REPRESENTACIONS DE GALOIS I CORBES EL.LÍPTIQUES

Joan-C. Lario

Impresión: Servicio de Publicaciones E.U.E.E.

Tiraje: 100 ejemplares.

Depósito Legal: B- 44929 - 90.

Representacions de Galois i corbes el·líptiques

Memòria presentada per
optar al grau de Doctor
en Ciències Matemàtiques

per

Joan-Carles Lario i Loyo

Universitat de Barcelona
1991

Direcció: Prof. Dra. P. BAYER

Departament d'Àlgebra i Geometria

Facultat de Matemàtiques

Universitat de Barcelona

CONTINGUTS

INTRODUCCIÓ 1

PART I

CAPÍTOL 1. FORMES MODULARS 9

§1. La corba modular $X_1(N)$ 9

§2. Formes modulars 14

§3. Formes modulars (mod p) 16

§4. Formes modulars complexes 20

§5. Corbes de Weil 27

CAPÍTOL 2. REPRESENTACIONS DE GALOIS MODULARS 29

§1. Representacions modulars p-àdiques 31

§2. Representacions modulars (mod p) 35

CAPÍTOL 3. PROPIETATS LOCALS 39

§1. Formes modulars ordinàries i representacions ordinàries 39

§2. Formes modulars supersingulars i representacions supersingulars 45

CAPÍTOL 4. LA CONJECTURA DE SERRE 47

§1. El conductor N_ρ 47

§2. El caràcter ε_ρ 48

§3. El pes k_ρ 50

§4. Enunciat de la conjectura 53

§5. Aportacions d'altres autors 53

PART II

CAPÍTOL 5. ESTUDI DEL COMPORTAMENT DE LA CONJECTURA DE SERRE PER TORCEMENT 59

§1. Obtenció de congruències 59

§2. Torcement de representacions 62

§3. Criteris per a la validesa de la conjectura 65

CAPÍTOL 6. CÀLCUL DELS INVARIANTS DE SERRE ASSOCIATS A LES CORBES EL·LÍPTIQUES 71

§1. Invariants associats a la p-torsió 71

§2. Invariants minimals. Invariants companys 78

CAPÍTOL 7. PROVA DE LA CONJECTURA DE SERRE PER AL CAS DE CORBES DE WEIL POTENCIALMENT ORDINÀRIES 85

§1. Una forma amb Nebentypus associada a E 85

§2. Coeficients ocults 88

§3. Ordinarietat 91

§4. La prova 92

CAPÍTOL 8. EXPERIMENTS NUMÈRICS 95

§1. Experiment No. 1: Avantatges de la representació minimal 95

§2. Experiment No. 2: Abaixament de nivells 98

§3. Experiment No. 3: Càlcul de coeficients ocults 105

APÈNDIX 1. CAS SEMISTABLE 109

APÈNDIX 2. CAS SUPERSINGULAR 113

REFERÈNCIES 121

Introducció

L'objecte d'aquesta tesi és l'estudi d'una conjectura de J.-P. Serre que preveu una relació entre certes representacions de Galois residuals de grau 2 i formes modulars ($\mathrm{mod}\, p$). L'objectiu és donar-ne una prova per al cas de les representacions que provenen de la p-torsió de les corbes de Weil potencialment ordinàries en p.

La conjectura en qüestió, formulada a [Se 87], sosté que tota representació contínua, irreductible i senar

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

prové d'una forma parabòlica de Hecke ($\mathrm{mod}\, p$)

$$f(q) = \sum_{n=1}^{\infty} a_n q^n ,$$

de tipus $(N_\rho, k_\rho, \varepsilon_\rho)$. El terme "prové" vol dir que el polinomi característic de $\rho(\mathrm{Frob}_\ell)$ és

$$X^2 - a_\ell X + \varepsilon_\rho(\ell)\ell^{k_\rho - 1} ,$$

per a tot primer $\ell \nmid N_\rho p$. El conductor N_ρ, el pes k_ρ, i el caràcter ε_ρ venen donats, en funció de ρ, per una recepta molt precisa.

Serre se situa en la perspectiva d'una "filosofia de Langlands": la teoria de les representacions interacciona amb la teoria de les formes automorfes, proporcionant nous resultats de natura aritmètico-geomètrica.

La conjectura esdevé interessant i inquietant alhora quan s'exploren les conseqüències plausibles a què conduiria en cas de ser certa. Entre d'altres, quedarien provats el darrer teorema de Fermat i la conjectura de

Hasse-Shimura-Taniyama-Weil. Quant aquest punt, cal destacar les valuoses aportacions de G. Frey en el treball [**Fr 86**].

Els antecedents de la conjectura no són pocs. La primera versió fou establerta en el transcurs de les *Journées Arithmétiques* celebrades a Bordeus l'any 1973. No obstant, no és fins tretze anys després que queda enllestida. Les idees de J. Tate per relacionar el pes amb l'acció de la inèrcia i els resultats de J.M. Fontaine sobre les representacions locals associades a la cohomologia fan possible que Serre precisi la conjectura en una forma que permet la seva verificació numèrica. Els primers exemples numèrics que la contrasten favorablement els trobem a [**Se 87**] i tracten casos per als primers $p = 2, 3$ i 7; la implementació a l'ordinador d'aquests exemples és deguda a J.F. Mestre.

Esmentem els treballs publicats fins al moment en relació amb aquesta conjectura. El primer es deu a K. Ribet [**Ri 90**]; en ell es fa un estudi profund de la part nova i vella de $J_0(Np)$, la jacobiana de la corba modular $X_0(Np)$, que permet provar la conjectura de Serre per a certes representacions residuals modulars i finites. En particular, aquests resultats proporcionarien la prova del darrer teorema de Fermat, en el ben entès que les corbes el·líptiques de Frey satisfessin la conjectura de Hasse-Shimura-Taniyama-Weil. El segon i tercer treballs, deguts a H. Carayol i W. Jordan-R. Livné, contenen l'adaptabilitat del nivell de la forma modular $(\mathrm{mod}\, p)$ a l'invariant conductor predit per la conjectura, en el cas de representacions residuals modulars amb condicions restrictives en p. Alguns resultats relacionats amb l'invariant pes, el més "misteriós", han estat donats per B.H. Gross a [**Gr 90**] i per B. Edixhoven a [**Ed 91¬**].

Tanmateix, en el Seminari de Teoria de Nombres de Barcelona 87/88: "*Contrastació numèrica de la conjectura de Serre sobre representacions de Galois modulars*", s'obtingueren exemples de la conjectura per al cas de representacions residuals de tipus diedral amb $p = 23, 157, 233...$ En el treball conjunt amb J. Quer [**La-Qu 87¬**] donàrem exemples de tipus octaedral, construïts a partir de resultats de T. Crespo [**Cr 90**] i de P. Bayer-G. Frey [**Ba-Fr 91**] relatius a la realització efectiva de dobles recobriments com a grup de Galois i al càlcul de les L-sèries d'Artin corresponents.

Malgrat l'ajust de la conjectura que en possibilita la verifació nu-

mèrica, cal destacar les dificultats pràctiques que apareixen a l'hora de tractar un exemple concret. En efecte, imaginem que volem contrastar la conjectura per a una representació donada. Serre prediu que prové d'una forma modular (mod p) que pertany a un cert espai, determinat a partir dels invariants (conductor, pes i caràcter) associats a la representació en qüestió. La primera dificultat rau en el càlcul d'aquests invariants.

En el cas particular de les representacions de Galois residuals associades als punts de p-torsió de corbes el·líptiques, el càlcul dels invariants fou presentat per l'autor en el Seminari Frey-Lamprecht-Zimmer a la Universität des Saarlandes el setembre de 1989. Sota la direcció de J. Oesterlé, A. Kraus retrobà els mateixos invariants a [**Kr 90¬**].

En el cas general, si s'han pogut determinar els invariants, el veredicte sobre el caràcter cert o fals de la conjectura podria ser resolt sota el coneixement d'una base de l'espai de formes modulars. Alguns treballs procuren la construcció d'una tal base, malgrat que els resultats que s'aconsegueixen no són sempre implementables. Citem els de Eichler i Selberg sobre les traces dels operadors de Hecke, els de Pizer sobre les matrius de Brandt i les àlgebres de quaternions; també, obtinguts més recentment, els mètodes dels grafs dissenyats per Mestre-Oesterlé (1985), Birch (1988) i Edixhoven (1989). Aquests darrers proporcionen algoritmes extramadament eficients, tot i que estan subjectes a fortes restriccions: donen informació només de certs subspais i tan sols tracten el cas de pes igual a 2 i nivell lliure de quadrats o p^2.

Els motius esmentats ens conduïren a intentar cercar la "llei" que regula la conjectura. El nostre intent ha resultat reeixit en el cas de les representacions associades a la p-torsió de les corbes de Weil potencialment ordinàries en p. Seguint un tractament diferent del que es presenta en la memòria, part dels resultats que aquesta conté s'exposen a [**Ba-La 91**].

Com ja hem dit abans, els antecedents de la conjectura són molts, estesos en el temps i dispersos en la literatura. La primera part de la tesi, distribuida en 4 capítols, està dedicada a recopilar i ordenar la part d'aquest material necessària per als nostres propòsits. La segona part de la tesi, distribuida en 4 capítols i dos apèndixs, conté les aportacions originals.

El Capítol 1 és de preliminars. Inclou una descripció d'un model canònic de la corba modular $X_1(N)$, sobre $\mathbb{Z}[1/N]$, que permet introduir les formes modulars en el sentit de Katz; exposem una sèrie de resultats sobre les formes modulars (mod p) i complexes. En acabar el capítol, revisem les corbes de Weil.

En el Capítol 2 es repassen els resultats clàssics sobre l'existència de representacions modulars p-àdiques i (mod p) associades a una forma modular. Predits per Serre i deguts a Shimura i Deligne, aquests resultats impulsaren la primera versió de la conjectura de Serre. Hem cregut oportú incloure un esbós de demostracions recents, obtingudes per Gross, que es recolzen en la teoria de Serre sobre els aixecaments de formes modulars (mod p).

El Capítol 3 està dedicat a l'estudi del comportament local de les representacions modulars (mod p). Hi trobem dos casos ben diferenciats: l'ordinari i el supersingular. El primer, molt més explorat en la literatura, es presenta amb cert detall; del segon, tractat en la correspondència entre Fontaine i Serre, ens limitem a donar-ne una breu descripció. Els resultats que exposem són claus per entendre el comportament del pes en la formulació definitiva de la conjectura.

En el Capítol 4 es transcriu la definició dels invariants de Serre associats a una representació, així com l'enunciat de la conjectura que ens ocupa. També fem revista de resultats que sobre la mateixa han estat obtinguts fins al moment.

En iniciar la segona part, en el Capítol 5, estudiem el comportament de la conjectura de Serre en una representació, prenent esment del comportament en les seves torçades. Obtenim congruències entre formes parabòliques de diferents espais i introduïm els conceptes de representació minimal i companya associada a una representació donada. Això ens permet provar uns criteris per a la validesa de la conjectura. Aquests criteris s'apliquen, posteriorment, en el Capítol 7 i en els apèndixs.

En el Capítol 6, calculem els invariants de Serre N_ρ, k_ρ, ε_ρ associats a les representacions de Galois residuals, ρ, que provenen de la p-torsió de les corbes el·líptiques definides sobre $\mathbb{Q}$. Concretament, obtenim un diccionari

entre els invariants de ρ i els tipus de Kodaira de la fibra especial del model de Néron de les corbes el·líptiques. En acabar aquest capítol, donem els invariants minimals i els invariants companys associats a ρ.

En el Capítol 7 provem la conjectura de Serre per a les representacions residuals que provenen de la p-torsió de les corbes de Weil potencialment ordinàries en p. La prova es porta a terme en tres etapes: en la primera, associem una forma nova amb Nebentypus (caràcter no necessàriament trivial) a la corba de Weil; en la segona, abaixem el nivell i augmentem el pes d'aquesta forma nova de manera simultània; finalment, a la vista dels resultats del Capítol 6, verifiquem els criteris suficients que hem obtingut en el Capítol 5.

El Capítol 8 conté diversos experiments numèrics i llistats de programes implementats en codi `FORTRAN`. La construcció d'aquests exemples ha estat decisiva per trobar la llei que regeix la conjectura en el cas de les corbes de Weil potencialment ordinàries. En els capítols previs hi trobarem sovint punters per dirigir l'atenció del lector cap a un d'aquests experiments. Considerem que, fent-ho així, pot quedar més clar el procés seguit en l'obtenció dels resultats parcials que ens han conduït a la prova.

L'Apèndix 1 recull les proves de la conjectura per a les representacions definides pels punts de p-torsió de les corbes de Weil amb reducció semistable o potencialment semistable en p.

En l'Apèndix 2 formulem una conjectura per al cas de les representacions de Galois associades als punts de p-torsió de les corbes el·líptiques potencialment supersingulars en p. Aquesta conjectura és contrastada numèricament i veiem que implica la de Serre.

* * *

En el text de la memòria, acompanyen cada resultat no-original sengles referències bibliogràfiques. Aquestes s'indiquen amb una abreviatura per a l'autor seguida de dues xifres per a l'any (sempre del segle XX); rera les xifres, el signe "¬" assenyala que es tracta d'un treball inèdit.

En cloure aquesta introducció, voldria expressar el meu agraïment:

• al Departament d'Àlgebra i Geometria de la UB, per la formació rebuda en els cursos del tercer cicle,

• al Departament de Matemàtica Aplicada II de la UPC, pel suport humà i material que m'ha ofert en tot moment,

• al Seminari de Teoria de Nombres de Barcelona (UB-UAB-UPC), per les discusions col·lectives que sovint m'han fet avançar, economitzant temps, en la comprensió de molts aspectes relacionats amb el tema,

• al Professor J. Quer, de qui he rebut nombroses i oportunes observacions,

• als Professors H. Carayol, G. Frey i D.B. Zagier que, amb la seva estada a Barcelona, m'han esperonat,

• i, molt especialment, a la Professora P. Bayer de qui he après el trajecte de la Teoria als Nombres i dels Nombres a la Teoria. Amb el seu fer, resolut i diligent, he disfrutat de valent en l'elaboració d'aquest treball.

PART I

CAPÍTOL 1

Formes modulars

En aquest capítol s'agrupen les definicions i alguns resultats sobre les formes modulars en el sentit de Katz. La selecció ha estat feta en funció de les necessitats posteriors; és per això que, a part dels resultats més bàsics, s'inclouen també alguns teoremes més específics.

§1. La corba modular $X_1(N)$

L'estudi de les corbes modulars constitueix un punt clau a l'hora de tractar la conjectura de Serre. En efecte, les corbes modulars despleguen el pont entre les formes modulars i certes representacions de Galois residuals. Aquesta secció conté un resum de les propietats més destacables de la corba modular $X_1(N)$ que podem trobar a **[De-Ra 73]**, **[De-Se 74]**, **[Ka-Ma 85]**, **[Gr 90]**, **[Ma-Ti 90]**. Comencem recordant algunes definicions.

Sigui S un esquema arbitrari. Una corba el·líptica E sobre S és un morfisme propi i llis

$$\begin{array}{c} E \\ \pi \downarrow \\ S \end{array}$$

amb fibres geomètriques corbes connexes de gènere 1, equipat amb una secció

$$\text{“0”} : S \to E .$$

La llei d'addició sobre les fibres dota E d'estructura d'esquema en grups commutatiu sobre S. Si $N \geq 1$ és un enter, denotem per $E[N]$ el nucli de

la multiplicació per N sobre E. Aleshores $E[N]$ és un esquema en grups finit i pla de rang N^2 sobre S; si N és invertible a S, es té que $E[N]$ és un esquema en grups étale localment isomorf a $(\mathbb{Z}/N\mathbb{Z})^2$. A més, existeix un aparellament canònic, alternat i no-degenrat,

$$e : E[N] \times E[N] \to \mu_N ,$$

on μ_N és l'esquema en grups de les arrels N-èsimes de la unitat o, equivalentment, és la N-torsió de l'esquema en grups multiplicatiu $\mathbb{G}_m$. Com és costum, anomenem e l'aparellament de Weil; proporciona un isomorfisme entre $E[N]$ i el seu dual de Cartier $E[N]^D = \mathrm{Hom}(E[N], \mathbb{G}_m)$.

