

Les conjectures de Serre

19.01.2004

Víctor Rotger

18è Seminari de Teoria de Nombres de Barcelona

CONTINGUT

- (1) Formes modulars mod p .
- (2) Representacions de Galois associades a formes modulars.
- (3) La conjectura forta de Serre.
- (4) Conseqüències

1. FORMES MODULARS MOD p

1.1. Formes modulars en característica 0.

Sigui $\mathcal{H} = \{z \in \mathbb{C}, \operatorname{Im}(z) > 0\}$ l'hiperplà superior de Poincaré. Dotat amb la mètrica Riemanniana hiperbòlica, $\mathcal{H}$ és una superfície de Riemann simplement connexa amb grup d'automorfismes $\operatorname{Aut}(\mathcal{H}) \simeq \operatorname{PSL}_2(\mathbb{R})$. L'acció de $\operatorname{PSL}_2(\mathbb{R})$ s'estén de manera natural a l'hiperplà superior de Poincaré compactificat $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Per qualsevol enter positiu $N \geq 1$, sigui

$$\Gamma_1(N) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

el grup modular de nivell N . Es tracta d'un subgrup discret de $\operatorname{SL}_2(\mathbb{R})$ i per tant actua en $\mathcal{H}^*$.

Donat un enter positiu k i una matriu $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, utilitzem la notació

$$F(z)|_\gamma = \det(\gamma)^{k/2} \cdot (cz + d)^{-k} \cdot F\left(\frac{az + b}{cz + d}\right).$$

Definició 1.1.

- (1) Una funció holomorfa $F : \mathcal{H} \longrightarrow \mathbb{C}$ és una forma modular de nivell N i pes k sobre $\mathbb{C}$ si:
 - $F|_\gamma = F \quad \forall \gamma \in \Gamma_1(N)$
 - $F|_\gamma$ és holomorfa en $i\infty$, $\forall \gamma \in \operatorname{SL}_2(\mathbb{Z})$:
Admet $F|_\gamma = \sum_{n \geq 0} A_n e^{\frac{2\pi i}{N} n}$
- (2) F és parabòlica si $A_0 = 0$, $\forall \gamma \in \operatorname{SL}_2(\mathbb{Z})$.

Els espais de formes modulars i parabòliques de *nivell* N i *pes* k són

$$\bullet \quad M_k(N)_{\mathbb{C}} = M_k(N)_{\mathbb{C}}$$

i

$$\bullet \quad S_k(N)_{\mathbb{C}} = S_k(N)_{\mathbb{C}},$$

respectivament.

Finalment, diem que una forma $F = \sum_{n \geq 0} A_n q^n$, $q = e^{2\pi i}$ està definida sobre un subanell $R \subset \mathbb{C}$ si $A_n \in R, \forall n \geq 0$. De manera anàloga als anteriors espais de formes modulars, denotem per

$$\bullet M_k(N)_R \text{ amb } M_k(N)_R \otimes \mathbb{C} = M_k(N)_{\mathbb{C}}$$

i

$$\bullet S_k(N)_R \text{ amb } S_k(N)_R \otimes \mathbb{C} = S_k(N)_{\mathbb{C}}$$

els R -mòduls de formes modulars i parabòliques.

1.2. Formes modulars sobre una $\mathbb{Z}[1/N]$ -àlgebra.

Sigui $X_1(N)/\mathbb{Z}[\frac{1}{N}]$ el model enter de Deligne-Rapoport de la corba modular de nivell $N \geq 5$. Amb les estructures respectives de superfícies de Riemann, tenim un isomorfisme

$$X_1(N)(\mathbb{C}) \simeq \mathcal{H}^*/\Gamma_1(N).$$

La corba $X_1(N)$ és l'espai de mòduli fi de corbes el·líptiques (E, P) amb un punt P de N -torsió marcat. Associada al problema de mòduli, existeix la corba el·líptica universal

$$\mathcal{E} \xrightarrow{\pi} X_1(N)$$

amb la $\Gamma_1(N)$ -estructura de nivell

$$\iota : (\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathcal{E}[N].$$

Denotem per

$$0 : X_1(N) \longrightarrow \mathcal{E}$$

la secció 0 de la corba el·líptica universal $\mathcal{E}$ i per

$$\Omega_{\mathcal{E}/X_1(N)}^1$$

el feix de diferencials relatives. Finalment, considerem el feix invertible sobre $X_1(N)$

$$\underline{\omega} := 0^*(\Omega_{\mathcal{E}/X_1(N)}^1)$$

Definició 1.2. [Katz]

Sigui R una $\mathbb{Z}[1/N]$ -àlgebra. El R -mòdul de formes modulars de nivell N i pes k sobre R és

$$M_k(N)_R = H^0(X_1(N) \otimes R, \underline{\omega}^{\otimes k})$$

En el que segueix, denotarem per

$$M_k(N)_{\mathbb{F}_p}$$

el R -mòdul de les formes modulars mod p segons Katz.

