theory Galois Representations





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



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

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



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

f level N $\begin{array}{ll} \mapsto & \rho_f \\ & \text{unramified outside } N\ell \\ & \mathsf{Tr}(\rho_f(\mathsf{Frob}_p)) = a_p \end{array}$

Shimura, Deligne, Serre.

Inverse Galois Problem



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

Hilbert


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

Hilbert

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



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

Hilbert

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.



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

Hilbert

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).



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

Hilbert

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.

| р | 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 | / doe | es $P(X) = X^6 - 6X^4 + 9X^2 + 23$ factor modulo p? |
|-----|-------|---|
| | p | factorisation |
| _ | 5 | |
| | 13 | ()() |
| | 17 | ()()() |
| | 19 | ()()() |
| | 31 | ()() |
| | 47 | ()() |
| | 53 | ()()() |
| | 59 | ()()()()()() |
| | 73 | ()() |
| | 97 | ()()() |
| | 101 | ()()()()() |

| р | factorisation | ap |
|-----|----------------|----|
| 5 | ()()() | 0 |
| 13 | ()() | -1 |
| 17 | ()()() | 0 |
| 19 | 000 | 0 |
| 31 | ()() | -1 |
| 47 | ()() | -1 |
| 53 | ()()() | 0 |
| 59 | ()()()()()() | 2 |
| 73 | ()() | -1 |
| 97 | 000 | 0 |
| 101 | ()()()()()()() | 2 |
| | | 1 |

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 $\Leftrightarrow a_p = 2$.

| р | factorisation | ap |
|-----|---------------|----|
| 5 | 000 | 0 |
| 13 | ()() | -1 |
| 17 | 000 | 0 |
| 19 | ()()() | 0 |
| 31 | ()() | -1 |
| 47 | ()() | -1 |
| 53 | ()()() | 0 |
| 59 | ()()()()()() | 2 |
| 73 | ()() | -1 |
| 97 | 000 | 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 .

| р | factorisation | a _p |
|-----|---------------|----------------|
| 5 | ()()() | 0 |
| 13 | ()() | -1 |
| 17 | ()()() | 0 |
| 19 | ()()() | 0 |
| 31 | ()() | -1 |
| 47 | 00 | -1 |
| 53 | ()()() | 0 |
| 59 | ()()()()()() | 2 |
| 73 | ()() | -1 |
| 97 | 000 | 0 |
| 101 | 000000 | 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 | $\rho(Frob_p)$ | 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 |

| р | factorisation | a _p |
|-----|---------------|----------------|
| 5 | ()()() | 0 |
| 13 | ()() | -1 |
| 17 | ()()() | 0 |
| 19 | 000 | 0 |
| 31 | 00 | -1 |
| 47 | 00 | -1 |
| 53 | 000 | 0 |
| 59 | ()()()()()() | 2 |
| 73 | ()() | -1 |
| 97 | 000 | 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 | $\rho(Frob_p)$ | 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 |

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

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

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!!

- 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:

- (1) How are the a_p distributed?
- (II) What information is contained in the Galois representation?

Arithmetic significance of coefficients of modular forms

Natural questions:

- (1) 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?

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

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

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

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]?

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).

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 | $\rho(Frob_p)$ | 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 | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta \\ \zeta^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^2 \\ \zeta & 0 \end{pmatrix}$ | 0 | 0 |

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.

| <i>P</i> mod <i>p</i> | Frob _p | $\rho(Frob_p)$ | 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 | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta \\ \zeta^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^2 \\ \zeta & 0 \end{pmatrix}$ | 0 | 0 |

- 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).

- 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.

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

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)

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?

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}_{ℓ} ?

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}_{ℓ} ?

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

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}_{ℓ} ?

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.

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



-0.567464 + x * 0.825435

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



-0.205983 + x * 0.833940

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



-0.404973 + x * 0.866407

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



-0.398383 + x * 0.868597

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



-0.590970 + x * 0.906161
Distribution of coefficients

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



-0.608967 + x * 0.917626

Distribution of coefficients

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



-0.608967 + x * 0.917626

Any idea?

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

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.

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 $\ell > 2$).

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

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

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

is unramified above ℓ .

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

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

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















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



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



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



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

 $\begin{array}{ccc} f & \mapsto & \overline{\rho}_f \\ \text{level } N & & \text{un} \end{array}$

 $\overline{
ho}_{f}$ unramified outside $N\ell$ $\operatorname{Tr}(\overline{
ho}_{f}(\operatorname{Frob}_{p})) = a_{p}$

Shimura, Deligne, Serre.