D'altra banda, el feix invertible Ω^1_E és de grau 0 en cada fibra i, per dualitat de Serre-Grothendieck, tenim un isomorfisme

$$R^1\pi_*\Omega^1_E \backsimeq \mathcal{O}_S$$

de formació compatible amb qualsevol canvi de base. Per tant,

$$\underline{\omega}_E := \pi_*\Omega^1_E$$

és un feix invertible sobre S, de formació compatible amb qualsevol canvi de base; el seu dual és el feix invertible $R^1\pi_*\mathcal{O}_E$, que és isomorf al feix $\underline{\mathrm{Lie}}(E)$.

Una corba el·líptica generalitzada E sobre S és un esquema en corbes (és a dir, un morfisme propi i pla, de presentació finita i dimensió relativa com a molt 1)

$$\begin{array}{c} E \\ {\scriptstyle\pi}\big\downarrow \\ S \end{array}$$

amb fibres geomètriques o bé corbes el·líptiques o bé polígons de Néron, equipat amb un morfisme

$$\text{“+”} : E^{\mathrm{reg}} \times_S E \to E$$

tal que:

1) la restricció de “+” a E^{reg} (la reunió dels punts llisos de les fibres) dota E^{reg} d'estructura d'esquema en grups commutatiu,

2) "+" defineix una acció de l'esquema en grups E^{reg} sobre E, i

3) sobre les fibres E_s amb punts singulars, les trasllacions segons "+" per E_s^{reg} actuen per rotacions sobre el graf de les components irreductibles de E_s.

Clarament es té que si $E_{|S}$ és una corba el·líptica generalitzada llisa (és a dir, el morfisme π és llis) aleshores $E_{|S}$ és una corba el·líptica genuïna. Es posa $E[N] := E^{\mathrm{reg}}[N]$. Es defineix el feix invertible $\underline{\omega}_E$ com el dual del feix $\underline{\mathrm{Lie}}(E^{\mathrm{reg}})$.

Amb aquestes definicions passem a considerar el problema de moduli que ens interessa. Prèviament, notem que Deligne i Rapoport tracten la classificació de corbes el·líptiques generalitzades amb unes estructures de nivell no adients per als nostres objectius en el sentit que obtenen una corba modular diferent de $X_1(N)$. D'altra banda, Mazur i Tilouine consideren la classificació que s'ajusta quant a les estructures de nivell, però només per a corbes el·líptiques genuïnes. Lleugeres modificacions permeten englobar els dos aspectes.

Sigui ara S un $\mathbb{Z}[1/N]$-esquema. Donada $E_{|S}$ una corba el·líptica generaltizada, denotem per $[\Gamma_1(N)](E_{|S})$ el conjunt format per les S-immersions $i : \mu_N \hookrightarrow E[N]$ tals que la imatge talla totes les components irreductibes en cada fibra geomètrica. Els elements de $[\Gamma_1(N)](E_{|S})$ s'anomenen $\Gamma_1(N)$-estructures de nivell sobre $E_{|S}$.

Un exemple de corba el·líptica generalitzada amb una $\Gamma_1(N)$-estructura de nivell és la corba de Tate $E = \mathrm{Tate(q)} = \mathbb{G}_m/q^{\mathbb{Z}}$ sobre $S = \mathrm{Spec}\,\mathbb{Z}[[q]]$ amb el morfisme canònic d'esquemes en grups $\mathrm{Id}_N : \mu_N \hookrightarrow E[N]$.

El problema de moduli $[\Gamma_1(N)]$ que classifica les $\Gamma_1(N)$-estructures de nivell és rígid si $N > 4$ (per a $N \leq 3$, existeixen parelles de corbes el·líptiques i estructura de nivell amb automorfismes no trivials i, per a $N = 4$, el mateix passa amb corbes el·líptiques generalitzades). D'altra banda, considerem el functor contravariant associat:

$$\widetilde{[\Gamma_1(N)]} : \left\{\mathbb{Z}[1/N] - \text{esquemes}\right\} \to \left\{\text{conjunts}\right\}$$
$$S \mapsto \left\{\begin{array}{l}\text{classes d'isomorfia} \\ \text{de parelles } (E_{|S}, i)\end{array}\right\}$$

on $E_{|S}$ és una corba el·líptica generalitzada, $i : \mu_N \hookrightarrow E[N]$ una $\Gamma_1(N)$-estructura de nivell sobre $E_{|S}$; els isomorfismes considerats en el sentit evident. Aquest functor és representable.

Per tant, si $N > 4$ el problema de moduli $[\Gamma_1(N)]$ és representable per $\pi : \mathbb{E} \to X_1(N)$. Per definició, $\mathbb{E}$ és la corba el·líptica generalitzada universal i $X_1(N)$ la corba modular per al subgrup de congruència $\Gamma_1(N)$. Es té que $X_1(N)$ és una corba algebraica sobre $\mathbb{Z}[1/N]$, pròpia, llisa i geomètricament connexa. Aleshores, si S és un $\mathbb{Z}[1/N]$-esquema, podem identificar cada punt de $X_1(N)(S)$ com una classe d'isomorfia d'una parella (E, i) formada per certa corba el·líptica generalitzada definida sobre S amb una $\Gamma_1(N)$-estructura de nivell. En el cas particular $S = \operatorname{Spec}\mathbb{C}$, els punts de la corba modular $X_1(N)$ racionals sobre $\mathbb{C}$ són els de la superfície de Riemann compacta i connexa

$$\Gamma_1(N)\backslash\mathbb{H}^*$$

on

$$\mathbb{H}^* = \{z \in \mathbb{C} \colon \operatorname{Im}(z) > 0\} \cup \mathbb{P}^1(\mathbb{Q})$$

i

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

S'anomena divisor cuspidal de $X_1(N)$ el divisor de $X_1(N)$ format per la suma dels punts (puntes) sobre els que les fibres de $\mathbb{E}$ són polígons de Néron. Aleshores posem $Y_1(N)$ l'obert de $X_1(N)$ obtingut traient les puntes.

Notem $J_1(N)$ la Jacobiana de $X_1(N)$. A continuació recordem diferents correspondències i morfismes de la corba modular $X_1(N)$. Tots ells es defineixen sobre $Y_1(N)$ i s'estenen de manera única a les puntes de $X_1(N)$.

Com a correspondències de $X_1(N)$, per a cada primer $\ell \nmid N$, considerem el ℓ-èsim operador de Hecke

$$T_\ell(E, i) = \sum (E', i')\,,$$

on la suma recorre les isogènies $E \to E'$ de grau ℓ i la immersió i' és la composició de i amb la isogènia.

Per a $\ell \mid N$, el ℓ-èsim operador de Hecke ve donat per

$$U_\ell(E,i) = \sum (E', i'),$$

on la suma recorre les isogènies $E \to E'$ de grau ℓ tals que el seu nucli no talli $\operatorname{Im} i$, i la immersió i' és la composició de i amb la isogènia.

Per a cada $d \in (\mathbb{Z}/N\mathbb{Z})^*$ considerem $\sigma_d : \mu_N \to \mu_N$, el morfisme "elevar a d". L'automorfisme diamant de $X_1(N)$ és

$$< d > (E,i) = (E, i \circ \sigma_d).$$

Notem que el grup $(\mathbb{Z}/N\mathbb{Z})^*$ opera sobre el problema de moduli $[\Gamma_1(N)]$; el problema de moduli quocient, $[\Gamma_0(N)]$, dóna lloc a la corba modular $X_0(N)$.

Si $\zeta \in \overline{\mathbb{Q}}$ és una arrel primitiva N-èsima de la unitat, la involució de Weil w_ζ es defineix segons

$$w_\zeta(E,i) = (E/\operatorname{Im} i, j)$$

on $j : \mu_N \hookrightarrow E/\operatorname{Im} i$ està determinat per la condició $e(i(\zeta^a), j(\zeta^b)) = \zeta^{ab}$, essent e l'aparellament de Weil. La involució de Weil w_ζ és un automorfisme de $X_1(N)_{/\mathbb{Z}[\frac{1}{N}][\zeta]}$. Si $\sigma_d \in \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ és $\sigma_d(\zeta) = \zeta^d$, aleshores es té

$$w_\zeta{}^{\sigma_d} = w_{\zeta^d} = w_\zeta \circ < d > .$$

Podem veure les correspondències de Hecke i els diamants com a endomorfismes de $J_1(N)_{/\mathbb{Q}}$, i les involucions de Weil com a endomorfismes de $J_1(N)_{/\mathbb{Q}(\zeta)}$; els denotarem per $T_{\ell,\mathrm{Pic}}$, $U_{\ell,\mathrm{Pic}}$, $< d >_{\mathrm{Pic}}$, $w_{\zeta,\mathrm{Pic}}$, si ho fem per functorialitat de Picard, o bé per $T_{\ell,\mathrm{Alb}}$, $U_{\ell,\mathrm{Alb}}$, $< d >_{\mathrm{Alb}}$, $w_{\zeta,\mathrm{Alb}}$ si ho fem per functorialitat d'Albanese. La relació entre la functorialitat de Picard i la functorialitat d'Albanese ve donada per les fórmules següents:

$$w_\zeta \circ T_{\ell,\mathrm{Pic}} \circ w_\zeta{}^{-1} = T_{\ell,\mathrm{Alb}}$$
$$w_\zeta \circ U_{\ell,\mathrm{Pic}} \circ w_\zeta{}^{-1} = U_{\ell,\mathrm{Alb}}$$
$$w_\zeta \circ < d >_{\mathrm{Pic}} \circ w_\zeta{}^{-1} = < d >_{\mathrm{Alb}} .$$

Definim l'àlgebra de Hecke $\mathbb{T}$ com la subàlgebra de $\mathrm{End}(J_1(N)_{/\mathbb{Q}})$ generada sobre $\mathbb{Z}$ pels endomorfismes $T_{\ell,\mathrm{Alb}}$ per a $\ell \nmid N$, i $< d >_{\mathrm{Alb}}$ per a $d \in (\mathbb{Z}/N\mathbb{Z})^*$. La polarització canònica de $J_1(N)_{/\mathbb{Q}}$ indueix una anti-involució $t \mapsto t^*$ de $\mathrm{End}(J_1(N)_{/\mathbb{Q}})$, anomenada involució de Rosati. Sobre l'àlgebra de Hecke $\mathbb{T}$ es té

$$t^* = w_\zeta \, t \, w_\zeta \, .$$

§2. Formes modulars

Per a aquesta secció i la següent reprenem la terminologia de **[De-Se 74]**, **[Ka 73]**, **[Ka 76]**.

Siguin N i k enters ≥ 1, i sigui R una $\mathbb{Z}[1/N]$-àlgebra. Una forma modular f de pes k per a $\Gamma_1(N)$, definida sobre R, és una llei que assigna a cada parella (E,i), on E és una corba el·líptica generalitzada sobre una R-àlgebra amb i una $\Gamma_1(N)$-estructura de nivell sobre E, una secció $f(E,i)$ del feix $\underline{\omega}_E^{\otimes k}$, de formació compatible amb els isomorfismes i les extensions d'escalars. Es denota per $M_k(\Gamma_1(N))(R)$ el R-mòdul de les formes modulars de pes k per a $\Gamma_1(N)$ definides sobre R o, simplement, per $M_k(\Gamma_1(N))$ si R està sobreentès.

Si $N > 4$, i $\omega = \underline{\omega}_{\mathbb{E}}$ designa el feix invertible associat a la corba el·líptica generalitzada universal $\mathbb{E}$, tenim l'isomorfisme de Kodaira-Spencer $\omega^{\otimes 2} \xrightarrow{\sim} \Omega^1_{X_1(N)}(\text{puntes})$. A més,

$$M_k(\Gamma_1(N))(R) = H^0(X_1(N), \omega^{\otimes k} \otimes R) \, .$$

Si $k \geq 2$, l'aplicació natural

$$H^0(X_1(N), \omega^{\otimes k}) \otimes R \to H^0(X_1(N), \omega^{\otimes k} \otimes R)$$

és un isomorfisme.

Si f és una forma modular de pes k per a $\Gamma_1(N)$, definida sobre R, s'anomena desenvolupament de Fourier en la punta ∞ de $X_1(N)$ la sèrie $f(q) = \sum_{n \geq 0} a_n q^n \in R[[q]]$ obtinguda per avaluació de f sobre la corba de Tate amb la seva $\Gamma_1(N)$-estructura de nivell. Concretament,

$$f(\mathrm{Tate}(q), \mathrm{Id}_N) = f(q)(dt/t)^{\otimes k} \, .$$

El principi del q-desenvolupament assegura que l'aplicació

$$\begin{aligned} H^0(X_1(N),\omega^{\otimes k}\otimes R) &\to R[[q]] \\ f &\mapsto f(q) \end{aligned}$$

és injectiva, i que f està definida sobre una sub $\mathbb{Z}[1/N]$-àlgebra R_0 de R si, i només si, $f(q)\in R_0[[q]]$.

Les accions de l'àlgebra de Hecke induïdes a l'espai de formes modulars poden ser descrites mitjançant els seus desenvolupaments de Fourier.

Definició 2.1. Sigui f una forma modular de pes k per a $\Gamma_1(N)$, definida sobre R. Es diu que f és de tipus (N,k,ε) si existeix un caràcter $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to R^*$ amb $\varepsilon(-1)=(-1)^k$ tal que $f|<d>=\varepsilon(d)f$ per a tot $d\in(\mathbb{Z}/N\mathbb{Z})^*$. Denotem per

$$M_k(N,\varepsilon)(R)$$

el R-mòdul de les formes modulars de tipus (N,k,ε) definides sobre R.

Si

$$f(q)=\sum a_n q^n \in M_k(N,\varepsilon)(R)\,,$$

fent ús de la corba de Tate es troba que

$$\begin{aligned} f|T_\ell(q) &= \sum a_{n\ell}q^n + \varepsilon(\ell)\ell^{k-1}\sum a_n q^{n\ell}\,, \\ f|U_\ell(q) &= \sum a_{n\ell}q^n\,. \end{aligned}$$

Definició 2.2. Una forma modular $f(q)=\sum a_n q^n$ de tipus (N,k,ε), definida sobre R, es diu:

- normalitzada si $a_1=1$;
- de Hecke si és normalitzada i vector propi simultani per als operadors T_ℓ $(\ell\nmid N)$ i U_ℓ $(\ell\mid N)$. En tal cas, es té:

$$\begin{aligned} f|T_\ell &= a_\ell f \quad \text{si } \ell\nmid N\,, \\ f|U_\ell &= a_\ell f \quad \text{si } \ell\mid N\,, \end{aligned}$$

$$\sum_{n\geq 1} a_n n^{-s} = \prod_{\ell | N} (1 - a_\ell \ell^{-s})^{-1} \prod_{\ell \nmid N} (1 - a_\ell \ell^{-s} + \varepsilon(\ell)\ell^{k-1-2s})^{-1};$$

• parabòlica si, com a secció de $\omega^{\otimes k}$ sobre $X_1(N)$, s'anul·la sobre el divisor cuspidal.

