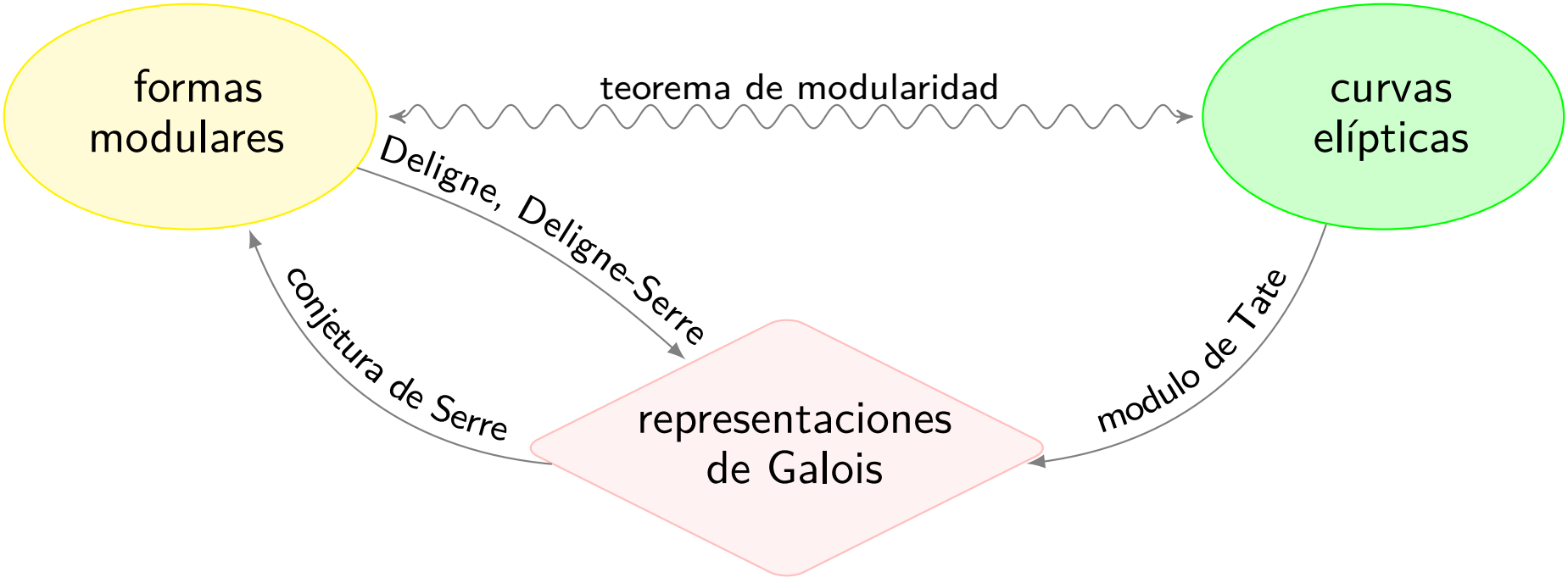
# La conjetura de modularidad de Serre

Marta Sánchez Pavón

Facultad de Matemáticas US

Octubre 2024

# Contexto




- Serre, 1975: *Valeurs propres des opérateurs de Hecke modulo* $\ell$.
- Serre, 1987: *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

# Representaciones de Galois módulo $p$

Fijamos clausuras algebraicas $\overline{\mathbb{Q}}$ y $\overline{\mathbb{F}}_p$, y denotamos $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

**Definición**

Sea $V$ un $\overline{\mathbb{F}}_p$-espacio vectorial. Una *representación de Galois módulo $p$* es un homomorfismo continuo

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}(V).$$

- La imagen $\rho(G_{\mathbb{Q}})$ es finita.
- $\mathrm{Aut}(V) \cong \begin{cases} \mathrm{GL}_2(\overline{\mathbb{F}}_p) & \text{si } \dim(V) = 2 \\ \mathrm{GL}_1(\overline{\mathbb{F}}_p) \cong \overline{\mathbb{F}}_p^{\times} & \text{si } \dim(V) = 1. \end{cases}$
- $\rho$ está determinada (salvo conjugación) por

$$\mathrm{tr}\,\rho(\mathrm{Frob}_\ell) \text{ y } \det\rho(\mathrm{Frob}_\ell),$$

para todo primo $\ell$ salvo un número finito de ellos.