Sigui $f \in M_k(N)_R$,

$$f = a_0 + a_1q + a_2q^2 + \dots \in R[[q]]$$

el desenvolupament en sèrie de potències al voltant d'un punt cuspidal c de $X_1(N)(R)$, on q és un uniformitzant de c . Denotarem per

$$S_k(N)_R = \{f \in M_k(N)_R : a_0 = 0 \forall c\}$$

el R -mòdul de les formes parabòliques mod p segons Katz.

1.3. Formes modulars mod p segons Serre.

Sigui $\bar{\mathbb{Q}}_p$ una clausura algebraica del cos $\mathbb{Q}_p$ de nombres p -àdics. Sigui $\bar{\mathbb{Z}}_p$ l'anell d'enters de $\mathbb{Q}_p$ i $\wp$ l'ideal maximal de $\bar{\mathbb{Z}}_p$.

Definició 1.3. [Serre]

Una sèrie formal

$$f = \sum_{n \geq 0} a_n q^n, a_n \in \bar{\mathbb{F}}_p$$

és una forma modular mod p de Serre de nivell N i pes k si existeix $F \in M_k(N)_{\bar{\mathbb{Z}}_p}$ tal que $F \bmod \wp = f$.

Denotem per

$$M_k^{\text{Serre}}(N)_{\bar{\mathbb{F}}_p}$$

el $\bar{\mathbb{F}}_p$ -espai vectorial de formes modulars mod p de Serre de nivell N i pes k . Tenim un isomorfisme natural

$$M_k^{\text{Serre}}(N)_{\bar{\mathbb{F}}_p} \simeq M_k(N)_{\bar{\mathbb{Z}}_p} \otimes \bar{\mathbb{F}}_p.$$

Proposició 1.4 (Edixhoven). *Sigui $k \geq 1$ i $(p, N) = 1$. Aleshores*

$$(1) \ S_k^{\text{Serre}}(N)_{\bar{\mathbb{F}}_p} \subseteq S_k(N)_{\bar{\mathbb{F}}_p}$$

- (2) Si $k \geq 2$, $S_k^{\text{Serre}}(N)_{\mathbb{F}_p} = S_k(N)_{\mathbb{F}_p}$, a no ser que $N = 1, p = 2$ o 3.

En general, per $k = 1$, no tota $f \in S_1(N)_{\mathbb{F}_p}$ es pot aixecar a característica 0 i per tant $S_k^{\text{Serre}}(N)_{\mathbb{F}_p} \subsetneq S_k(N)_{\mathbb{F}_p}$.

Exemple 1.5. L'invariant de Hasse $E/\mathbb{F}_p \mapsto \text{inv}(E)$ és una forma modular de pes $p - 1$. En característica $p = 2$ no es pot aixecar a $\mathbb{Z}_2$.

1.4. L'àlgebra de Hecke.

Segui $N \geq 1$. L'àlgebra de Hecke de nivell N és

$$\mathbb{T} = \langle T_\ell, \ell \nmid N, \langle d \rangle, d \in (\mathbb{Z}/N\mathbb{Z})^* \rangle_{\mathbb{Z}}$$

on $T_\ell, \langle d \rangle$ es defineixen com a operadors que actuen

- En $X_1(N)$ com a correspondències,
- En $J(X_1(N))$ com a endomorfismes de varietats abelianes,
- En $M_k((N))_R$ i $S_k((N))_R$ com a endomorfismes lineals.

1.5. Formes noves.

Segui $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \rightarrow R^*$ un homomorfisme de grups tal que $\varepsilon(-1) = (-1)^k$.