Aleshores, $a_0 = 0$ i f ve determinada pel seu caràcter ε i els valors propis a_ℓ amb ℓ primer. Denotem per

$$S_k(N, \varepsilon)(R)$$

el R-mòdul de les formes parabòliques de tipus (N, k, ε) definides sobre R.

• nova si és de Hecke, parabòlica i per a cap divisor propi M de N existeix una forma de Hecke, parabòlica, de pes k per a $\Gamma_1(M)$ amb sistema de valors propis $\{a_\ell, \varepsilon\}_{\ell \nmid M}$ pels operadors de Hecke T_ℓ amb $\ell \nmid M$.

Denotem per

$$S_k^{\text{noves}}(N, \varepsilon)(R)$$

el sub R-mòdul de les formes parabòliques de tipus (N, k, ε), definides sobre R, generat per les formes noves.

§3. Formes modulars (mod p)

Sigui p un nombre primer tal que $p \nmid N$, i considerem $R = \overline{\mathbb{F}}_p$. Les formes modulars que així s'obtenen són les que anomenem formes modulars (mod p). Aleshores $S_k(N, \varepsilon)(\overline{\mathbb{F}}_p)$ és un $\overline{\mathbb{F}}_p$-espai vectorial de dimensió finita; si $f(q) = \sum a_n q^n$ és una forma nova (mod p) de tipus (N, k, ε), aleshores està definida sobre el cos finit $\mathbb{F}_q$ generat pels coeficients de Fourier a_n i els valors del caràcter ε.

Existeix una forma modular (mod p) distingida: la forma modular associada a l'invariant de Hasse. Per ser més explícits, es tracta de la llei que assigna a cada corba el·líptica E, definida sobre un $\mathbb{Z}/p\mathbb{Z}$-esquema, el seu invariant de Hasse $A(E)$, que és la secció de $\underline{\omega}_E^{\otimes p-1}$ que prové de considerar la formació de l'aplicació tangent $\mathrm{tg}(V)$ del Verschiebung sobre E. Aquesta llei proporciona una forma modular A de pes $p-1$ per a $\Gamma_1(N)$, definida sobre $\mathbb{Z}/p\mathbb{Z}$; el seu desenvolupament de Fourier és $A(q) = 1$.

A part dels operadors de Hecke i els diamants, per a les formes modulars (mod p) tenim les aplicacions lineals següents:

• En primer lloc,

$$V_p : M_k(\Gamma_1(N)) \to M_{pk}(\Gamma_1(N)) \qquad f \mapsto f^p ,$$

i l'efecte sobre els desenvolupaments de Fourier és

$$f|V_p(q) = \sum a_n q^{np} ,$$

si $f(q) = \sum a_n q^n$.

• Existeix una derivació, que anomenem de Ramanujan-Katz,

$$\theta : M_k(\Gamma_1(N)) \to M_{k+(p+1)}(\Gamma_1(N))$$

que es caracteritza per

$$\theta f(q) = \sum n a_n q^n .$$

És injectiva si k és primer amb p, i el nucli de θ sobre $M_{pk}(\Gamma_1(N))$ és la imatge de l'operador V_p.

• La multiplicació per la forma modular A dóna lloc a una aplicació injectiva

$$M_k(\Gamma_1(N)) \to M_{k+(p-1)}(\Gamma_1(N)) \qquad f \mapsto Af .$$

L'operador V_p commuta amb els operadors de Hecke i els diamants; si $k \geq 2$, el mateix passa amb la multiplicació per A. Les regles de commutació per a l'operador de Ramanujan-Katz són:

$$\begin{aligned} (\theta f)|T_\ell &= \ell\,\theta(f|T_\ell) , \\ (\theta f)|U_\ell &= \ell\,\theta(f|U_\ell) , \\ (\theta f)|U_p &= \theta(f|V_p) = 0 . \end{aligned}$$

Considerem l'àlgebra

$$M = \bigoplus_{k \geq 0} M_k(\Gamma_1(N)) ,$$

on $M_0(\Gamma_1(N)) := \overline{\mathbb{F}}_p$. Es té que el nucli de l'homorfisme

$$M \to \overline{\mathbb{F}}_p[[q]] \qquad f \mapsto f(q) = \sum a_n q^n$$

és l'ideal principal $(A-1)M$. Per tant, si $\widetilde{M}$ és la imatge de $M/(A-1)M$ dins $\overline{\mathbb{F}}_p[[q]]$, es tracta d'una àlgebra graduada per $\mathbb{Z}/(p-1)\mathbb{Z}$. Posem $\widetilde{M} = \oplus_\alpha \widetilde{M}_\alpha$, on $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$.

Definició 3.1. Es diu que $\sum a_n q^n \in \widetilde{M}_\alpha$ té filtració k si és la imatge d'una forma modular $f \in M_k(\Gamma_1(N))$ no divisible per A dins M; aleshores $k \equiv \alpha \pmod{p-1}$. El principi del q-desenvolupament permet parlar de la filtració de f.

Definició 3.2. S'anomena θ-cicle de Tate de f la seqüència dels $p-1$ nombres enters formada per les filtracions de θf, $\theta^2 f$, ..., $\theta^{p-1} f$.

Recordem alguns resultats sobre les filtracions de les formes modulars $(\mathrm{mod}\, p)$; en ells hi trobem la relació de l'operador de Hecke U_p i les filtracions.

Proposició 3.3. (cf. **[Se 73]**, **[Ka 76]**, **[Jo 82]**, **[Gr 90]**). *Sigui* $f(q) = \sum a_n q^n$ *una forma modular* $(\mathrm{mod}\, p)$ *per a* $\Gamma_1(N)$. *Aleshores es té:*

i) *Si* f *té filtració* k *amb* $\mathrm{m.c.d.}(k,p) = 1$, *aleshores* θf *té filtració* $k+p+1$; *a més, si la filtració de* f *satisfà* $2 \le k \le p$ *i* $k' = p+1-k$, *es té que* $\theta^{k'} f$ *té filtració* $\le p+1+k'$, *amb igualtat si, i només si,* $f|U_p \neq 0$.

ii) *Si* f *és una forma de Hecke* $(\mathrm{mod}\, p)$ *amb* $a_p \neq 0$, *aleshores* f *té filtració* k *amb* $2 \le k \le p+1$.

iii) *Si* $f(q) = \sum a_n q^n$ *és una forma de Hecke* $(\mathrm{mod}\, p)$ *amb* $a_p = 0$ *i filtració* k *amb* $3 \le k \le (p+3)/2$, *aleshores* $\theta^{p+1-k} f$ *té filtració* $p+3-k$.

També recordem el teorema d'Ash i Stevens que facilita un procediment per tal d'obtenir tots els sitemes de valors propis $(\mathrm{mod}\, p)$ a partir d'aquells que provenen de pes $\le p+1$.

Teorema 3.4. (cf. **[Ash-St 86]**). *Si* f *és una forma de Hecke* $(\mathrm{mod}\, p)$ *de tipus* (N,k,ε), *aleshores existeixen enters* m *i* k' *amb* $0 \le m \le p-1$,

$k' \leq p+1$ i una forma de Hecke (mod p), *g, de tipus (N, k', ε) tal que f i $\theta^m g$ tenen els mateixos valors propis per a tots els operadors de Hecke llevat, potser, de U_p.*

Per acabar aquesta secció esmentem breument la teoria dels aixecaments de formes modulars (mod p) a formes modulars en característica zero.

Triem $\overline{\mathbb{Q}}_p$ una clausura de $\mathbb{Q}_p$ i posem $\overline{\mathbb{Z}}_p$ la clausura entera de $\mathbb{Z}_p$ dins $\overline{\mathbb{Q}}_p$. Sigui $\mathfrak{P}$ l'ideal maximal de $\overline{\mathbb{Z}}_p$. Si $\mathbb{F}_q$ és un cos finit de característica p, fixem una immersió de $\mathbb{F}_q$ dins $\overline{\mathbb{F}}_p = \overline{\mathbb{Z}}_p/\mathfrak{P}$, el cos residual de $\overline{\mathbb{Z}}_p$.

Definició 3.5. Sigui $f(q) = \sum a_n q^n$ una forma nova (mod p) de tipus (N, k, ε), definida sobre $\mathbb{F}_q$. Una forma nova $F(q) = \sum A_n q^n$ per a $\Gamma_1(M)$, definida sobre $\overline{\mathbb{Z}}_p$, és diu que és un aixecament de f si

$$A_n \equiv a_n \pmod{\mathfrak{P}},$$

per a tot $n \geq 1$.

Definició 3.6. Si ε és un caràcter de Dirichlet mòdul N amb valors a $\overline{\mathbb{F}}_p$, existeix un únic caràcter de Dirichlet ε_N mòdul N amb valors a $\overline{\mathbb{Z}}_p$ tal que

$$\varepsilon_N(\ell) \equiv \varepsilon(\ell) \pmod{\mathfrak{P}},$$

per a tot $\ell \in (\mathbb{Z}/N\mathbb{Z})^*$. El caràcter ε_N s'anomena l'aixecament multiplicatiu de ε.

D'altra banda, denotem per $\chi_p : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z}_p^*$ el caràcter de Teichmüller, que satisfà

$$\chi_p(n) \equiv n \pmod{p} \qquad \text{per a tot } n \in \mathbb{Z}, \text{m. c. d.}(n,p) = 1\,.$$

El resultat següent mostra com certes formes noves (mod p) admeten aixecaments de pes 2.

Teorema 3.7. (cf. [Se 88], [Gr 90]). 1) *Sigui f una forma nova* (mod p) *de tipus $(N, 2, \varepsilon)$. Aleshores existeix un aixecament de f a una forma nova F de tipus $(N, 2, \varepsilon_N)$, definida sobre $\overline{\mathbb{Z}}_p$.*

2) *Sigui f una forma nova* $(\mathrm{mod}\, p)$ *de tipus* (N, k, ε), *amb* $3 \leq k \leq p+1$. *Si* $k = p+1$, *suposem a més que la filtració de* f *és* $p+1$. *Aleshores existeix un aixecament de* f *a una forma nova* F *de tipus* $(Np, 2, \varepsilon_N \chi_p^{k-2})$ *amb coeficients a* $\overline{\mathbb{Z}}_p$.

Per raons d'ús futur, introduïm les definicions següents:

Definició 3.8. Una forma parabòlica de Hecke $(\mathrm{mod}\, p)$

$$f(q) = \sum a_n q^n$$

es diu p-ordinària si el valor propi de l'operador de Hecke U_p és no nul o, equivalentment, si

$$a_p \not\equiv 0 \quad \text{a } \overline{\mathbb{F}}_p\,.$$

En cas contrari, diem que f és p-supersingular.

Definició 3.9. Una forma parabòlica de Hecke, definida sobre $\overline{\mathbb{Z}}_p$,

$$F(q) = \sum A_n q^n$$

es diu $\mathfrak{P}$-ordinària si

$$A_p \not\equiv 0 \pmod{\mathfrak{P}}\,.$$

En cas contrari, diem que F és $\mathfrak{P}$-supersingular.

§4. Formes modulars complexes

Una vegada introduïdes les formes modulars en el sentit de Katz, en aquesta secció es recuperen les formes modulars clàssiques (definides sobre $\mathbb{C}$). Per bé que la teoria és molt extensa en aquest camp, passem a recordar únicament els estris que usarem a partir del capítol 5: involucions de Fricke, operadors traça i sèries d'Eisenstein de pes 1.

Sigui $F(z)$ una funció holomorfa del semiplà superior de Poincaré $\mathbb{H}$, k un enter positiu i $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un element de $\mathrm{GL}_2^+(\mathbb{R})$. Es defineix la funció

$$F(z)|[\gamma]_k = \det(\gamma)^{k/2}(cz+d)^{-k} F(\frac{az+b}{cz+d})\,.$$

Quan l'enter k estigui sobreentès escriurem simplement $F|\gamma$.

Sigui N un enter positiu. El grup modular $\Gamma_0(N)$ es defineix com usualment:

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

Amb les notacions del §2, en el cas particular $R = \mathbb{C}$, obtenim el $\mathbb{C}$-espai vectorial de les formes modulars

$$M_k(\Gamma_1(N))$$

definides sobre $\mathbb{C}$. És clar que

$$M_k(\Gamma_1(N)) = \oplus_\varepsilon M_k(N, \varepsilon) ,$$

on ε descriu els caràcters de Dirichlet mòdul N. A més, l'espai $M_k(N, \varepsilon)$ es pot identificar (cf. **[Ba-Ne 81]**) amb el de les funcions holomorfes

$$F : \mathbb{H} \to \mathbb{C}$$

que satisfan:

1) $F|\gamma = \varepsilon(d)F$, $\forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \Gamma_0(N)$ i

2) $F|\gamma_0$ admet una expressió $\sum_{n \geq 0} B_n e^{2\pi i z n/N}$, $\forall \gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$.

A continuació recordem les involucions de Fricke (cf.**[Fri 22]**, **[Fri 28]**, **[At-Li 78]**) i l'operador traça entre certs espais de formes modulars definides sobre $\mathbb{C}$.

Considerem les descomposicions de $N = MQ$ com a producte de dos enters positius i primers entre ells. Cada caràcter de Dirichlet ε mòdul N pot ser expressat com $\varepsilon = \varepsilon_M \varepsilon_Q$, on ε_M i ε_Q són caràcters de Dirichlet mòdul M i Q, respectivament. Posem

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix}$$

on $x, y, z, w \in \mathbb{Z}$, $y \equiv 1 \pmod{Q}$, $x \equiv 1 \pmod{N/Q}$, i $\det W_Q = Q$.

Llistem algunes de les propietats més interessants de l'acció de l'operador W_Q sobre l'espai de formes modulars definides sobre $\mathbb{C}$:

• Si F és una forma modular (resp. parabòlica) de tipus $(N, k, \varepsilon_M \varepsilon_Q)$, $F|W_Q$ és una forma modular (resp. parabòlica) de tipus $(N, k, \varepsilon_M \bar{\varepsilon}_Q)$, on "$\bar{}$" denota la conjugació complexa. A més,

$$F|W_Q|W_Q = \bar{\varepsilon}_M(Q)\varepsilon_Q(-1)F\,.$$

• Si

$$W'_Q = \begin{pmatrix} Qx' & y' \\ Nz' & Qw' \end{pmatrix}$$

amb $x', y', z', w' \in \mathbb{Z}$ i $\det W'_Q = Q$, aleshores

$$F|W'_Q = \bar{\varepsilon}_M(x')\bar{\varepsilon}_Q(y')F|W_Q\,.$$

En particular, l'acció de W_Q no depèn de l'elecció dels enters x, y, z, i w.

• Si $\ell \nmid N$ i F és una forma modular de tipus $(N, k, \varepsilon_M \varepsilon_Q)$ funció pròpia per l'operador de Hecke T_ℓ amb valor propi A_ℓ, aleshores $F|W_Q$ és funció pròpia per T_ℓ amb valor propi $A_\ell \bar{\varepsilon}_Q(\ell)$.