# Representaciones irreducibles e impares

## Definiciones

Sea $\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}(V)$ una representación de Galois módulo $p$.

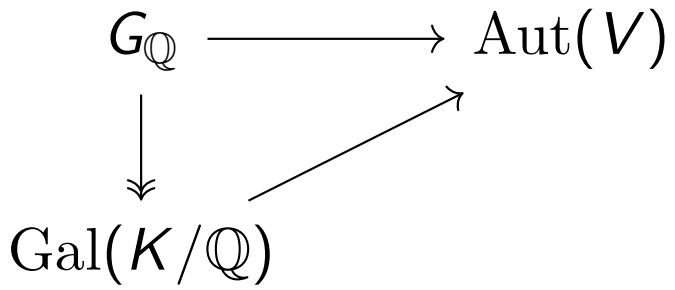
- Si existe un subespacio $W \subset V$ invariante por la acción de $\rho$, se dice que $\rho$ *admite una subrepresentación* $\rho^W\colon G_{\mathbb{Q}} \to \mathrm{Aut}(W)$.
- $\rho$ se dice *irreducible* si no admite subrepresentaciones propias no triviales.
- $\rho$ se dice *semisimple* si se descompone en suma directa de subrepresentaciones irreducibles.
- Después de fijar una inclusión $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, se dice que $\rho$ es *impar* si

$$\det \rho(c) = -1,$$

donde $c$ es la conjugación compleja.

# Ramificación

Sea $\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}(V)$ una representación de Galois módulo $p$. Como $\rho(G_{\mathbb{Q}})$ es finita, existe una extensión finita de Galois $K/\mathbb{Q}$ tal que




Dado un primo $\ell$, existen ideales primos $\mathfrak{l}_1, \ldots, \mathfrak{l}_r \subset \mathcal{O}_K$ tales que

$$(\ell)\mathcal{O}_K = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_r^{e_r} = (\mathfrak{l}_1 \cdots \mathfrak{l}_r)^e \text{ de manera única.}$$

**Definición**

Se dice que $\rho$ es *no ramificada en* $\ell$ si $e = 1$.

Además, $\rho$ es no ramificada fuera de un conjunto finito de primos.

# Grupo modular

Sea $\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. El grupo modular $\mathrm{SL}_2(\mathbb{Z})$ actúa en $\mathcal{H}$ mediante *transformaciones de Möbius*:

$$\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathcal{H}$$

$$M(z) = \frac{az+b}{cz+d} \text{ para toda } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Para todo entero positivo $N$, consideramos el subgrupo normal

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\} \lhd \mathrm{SL}_2(\mathbb{Z}).$$

# Formas cuspidales

Fijamos enteros positivos $N$ y $k$, y un carácter de Dirichlet

$$\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times.$$

## Definición

Una *forma cuspidal de peso $k$, nivel $N$ y carácter $\varepsilon$* es una función holomorfa $f\colon \mathcal{H} \to \mathbb{C}$ tal que:

- $f(M(z)) = \varepsilon(d)(cz+d)^k f(z)$ para todo $M \in \Gamma_0(N)$ y todo $z \in \mathcal{H}$.
- $f$ se anula en las cúspides.

$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, luego $f(z+1) = f(z)$ para todo $z \in \mathcal{H}$. Por tanto,

$$f(z) = \sum_{n\in\mathbb{Z}} \sum_{n=1}^{\infty} a_n(f) q^n, \text{ con } q = e^{2\pi i z}.$$

Si $a_1(f) = 1$, se dice que $f$ está *normalizada*.

# Autoformas cuspidales

- El conjunto $\mathcal{S}_k(N, \varepsilon)$ de formas cuspidales de peso $k$, nivel $N$ y carácter $\varepsilon$ es un $\mathbb{C}$-espacio vectorial de dimensión finita.
- Para cada primo $\ell$, se define el $\ell$-ésimo *operador de Hecke*

$$T_\ell \colon \mathcal{S}_k(N, \varepsilon) \to \mathcal{S}_k(N, \varepsilon).$$

**Definición**

Una forma cuspidal $f \in \mathcal{S}_k(N, \varepsilon)$ es una *autoforma* si es un autovector para todos los operadores de Hecke $T_\ell$, simultáneamente.