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





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

 $egin{array}{lll} \mapsto & \overline{
ho}_f \ & ext{unramified outside } N\ell \ & ext{Tr}(\overline{
ho}_f(ext{Frob}_p)) = a_p \end{array}$

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 'Eurekal' In Age-Old Math Mystery

By GINA KOLATA

More than 210 years agn, a prench mathematician wrote a deceptively simple theorem in the mergins of a book, adding that he addiscovered a marveleus proof of it but lacked space to include in the margins. He died writhout ever affering his proof, and mathmatician, have been trying ever direct to supply it. New, after theoremults of claims.

Now, after thorasauds of claims of success that proved untrue, mathematicians say the duasting challenge, perhaps the most famoas of unsalved mathematical problems, bis at last been surmounted.

The problem is Fermat's last theorem, and its apparent congueror is Dr. Andrew Wiles, a 40year-old English mathematician



Pierrs de l'ermat, whoat theorem may have been proved.

scho works at Princeton University. Dr. Wiles amounced the result yesterday at the last of three lactures given over three days at Cambridge University in England.

Wahin a few minutes of the conclusion of his final locatore, computer mail messages were winging around the world as mathematicians idented each other to the startling and almost wholy unexpected result.

Impossible Is Possible

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

The discrete, an overaching statement vious what solutions are possible for certain simple equation, was stated in 1677 by Petre de Perrant, a 17th-century Petre de Petrant, a 17th-century petro en describe have strugged to classin, hed probably failed to devision ene describe his considerable

Continued on Page D22, Column 1

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

CREATING TOOL Page 42

"Biblioscience Laboration - Configuration - The Construction of the State and The Construction of the State and Bibliogenetic Association - State and the State and State and Bibliogenetic Association - State and the State and State and State and the State and State and State and State and the State and St

Tomorium Prosperiol Prevent 's soit them stilled to the sesources of the formula of the strength sources of the formula of the strength of the spoore of the couplet of "sources" of a single suggest of the second of the spoore citize to shall all the starting of the spoore citize to shall all the starting of the spoore citize to shall all the starting of the spoore citize to shall all the starting of the spoore citize to shall all the starting of the spoore citize to shall all the starting to the spoore citize to shall all the starting to the spoore citize to shall all the starting to the spoore citize to shall all the starting to the spoore citize

• 2. 30 June dependent states the dependent of the dependent states of the dependent of the dependent states of the dependent of the dependent states of the states of the magnitude of the dependent states of the dependent of the dependent of the dependent states of the dependent of the dependent of the dependent states of the dependent of the dependent of the dependent states of the dependent of the dependent of the dependent states of the dependent of the dependent of the dependent states of the dependent of the dependent of the dependent of the dependent states of the dependent of the dependent

Torpeda Last Theorem Market States Market St

[1] Simple and Simp

(b) (per la construction) postalité incluent qual que particule de performantion de la construction de la contempo de la construction de la construction de la construction de la construction de la contempo de la construction de la constructi

the second to used that the Willing and an address the three mains and the second second second second second α manufa in contra transmission de la contra de la con

(b) Control of the second s

Testanas Call to Dote!

Dr. 19 Ku, and Ku, Thursdon, J. 20 Ku, and K. 20 Ku, an

And the second s

ted transmission and the kendbh mailthe s pain due ted to 10° De Redered Andre semeritable segre b, but

Weid inserts data September 2018 Biological Control Control Control Control of the prevent of machine inserts of the machine of the prevent of machine inserts of the retrieved to the start data of the the retrieved to the start data of the start of the prevent of the start o

ELGLAR, It is briefing when since a reaction in the second s

(all here is note in second to be been

the second secon

more, the local black They "Here type is any encoded, a application black and black of any encoded a application. Baseline a set of the second and the second application of the flatter and the second application of the flatter application of the second application of the second



The Anticum White completions it is read of Persistin the inscrete parameter as Cambridge Descretering in Multiple.

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 210 years agn, a prench mathematician wrote a deceptively simple theorem in the mergins of a book, adding that he addiscovered a marveleus proof of it but lacked space to include in the margins. He died writhout ever affering his proof, and mathmatician, have been trying ever direct to supply it. New, after theoremults of claims.

Now, after thousands of claims of success that proved unrole, mathematicians say the data ting challenge, perhaps the most famoust of unsalved mathematical problems, bis at last been surmounted.