• Les involucions de Fricke preserven les formes noves. Concretament, si F és una forma nova de tipus $(N, k, \varepsilon_M \varepsilon_Q)$, aleshores existeix una forma nova F' de tipus $(N, k, \varepsilon_M \bar{\varepsilon}_Q)$ i una constant $\lambda_Q(F)$ (anomenada el pseudo-valor propi de W_Q en F) tal que

$$F|W_Q = \lambda_Q(F)F'\,.$$

Es prova que el nombre complex $\lambda_Q(F)$ és un enter algebraic de mòdul 1. Es té

$$\lambda_Q(F)\lambda_Q(F') = \bar{\varepsilon}_M(Q)\varepsilon_Q(-1)\,,$$

i si escrivim els desenvolupaments de Fourier

$$F(q) = \sum_{n\geq 1} A_n q^n\,, \quad F'(q) = \sum_{n\geq 1} A'_n q^n\,,$$

aleshores

$$A'_p = \begin{cases} A_p \bar{\varepsilon}_Q(p) & \text{si } p \nmid Q \\ \overline{A}_p \varepsilon_M(p) & \text{si } p \mid Q\,. \end{cases}$$

També

$$F|W_N = \lambda_N(F)\overline{F}\,,$$

on

$$\overline{F}(q) := \sum_{n\geq 1} \overline{A}_n q^n\,.$$

• Si $Q = p^n$ és potència d'un primer amb m. c. d. $(Q, N/Q) = 1$, i $F(q) = \sum A_n q^n$ és una forma nova de tipus $(N, k, \varepsilon_M \varepsilon_Q)$ tal que $A_p \neq 0$, aleshores el pseudo-valor propi ve donat per la fórmula següent:

$$\lambda_Q(F) = Q^{k/2-1} C(\varepsilon_Q)/A_Q\,,$$

on $C(\varepsilon_Q) = \sum_{1\leq n\leq Q-1} \varepsilon_Q(n) e^{2\pi i n/(Q-1)}$ és la suma de Gauss del caràcter ε_Q, amb el conveni $C(\varepsilon_Q) = -1$ quan $Q = p$ i ε_Q és el caràcter trivial.

Les involucions de Fricke estan estretament lligades a les involucions de Weil a la vista del següent

Teorema 4.1. (cf. **[At-Li 78]**, **[Gr 90]**). *Sigui $F(q) = \sum A_n q^n$ una forma nova de tipus $(Np, 2, \varepsilon_N \varepsilon_p)$, definida sobre un cos de nombres, $p \nmid N$. Aleshores*

$$F|w_\zeta = \lambda_\zeta(F)\, F'\,,$$

on $F'(q) = \sum {A'}_n q^n$ és una forma nova de tipus $(Np, 2, \varepsilon_N \overline{\varepsilon}_p)$ i $\lambda_\zeta(F)$ és una constant no nul·la. A més,

$${A'}_n = A_n\, \overline{\varepsilon}_p(n) \quad \textit{per a tot } n \textit{ primer amb } p\,.$$

Si $\varepsilon_p = 1$, aleshores $F' = F$, ${A_p}^2 = \varepsilon_N(p)$, i $\lambda_\zeta(F) = -A_p$.

Si $\varepsilon_p \neq 1$, aleshores ${A'}_p A_p = p\varepsilon_N(p)$ i la constant $\lambda_\zeta(F)$ ve donada per

$$\lambda_\zeta(F) = \frac{\varepsilon_p(-1)\varepsilon_N(p) \sum_d \varepsilon_p(d)\zeta^d}{A_p}\,.$$

Observació 4.2. Quan ε_p és el caràcter trivial es té $F|W_p = F|w_\zeta$; és a dir, $\lambda_p(F) = \lambda_\zeta(F) = -A_p$. En general, si F és nova de tipus $(Np, 2, \varepsilon_N \varepsilon_p)$, les formes $F|W_p$ i $F|w_\zeta$ difereixen en un múltuple de la forma nova F'.

D'altra banda, les involucions de Fricke permeten donar una expressió senzilla de l'operador traça entre certs espais de formes modulars definides sobre $\mathbb{C}$ (cf. **[Sh-2 73]**, **[Ko 76]**). Concretament, si N és un enter positiu primer amb p, tenim la igualtat

$$\Gamma_0(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_0(N) = \Gamma_0(N)W_p \cup \bigcup_{j=1}^{p}\Gamma_0(N)\gamma_j\,,$$

on $\gamma_j = \begin{pmatrix}1 & j\\ 0 & p\end{pmatrix}$ i la reunió és disjunta. Si posem $\sigma_j = {W_p}^{-1}\gamma_j$, $1 \le j \le p$, i $\sigma_{p+1} = 1$ s'obté un sistema de representants de $\Gamma_0(Np)\backslash\Gamma_0(N)$:

$$\Gamma_0(N) = \bigcup_{j=1}^{p+1}\Gamma_0(Np)\sigma_j\,.$$

Sigui ara ϕ un caràcter de Dirichlet mòdul N. Aleshores es pot definir l'operador traça

$$\mathrm{Tr}\ :\ S_k(Np,\phi) \to S_k(N,\phi)\,, \qquad \mathrm{Tr}\,(G) = \sum_{j=1}^{p+1} G|[\sigma_j]_k\,.$$

És fàcil veure que

$$\mathrm{Tr}\,(G) = G + \phi(p)^{-1}p^{1-k/2}G|[W_p]_k|U_p\,;$$

relació que usarem posteriorment.

Recordem finalment les definicions i propietats bàsiques de les sèries d'Eisenstein de pes 1 definides sobre $\mathbb{C}$. Una informació més detallada es troba en el vast treball de Hecke **[He 27]**.

La lletra p segueix denotant un nombre primer, ara amb $p \ge 3$. Fixem una extensió a $\overline{\mathbb{Q}}$ de la valoració p-àdica v_p de $\mathbb{Q}$, normalitzada de manera que $v_p(p) = 1$. Sigui $\mathfrak{P}$ el primer de $\overline{\mathbb{Q}}$, dividint p, que l'extensió determina.

Denotem per ψ el caràcter de Dirichlet mòdul p,

$$\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \overline{\mathbb{Q}}^*\,,$$

tal que

$$\psi(n)\,n \equiv 1 \pmod{p} \qquad \text{per a tot } n \in \mathbb{Z},\ \text{m. c. d.}\,(n,p) = 1\,.$$

Observem que, després de la immersió $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ determinada, ψ és l'invers del caràcter de Teichmüller χ_p.

Resulta de Hecke que l'espai de les sèries d'Eisenstein de pes 1 per al grup de congruència

$$\Gamma(N) = \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N\right\}$$

està generat per les formes

$$\{G_1(z; a_1, a_2, p)\}_{a_1, a_2 \in \mathbb{Z}}$$

definides per

$$G_1(z; a_1, a_2, p) = C(a_1, a_2, p) - \frac{2\pi i}{p} \cdot \sum_{\substack{m \cdot m_1 > 0 \\ m_1 \equiv a_1 \pmod p}} \operatorname{sgn} m \, \zeta_p^{a_2 m} e^{2\pi i (m\, m_1\, z/p)},$$

amb

$$\begin{aligned} C(a_1, a_2, p) = &\delta(\frac{a_1}{p}) \sum_{m_2 \equiv a_2 \pmod p}{}' \frac{\operatorname{sgn} m_2}{|m_2|^{1+s}}\Big|_{s=0} \\ &- \frac{\pi i}{p} \sum_{m_1 \equiv a_1 \pmod p}{}' \frac{\operatorname{sgn} m_1}{|m_1|^{s}}\Big|_{s=0}, \end{aligned}$$

on $\zeta_p = e^{2\pi i/p}$, δ és la funció quasi-nul·la que pren el valor 1 sobre els enters, i $\sum'$ denota que la suma s'estén a totes les parelles, llevat de $m_1 = m_2 = 0$.

Si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, se satisfà l'equació funcional

$$G_1(\frac{az+b}{cz+d}; a_1, a_2, p) = (cz+d) G_1(z; aa_1 + ca_2, ba_1 + da_2, p).$$

Per a cada caràcter de Dirichlet φ mòdul p tal que $\varphi(-1) = -1$, siguin

$$\begin{aligned} G_{1,\varphi} &= \sum_{n \bmod p} \overline{\varphi}(n) G_1(z; 0, n, p), \\ G_{2,\varphi} &= \sum_{n,m \bmod p} \varphi(n) G_1(z; n, m, p). \end{aligned}$$

Les formes $G_{1,\varphi}$ i $G_{2,\varphi}$ són sèries d'Eisenstein de tipus $(p,1,\varphi)$ definides sobre $\mathbb{C}$; en la punta ∞, tenen per desenvolupaments de Fourier:

$$G_{1,\varphi} = 2L(1,\overline{\varphi}) - \frac{4\pi i C(\overline{\varphi})}{p} \sum_{\substack{m>0 \\ m_1>0}} \varphi(m) e^{2\pi i m m_1 z},$$

$$G_{2,\varphi} = -2\pi i L(0,\varphi) - 4\pi i \sum_{\substack{m>0 \\ m_1>0}} \varphi(m_1) e^{2\pi i m m_1 z},$$

on $L(s,\varphi)$ és la funció L de Dirichlet i $C(\varphi)$ és la suma de Gauss per al caràcter φ. Per ser φ un caràcter senar, l'equació funcional

$$\pi^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)p^s L(s,\varphi) = -iC(\varphi)\pi^{-(2-s)/2}\Gamma\left(\frac{2-s}{2}\right)L(1-s,\overline{\varphi})$$

porta a la igualtat $L(0,\varphi) = (C(\varphi)/\pi i)L(1,\overline{\varphi})$. D'altra banda, les relacions d'ortogonalitat ens proporcionen $C(\varphi)C(\overline{\varphi}) = -p$. D'on

$$G_{1,\varphi} = \frac{C(\overline{\varphi})}{p} G_{2,\varphi}.$$

Siguin

$$E_{1,\varphi} = \frac{G_{1,\varphi}}{2L(1,\overline{\varphi})}, \qquad c_\varphi = -\frac{2\pi i C(\overline{\varphi})}{pL(1,\overline{\varphi})} = \frac{2}{L(0,\varphi)},$$

aleshores

$$E_{1,\varphi} = 1 + c_\varphi \sum_{\substack{m>0 \\ m_1>0}} \varphi(m) e^{2\pi i m m_1 z}.$$

Ja que $L(1,\overline{\varphi}) = -\dfrac{C(\overline{\varphi})}{p}\dfrac{\pi}{ip}\displaystyle\sum_{1\le n\le p-1}\varphi(n)n$, tenim

$$c_\varphi = -\frac{2p}{\sum_{1\le n\le p-1}\varphi(n)n}.$$

El caràcter ψ, abans introduït, és un generador del grup de caràcters de Dirichlet mòdul p. Per tant, existeix un únic enter t amb $1 \le t \le p-1$ tal que $\varphi = \psi^{-t}$. Un càlcul estàndard en sumes de Gauss condueix a

$$c_\varphi \equiv 0 \pmod{\mathfrak{P}} \iff t = p-2 \iff \varphi = \psi.$$

Notem que la sèrie d'Eisenstein $E_{1,\psi}$ és de tipus $(p,1,\psi)$ i satisfà

$$E_{1,\psi} \equiv 1 \pmod{\mathfrak{P}}.$$

§5. Corbes de Weil

Acabem aquest capítol recordant les diferents definicions equivalents de les corbes el·líptiques dites de Weil, així com la important conjectura de Hasse-Shimura-Taniyama-Weil.

Sigui E una corba el·líptica sobre $\mathbb{Q}$, N_E el seu conductor geomètric i

$$L(E,s) = \prod_{\ell | N_E} \frac{1}{1 - A_\ell \ell^{-s}} \prod_{\ell \nmid N_E} \frac{1}{1 - A_\ell \ell^{-s} + \ell^{1-2s}} = \sum_{n \geq 1} \frac{A_n}{n^s}$$

la seva L-sèrie de Hasse-Weil. Recordem que

$$A_\ell = 1 + \ell - \text{ nombre de punts a } \tilde{E}(\mathbb{F}_\ell),$$

on $\tilde{E}$ és la corba que s'obté en reduir una equació minimal de E mòdul el primer ℓ. Sabem que $L(E,s)$ convergeix en el semiplà

$$\mathrm{Re}(s) > 3/2.$$

En afegir els factors d'Euler a l'infinit, considerem la funció

$$\Lambda_E(s) = N_E^{s/2} (2\pi)^{-s} \Gamma(s) L(E,s),$$

que és holomorfa per a $\mathrm{Re}(s) > 3/2$.

Definició 5.1. Una corba el·líptica E sobre $\mathbb{Q}$ es diu de Weil si satisfà una de les condicions equivalents següents:

i) La funció $\Lambda_E(s)$ admet prolongació analítica a tot $\mathbb{C}$ i satisfà l'equació funcional

$$\Lambda_E(2-s) = w\, \Lambda_E(s),$$

on $w = \pm 1$.

ii) L'anti-transformada de Mellin de $\Lambda_E(s)$ és una forma nova, definida sobre $\mathbb{C}$, de tipus $(N_E, 2, 1)$. És a dir, existeix una forma nova $F \in S_2(N_E, 1)$ tal que

$$(-i)^s N_E^{s/2} \int_0^{i\infty} F(z) z^{s-1}\, dz = \Lambda_E(s).$$

A més, la forma F satisfà

$$F\left(-\frac{1}{N_E z}\right) = -w\, F(z)\,.$$

iii) La corba E és isògena a un factor de la jacobiana $J_0(N_E)_{/\mathbb{Q}}$ de la corba modular $X_0(N_E)_{/\mathbb{Q}}$.

iv) Existeix un morfisme $\mathbb{Q}$-racional no constant $\phi : X_0(N_E)_{/\mathbb{Q}} \to E$ tal que

$$\phi^*(\omega_E) = c \sum_{n\geq 1} A_n e^{2\pi i n z}\, dz\,,$$

per a certa constant c (la constant de Manin).

Conjectura 5.2. (Hasse-Shimura-Taniyama-Weil). *Tota corba el·líptica E sobre $\mathbb{Q}$ és de Weil.*

L'origen d'aquesta conjectura es remunta a una exposició de Taniyama (cf. [**Tan 55¬**], o bé el recull, escrit en japonès, que es troba en les seves obres completes). Des d'aleshores ençà ha estat contrastada numèricament en diversos treballs. Àdhuc és ben conegut que algunes famílies de corbes el·líptiques satisfan la conjectura; per exemple, les corbes el·líptiques amb multiplicació complexa [**Sh-2 71**]. Com ja s'ha esmentat en la introducció, aquesta conjectura implica el darrer teorema de Fermat (cf. [**Fr 86**], [**Se 87**], [**Ri 90**]).

CAPÍTOL 2

Representacions de Galois modulars

Ramanujan a **[Ra 16]**, a la vista del desenvolupament del discriminant

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n ,$$

conjecturà

$$\tau(m\,n) = \tau(m)\,\tau(n) , \tag{1}$$

$$\tau(p^{n+1}) = \tau(p^n)\,\tau(p) - p^{11}\,\tau(p^{n-1}) , \tag{2}$$

$$|\tau(p)| < 2\,p^{11/2} , \tag{3}$$

i provà

$$\tau(p) \equiv 1 + p^{11} \pmod{691} , \tag{4}$$

per a m i n enters positius primers entre ells i p un primer.

Les dues primeres relacions foren provades per Mordell un any més tard a **[Mo 17]**, i no fan sinó traduir el fet que Δ és una forma de Hecke. En efecte, Δ és l'única forma nova de tipus $(1,12,1)$, definida sobre $\mathbb{C}$ (per exemple, cf. **[He 37]**). La tercera relació conjecturada per Ramanujan era la que més es resistia.

Serre **[Se 67]** i Swinerton-Dyer **[Sw 73]** compilen les congruències per als coeficients $\tau(n)$ obtingudes per Wilton en la dècada dels 30, Bambah, Lahivi, Lehmer i Ramanathan en la dècada dels 40, i Kolberg, Ashworth i el mateix Swinnerton-Dyer en la dels 60. Aquestes congruències s'afegien a la ja provada per Ramanujan (4). Citem, per exemple:

$$\tau(p) \equiv p + p^4 \pmod 7,$$

$$\tau(p) \equiv 1 + p \pmod 3,$$

$$\tau(p) \equiv \begin{cases} 0 \pmod{23} & \text{si } \left(\frac{p}{23}\right) = -1, \\ 2 \pmod{23} & \text{si } p \text{ és de la forma } u^2 + 23v^2, \\ -1 \pmod{23} & \text{si } \left(\frac{p}{23}\right) = +1, \text{ però no és de la forma } u^2 + 23v^2. \end{cases}$$

Més congruències es troben a [**Sw 73**].