**Propiedad**

Si $f \in \mathcal{S}_k(N, \varepsilon)$ es una autoforma normalizada, entonces

$$a_n(f) \in \overline{\mathbb{Z}} \text{ para todo } n \geq 1.$$

# Reducción de formas cuspidales

- Fijamos un entero positivo $N$ coprimo con $p$, un entero $k \geq 2$, y un carácter de Dirichlet $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$.
- Fijamos inclusiones $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ y $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. La segunda induce un homomorfismo reducción $\widetilde{\cdot}\,: \overline{\mathbb{Z}} \to \overline{\mathbb{F}}_p$.
- $\varepsilon_0\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Z}}^\times$ es el único carácter tal que $\widetilde{\varepsilon_0} = \varepsilon$.

## Definición

Una *forma cuspidal con coeficientes en* $\overline{\mathbb{F}}_p$ *de peso* $k$*, nivel* $N$ *y carácter* $\varepsilon$ es una serie formal

$$f = \sum_{n=1}^{\infty} a_n(f) q^n, \text{ con } a_n(f) \in \overline{\mathbb{F}}_p,$$

tal que existe una forma cuspidal $F \in \mathcal{S}_k(N, \varepsilon_0)$ con coeficientes de Fourier en $\overline{\mathbb{Z}}$ verificando $\widetilde{a_n(F)} = a_n(f)$ para todo $n \geq 1$.

# Reducción de autoformas cuspidales

El conjunto $\widetilde{\mathcal{S}}_k(N,\varepsilon)$ de formas cuspidales de peso $k$, nivel $N$ y carácter $\varepsilon$ es un $\overline{\mathbb{F}}_p$-espacio vectorial de dimensión finita tal que

$$\dim_{\overline{\mathbb{F}}_p}(\widetilde{\mathcal{S}}_k(N,\varepsilon)) = \dim_{\mathbb{C}}(\mathcal{S}_k(N,\varepsilon_0)).$$

**Definición**

Se dice que $f \in \widetilde{\mathcal{S}}_k(N,\varepsilon)$ es una *autoforma normalizada* si existe una autoforma normalizada $F \in \mathcal{S}_k(N,\varepsilon_0)$ tal que $\widetilde{a_n(F)} = a_n(f)$ para todo $n \geq 1$.

# Representaciones asociadas a autoformas

## Teorema de Deligne, 1971

Sea $f \in \widetilde{\mathcal{S}}_k(N, \varepsilon)$ autoforma normalizada. Existe una única representación de Galois $\rho_f \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ tal que:

- $\rho_f$ es semisimple e impar.
- $\rho_f$ es no ramificada fuera de $Np$.
- Para todo primo $\ell$ tal que $\ell \nmid Np$, se verifica

$$\operatorname{tr} \rho_f(\mathrm{Frob}_\ell) = a_\ell(f) \quad \text{y} \quad \det \rho_f(\mathrm{Frob}_\ell) = \varepsilon(\ell)\ell^{k-1}.$$

Se tiene un resultado similar para $k = 1$ (Deligne-Serre, 1974).

# Conjetura de modularidad de Serre

**Conjetura de modularidad de Serre (Khare-Wintenberger, 2008)**

Dada una representación de Galois $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ impar e irreducible, existe una autoforma cuspidal $f$ normalizada con coeficientes en $\overline{\mathbb{F}}_p$ tal que $\rho \cong \rho_f$.

- Existen $N(\rho)$, $k(\rho)$ y $\varepsilon(\rho)$ tales que $f \in \widetilde{S}_{k(\rho)}(N(\rho), \varepsilon(\rho))$.
- Si $g \in \widetilde{S}_k(N, \varepsilon)$ es otra autoforma normalizada tal que $\rho \cong \rho_g$,

$$N(\rho) \mid N \quad \text{y} \quad k \geq k(\rho).$$

- $N(\rho) \geq 1$ es coprimo con $p$ y depende de la ramificación de $\rho$ fuera de $p$.
- $k(\rho) \geq 2$ depende de la ramificación de $\rho$ en $p$.
- $\varepsilon(\rho)\colon (\mathbb{Z}/N(\rho)\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ es tal que $\det \rho = \varepsilon(\rho)\chi_p^{k(\rho)-1}$.