Diem que una forma modular $f \in M_k(\Gamma_1(N))_R$ té caràcter ε si

$$\langle d \rangle (f) = \varepsilon(d)f, \quad \forall d \in (\mathbb{Z}/N\mathbb{Z})^*.$$

Obtenim unes descomposicions naturals:

$$M_k(\Gamma_1(N))_R = \oplus_{\varepsilon} M_k(\Gamma_1(N), \varepsilon)_R$$

i

$$S_k(\Gamma_1(N))_R = \oplus_{\varepsilon} S_k(\Gamma_1(N), \varepsilon)_R.$$

Diem que una forma parabòlica $f = \sum a_n q^n$ de tipus (N, k, ε) és *nova* si:

- (1) $a_0 = 0, a_1 = 1$
- (2) $T_\ell(f) = a_\ell f$
- (3) $\nexists g \in S_k(M, \varepsilon)$ per $M \mid N$ amb 1) i 2)

Denotem per $S_k^{\text{new}}(N, \varepsilon)$ el R -submòdul de $S_k(N, \varepsilon)$ de rang finit generat per les formes noves.

1.6. Aixecaments de formes modulars mod p .

Proposició 1.6. *Sigui $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \rightarrow \bar{\mathbb{F}}_p^*$ un homomorfisme de grups. Aleshores existeix un únic caràcter $\varepsilon_N : (\mathbb{Z}/N\mathbb{Z})^* \rightarrow \bar{\mathbb{Z}}_p^*$ tal que $\varepsilon_N \equiv \varepsilon \pmod{p}$.*

Definició 1.7. El caràcter de Teichmüller és l'homomorfisme

$$\chi_p : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow \mathbb{Z}_p^*$$

definit per

$$\chi_p(n) \equiv n \pmod{p}, \forall n \in \mathbb{Z}, (n, p) = 1.$$

Teorema 1.8 (Serre, Gross). *Sigui $f = \sum a_n q^n$ una forma nova definida sobre $\bar{\mathbb{F}}_p$ de tipus (N, k, ε) .*

- (1) *Si f és de tipus $(N, 2, \varepsilon)$, existeix una forma nova F de tipus $(N, 2, \varepsilon_N)$ sobre $\bar{\mathbb{Z}}_p$ tal que $F \equiv f \pmod{\wp}$.*
- (2) *Si f és de tipus (N, k, ε) , $2 < k \leq' p + 1$, existeix una forma nova F de tipus $(Np, 2, \varepsilon_N \chi_p^{k-2})$ sobre $\bar{\mathbb{Z}}_p$ tal que $F \equiv f \pmod{\wp}$.*

En el segon apartat del teorema, per $k \leq' p + 1$ volem significar $k < p + 1$ o $k = p + 1$ sota una condició tècnica que no precisarem en aquestes notes.

2. REPRESENTACIONS DE GALOIS ASSOCIADAES A FORMES MODULARS

Sigui V un espai vectorial sobre $\bar{\mathbb{F}}_p$ i sigui

$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V)$$

una representació del grup absolut de Galois $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ en el grup de transformacions lineals de V .

Diem que la representació ϱ és:

- (1) *continua*, si $\mathrm{Ker} \varrho = \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ per algun cos de nombres K , $[K : \mathbb{Q}] < \infty$.

Les representacions contínues indueixen una representació

$$\varrho : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}(V).$$

- (2) *irreductible*, si no existeixen subespais propis $W \subset V$ invariants per l'acció de $\varrho(G_{\mathbb{Q}})$.
- (3) *semisimple*, si $V = \bigoplus_{i=1}^k$ és la suma directa de $G_{\mathbb{Q}}$ -subespais irreductibles W_i .

(4) *parell*, si $\det(\varrho(c)) = 1$, *senar* si $\det(\varrho(c)) = -1$.

Teorema 2.1 (Shimura, Deligne). *Sigui $f = \sum a_n q^n$ una forma nova definida sobre $\mathbb{F}_q$ de tipus (N, k, ε) .*

Aleshores existeix una única representació de Galois contínua i semi-simple

$$\varrho_f : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_q)$$

tal que:

- (1) *s no ramificada en $\ell \nmid Np$*
- (2) *Per tot $\ell \nmid Np$:*

$$\mathrm{tr}(\varrho_f(\mathrm{Frob}_{\ell})) = a_{\ell},$$

$$\det(\varrho_f(\mathrm{Frob}_{\ell})) = \varepsilon(\ell)\ell^{k-1}.$$

Demostració.