Degut a aquests fets, a [**Se 67**] es planteja la qüestió de si hom podia esperar noves congruències de la funció τ de Ramanujan per a altres primers. El camí per trobar la resposta, indicat per Serre, es val dels treballs de Shimura sobre lleis de reciprocitat per a extensions no resolubles [**Sh 66**], on s'interpreten els coeficients de Fourier de certes formes de Hecke de pes 2 com a traces de les imatges dels elements de Frobenius, mitjançant representacions de Galois p-àdiques. A [**Se 67**] es conjectura l'existència d'un sistema compatible de representacions galoisianes, p-àdiques i $(\mathrm{mod}\, p)$, associat a una forma de Hecke de tipus (N, k, ε).

En aquesta direcció, Shimura obté conclusions satisfactòries per al cas de pes $k = 2$ (cf. [**Ei 54**], [**Sh 71**]). Per a $k > 2$, el teorema d'existència d'aquestes representacions s'atribueix a Deligne, qui a [**De 71**] en dóna una prova completa per al cas de la forma modular Δ. Aquest teorema serví a Deligne, com a punt de partida, per provar la relació (3) conjecturada per Ramanujan.

Posteriorment, Langlands i Ohta, sota el punt de vista de la teoria de les representacions automorfes, ho generalitzen per a un nivell N arbitrari (cf. [**Lan 73**], [**Oh 82**]). També Hida a [**Hi 86**], a partir de la cohomologia parabòlica i les àlgebres de Hecke universals i d'Iwasawa, aconsegueix una prova de l'existència de la representació p-àdica per al cas de formes modulars p-ordinàries. Recentment, a [**Gr 90**], Gross ha obtingut una demostració senzilla de l'existència de la representació $(\mathrm{mod}\, p)$ aprofitant els resultats de Serre, esmentats en el capítol 1, sobre els aixecaments de formes modulars.

En aquest capítol recordem dos teoremes de Shimura i Deligne on es relacionen les formes modulars amb les representacions del grup de Galois

absolut $\mathrm{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Pel seu interés, hem cregut oportú incloure un esbós de les demostracions d'ambdos.

§1. Representacions modulars p-àdiques

El primer resultat que recordem és el

Teorema 1.1. (cf. [**Sh 71**]). *Sigui $F(q) = \sum A_n q^n$ una forma nova de tipus $(M, 2, \varepsilon_F)$, definida sobre una extensió finita K de $\mathbb{Q}_p$. Sigui $\mathcal{O}_K$ l'anell de valoració discreta corresponent.*

Aleshores existeix una representació de Galois contínua

$$\rho_F : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_K),$$

tal que:

1) *És no-ramificada en els primers $\ell \nmid Mp$.*

2) *Per a cada primer $\ell \nmid Mp$ se satisfà*

$$\mathrm{tr}\,(\rho_F(\mathrm{Frob}_\ell)) = A_\ell \qquad \det(\rho_F(\mathrm{Frob}_\ell)) = \varepsilon_F(\ell)\ell.$$

DEMOSTRACIÓ (cf. [**Gr 90**]). Sigui $J_1(M)_{/\mathbb{Q}}$ la Jacobiana de la corba modular $X_1(M)_{/\mathbb{Q}}$; aquesta varietat abeliana té bona reducció en tot primer $\ell \nmid M$. Les congruències d'Eichler-Shimura [**Sh 71,** teorema **7.9**] asseguren que

$$T_{\ell,\mathrm{Alb}} = \mathrm{Ver}_\ell + <\ell>_{\mathrm{Alb}} \mathrm{Fr}_\ell$$
$$\mathrm{Ver}_\ell \mathrm{Fr}_\ell = \mathrm{Fr}_\ell \mathrm{Ver}_\ell = \ell,$$

a $\mathrm{End}(J_1(M)_{/\mathbb{F}_\ell})$, on Fr_ℓ i Ver_ℓ denoten l'endomorfisme de Frobenius i el Verschiebung, respectivament.

Sigui $T_p\, J_1(M) = \varprojlim J_1(M)[p^n](\overline{\mathbb{Q}})$ el p-mòdul de Tate de $J_1(M)_{/\mathbb{Q}}$, i considerem $V = T_p\, J_1(M) \otimes_{\mathbb{Z}_p} K$, que és un mòdul sobre la K-àlgebra $\mathbb{T} \otimes K$. El grup de Galois $\mathrm{G}_{\mathbb{Q}}$ opera K-linealment sobre V, i la representació que indueix aquesta acció és no-ramificada fora de Mp. D'altra banda, ja que

els endomorfismes que generen $\mathbb{T}$ estan definits sobre $\mathbb{Q}$, les accions de $G_{\mathbb{Q}}$ i $\mathbb{T} \otimes K$ sobre V commuten.

La forma nova F proporciona un morfisme de $\mathbb{T} \otimes K$ amb valors a K

$$\lambda : \mathbb{T} \otimes K \to K ,$$

tal que $\lambda(T_\ell \otimes 1) = A_\ell$ per a $\ell \nmid M$ i $\lambda(< d > \otimes 1) = \varepsilon_F(d)$ per a $d \in (\mathbb{Z}/M\mathbb{Z})^*$.

Prenem W el subspai vectorial de V sobre K on $\mathbb{T} \otimes K$ hi opera a través del caràcter λ. L'espai W té dimensió 2 sobre K. En efecte, per ser F una forma nova, el teorema de multiplicitat 1 d'Atkin-Lehner-Li (cf. **[At-Le 70]**, **[Li 75]**) ens assegura que l'espai propi per a tots els operadors de Hecke amb els valors propis de F és de dimensió 1. D'altra banda, tenint en compte el teorema de comparació entre la cohomologia étale i la singular (cf. **[Fre-Ki 88]**), la representació de $\mathbb{T} \otimes K$ sobre V és la suma directa de l'acció sobre les diferencials i la representació dual (cf. **[De 71]**).

Obtenim així una representació contínua

$$r_F : G_{\mathbb{Q}} \to \mathrm{Aut}_K(W) \backsimeq \mathrm{GL}_2(K) ,$$

que és no-ramificada en els primers $\ell \nmid Mp$. Per ser r_F contínua, i $G_{\mathbb{Q}}$ compacte, la imatge de r_F deixa estable una $\mathcal{O}_K$-ret de rang 2.

Sigui Frob_ℓ un automorfisme de Frobenius en ℓ. Per les congruències d'Eichler-Shimura tenim que

$$A_\ell = \ell r_F(\mathrm{Frob}_\ell)^{-1} + \varepsilon_F(\ell) r_F(\mathrm{Frob}_\ell) ,$$

a $\mathrm{End}_K(W)$. D'on, $r_F(\mathrm{Frob}_\ell)$ satisfà l'equació matricial

$$x^2 - A_\ell/\varepsilon_F(\ell)x + \ell/\varepsilon_F(\ell) .$$

Per tal de veure que es tracta efectivament del seu polinomi característic comprovem que $\det(r_F(\mathrm{Frob}_\ell)) = \ell/\varepsilon_F(\ell)$. Estudiem, doncs, la representació $\det(r_F)$. Observem d'entrada que, per ser W de dimensió 2 sobre K, l'espai vectorial de les formes bilineals alternades definides sobre W és de dimensió 1. Es construeix una forma bilineal alternada definida sobre W de la manera següent:

Considerem l'aparellament de Weil

$$(\ , \ ) : T_p\, J_1(M) \times T_p\, J_1(M) \to T_p(\mathbb{G}_m) = \mathbb{Z}_p(1)\,,$$

que és alternat, respecta l'acció de Galois, i satisfà $(t\,a, b) = (a, t^*\,b)$ per a tot $t \in \mathrm{End}(J_1(M)_{/\mathbb{Q}})$, on * és la involució de Rosati. Es defineix

$$< \ , \ > : T_p\, J_1(M) \times T_p\, J_1(M) \to T_p\,(\mathbb{G}_m) = \mathbb{Z}_p(1)$$

per la fórmula

$$< a, b >= (a, w_\zeta\, b)\,,$$

on w_ζ és la involució de Weil, abans introduïda. Indueix un aparellament alternat i no-degenerat

$$< \ , \ > : W \times W \to K\,.$$

Si $a, b \in W$ i σ_ℓ és la projecció de Frob_ℓ a $\mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q})$ tenim:

$$\begin{aligned} < a, b >^{\sigma_\ell} &= (a, w_\zeta\, b)^{\sigma_\ell} = (a^{\sigma_\ell}, {w_\zeta}^{\sigma_\ell}\, b^{\sigma_\ell}) = (a^{\sigma_\ell}, w_\zeta < \ell > \, b^{\sigma_\ell}) \\ &= (a^{\sigma_\ell}, w_\zeta \varepsilon_F(\ell)\, b^{\sigma_\ell}) =< a^{\sigma_\ell}, \varepsilon_F(\ell)\, b^{\sigma_\ell} >= \varepsilon_F(\ell) < a^{\sigma_\ell}, b^{\sigma_\ell} > \,. \end{aligned}$$

I també,

$$< a, b >^{\sigma_\ell} = (a, w_\zeta\, b)^{\sigma_\ell} = \ell(a, w_\zeta\, b) = \ell < a, b > \,.$$

D'on s'obté que

$$< a^{\sigma_d}, b^{\sigma_d} >=< a, b > \ell/\varepsilon_F(\ell)$$

i, per tant, $\det(r_F(\mathrm{Frob}_\ell)) = \ell/\varepsilon_F(\ell)$.

Finalment, podem veure el caràcter de Dirichlet ε_F com un caràcter galoisià fent

$$\varepsilon_F : \ \mathrm{G}_\mathbb{Q} \to \mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq \mathbb{Z}/M\mathbb{Z}^* \to K^*\,,$$

i definir

$$\rho_F = r_F \otimes \varepsilon_F\,.$$

La representació ρ_F és no-ramificada fora de Mp, i per a cada $\ell \nmid Mp$,

$$x^2 - A_\ell x + \ell\varepsilon_F(\ell)$$

és el polinomi característic de $\rho_F(\mathrm{Frob}_\ell)$. □

És per raons d'ús posterior que recordem també la prova original del teorema de Shimura.

DEMOSTRACIÓ (cf. **[Sh 71]**, **[Sh 73]**). Primer s'utilitza el teorema de Wedderburn per descompondre l'àlgebra de Hecke; el factor simple de l'àlgebra associat a F proporciona una varietat abeliana A_F que és un "factor" de $J_1(M)_{/\mathbb{C}}$. Existeix una distinció subtil segons que es prengui aquest "factor" com a subvarietat o com a quocient de $J_1(M)_{/\mathbb{C}}$; aquesta dualitat prové del fet que, sobre $\mathbb{C}$, tenim un aparellament

$$(\ ,\ )_{J_1(M)_{/\mathbb{C}}} : \Omega_{J_1(M)_{/\mathbb{C}}} \times T_{J_1(M)_{/\mathbb{C}},0} \to \mathbb{C},$$

entre els espais cotangent i tangent a l'origen. Aquest fet fa que es dupliquin les fórmules (relacions de commutativitat entre els operadors, congruències d'Eichler-Shimura ...).

L'espai de les diferencials invariants $\Omega_{J_1(M)_{/\mathbb{Q}}}$ sobre $J_1(M)_{/\mathbb{Q}}$ s'identifica amb l'espai de les diferencials regulars sobre $X_1(N)_{/\mathbb{Q}}$, d'on es té que $\Omega_{J_1(M)_{/\mathbb{C}}} = \Omega_{J_1(M)_{/\mathbb{Q}}} \otimes \mathbb{C} = H^0(X_1(N)_{/\mathbb{C}}, \Omega^1_{X_1(N)_{/\mathbb{C}}})$ i, per tant, en tractar les formes modulars és més natural treballar a l'espai cotangent.

Aleshores la construcció de Shimura del quocient de $J_1(M)_{/\mathbb{C}}$,

$$\nu : J_1(M)_{/\mathbb{C}} \to A_F,$$

satisfà:

1) A_F i ν estan definits sobre $\mathbb{Q}$; el nucli de ν és connex,

2) $\dim A_{F|\mathbb{Q}}=[K_F : \mathbb{Q}]$, on K_F és el cos de nombres definit per F, amb anell d'enters $\mathcal{O}_F$,

3) en reemplaçar la varietat abeliana A_F per una altra d'isògena, si és necessari, es té que $A_{F|\mathbb{Q}}$ té multiplicació $\mathbb{Q}$-racional per l'anell $\mathcal{O}_F$,

$$i : \mathcal{O}_F \to \mathrm{End}(A_{F|\mathbb{Q}}),$$

de manera que $i(A_n)$ ve donat pel diagrama commutatiu següent

$$\begin{array}{ccc} J_1(M)_{/\mathbb{Q}} & \xrightarrow{T_{n,\mathrm{Alb}}} & J_1(M)_{/\mathbb{Q}} \\ \nu\downarrow & & \nu\downarrow \\ A_{F|\mathbb{Q}} & \xrightarrow{i(A_n)} & A_{F|\mathbb{Q}}, \end{array}$$

4) l'espai $\Omega_{A_F/\mathbb{C}}$ de les diferencials invariants s'identifica (via ν^*) amb l'espai de les formes parabòliques generat per les formes conjugades F^σ de la forma F ($\sigma \in \mathrm{Aut}\,\mathbb{C}$).

El criteri de Néron-Ogg-Šafarevič assegura que $A_{F|\mathbb{Q}}$ té bona reducció fora de M. Si $V(A_F) = T_p(A_F) \otimes \mathbb{Q}_p$ és el $\mathbb{Q}_p$-mòdul de Tate associat a la varietat abeliana $A_{F|\mathbb{Q}}$, en fer ús de les congruències d'Eichler-Shimura, es troba, com abans, que la representació p-àdica

$$r_F : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}_K(V(A_F)) \backsimeq \mathrm{GL}_2(K)\,,$$

convenientment torçada, satisfà les condicions del teorema. □

Observació 1.2. Notem que aquests torçaments addicionals són deguts al model de $X_1(N)$ que hem triat. Si, d'entrada, haguéssim escollit el problema de moduli que classifica les parelles (E, a) on $a : \mathbb{Z}/N\mathbb{Z} \to E[N]$ hauriem trobat una altra corba $X_1(N)'$; en aquest cas, les congruències d'Eichler-Shimura corresponents ens haurien estalviat aquest torçament pel caràcter ε_F.