# Ejemplo con SageMath y LMFDB

Sean:

- $g(x) = x^4 - 4x^2 + 5$, con raíces

$$\alpha_1 = \sqrt{2+i}, \quad \alpha_2 = \sqrt{2-i}, \quad \alpha_3 = -\alpha_1, \quad \alpha_4 = -\alpha_2.$$

- $K = \mathbb{Q}(\alpha_1, \alpha_2)$ cuerpo de descomposición de $g$ sobre $\mathbb{Q}$.
- $G = \mathrm{Gal}(K/\mathbb{Q})$.

Calculamos:

- $G = D_8 = \langle \sigma, \tau \rangle$, donde

$$(\alpha_1, \alpha_2) \overset{\sigma}{\mapsto} (\alpha_2, -\alpha_1) \quad \text{y} \quad (\alpha_1, \alpha_2) \overset{\tau}{\mapsto} (\alpha_1, -\alpha_2).$$

- Los primos que dividen al discriminante $\Delta_K$: 2 y 5.
- Elegimos un primo $p$ distinto de 2 y 5. Por ejemplo, $p = 3$.

- Definimos el homomorfismo

$$\overline{\rho}\colon G \to \mathrm{GL}_2(\mathbb{F}_3)$$

$$(\sigma, \tau) \mapsto \left( \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right).$$

- El homomorfismo $\overline{\rho}$ induce una representación de Galois **impar** e **irreducible**

$$\rho\colon G_{\mathbb{Q}} \to G \xrightarrow{\overline{\rho}} \mathrm{GL}_2(\mathbb{F}_3),$$

luego podemos aplicar la conjetura de modularidad de Serre: $\rho$ proviene de una autoforma cuspidal normalizada con coeficientes en $\overline{\mathbb{F}}_3$.

- Calculamos con SageMath los grupos de ramificación alta de $G$ en $\ell = 2, 5$, y la dimensión de los subespacios de $\mathbb{F}_3^2$ fijos por dichos grupos. Obtenemos $\boldsymbol{N(\rho) = 2^6 \cdot 5^1 = 320}$.
- Como $\rho$ es no ramificada en $p = 3$, entonces $\boldsymbol{k(\rho) = 3}$.
- Como $\det \rho(G_{\mathbb{Q}}) \cong \mathbb{F}_3^\times \cong (\mathbb{Z}/2\mathbb{Z})$, entonces $\boldsymbol{\varepsilon(\rho)}\colon (\mathbb{Z}/\mathbf{320}\mathbb{Z})^\times \to \overline{\mathbb{F}}_{\mathbf{3}}^\times$ es un carácter de **orden 2**.

# LMFDB: https://www.lmfdb.org

LMFDB

⌂

Citation · Feedback · Hide Menu

## The L-functions and modular forms database (LMFDB)

**Introduction**
Overview Random
Universe Knowledge

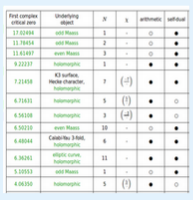
**L-functions**
Rational All

**Modular forms**
Classical Maass
Hilbert Bianchi

**Varieties**
Elliptic curves over $\mathbb{Q}$
Elliptic curves over $\mathbb{Q}(\alpha)$
Genus 2 curves over $\mathbb{Q}$
Higher genus families
Abelian varieties over $\mathbb{F}_q$

**Fields**
Number fields
$p$-adic fields

**Representations**
Dirichlet characters
Artin representations



### A database

The LMFDB is a database of mathematical objects arising in number theory and arithmetic geometry that illustrates some of the mathematical connections predicted by the Langlands program.

Click a heading on the left to browse, or go to a random page.

### Announcements

The first LuCaNT conference took place July 10-14, 2023 at ICERM. Thanks to everyone who attended! Conference proceedings will be published soon.