- Ens reduïm a $2 \leq k \leq' p+1$ mitjanant la derivació de Ramanujan-Katz.
 - Per Serre i Gross, aixequem f a una forma nova $F = \sum A_n q^n$ nova de pes 2 i nivell N o Np .
 - Associada per Shimura a la forma nova F , considerem la varietat abeliana $A_F/\mathbb{Q}$, que satisfà les següents propietats:
 - (i) A_F és isògena a una subvarietat de $J(X_1(N))$
 - (ii) El cos $E = \mathbb{Q}(A_N)$ generat pels coeficients de Fourier de F és un cos de nombres: $\mathcal{O}_E = \mathrm{End}_{\mathbb{Q}}(A_F)$.
 - (iii) $\dim(A_F) = [E : \mathbb{Q}]$.
 - $T_p(A_F) \simeq \mathcal{O}_{E_{\wp}} \oplus \mathcal{O}_{E_{\wp}}$, per qualsevol ideal primer $\wp$ a sobre de p .
 - En considerar l'acció de Galois sobre la torsió de A_F , obtenim una representació $\varrho_F : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathcal{O}_{E_{\wp}})$.
 - Reduint mod $\wp$, obtenim $\varrho_f : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_q)$.
 - La representació ϱ_f és no ramificada en $\ell \nmid Np$. Pel criteri de Serre-Tate, obtenim que A_F té bona reducció fora de N .
 - Les relacions d'Eichler-Shimura demostren que els valors de $\mathrm{tr}(\varrho_f(\mathrm{Frob}_{\ell}))$ i $\det(\varrho_f(\mathrm{Frob}_{\ell}))$ són els enunciatats en el teorema.
-

Definició 2.2. Diem que una representació de Galois

$$\varrho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

és modular si $\varrho = \varrho_f$ per alguna forma modular nova mod p .

Conjectura 2.3 (La conjectura dèbil de Serre). *Totes les representacions de Galois*

$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

continues, irreductibles i senars són modulars.

3. LA CONJECTURA FORTA DE SERRE

Donada una representació de Galois $\varrho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, Serre n'associa uns invariants N_{ϱ} , ε_{ϱ} i k_{ϱ} que ara introduïrem.

Destaquem però que N_{ϱ} depèn del comportament dels grups de descomposició $D_{\ell} = \mathrm{Gal}(\overline{\mathbb{Q}}_{\ell}/\mathbb{Q}_{\ell}) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ per $\ell \neq p$.

En canvi, la definició del pes de Serre k_{ϱ} depèn de $D_p \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Finalment, ε_{ϱ} s'introdueix a partir del caràcter. $\det(\varrho) : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{F}}_p^*$.

3.1. Els invariants de Serre. Sigui

$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V)$$

una representació de Galois en un espai vectorial sobre $\overline{\mathbb{F}}_p$ de dimensió $\dim_{\overline{\mathbb{F}}_p}(V) = 2$.

3.1.1. El conductor N_{ϱ} de Serre. Sigui $\bar{v}_{\ell}$ una extensió a $\overline{\mathbb{Q}}$ de la valoració ℓ -àdica de $\mathbb{Q}_{\ell}$ i sigui

$$G = \varrho(G_{\mathbb{Q}}) \subseteq \mathrm{GL}(V)$$

el subgrup finit imatge de la representació ϱ .

Considerem la cadena

$$G_0 \supset G_1 \supset G_2 \supset \dots$$

de grups de ramificació associats a $\bar{v}_{\ell}$ i siguin

$$V^{G_i} = \{v \in V : v^g = v, g \in G_i\} \subseteq V$$

els subespais invariants de V per l'acció de G_i .

Definició 3.1.

$$N_{\varrho} = \prod_{\ell \neq p} \ell^{n(\ell)}$$

on $n(\ell) = \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \mathrm{codim}_{\overline{\mathbb{F}}_p} V^{G_i} \geq 0$.

Remarquem que de la pròpia definició, tenim que

$$n(\ell) = 0 \Leftrightarrow \varrho \text{ no ramifica en } \ell$$

i que N_{ϱ} és coprimer amb p .