§2. Representacions modulars (mod p)

El segon resultat que recordem és el

Teorema 2.1. (cf. [De 71]). *Sigui $f(q) = \sum a_n q^n$ una forma de Hecke (mod p), definida sobre $\mathbb{F}_q$, de tipus (N, k, ε). Aleshores existeix, llevat d'isomorfismes, una única representació de Galois contínua i semi-simple*

$$\rho_f : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)\,,$$

tal que:

1) *És no-ramificada en els primers $\ell \nmid Np$.*

2) *Per a cada primer $\ell \nmid Np$ se satisfà*

$$\mathrm{tr}\,(\rho_f(\mathrm{Frob}_\ell)) = a_\ell \qquad \det(\rho_f(\mathrm{Frob}_\ell)) = \varepsilon(\ell)\ell^{k-1}\,.$$

DEMOSTRACIÓ (cf. [Gr 90]). És fàcil veure que ens podem reduir al cas en què f sigui una forma nova (mod p) de pes k, amb $2 \leq k \leq p+1$. En cas que $k = p+1$ podem suposar també que f té filtració $p+1$. En efecte, si f és una sèrie d'Eisenstein, l'existència de ρ_f resulta de la teoria de cossos ciclotòmics i aleshores ρ_f redueix. Es pot suposar, doncs, que f és paràbolica. Si f és parabòlica de pes $k = 1$, és senzill trobar $g(q) = \sum b_n q^n$ una forma de Hecke (mod p) de tipus (N, p, ε) en l'espai $< A f, V_p f >$ amb $b_\ell = a_\ell$ per a $\ell \neq p$; aleshores l'existència de ρ_f queda reduïda a la de ρ_g ja que, en tal cas, tindrem $\rho_f = \rho_g$. D'altra banda, si f és parabòlica de pes $k \geq 2$ el seu sistema de valors propis $\{a_\ell\}_{\ell \nmid Np}$ pot ser recuperat a partir d'una forma parabòlica g de pes k amb $2 \leq k \leq p+1$. Més concretament, es té $\theta^i g = f$ per a certa i amb $0 \leq i \leq p-1$ i, aleshores, l'existència de ρ_g propociona l'existència de $\rho_f = \rho_g \otimes \chi^{-i}$, essent χ la reducció mòdul p de χ_p (cf. capítol 1, teorema 3.4). Quan $k = p+1$ i la filtració de f no és $p+1$, tenim $f = Ag$ amb g de pes 2, i $\rho_f = \rho_g$. Finalment, és clar que podem suposar, a més, que f és nova.

Pel teorema 3.7 del capítol 1, existeix $F(q) = \sum A_n q^n$, definida sobre $\overline{\mathbb{Z}}_p$, un aixecament de f, que és una forma nova de tipus $(N, 2, \varepsilon_F)$ si $k = 2$ o de tipus $(Np, 2, \varepsilon_F)$ si $3 \leq k \leq p+1$, on $\varepsilon_F = \varepsilon_N \chi_p^{k-2}$ i ε_N és l'aixecament multiplicatiu de ε. Recordem que els coeficients de Fourier A_n de F, així com els valors del caràcter ε_F, pertanyen a $\mathcal{O}_K$, una extensió entera i finita de $\mathbb{Z}_p$ amb cos de fraccions K. Per construir la representació modular (mod p), ρ_f, s'aplica el teorema 1.1 (amb $M = N$ o Np) a la forma nova F aixecada de f. Es considera la reducció de ρ_F mòdul l'ideal maximal $\mathfrak{p} := \mathcal{O}_K \cap \mathfrak{P}$ de $\mathcal{O}_K$, i es defineix ρ_f com la semi-simplificada d'aquesta reducció. El teorema de Brauer-Nesbitt garanteix, isomorfismes a part, la unicitat de la representació ρ_f.

Comprovem finalment que ρ_f satisfà les condicions que requereix el teorema. Clarament ρ_f és no-ramificada fora de Np per ser-ho ρ_F. També, per tenir

$$A_\ell \equiv a_\ell \pmod{\mathfrak{p}}$$

$$\varepsilon_F(\ell)\ell \equiv \varepsilon_N(\ell)\chi_p^{k-2}(\ell)\ell \equiv \varepsilon(\ell)\ell^{k-1} \pmod{\mathfrak{p}},$$

el polinomi característic de $\rho_f(\mathrm{Frob}_\ell)$ és $x^2 - a_\ell x + \varepsilon(\ell)\,\ell^{k-1}$. □

L'anterior resultat porta a la noció clau de representació de Galois residual modular:

Definició 2.2. Una representació residual

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

es diu modular si existeix una forma de Hecke (mod p)

$$f(q) = \sum a_n q^n$$

tal que $\rho \simeq \rho_f$, on ρ_f és la representació associada a f pel teorema 2.1.

CAPÍTOL 3

Propietats locals

En aquest capítol es revisa el comportament local en p de la representació modular ρ_f associada a una forma nova (mod p). Copsar aquest comportament ha estat un punt clau per a que Serre pogués precisar l'invariant pes associat a una representació.

Es presenten dues situacions, ben diferenciades, segons que la forma modular (mod p) sigui p-ordinària o bé p-supersingular. El cas ordinari ha estat tractat per diferents autors: Deligne, Hida, Mazur, Tilouine, Wiles ... El seu punt de contacte amb les "conjectures principals", la teoria de deformacions, etc. ha provocat un estudi exhaustiu d'aquest cas. Algunes referències són: **[Hi 86]**, **[Ma-Ti 90]**, **[Ma-Wi 84]**, **[Ma-Wi 86]**, **[Ma 90]**, **[Ti 87]**, **[Ti 88]**, **[Wi 86]**.

Per contra, el cas supersingular roman molt més inexplorat. Tractat en la correspondència, no publicada, entre Fontaine i Serre, ens limitem a donar-ne una breu descripció.

§1. Formes modulars ordinàries i representacions ordinàries

Sigui $\mathbb{F}_q$ un cos finit de característica p. Denotem per $\mathcal{C}$ la categoria dels anells locals, noetherians, complets i amb cos residual $\mathbb{F}_q$. Els objectes de $\mathcal{C}$ els anomenem "anells locals de $\mathcal{C}$", i els morfismes de la categoria són els homomorfismes de anells locals que indueixen la identitat sobre els cossos residuals.

Triem una extensió a $\overline{\mathbb{Q}}$ de la valoració p-àdica de $\mathbb{Q}$ i sigui $\mathfrak{P}$ el primer de $\overline{\mathbb{Q}}$ sobre p corresponent. Denotem I_p el grup d'inèrcia de $G_{\mathbb{Q}}$ que correspon a $\mathfrak{P}$.

Definició 1.1. Una representació 2-dimensional

$$\rho : G_{\mathbb{Q}} \to GL_2(A) \qquad (A \in \mathcal{C})$$

es diu $\mathfrak{P}$-ordinària si per a $M = A \times A$, vist com a $G_{\mathbb{Q}}$-mòdul via ρ, el mòdul quocient M_{I_p} dels elements de M co-invariants per I_p és un A-mòdul lliure de rang 1 i un factor directe de M com a A-mòdul.

Observació 1.2. Notem que la nostra definició de representació ordinària es correspon amb la definició de representació co-ordinària de Mazur a [**Ma 90**]. La transformació

$$\rho \mapsto \rho \otimes \det(\rho^{-1})$$

intercanvia les representacions ordinàries i co-ordinàries.

Retornem a les formes modulars definides sobre $\overline{\mathbb{Z}}_p$ i $(\mathrm{mod}\, p)$. Sigui $f(q) = \sum a_n q^n$ una forma de Hecke $(\mathrm{mod}\, p)$, definida sobre $\mathbb{F}_q$, de tipus (N, k, ε) amb $2 \leq k \leq p+1$. Posem ρ_f la representació modular $(\mathrm{mod}\, p)$ semi-simple associada a f. Considerem $F(q) = \sum A_n q^n$ un aixecament de f, definit sobre $K \subset \overline{\mathbb{Q}}_p$. Posem ρ_F la representació p-àdica associada a la forma nova F. A continuació, estudiem el comportament ordinari de les representacions ρ_F i ρ_f segons la forma modular f.

Teorema 1.3. (cf. [**Wi 86**]). *Sigui $F(q) = \sum A_n q^n$ una forma nova, definida sobre $K \subset \overline{\mathbb{Q}}_p$, de tipus $(M, 2, \varepsilon_F)$. Sigui*

$$\rho_F : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_K)$$

la representació p-àdica associada a F. Es té que

$$F \text{ és } \mathfrak{P}\text{-ordinària} \Longrightarrow \rho_F \text{ és } \mathfrak{P}\text{-ordinària}.$$

Més encara, la restricció de ρ_F al grup de descomposició $D_p \simeq \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ es veu, en una base adequada, com

$$\rho_F|_{D_p} = \begin{pmatrix} \varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix},$$

on ε_2 és un caràcter no-ramificat.

DEMOSTRACIÓ (cf. **[Wi 86]**, **[Ma-Ti 90]**). Sigui $A_{F|\mathbb{Q}}$ la varietat abeliana associada, per Shimura, a la forma nova F. Per un teorema de Langlands **[Lan 73]** podem assegurar que si $A_p \neq 0$, la varietat abeliana $A_{F|\mathbb{Q}}$ té reducció semistable sobre el cos de descomposició $\mathbb{Q}_{\varepsilon_F}$ associat, per la teoria de cossos de classes, al caràcter ε_F. A més, si ε_F és ramificat en p, aleshores $A_{F|\mathbb{Q}}$ té bona reducció potencial en p.

Ens podem reduir al cas en què $A_{F|\mathbb{Q}}$ té bona reducció potencial en p; altrament, la reducció de $A_{F|\mathbb{Q}}$ en p és purament multiplicativa i la forma requerida per a la restricció de ρ_F al grup de descomposició resulta de la generalització de la corba de Tate per a varietats de dimensió superior donada en el teorema 1 de **[Ray 70]**.

Per consegüent, ens cal considerar dues possibiltats: que $p \nmid M$ i aleshores $A_{F|\mathbb{Q}}$ té bona reducció sobre $\mathbb{Q}_p$, o bé que $p \mid M$ i aleshores, en aplicar el teorema de Langlands, tenim que $A_{F|\mathbb{Q}}$ adquireix bona reducció després de fer el canvi de base de $\mathbb{Q}$ a $\mathbb{Q}_{\varepsilon_F}$. Denotem per L el cos (contingut a $\overline{\mathbb{Q}}_p$) següent: $L = \mathbb{Q}_p$ si $p \nmid M$ o $L = \mathbb{Q}_{\varepsilon_F,\mathfrak{p}}$, la completació de $\mathbb{Q}_{\varepsilon_F}$ segons $\mathfrak{p}$, si $p \mid M$.

Considerem el grup $\mathfrak{p}$-divisible sobre L de $A_{F/L}$

$$A_{F/L}[\mathfrak{p}^\infty] = \varinjlim A_{F/L}[\mathfrak{p}^n].$$

Es tracta d'un grup p-divisible amb bona reducció sobre L; això vol dir que és la fibra genèrica d'un cert grup p-divisible sobre $\mathcal{O}_L$, l'anell d'enters de L. El teorema fonamental dels grups p-divisibles (cf. **[Ta 67]**) garenteix que el grup p-divisible en qüestió, sobre $\mathcal{O}_L$, és

$$A_{F|\mathcal{O}_L}[\mathfrak{p}^\infty] = \varinjlim A_{F|\mathcal{O}_L}[\mathfrak{p}^n].$$

on $A_{F|\mathcal{O}_L}$ és el model de Néron de $A_{F/L}$ sobre $\mathcal{O}_L$.

Posem $\mathbb{F}_q$ el cos residual de $\mathcal{O}_L$. Per teoria general de grups p-divisibles (cf. **[Ta 67]**, **[Fo 77]**), la fibra especial de $A_{F|\mathcal{O}_L}[\mathfrak{p}^\infty]$ és un grup p-divisible que descompon com a producte de dos grups p-divisibles. És a dir,

$$A_{F/\mathbb{F}_q}[\mathfrak{p}^\infty] = A^0_{F/\mathbb{F}_q}[\mathfrak{p}^\infty] \times A^{et}_{F/\mathbb{F}_q}[\mathfrak{p}^\infty],$$

on $A^0_{F|\mathbf{F}_q}[\mathfrak{P}^\infty]$ és la component connexa de l'element neutre i $A^{et}_{F|\mathbf{F}_q}[\mathfrak{P}^\infty]$ és el seu grup de components. Aquesta descomposició reflecteix una successió exacta

$$0 \to A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty] \to A_{F|\mathcal{O}_L}[\mathfrak{P}^\infty] \to A^{et}_{F|\mathcal{O}_L}[\mathfrak{P}^\infty] \to 0$$

de grups p-divisibles sobre $\mathcal{O}_L$. Al seu torn, aquesta dóna una successió exacta

$$0 \to T_p(A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]) \to T_p(A_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]) \to T_p(A^{et}_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]) \to 0$$

de $\mathrm{Gal}\,(\overline{\mathbb{Q}}_p/L)$-mòduls de Tate, on l'acció sobre el quocient $T_p(A^{et}_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$ és no-ramificada.

Notem que els mòduls de Tate $T_p(A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$ i $T_p(A^{et}_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$ són $\mathcal{O}_K$-mòduls, i la suma dels seus rangs és igual a dos. Hem de veure que algun d'ells (i per tant tots dos) és de rang 1. Dit d'alta manera: el grup p-divisible $A_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]$ és ordinari.

Comencem pel cas més senzill; és a dir, quan $p \nmid M$. En tal cas escollim un primer $\ell \nmid Mp$ i, per a un primer $\mathfrak{L}$ de K_F dividint ℓ, considerem la representació $\mathfrak{L}$-àdica associada a $A_{F|\mathbb{Q}}$. L'element de Frobenius Frob_p satisfà l'equació

$$x^2 - A_p x + \epsilon_F(p)p = 0\,,$$

i, per ser A_p de valoració $\mathfrak{P}$-àdica nul·la, una arrel és una unitat $\mathfrak{P}$-àdica i l'altra no. Ara bé, l'endomorfisme de Frobenius Fr_p de $\mathrm{End}(A_{F/\mathbf{F}_q})$ també satisfà l'equació i les dues arrels es donen, ja que la representació $\mathfrak{L}$-àdica és fidel. Per tant, els grups p-divisibles $A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]$ i $A^{et}_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]$ són no-trivials; aleshores és immediat que la restricció de ρ_F a D_p sigui com a l'enunciat.

Veiem ara el cas en què $p \mid M$. Gràcies a resultats de Carayol a **[Ca 86]** es té que una de les arrels de l'element de Frobenius $\mathrm{Frob}_{p,L}$, sobre L, és una potència de A_p; de nou, una arrel és una unitat $\mathfrak{P}$-àdica i l'atra no. Per tant, s'obté que els mòduls de Tate $T_p(A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$ i $T_p(A^{et}_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$ són $\mathcal{O}_K$-mòduls de rang 1 i la successió exacta

$$0 \to T_p(A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]) \to T_p(A_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]) \to T_p(A^{et}_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]) \to 0$$

és compatible amb l'acció de $\mathrm{Gal}\,(\overline{\mathbb{Q}}_p/L)$. Si veiem $\mathrm{Gal}\,(\overline{\mathbb{Q}}_p/L)$ com a subgrup de $D_p \backsimeq \mathrm{Gal}\,(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, certament ρ_F pot venir donada per matrius

triangulars superiors en restringir-nos a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$. En particular, hem determinat dos caràcters: ε_1 actuant a $T_p(A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$ que és ramificat i ε_2 actuant a $T_p(A^{et}_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$ que és no-ramificat. Ja que són diferents, podem recobrir $T_p(A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$ segons

$$T_p(A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]) = \bigcap_{\gamma\in\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)} \mathrm{Ker}(\gamma - \varepsilon_1(\gamma))\,,$$

on els nuclis es prenen a $T_p(A_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$. Si $g \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ aleshores l'acció de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$ sobre $g(T_p(A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty]))$ es realitza via el caràcter ε_1^g, on $\varepsilon_1^g(\gamma) := \varepsilon_1(g^{-1}\gamma g)$. Ja que ε_1^g ha de ser ε_1 o ε_2, i ε_2 és no-ramificat, es pot veure que $\varepsilon_1^g = \varepsilon_1$; per tant, $T_p(A^0_{F|\mathcal{O}_L}[\mathfrak{P}^\infty])$ és estable per l'acció de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Així doncs, s'arriba a que

$$\rho_F|_{D_p} \backsimeq \begin{pmatrix} \varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix},$$

on ε_1 és un caràcter ramificat; resta per provar que ε_2 és un caràcter no-ramificat de D_p.