Check out the recently updated abstract groups database [beta].

Check out the new modular curves database [beta].


### Learn more

Information is available regarding the source, reliability, and completeness of the database.

Knowls provide explanations when you need them.

Overview LMFDB universe Knowledge Data

### Citations and acknowledgments

- How to cite the LMFDB
- Source code repository
- Editorial board
- Acknowledgments

## Search

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Level | | 320 | e.g. 4, 1-20 | Weight | any parity | 3 | e.g. 2, 4-8 |
| Bad $p$ | include | 2,3 | e.g. 2,3 | Character | any parity | 20.d | e.g. 20.d |
| Character order | | 2 | e.g. 1, 2-4 | Primitive character | | 1.a | e.g. 1.a |
| Dimension | absolute | 1 | e.g. 2, 1-6 | Is maximal/largest | | | |
| Analytic conductor | | 1-10 | e.g. 1-10 | Analytic rank | | 1 | e.g. 1, 2-4 |
| Coefficient field | | 1.1.1.1 | e.g. 2.0.5.1, Qsqrt5 | Is self-dual | | | |
| Coefficient ring index | | 1 | e.g. 1, 2-4 | Coefficient ring gens. | | 20 | e.g. 7, 1-10 |
| CM/RM discriminant | | -3 | e.g. -3 | Self-twists | any CM | any RM | |
| Inner twist count | | 1- | e.g. 0, 1-, 2-3 | Is twist minimal | | | |
| Results to display | | 50 | | Projective image | | Dn | A5, D7, or Dn; weight 1 only |

Display: List of forms | Dimension table | Traces table | Random form

Search again | Dimension table | Traces table | Random form | Sort order: ▲ analytic conductor | Select: columns to display

**Results (15 matches)** Download displayed columns for all results to Text

| Label | Dim | $A$ | Field | CM | Traces $a_2$ | $a_3$ | $a_5$ | $a_7$ | $q$-expansion |
|---|---|---|---|---|---|---|---|---|---|
| 320.3.b.a | 4 | 8.719 | $\mathbb{Q}(\sqrt{-3},\sqrt{5})$ | None | 0 | 0 | 0 | 0 | $q+\beta_2q^3-\beta_1q^5+\beta_3q^7+(-9+6\beta_1+\cdots)q^9+\cdots$ |
| 320.3.b.b | 4 | 8.719 | $\mathbb{Q}(i,\sqrt{5})$ | None | 0 | 0 | 0 | 0 | $q-\beta_1q^3+\beta_3q^5+(\beta_1-4\beta_2)q^7+(-5+\cdots)q^9+\cdots$ |
| 320.3.b.c | 4 | 8.719 | $\mathbb{Q}(\zeta_{10})$ | None | 0 | 0 | 0 | 0 | $q+\zeta_{10}^3q^3+\zeta_{10}^2q^5+(-\zeta_{10}+\zeta_{10}^3)q^7+\cdots$ |
| 320.3.b.d | 4 | 8.719 | $\mathbb{Q}(i,\sqrt{5})$ | None | 0 | 0 | 0 | 0 | $q+\beta_1q^3-\beta_2q^5-\beta_1q^7+(3+2\beta_2+\cdots)q^9+\cdots$ |
| 320.3.e.a | 8 | 8.719 | 8.0.$\cdots$.3 | None | 0 | 0 | 0 | 0 | $q-\beta_5q^3+(-\beta_4-\beta_6)q^5+\beta_2q^7+\cdots$ |
| 320.3.e.b | 16 | 8.719 | $\mathbb{Q}[x]/(x^{16}+\cdots)$ | None | 0 | 0 | 0 | 0 | $q+\beta_1q^3+\beta_4q^5-\beta_{11}q^7+(-6-\beta_5+\cdots)q^9+\cdots$ |
| 320.3.g.a | 8 | 8.719 | 8.0.12960000.1 | None | 0 | 0 | 0 | 0 | $q-\beta_2q^3-\beta_6q^5+(-3\beta_4-\beta_5)q^7+\cdots$ |
| 320.3.g.b | 8 | 8.719 | 8.0.2342560000.1 | None | 0 | 0 | 0 | 0 | $q+\beta_3q^3-\beta_4q^5+(-2\beta_5-\beta_7)q^7+\cdots$ |
| 320.3.h.a | 1 | 8.719 | $\mathbb{Q}$ | $\mathbb{Q}(\sqrt{-5})$ | 0 | −4 | 5 | −4 | $q-4q^3+5q^5-4q^7+7q^9-20q^{15}+\cdots$ |
| 320.3.h.b | 1 | 8.719 | $\mathbb{Q}$ | $\mathbb{Q}(\sqrt{-5})$ | 0 | 4 | 5 | 4 | $q+4q^3+5q^5+4q^7+7q^9+20q^{15}+\cdots$ |
| 320.3.h.c | 2 | 8.719 | $\mathbb{Q}(\sqrt{5})$ | $\mathbb{Q}(\sqrt{-5})$ | 0 | 0 | −10 | 0 | $q-\beta q^3-5q^5-3\beta q^7+11q^9+5\beta q^{15}+\cdots$ |
| 320.3.h.d | 2 | 8.719 | $\mathbb{Q}(\sqrt{-1})$ | $\mathbb{Q}(\sqrt{-1})$ | 0 | 0 | −6 | 0 | $q+(-3+i)q^5-9q^9-6iq^{13}-4iq^{17}+\cdots$ |
| 320.3.h.e | 4 | 8.719 | $\mathbb{Q}(\sqrt{2},\sqrt{-3})$ | None | 0 | 0 | 4 | 0 | $q+\beta_1q^3+(1+\beta_2)q^5-3\beta_1q^7-q^9+\cdots$ |
| 320.3.h.f | 6 | 8.719 | 6.0.1827904.1 | None | 0 | −4 | 2 | 12 | $q+(-1-\beta_1)q^3+\beta_3q^5+(2+\beta_3-\beta_4+\cdots)q^7+\cdots$ |
| 320.3.h.g | 6 | 8.719 | 6.0.1827904.1 | None | 0 | 4 | 2 | −12 | $q+(1+\beta_1)q^3+(1+\beta_1+\beta_3)q^5+(-2+\cdots)q^7+\cdots$ |