3.1.2. *El caràcter ε_ϱ de Serre.* Serre defineix el caràcter ε_ϱ com segueix. El homomorfisme

$$\det(\varrho) : G_{\mathbb{Q}} \rightarrow \bar{\mathbb{F}}_p^*$$

és continu i té per imatge un subgrup cíclic de $\bar{\mathbb{F}}_p^*$. A més, el conductor del homomorfisme divideix $N_\varrho p$.

D'aquí obtenim un caràcter

$$\det(\varrho) : (\mathbb{Z}/N_\varrho p \mathbb{Z})^* \rightarrow \bar{\mathbb{F}}_p^*$$

que al seu torn n'indueix dos, un dels quals és el que ens interessa:

$$\varphi : (\mathbb{Z}/p \mathbb{Z})^* \rightarrow \bar{\mathbb{F}}_p^*$$

i

$$\varepsilon_\varrho : (\mathbb{Z}/N_\varrho \mathbb{Z})^* \rightarrow \bar{\mathbb{F}}_p^*,$$

amb $\det \varrho(Frob_\ell) = \varphi(\ell) \cdot \varepsilon_\varrho(\ell)$ per $\ell \nmid N_\varrho p$.

3.1.3. *El pes k_ϱ de Serre.* Considerem les extensions de cossos

$$\mathbb{Q}_p \subset \mathbb{Q}_p^{nr} \subset \mathbb{Q}_p^t \subset \bar{\mathbb{Q}}_p$$

i els grups galoisians

- $D_p \simeq \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$,
- $I_p = \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{nr})$,
- $D_p/I_p \simeq \text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$,
- $I_s = \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^t)$,
- $I_t = I_p/I_s = \text{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p^{nr}) \simeq \lim \mathbb{F}_{p^n}^*$

El grup d'homomorfismes continus de I_t en $\bar{\mathbb{F}}_p^*$ es pot descriure com segueix:

$$\hat{I}_t = \text{Hom}_{cont}(I_t, \bar{\mathbb{F}}_p^*) \stackrel{inv}{\simeq} (\mathbb{Q}/\mathbb{Z})' = \{[\frac{a}{d}], p \nmid d\}$$

D'entre els elements de $\hat{I}_t$, en destaquem els següents:

- $\chi : I_t \rightarrow \bar{\mathbb{F}}_p^*$ amb $\text{inv}(\chi) = \frac{1}{p-1}$, el caràcter ciclotòmic,
- $\psi : I_t \rightarrow \bar{\mathbb{F}}_{p^2}^*$ amb $\text{inv}(\psi) = \frac{1}{p^2-1}$,
- $\psi' : I_t \rightarrow \bar{\mathbb{F}}_{p^2}^*$ amb $\text{inv}(\psi') = \frac{p}{p^2-1}$

Considerem la restricció de la representació al grup de descomposició en p :

$$\varrho : D_p \longrightarrow \text{GL}(V) \simeq \text{GL}_2(\bar{\mathbb{F}}_p).$$

El subgrup d'inèrcia I_s opera trivialment sobre la semisimplificació V^{ss} de V i l'acció de I_t sobre V^{ss} diagonalitza:

$$I_t \xrightarrow{\varrho} \begin{pmatrix} \varphi & 0 \\ 0 & \varphi' \end{pmatrix}.$$

Hi ha dues possibilitats:

- Nivell 1: $\varphi, \varphi' : I_t \rightarrow \mathbb{F}_p^*$ o
- Nivell 2: $\varphi, \varphi' : I_t \rightarrow \mathbb{F}_{p^2}^*$ amb $\varphi' = \varphi^p$.

Definició 3.2. El pes k_ϱ és l'enter en $[1, p^2 - 1]$:

- (1) Si φ, φ' són de nivell 2, aleshores

$$\varphi = \psi^a \psi'^b, \varphi' = \psi^b \psi'^a$$

per $0 \leq a < b \leq p - 1$. Definim

$$k_\varrho := 1 + pa + b.$$

- (2) Si φ, φ' són de nivell 1, tenim:

- (a) Si $\varrho|_{I_p} \simeq \begin{pmatrix} \chi^a & 0 \\ 0 & \chi^b \end{pmatrix}$, $0 \leq a \leq b \leq p - 2$, definim

$$k_\varrho := 1 + pa + b.$$

- (b) Si $\varrho|_{I_p} \simeq \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}$, $0 \leq \alpha \leq p - 2, 1 \leq \beta \leq p - 1$, siguin

$a = \min(\alpha, \beta)$ i $b = \max(\alpha, \beta)$. Definim

$$k_\varrho := 1 + pa + b \text{ o } 1 + pa + b + p - 1.$$

Conjectura 3.3 (Conjectura forta de Serre). *Sigui*

$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

una representació contínua, irreductible i senar.