Ja que $A_{F|\mathcal{O}_L}$ és un esquema abelià sobre $\mathrm{Spec}\,\mathcal{O}_L$, podem considerar l'aplicació de reducció $A_{F|\mathcal{O}_L}(\overline{L}) \to A_{F/\mathbb{F}_q}(\overline{\mathbb{F}}_p)$. La propietat universal del model de Néron garanteix que el nucli

$$\mathrm{Ker}\,(A_{F|\mathcal{O}_L}(\overline{L}) \to A_{F/\mathbb{F}_q}(\overline{\mathbb{F}}_p))$$

és estable per l'acció del grup de descomposició D_p. Per provar que ε_2 és no-ramificat, ens cal usar també el model de Néron, $A_{F|\mathbb{Z}_p}$, de $A_{F/\mathbb{Q}_p}$ sobre $\mathbb{Z}_p$; escruirem la seva fibra especial $A_{F/\mathbb{F}_p}$.

Per ser $A_{F/\mathbb{Q}_p}$ amb bona reducció potencial, per a $\ell \nmid M$ es té

$$T_\ell(A_{F/\mathbb{F}_p}) \backsimeq T_\ell(A_{F/\mathbb{Q}_p})^{I_p}\,,$$

on I_p és el grup d'inèrcia de D_p. Ja que $A_p \neq 0$, pel resultat de Carayol (que dóna els factors d'Euler de la L sèrie de la representació ℓ-àdica), tenim que

$$\mathrm{rang}_{\mathbb{Z}_\ell} T_\ell(A_{F/\mathbb{F}_p}) = 1 \qquad \mathrm{Fr}_p = A_p$$

sobre $T_\ell(A_{F/\mathbb{Q}_p})^{I_p}$.

La propietat universal del model de Néron sobre L proporciona un únic morfisme

$$A_{F|\mathbb{Z}_p} \times \mathcal{O}_L \to A_{F|\mathcal{O}_L}$$

que estén l'isomorfisme en la fibra genèrica; s'obté així un morfisme entre les fibres especials: $A_{F/\mathbb{F}_p} \to A_{F/\mathbb{F}_q}$. Si $\mathrm{ab}(A_{F/\mathbb{F}_p})$ denota la màxima varietat abeliana quocient de $A_{F/\mathbb{F}_p}$, tenim un morfisme $\mathrm{ab}(A_{F/\mathbb{F}_p}) \to A_{F/\mathbb{F}_q}$ que indueix un morfisme injectiu entre els seus ℓ-mòduls de Tate i, per tant, té nucli finit. A més, per ser A_p una unitat mòdul $\mathfrak{P}$, $\mathrm{ab}(A_{F/\mathbb{F}_p})(\overline{\mathbb{F}}_p) \neq 0$; d'on s'arriba a que

$$\mathrm{ab}(A_{F/\mathbb{F}_p})[\mathfrak{P}^\infty](\overline{\mathbb{F}}_p) \to A_{F/\mathbb{F}_q}[\mathfrak{P}^\infty](\overline{\mathbb{F}}_p)\,,$$

és exhaustiu. Dit d'altra manera: els grups p-divisbles $\mathrm{ab}(A_{F/\mathbb{F}_p})[\mathfrak{P}^\infty]$ i $A_{F/\mathbb{F}_q}[\mathfrak{P}^\infty]$ són isògens.

Finalment, de la commutativitat de diagrama

$$\begin{array}{ccc} A_{F|\mathbb{Z}_p}(\mathbb{Z}_p^{nr}) & \twoheadrightarrow & A_{F/\mathbb{F}_q}(\overline{\mathbb{F}}_p) \\ \downarrow & & \downarrow \\ A_{F|\mathcal{O}_L}(\mathcal{O}_L^{nr}) & \twoheadrightarrow & A_{F/\mathbb{F}_q}(\overline{\mathbb{F}}_p) \end{array}$$

podem deduir que tots els elements de $A_{F/\mathbb{F}_q}[\mathfrak{P}^\infty](\overline{\mathbb{F}}_p)$ són de la imatge de $A_{F|\mathbb{Z}_p}(\mathbb{Z}_p^{nr})$. Fent servir que el nucli del morfisme de reducció és estable per D_p, s'obté que ε_2 és no-ramificat com a caràcter des de D_p. □

Teorema 1.4. (Deligne, cf. **[Gr 90]**). *Sigui $f(q) = \sum a_n q^n$ una forma de Hecke* (mod p), *definida sobre $\mathbb{F}_q$, de tipus (N, k, ε), amb $2 \leq k \leq p+1$. Sigui ρ_f la representació residual associada a f. Es té que*

$$f \text{ és } p\text{-ordinària} \Longrightarrow \rho_f \text{ és } \mathfrak{P}\text{-ordinària, per a tot } \mathfrak{P} \mid p\,.$$

Més encara, la restricció de ρ_f a un grup de descomposició D_p es veu, en una base adequada, com

$$\begin{pmatrix} \chi^{k-1}\lambda(\varepsilon(p)/a_p) & * \\ 0 & \lambda(a_p) \end{pmatrix}$$

on $\lambda(\alpha)$ és el caràcter no-ramificat de D_p que envia $\mathrm{Frob}_\mathfrak{p}$ *a l'element α de $\mathbb{F}_q$.*

DEMOSTRACIÓ. Considerem una forma nova F que sigui un aixecament de f com en el teorema 3.7 del capítol 1; recordem que F depèn de l'elecció d'un primer $\mathfrak{P}$ de $\overline{\mathbb{Q}}_p$ dividint p. Aleshores tenim que F és $\mathfrak{P}$-ordinària pel fet de ser f una forma p-ordinària. Del teorema anterior resulta que, si ρ_F denota la representació $\mathfrak{P}$-àdica associada a la forma nova F, ρ_F és una representació $\mathfrak{P}$-ordinària; d'on la representació ρ_f resulta ser $\mathfrak{P}$-ordinària. Els caràcters que apareixen en l'acció del grup de descomposició per matrius triangulars superiors poden ser descrits a partir de la demostració del teorema anterior i l'expressió $\det(\rho_F) = \chi\varepsilon_F = \chi^{k-1}\varepsilon$. □

§2. Formes modulars supersingulars i representacions supersingulars

Conservem les notacions de la secció anterior.

Definició 2.1. Una representació 2-dimensional

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

direm que és $\mathfrak{P}$-supersingular si la restrcció de ρ al grup de descomposició D_p és irreductible.

Observació 2.2. Tindrem que si ρ és $\mathfrak{P}$-supersingular, aleshores la restricció de ρ al grup d'inèrcia I_p diagonalitza amb dos caràcters ramificats; el recíproc no és cert.

El comportament local en p d'una representació modular $(\mathrm{mod}\, p)$ que prové d'una forma modular p-supersingular es descriu en el següent

Teorema 2.3. (Fontaine, cf. [Ed 91¬]). *Sigui f una forma parabòlica de Hecke* $(\mathrm{mod}\, p)$ *de tipus (N, k, ε), amb $2 \leq k \leq p+1$. Es té que*

$$f \text{ és } p\text{-supersingular} \Longrightarrow \rho_f \text{ és } \mathfrak{P}\text{-supersingular}.$$

Més encara, la restricció de ρ_f al grup d'inèrcia I_p es veu, en una base adequada, com

$$\begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi^{p(k-1)} \end{pmatrix},$$

on ψ és el caràcter de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{nr})$ *amb valors a* $\mathbb{F}_p^2$ *que dóna l'acció sobre les arrels* p^2-1 *d'un uniformitzant.*

L'anterior resultat juntament amb el teorema 1.4 ens porten al

Corol·lari 2.4. *Sigui f una forma parabòlica de Hecke* $(\mathrm{mod}\, p)$ *de tipus* (N,k,ε), *amb* $2 \leq k \leq p+1$. *Es té que*

i) *f és p-ordinària* $\Longleftrightarrow$ *ρ_f és $\mathfrak{P}$-ordinària.*

ii) *f és p-supersingular* $\Longleftrightarrow$ *ρ_f és $\mathfrak{P}$-supersingular.*

CAPÍTOL 4

La conjectura de Serre

Ens interessem per representacions ($\mathrm{mod}\, p$) contínues del grup de Galois absolut $\mathrm{G}_{\mathbb{Q}}$

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}(V),$$

on V un $\overline{\mathbb{F}}_p$-espai vectorial de dimensió 2.

Observem que, pel fet de ser ρ contínua, la seva imatge G és un grup finit; això fa que el cos de racionalitat de ρ sigui un cos finit $\mathbb{F}_q$. Per exemple, si $p \neq 2$ o bé si ρ és irreductible, $\mathbb{F}_q$ està generat sobre $\mathbb{F}_p$ per les traces dels elements de G. A més, el nucli de ρ individua un cos de nombres galoisià.

A una tal representació, Serre associa dos enters positius N_ρ i k_ρ, així com un caràcter de Dirichlet $\varepsilon_\rho : (\mathbb{Z}/N_\rho\mathbb{Z})^* \to \overline{\mathbb{F}}_p^*$. Aquests són els anomenats invariants de Serre de la representació ρ: N_ρ el seu conductor, k_ρ el seu pes i ε_ρ el seu caràcter. A continuació recordem la recepta donada per Serre a [**Se 87**] per al càlcul de cadascun d'ells.

§1. El conductor N_ρ

L'enter N_ρ es defineix com el "conductor d'Artin ($\mathrm{mod}\, p$)" de ρ. És a dir, s'imita la definició del conductor d'Artin en característica 0, en el ben entès de restringir-se a les places primeres amb p.

Concretament, per a cada primer $\ell \neq p$ escollim una extensió a $\overline{\mathbb{Q}}$ de la valoració ℓ-àdica de $\mathbb{Q}$ i considerem

$$G_0 \supset G_1 \supset \cdots \supset G_i \supset \ldots$$

la cadena de grups de ramificació superior de G que correspon a aquesta valoració. Per a cada i, denotem V^{G_i} el subspai de V format pels elements fixos per G_i. L'exponent de ramificació de ρ en ℓ ve donat per

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

Es tenen els fets següents:

- $n(\rho,\ell)=\mathrm{codim}_{\overline{\mathbf{F}}_p}V^{G_0}+b(V)$, on $b(V)$ és l'exponent de Swan o, equivalentment, l'"invariant salvatge" del G_0-mòdul V;
- l'exponent de ramificació $n(\rho,\ell)$ és un enter positiu;
- l'exponent de ramificació $n(\rho,\ell)$ no depèn de l'extensió de la valoració ℓ-àdica escollida;
- $n(\rho,\ell)=0\iff\rho$ és no-ramificada en ℓ;
- $n(\rho,\ell)=\mathrm{codim}_{\overline{\mathbf{F}}_p}V^{G_0}\iff\rho$ és moderadament ramificada en ℓ.

Aleshores es defineix el conductor de ρ, N_ρ, per la fórmula:

$$N_\rho=\prod_{\ell\neq p}\ell^{n(\ell,\rho)}\,.$$

§2. El caràcter ε_ρ

El determinant de la representació ρ és un homomorfisme

$$\det\rho:\ \mathrm{G}_{\mathbf{Q}}\to\overline{\mathbf{F}}_p^{*}\,.$$

Per ser ρ contínua, aleshores $\det\rho$ és també contínu i, en conseqüència, la seva imatge és un subgrup finit (cíclic) de $\overline{\mathbf{F}}_p^{*}$. Això permet veure $\det\rho$ com un caràcter de Dirichlet. Un càlcul senzill, comparant els exponents de ramificació, mostra que el seu conductor divideix a $N_\rho p$. Podem identificar, doncs, $\det\rho$ a un caràcter de $(\mathbf{Z}/N_\rho p\mathbf{Z})^{*}$ amb valors a $\overline{\mathbf{F}}_p^{*}$ i, per ser N_ρ i p

primers entre ells, això ens proporciona dos homomorfismes

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

i

$$\varepsilon_\rho : (\mathbb{Z}/N_\rho\mathbb{Z})^* \to \overline{\mathbb{F}}_p^* .$$

D'aquesta manera

$$\det\rho : \mathrm{G}_\mathbb{Q} \to (\mathbb{Z}/N_\rho p\mathbb{Z})^* \backsimeq (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/N_\rho\mathbb{Z})^* \to \overline{\mathbb{F}}_p^* ,$$

on, si $\mathrm{Frob}_{\ell,\rho}$ designa l'element de Frobenius corresponent a G (definit mòdul conjugació) en un primer ℓ no dividint $N_\rho p$, es té que

$$\det\rho(\mathrm{Frob}_{\ell,\rho}) = \varphi(\ell)\varepsilon_\rho(\ell) .$$

És més, ja que $(\mathbb{Z}/p\mathbb{Z})^*$ és un grup cíclic d'ordre $p-1$ podem escriure

$$\varphi = \chi^h \quad \text{per a certa } h \in \mathbb{Z}/(p-1)\mathbb{Z} ,$$

on $\chi : \mathrm{G}_\mathbb{Q} \to \mathbb{F}_p{}^*$ designa el p-èsim caràcter ciclotòmic, que descriu l'acció de Galois sobre les arrels p-èsimes de la unitat. Si bé serà en la propera secció on recordarem la recepta per al pes k_ρ associat a ρ, avancem que resultarà $h \equiv k_\rho - 1 \,(\mathrm{mod}\, p-1)$.

Observació 2.1. A l'hora d'enunciar la conjectura de Serre cal fer fins a tres hipòtesis sobre la representació $\rho : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}(V)$. Una primera ja ha estat feta més amunt: que ρ sigui contínua. La segona és que ρ sigui irreductible. La tercera vol que la representació ρ sigui senar per tal que pugui proporcionar veritablement formes modulars.

Recordem tot seguit quina és la noció de representació galoisiana senar. Existeix un element privilegiat c de $\mathrm{G}_\mathbb{Q}$: el Frobenius en l'infinit. Es carcteritza per ser, a menys de conjugació, l'únic element d'ordre 2 o bé, si es prefereix, per ser el que dóna la conjugació complexa un cop triada una immersió de $\overline{\mathbb{Q}}$ a $\mathbb{C}$. La imatge de c a $(\mathbb{Z}/N_\rho p\mathbb{Z})^*$ és -1 i, per tant, tenim:

$$\det\rho(c) = (-1)^{k_\rho - 1}\varepsilon_\rho(-1) .$$

Definició 2.2. La representació ρ es diu senar si $\det \rho(c) = -1$; equivalentment, si $\varepsilon_\rho(-1) = (-1)^{k_\rho}$ a $\overline{\mathbb{F}}_p^*$.

§3. El pes k_ρ

Aquest és, sense dubte, l'invariant de la conjectura més "misteriós". Tal vegada, com expressa Serre a [Se 87], un dia podrà reformular-se la conjectura en el marc d'una teoria de representacions (mod p) dels grups adèlics ("filosofia de Langlands (mod p)") de manera que possibiliti una definició més natural del pes k_ρ associat a ρ.

L'enter k_ρ, a diferència del conductor N_ρ que s'obté a partir de la ramificació de ρ fora de p, depèn només de l'acció de la monodromia en p.