The problem is Permat's last theorem, and its apparent congueror is Dr. Andrew Wiles, a 40year-old English mathematician



Pierrs de Fermat, whoat theorem may have been proved.

who works at Princeton University. Dr. Wiles amounced the result yesterday at the last of three lactures given over three days at Cambridge University in England.

Wahin a few minutes of the conclusion of his final locatore, computer mail messages were winging around the world as mathematicians idented each other to the startling and almost wholy unexpected result.

Dr. Lecawrd Ademan of the University of Southern California and be repetived a message about an hour after Dr. Wiley's unnouncement. The frenty is justified, he said. "It's the most excliing, thing that's happened in ger, --maybe ever, is mathematies."

Impossible Is Possible

Mathematicians présent às the lecture said they feit "an elation," said Dr. Kenneth Ribet of the University of California at Berlorley, in a téléphone interview from Cambridge.

This therean, an overaching statement yhou, what solutions are possible for certain simple equation, was stated in 1677 by Pretre de Pernan, a 17th-century Pretre de Pernan, a 17thcentury for the proof even ince, and in mothematics have struggled to field the proof even ince, and in mothematics have struggled to field the proof even ince, and provide the descent in the structure vision per descent his considerable

Continued on Page D22, Column 1

At Last, a 'Eurekal' in an Age-Oid Math Mystery

CREATING TOOL Page 42

"Biblioscience Laboration - Configuration - Co

Environment Processoriel Terrene V des Bernes et Molt V & VYN southeast of the Ferrer of the VYN the southeast of the Ferrer of the VYN of the southeast of the VYN and VYN the southeast of the transition of the VYN and the southeast of the southeast of the southeast of the transit of the locations of the southeast of the

¹ Province, and property strates the determinant of the strates and constraints of the strates and the strates of the strates of the strates of the strates of the strates would be strate at the strates of the st

Terpeta Last Terpeta Last Terpeta Last Seguidante

Interface a control provident characteristic (2) Completion and characteristic) and the control of the control of the control of the control of the Characteristic (2) Completion and the Characteristic (2) Completion (2) Comp

Intering the Mericle Could bet your to ward thick for Winfeld and a databate for the small being man then with a black way a databate To data the support of the small of the the small and the support of the small for the small of the support of the small party and and the strengt of the small states and the strengt of the small of the foregoing water is in the black counts water in the strengt of the strengt of the strengt water is in the black counts water is the strengt of the str and in the second secon

Berry, and Konstein Verfahrt herpiteligt windig par in Cherr Sector of Sectore reverse, wer in Association in Sectore manadrows, 2008/09 Meter VI Meter-meterse auxiliar Ortho 1988 Weiter-meterse auxiliar Ortho 1988 Weiter-meterse auxiliar Ortho 1988 Weiter-meterse auxiliarity of Sectore of Press, weiter auxiliarity of Sectore Press, Sectore 2019, weiter science of a pageont press.

Transact Field in Deef 1 De 11 the and det 7 Proceedings where more development with Latt 2 pays where more development and 2 pays or and 2 pays and 2 pays of a resultant where the standard of the set of a resultant where the standard of the set of a resultant where the standard of the set of a resultant where the standard of the set of a resultant where the standard of the set of a resultant where the standard of the set of the

2. A. Valor party from the step of these references in the Train to the second step of the second step to a set based on the second step of the

and the second state of the second state of

explored in 1997 for Extended and the calculate rise, for the function of the the second second second second forms the and the full indices the Person (1997) for the second second second Person (1997) for the second second for a large design field field for and field cates of the two functions of the second second second for the second second second for the second second second for the second second second second for the second second second second for the second sec

conditions path day being 10° Dibottower south a securitable segres to that south a securitable segres to that

big the generation of markmake tab. where A 20 as a calculated by a restructure of the calculated by a redifference of the calculated by a second by the restructure of the calculated by the calculated by a second by a second by the calculated by the calculated

Contrast, et als descent som i formanne descenters indere i descente at de 70met opsicilités à problet care soutre problet. Une parte mouse au signation de la contrastante des descentes de la contrastante descentes de la contrastante de

Br film out 5 net in Gebermann gener in mite fin seeling fr 100 1 1.1. Construction of the second se

more the largest told. They will be a server and a application will be addenation and a sequence of the addention of the sequence of the addentic of the sector of the addentic of the sector of the addentic of the sector of the sector of the first sector of the sector of the first sector of the sec



The Antisene White seminary in such of Persists the charges



Thank you for your attention!