Ahora bien, $\rho$ no proviene de la reducción en $\overline{\mathbb{F}}_3$ de todas estas.

- Por el teorema de Deligne, si $\rho$ proviene de $f \in \widetilde{S}_3(320, \varepsilon(\rho))$, entonces

$$\operatorname{tr} \rho(\mathrm{Frob}_\ell) = a_\ell(f) \text{ para todo } \ell \notin \{2, 3, 5\}$$

- Calculamos con SageMath el conjunto de los primeros primos que son totalmente descompuestos en $K/\mathbb{Q}$,

$$D = \{61, 89, 109, 149, 269, 389, 401\}.$$

- Para todo $\ell \in D$, se verifica que

$$\operatorname{tr} \rho(\mathrm{Frob}_\ell) = 2 \text{ en } \overline{\mathbb{F}}_3.$$

- Por tanto, si $f$ es la reducción en $\overline{\mathbb{F}}_3$ de $F$, se debe verificar

$$a_\ell(F) \equiv 2 \bmod 3 \text{ para todo } \ell \in D.$$

Columns to display: 61,89,109,149,269,38 (e.g. 3,7,19, 40-90)

Show: primes only

Trace constraints: a3=2,a5=0 (e.g. a17=1, a8=0)

Modulo: 3 (e.g. 5, 16)

View: reductions

## Results (15 matches)

Download displayed columns for all results to Text

The following table gives traces of $a_n$ for the search results.