Aleshores existeix una forma nova $f \in S_{k_\varrho}(N_\varrho, \varepsilon_\varrho)_{\overline{\mathbb{F}}_p}$ tal que

$$\varrho \simeq \varrho_f.$$

Teorema 3.4 (Serre, Mazur, Ribet, Carayol, Jordan, Livné, Gross, Edixhoven, Diamond). *Sigui*

$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p), p > 2$$

una representació contínua, irreductible i senar. Aleshores

- (1) *Si ϱ és modular, ϱ satisfà la conjectura forta de Serre.*
- (2) *Si $\varrho = \varrho_f, f \in M_k(N, \varepsilon)_{\overline{\mathbb{F}}_p}$, $(N, p) = 1$, aleshores*

$$N_\varrho \mid N, k_\varrho \leq k$$

i

$$\epsilon : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/N_\varrho\mathbb{Z} \xrightarrow{\epsilon_\varrho} \overline{\mathbb{F}}_p^*.$$

4. CONSEQÜÈNCIES

4.1. Comportament per twists. Sigui $\varrho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ una representació contínua, irreductible i senar.

Per cada $i \geq 0$, siguin

$$\varrho(i) = \varrho \otimes \chi^{-i} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

les representacions torades de ϱ .

Proposició 4.1 (Atkin-Serre-Tate, Lario).

$$N_{\varrho(i)} = N_{\varrho}, \epsilon_{\varrho(i)} = \epsilon_{\varrho}, \forall i$$

Existeix $0 \leq i \leq p-1 : k_{\varrho(i)} \leq p+1$

ϱ és modular $\Leftrightarrow \varrho(i)$ és modular per algun $0 \leq i \leq p-1$.

La Conjectura Forta de Serre implica la següent

Conjectura 4.2. (1) Si $\varrho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ és no-ramificada fora de p , aleshores $\exists f \in S_k(SL_2(\mathbb{Z})), k \leq p+1$ tal que $\varrho = \varrho_f$.
 (2) Si $p = 2, 3, 5$ o 7 , aleshores $S_k(SL_2(\mathbb{Z})) = \emptyset$ per $k \leq p+1$ i per tant no existeixen representacions $\varrho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ no ramificades fora de p .

La conjectura ha estat provada per $p = 2$ (Tate), $p = 3$ (Serre), $GRH \Rightarrow p = 5$ (Brueggeman)

4.2. El teorema de Fermat.

Teorema 4.3 (Serre). Si la conjectura forta de Serre és certa,

$$a^p + b^p + c^p = 0, \quad p \geq 5$$

no té solució amb $a, b, c \in \mathbb{Z}$, $abc \neq 0$.

Demostració.

- Ens podem reduir amb arguments elementals al cas en què a, b, c són primers entre ells, b és parell i $a \equiv 3 \pmod{4}$.
- Sigui $E_{a,b,c} : y^2 = x(x - a^p)(x + b^p)$ la corba el·líptica de Frey.
- Sigui $\varrho_{a,b,c} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ la representació associada a la p -torsió de $E_{a,b,c}$.
- $N_{\varrho_{a,b,c}} = 2, \epsilon_{\varrho_{a,b,c}} = 1$ i $k_{\varrho_{a,b,c}} = 2$.
- $\exists f \in S_2(2) = H^0(X_0(2), \Omega_{X_0(2)}^1) : \varrho_{a,b,c} = \varrho_f$.
- Però $X_0(2) \simeq \mathbb{P}_{\mathbb{Q}}^1$!!!

4.3. Conjectura de Shimura-Taniyama-Weil generalitzada. Serre va demostrar també que si la conjectura forta de Serre és certa, la següent conjectura és certa.

Conjectura 4.4 (Conjectura de Shimura-Taniyama-Weil generalitzada). *Si $A/\mathbb{Q}$ una varietat abeliana de dimensió $n \geq 1$. Si $\text{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ és un cos de nombres de grau n , aleshores A és isògena a una subvarietat abeliana de $J(X_1(N))$ per algun N .*