| Label | Dim | $a_{61}$ | $a_{89}$ | $a_{109}$ | $a_{149}$ | $a_{269}$ | $a_{389}$ | $a_{401}$ |
|---|---|---|---|---|---|---|---|---|
| 320.3.b.a | 4 | 1 | 0 | 2 | 0 | 0 | 0 | 0 |
| 320.3.b.b | 4 | 2 | 0 | 1 | 1 | 2 | 1 | 0 |
| 320.3.b.c | 4 | 1 | 2 | 2 | 0 | 0 | 0 | 0 |
| 320.3.b.d | 4 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 320.3.e.a | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 320.3.e.b | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 320.3.g.a | 8 | 0 | 1 | 0 | 0 | 0 | 0 | 2 |
| 320.3.g.b | 8 | 0 | 2 | 0 | 0 | 0 | 0 | 1 |
| 320.3.h.a | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 2 |
| 320.3.h.b | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 2 |
| 320.3.h.c | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 320.3.h.d | 2 | 1 | 0 | 2 | 0 | 0 | 0 | 0 |
| 320.3.h.e | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 320.3.h.f | 6 | 1 | 1 | 2 | 1 | 2 | 0 | 0 |
| 320.3.h.g | 6 | 1 | 1 | 2 | 1 | 2 | 0 | 0 |

# Newform orbit 320.3.h.e

## Newspace parameters

Show commands: Magma / PariGP / SageMath

| | | | |
|---|---|---|---|
| Level: | $N$ | $=$ | $320 = 2^6 \cdot 5$ |
| Weight: | $k$ | $=$ | $3$ |
| Character orbit: | $[\chi]$ | $=$ | 320.h (of order 2, degree 1, not minimal) |

## Newform invariants

| | |
|---|---|
| Self dual: | no |
| Analytic conductor: | $8.71936845953$ |
| Analytic rank: | $0$ |
| Dimension: | $4$ |
| Coefficient field: | $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$ |
| Defining polynomial: | $x^4 + 2x^2 + 4$ |
| Coefficient ring: | $\mathbb{Z}[a_1, \ldots, a_5]$ |
| Coefficient ring index: | $2^7$ |
| Twist minimal: | no (minimal twist has level 80) |
| Sato-Tate group: | $\mathrm{SU}(2)[C_2]$ |

## $q$-expansion

Coefficients of the $q$-expansion are expressed in terms of a basis $1, \beta_1, \beta_2, \beta_3$ for the coefficient ring described below. We also show the integral $q$-expansion of the trace form.

$$f(q) = q + \beta_1 q^3 + (\beta_2 + 1)q^5 - 3\beta_1 q^7 - q^9 - \beta_3 q^{11} + 2\beta_2 q^{13} + (-\beta_3 + \beta_1)q^{15} + 4\beta_2 q^{17} + \beta_3 q^{19} - 24q^{21} + 9\beta_1 q^{23} + (2\beta_2 - 23)q^{25} - 10\beta_1 q^{27} + 22q^{29} + 4\beta_3 q^{31} + 8\beta_2 q^{33} + (3\beta_3 - 3\beta_1)q^{35} + 10\beta_2 q^{37} - 2\beta_3 q^{39} + 22q^{41} + 21\beta_1 q^{43} + (-\beta_2 - 1)q^{45} - 3\beta_1 q^{47} + 23q^{49} - 4\beta_3 q^{51} + 6\beta_2 q^{53} + (-\beta_3 - 24\beta_1)q^{55} - 8\beta_2 q^{57} - \beta_3 q^{59} - 46q^{61} + 3\beta_1 q^{63} + (2\beta_2 - 48)q^{65} + 21\beta_1 q^{67} + 72q^{69} - 2\beta_3 q^{71} - 16\beta_2 q^{73} + (-2\beta_3 - 23\beta_1)q^{75} - 24\beta_2 q^{77} - 71q^{81} - 27\beta_1 q^{83} + (4\beta_2 - 96)q^{85} + 22\beta_1 q^{87} + 146q^{89} + 6\beta_3 q^{91} - 32\beta_2 q^{93} + (\beta_3 + 24\beta_1)q^{95} + 12\beta_2 q^{97} + \beta_3 q^{99} + O(q^{100})$$

$$\mathrm{Tr}(f)(q) = 4q + 4q^5 - 4q^9 - 96q^{21} - 92q^{25} + 88q^{29} + 88q^{41} - 4q^{45} + 92q^{49} - 184q^{61} - 192q^{65} + 288q^{69} - 284q^{81} - 384q^{85} + 584q^{89} + O(q^{100})$$

Hoy en día, se utiliza otra definición de autoformas cuspidales con coeficientes en $\overline{\mathbb{F}}_p$ (definición de Katz), lo que nos permite considerar autoformas con peso 1.

Level: 320 | Weight: any parity: 1 | Analytic conductor: 1-10 | Analytic rank: 1 | Dim.: absolute: 1

Bad $p$: include: 2,3 | Char.: any parity: 20.d | Primitive character: 1.a | Character order: 2 | Is maximal/largest:

Coefficient field: 1.1.1.1 | Self-twists: any CM, any RM | CM/RM discriminant: -3 | Inner twist count: 1- | Is self-dual:

Coefficient ring index: 1 | Coefficient ring gens.: 20 | Is twist minimal: | Projective image: Dn

Search again | List of forms | Dimension table | Random form | Sort order: ▲ analytic conductor

Columns to display: 61,89,109,149,269,38 (e.g. 3,7,19, 40-90) | Show: primes only

Trace constraints: a3=2,a5=0 (e.g. a17=1, a8=0) | Modulo: 3 (e.g. 5, 16) | View: reductions

**Results (unique match)** Download displayed columns for all results to Text

The following table gives traces of $a_n$ for the search results.

| Label | Dim | $a_{61}$ | $a_{89}$ | $a_{109}$ | $a_{149}$ | $a_{269}$ | $a_{389}$ | $a_{401}$ |
|---|---|---|---|---|---|---|---|---|
| 320.1.h.a | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |

# Newform orbit 320.1.h.a

## Newspace parameters

Show commands: Magma / PariGP / SageMath

| | | | |
|---|---|---|---|
| Level: | $N$ | $=$ | $320 = 2^6 \cdot 5$ |
| Weight: | $k$ | $=$ | $1$ |
| Character orbit: | $[\chi]$ | $=$ | 320.h (of order $2$, degree $1$, not minimal) |

## Newform invariants

| | |
|---|---|
| Self dual: | yes |
| Analytic conductor: | $0.159700804043$ |
| Analytic rank: | $0$ |
| Dimension: | $1$ |
| Coefficient field: | $\mathbb{Q}$ |
| Coefficient ring: | $\mathbb{Z}$ |
| Coefficient ring index: | $1$ |
| Twist minimal: | no (minimal twist has level 80) |
| Projective image: | $D_2$ |
| Projective field: | Galois closure of $\mathbb{Q}(i, \sqrt{5})$ |
| Artin image: | $D_4$ |
| Artin field: | Galois closure of 4.0.1280.1 |

## $q$-expansion

$$f(q) = q + q^5 - q^9 + q^{25} - 2q^{29} - 2q^{41} - q^{45} - q^{49} + 2q^{61} + q^{81} + 2q^{89} + O(q^{100})$$

Display 10 coefficients

# Último teorema de Fermat

## Último teorema de Fermat (Wiles, 1995)

*La ecuación*

$$x^n + y^n = z^n$$

*no tiene soluciones enteras no triviales para todo entero* $n \geq 3$.

- Caso $n = 4$: Fermat, aproximadamente en 1670.
- Caso $n = 3$: Euler, 1770.
- Podemos suponer que $n \geq 5$.
- Es más, podemos suponer que $n = p$ con $p \geq 5$ primo.

# Demostración

Por reducción al absurdo: supongamos que existe $(a, b, c)$ solución entera no trivial. Entonces, existe una curva elíptica dada por

$$E : y^2 = x(x - a^p)(x + b^p).$$

Sea $E[p] \subset E(\overline{\mathbb{Q}})$ el subgrupo de puntos de $p$-torsión de $E$.La representación de Galois

$$\overline{\rho}_{E,p} \colon G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

es impar. Además, en este caso, es irreducible.
Por la conjetura de modularidad de Serre, $\overline{\rho}_{E,p}$ proviene de una autoforma cuspidal normalizada con coeficientes en $\overline{\mathbb{F}}_p$. Además, $N(\rho) = k(\rho) = 2$ y $\varepsilon(\rho) = \mathrm{id}$. Sin embargo, $\dim(\mathcal{S}_2(2, \mathrm{id})) = 0$. $\square$

¡Muchas gracias!