Escollim ara una extensió a $\overline{\mathbb{Q}}$ de la valoració p-àdica de $\mathbb{Q}$ (la definició del pes k_ρ resultarà obviament independent d'aquesta elecció). D'aquesta manera podem restringir la representació ρ al grup de descomposició $D_p \simeq \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$,

$$\rho_p : D_p \to \mathrm{GL}(V) \simeq \mathrm{GL}_2(\overline{\mathbb{F}}_p)\,.$$

Considerem les subextensions de $\overline{\mathbb{Q}}_p$ següents:

$$\mathbb{Q}_p \subset \mathbb{Q}_p^{nr} \subset \mathbb{Q}_p^t \subset \overline{\mathbb{Q}}_p\,,$$

on $\mathbb{Q}_p^{nr}$ és la subextensió maximal de $\overline{\mathbb{Q}}_p$ no-ramificada sobre $\mathbb{Q}_p$, i $\mathbb{Q}_p^t$ és la subextensió maximal de $\overline{\mathbb{Q}}_p$ moderadament ramificada sobre $\mathbb{Q}_p$. Els corresponen

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \supset \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{nr}) \supset \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^t)\,.$$

Posem

$$I_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{nr})\,, \qquad I_s = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^t)\,.$$

Aleshores, I_p és el grup d'inèrcia de D_p i I_s, el més gran pro-p-subgrup de I_p, és el grup d'inèrcia salvatge. El quocient $I_t = I_p/I_s = \mathrm{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p^{nr})$ és un grup pro-finit commutatiu, d'ordre primer amb p, anomenat el grup

d'inèrcia moderada en p; i s'identifica amb $\varprojlim \mathbb{F}_{p^n}^*$. Els caràcters d'aquest grup juguen un paper essencial en la definició del pes k_ρ associat a la representació ρ.

Passem, doncs, a recordar els resultats principals relatius al grup d'inèrcia moderada en p i als seus caràcters (cf. [Se 72]). Per a cada enter $d \geq 1$, primer amb p, considerem el cos $K_d = \mathbb{Q}_p^{nr}(\sqrt[d]{p})$ i l'isomorfisme

$$\vartheta_d : \mathrm{Gal}(K_d/\mathbb{Q}_p^{nr}) \to \mu_d(\mathbb{Q}_p^{nr}),$$

donat per $s(\sqrt[d]{p}) = \vartheta_d(s)\sqrt[d]{p}$. En ser $\mathbb{Q}_p^t$ la reunió dels K_d tenim

$$I_t = \varprojlim_d \mathrm{Gal}(K_d/\mathbb{Q}_p^{nr}),$$

i els isomorfismes ϑ_d indueixen un isomorfisme

$$\vartheta : I_t \to \varprojlim \mu_d(\mathbb{Q}_p^{nr}).$$

Reduint mòdul l'ideal maximal de $\mathbb{Q}_p^{nr}$, es fàcil explicitar l'equivalència entre els sistemes projectius $\varprojlim \mu_d$ amb morfismes de pas $\mu_{dd'} \to \mu_d$, $(\alpha \mapsto \alpha^{d'})$ i $\varprojlim \mathbb{F}_{p^n}^*$ amb morfismes de pas les aplicacions "norma". D'aquesta manera obtenim un isomorfisme

$$\vartheta : I_t \to \varprojlim \mathbb{F}_{p^n}^*.$$

Considerem el grup $\widehat{I}_t = \mathrm{Hom}_{\mathrm{cont}}(I_t, \overline{\mathbb{F}}_p^*)$ dels caràcters continus a valors en el cos $\overline{\mathbb{F}}_p^*$. Aquest grup es pot parametritzar per $(\mathbb{Q}/\mathbb{Z})'$, el conjunt dels nombres racionals amb denominador primer amb p. Més concretament, es té l'isomorfisme següent:

$$(\mathbb{Q}/\mathbb{Z})' \to \widehat{I}_t, \qquad a/d \mapsto \vartheta_d^a.$$

D'aquesta manera hom pot identificar cada caràcter φ del grup d'inèrcia moderada I_t en p amb un nombre racional $\alpha \pmod{\mathbb{Z}[1/p]}$, $\alpha = \mathrm{inv}(\varphi)$, que s'anomena l'invariant del caràcter. Un caràcter de I_t es diu de nivell n si factoritza per $\mathbb{F}_{p^n}^*$ i no ho fa per cap $\mathbb{F}_{p^m}^*$, on m és un divisor estricte de n. S'anomenen caràcters fonamentals de nivell n els caràcters de I_t que tenen per invariants $\dfrac{p^i}{p^n - 1}$, per a $i = 0, 1, \ldots, n-1$.

La relació entre els caràcters de I_t i les representacions (mod p) locals i contínues $\rho_p : D_p \to \mathrm{GL}(V) \simeq \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ queda garantida pel fet següent:

Si V^{ss} denota la semi-simplificació de V respecte a l'acció de D_p, aleshores el grup d'inèrcia salvatge I_s opera trivialment sobre V^{ss}, de manera que es té un acció diagonalitzable de I_t sobre V^{ss} donada per dos caràcters

$$\varphi\,,\,\varphi' : I_t \to \overline{\mathbb{F}}_p^*\,,$$

que són de nivell 1 ó 2. A més, si són de nivell 2 aleshores són conjugats: $\varphi = \varphi'^p$ i $\varphi' = \varphi^p$.

Estem en condicions de recordar la recepta per a l'invariant pes de la conjectura associat a la representació ρ. Aquest és un enter $k_\rho \in [2, p^2-1]$ que ve donat en funció de $\mathrm{inv}(\varphi)$ i $\mathrm{inv}(\varphi')$, els invariants dels caràcters de la inèrcia moderada que diagonalitzen l'acció sobre V^{ss}. La taula següent conté els diferents valors per al pes k_ρ:

$\rho\vert_{D_p}$	$\mathrm{inv}(\varphi)$	$\mathrm{inv}(\varphi')$	on	condicions	pes k_ρ
irreductible	$\frac{a+pb}{p^2-1}$		$0 \le a < b \le p-1$		$1+pa+b$
reductible completament	$\frac{a}{p-1}$	$\frac{b}{p-1}$	$0 \le a \le b \le p-2$	$(a,b) \neq (0,0)$ $(a,b) = (0,0)$	$1+pa+b$ p
reductible no-completament $\begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}$	$\frac{\beta}{p-1}$	$\frac{\alpha}{p-1}$	$0 \le \alpha \le p-2$ $1 \le \beta \le p-1$ $a = \min\{\alpha,\beta\}$ $b = \max\{\alpha,\beta\}$	$\beta \neq \alpha+1$ P.R. M.R.($p \neq 2$) M.R.($p = 2$)	$1+pa+b$ $2+\alpha(p+1)$ $(\alpha+1)(p+1)$ 4

Observació 3.1. El caràcter χ que apareix a la taula és el p-èsim caràcter ciclotòmic que abans hem introduït.

Observació 3.2. Els casos P.R., M.R.($p \neq 2$) i M.R.($p = 2$) de la taula estan subjectes a la condició $\beta = \alpha + 1$ i són abreviatures per a quan ρ és poc ramificada o molt ramificada en p, en el sentit de Serre. Esmentem que, quan $\beta = \alpha+1$, el grup $\rho(I_p)$ és el grup de Galois d'una certa extensió K de $\mathbb{Q}_p^{nr}$ totalment ramificada. Fent ús de la teoria de Kummer, podem escriure

$$K = K_t(x_1^{1/p}, \ldots, x_m^{1/p})\,,$$

on K_t designa la màxima extensió moderadement ramificada de $\mathbb{Q}_p^{nr}$ continguda dins K, i $x_1, \ldots, x_m$ són elements de $\mathbb{Q}_p^{nr*}$ no-potències de p. Aleshores es diu que ρ és poc ramificada si els x_i poden ser escollits entre les unitats de $\mathbb{Q}_p^{nr}$, i molt ramificada en cas contrari.

§4. Enunciat de la conjectura

Una vegada definits els tres invariants associats a una representació residual 2-dimensional i contínua, Serre formula de manera precisa la següent

Conjectura 4.1. (cf. [Se 87, (3.2.4?)]). *Sigui V un espai vectorial sobre $\overline{\mathbb{F}}_p$ de dimensió 2, i sigui*

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}(V)$$

una representació contínua, irreductible i senar. Posem N_ρ, k_ρ, ε_ρ els invariants associats a ρ. Aleshores existeix una forma parabòlica de Hecke (mod p)

$$f(q) = \sum a_n q^n$$

de tipus $(N_\rho, k_\rho, \varepsilon_\rho)$ tal que

$$\mathrm{tr}\,(\mathrm{Frob}_{\ell,\rho}) = a_\ell \qquad \det(\mathrm{Frob}_{\ell,\rho}) = \varepsilon_\rho(\ell)\ell^{k_\rho - 1}\,,$$

per a tot primer $\ell \nmid N_\rho p$.

§5. Aportacions d'altres autors

Transcrivim tot seguit els resultats més destacables que han estat publicats fins al moment en relació amb aquesta conjectura. Amb aquest fi, introduïm ràpidament alguna terminologia.

Sigui

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

una representació com abans. Posem N_ρ, k_ρ, ε_ρ els seus invariants associats.

Definició 5.1. Sigui ℓ un nombre primer. Es diu que la representació ρ és finita en ℓ si existeix un esquema $\mathbf{V}$ en $\mathbb{F}_q$-espais vectorials sobre $\operatorname{Spec}\mathbb{Z}$, finit i pla, tal que l'acció del grup de descomposició $D_\ell \backsimeq \operatorname{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ sobre $\mathbf{V}(\overline{\mathbb{Q}}_\ell)$ proporciona la restrició de ρ a D_ℓ.

Observació 5.2. A [Se 87] es troba que la definició anterior és equivalent a les condicions pràctiques següents:

$$\text{o bé, } \begin{cases} \rho \text{ és no-ramificada en } \ell & \text{si } \ell \neq p \\ \det\rho = \chi \text{ i } k_\rho = 2 & \text{si } \ell = p. \end{cases}$$

Passem ja als resultats.

Teorema 5.3. (cf. [Ma 85¬], [Ri 90]). *Sigui $p \geq 3$. Suposem que ρ prové d'una forma parabòlica de Hecke, definida sobre $\overline{\mathbb{Z}}_p$, de tipus $(M, 2, 1)$. Si*

i) *ρ és finita en un primer ℓ, i*

ii) *$\ell \| M$,*

aleshores

ρ prové d'una forma parabòlica de Hecke, sobre $\overline{\mathbb{Z}}_p$, de tipus $(M/\ell, 2, 1)$.

Teorema 5.4. (cf. [Ca 89]). *Sigui $p \geq 5$. Suposem que ρ prové d'una forma parabòlica de Hecke, sobre $\overline{\mathbb{Z}}_p$, de tipus $(M, 2, 1)$. Si*

i) $\text{m. c. d.}\,(M, p) = 1$,

aleshores

ρ prové d'una forma parabòlica de Hecke, sobre $\overline{\mathbb{Z}}_p$, de tipus $(N_\rho, 2, 1)$.

Teorema 5.5. (cf. [Jor-Liv 89]). *Sigui $p \geq 3$. Suposem que ρ prové d'una forma parabòlica de Hecke, definida sobre $\overline{\mathbb{Z}}_p$, de tipus (M, k, ε). Si*

i) $\text{m. c. d.}\,(M, p) = 1$,

ii) $3 \leq k < p$,

iii) *ρ és finita en $\ell \neq p$, i*

iv) *el caràcter ε és no-ramificat en ℓ,*

aleshores

ρ prové d'una forma parabòlica de Hecke, sobre $\overline{\mathbb{Z}}_p$, de tipus $(M/\ell, k, \varepsilon)$.

Teorema 5.6. (cf. **[Liv 89]**). *Suposem que ρ prové d'una forma parabòlica de Hecke, definida sobre $\overline{\mathbb{Z}}_p$, de tipus (N, k, ε)*

aleshores

$N_\rho \mid N$.

Teorema 5.7. (cf. **[Gr 90]**). *Suposem que ρ prové d'una forma parabòlica de Hecke* (mod p)*, f, de tipus (N, k, ε) amb $2 \leq k \leq p$ i $a_p^2 \neq \varepsilon(p)$ si $k = p$. Suposem, a més, que f és p-ordinària. Aleshores són equivalents:*

i) *$\rho|_{D_p}$ redueix completament.*

ii) *Existeix una forma parabòlica de Hecke* (mod p)*, g, de tipus $(N, p+1-k, \varepsilon)$ tal que $\rho \backsimeq \rho_g \otimes \chi^{k-1}$.*

En tal cas, Serre diu que les formes f i g són companyes.

Teorema 5.8. (cf. **[Ed 91¬]**). *Suposem que ρ prové d'una forma parabòlica de Hecke, definida sobre $\overline{\mathbb{Z}}_p$, de tipus (M, k, ε). Si*

i) m. c. d. $(M, p) = 1$,

aleshores

ρ prové d'una forma parabòlica de Hecke, sobre $\overline{\mathbb{Z}}_p$, de tipus (M, k_ρ, ε).

PART II

CAPÍTOL 5

Estudi del comportament de la conjectura de Serre per torcement

En aquest capítol s'estudia el comportament de la conjectura de Serre en una representació, prenent esment en el de les representacions torçades per les potències del caràcter ciclotòmic. Obtenim criteris per a la validesa de la conjectura, que s'aplicaran en posteriors capítols al tractar les representacions associades a la p-torsió de les corbes de Weil.

Prèviament, però, ens cal obtenir un resultat sobre congruències entre els desenvolupaments de Fourier de formes modulars.

§1. Obtenció de congruències

Al llarg de tota aquesta secció tractarem només formes modulars definides sobre $\overline{\mathbb{Q}}$. El resultat que provem tot seguit (teorema 1.2) estableix congruències entre els coeficients de Fourier de formes parabòliques de tipus (Np, k, ε) i de tipus (N, k', ε'). Com veurem, el pes k' i el caràcter ε' estan estretament lligats als invariants de la conjectura de Serre.

Sigui $p \geq 3$ un nombre primer. Fixem una extensió a $\overline{\mathbb{Q}}$ de la valoració p-àdica v_p de $\mathbb{Q}$, normalitzada de manera que $v_p(p) = 1$. Sigui $\mathfrak{P}$ el primer de $\overline{\mathbb{Q}}$, dividint p, que aquesta extensió determina.

Definició 1.1. Direm que dues formes modulars $F(q) = \sum_{n\geq 0} A_n q^n$ i $G(q) = \sum_{n\geq 0} B_n q^n$ són còngrues, i escriurem

$$F \equiv G \pmod{\mathfrak{P}},$$

si $A_n \equiv B_n \pmod{\mathfrak{P}}$, per a tot $n \geq 0$.

Essent $\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \overline{\mathbb{Q}}^*$ el caràcter associat a l'invers del caràcter de Teichmüller, considerem la sèrie d'Eisenstein (cf. capítol 1, §4)

$$E_{1,\psi} = 1 + c_\psi \sum_{\substack{m>0 \\ m_1>0}} \psi(m) e^{2\pi i m\, m_1 z}\,.$$

Sabem que $E_{1,\psi}$ és una forma modular de tipus $(p, 1, \psi)$, definida sobre $\overline{\mathbb{Q}}$.

En el següent teorema, les involucions de Fricke i l'operador traça, descrits en el capítol 1, ens permeten donar resultats que generalitzen sengles de Koike a [**Ko 76**].

Teorema 1.2. *Sigui $G(q) = \sum B_n q^n \in S_k(Np, \phi\psi^{-t})$ una forma nova amb $1 \leq t < p-1$ i ϕ un caràcter de Dirichlet mòdul N, $p \nmid N$. Sigui d un enter positiu tal que $d \equiv t \pmod{p-1}$. Aleshores*

i) $\mathrm{Tr}\,(GE_{1,\psi}^d) \in S_k(N, \phi)$,

ii) $\mathrm{Tr}\,(GE_{1,\psi}^d) \equiv G \pmod{\mathfrak{P}} \iff 2 - k + \dfrac{d-t}{p-1} + v_p(\overline{B}_p) > 0\,.$

DEMOSTRACIÓ. Ja que ψ és no-ramificat fora de p i $d \equiv t \pmod{p-1}$, observem que el conductor del caràcter de la forma parabòlica $GE_{1,\psi}^d$ és primer amb p. Per tant, l'operador traça pot ser aplicat a la forma $GE_{1,\psi}^d$ (cf. capítol 1, §4), d'on i). En aplicar-lo, obtenim

$$\mathrm{Tr}\,(GE_{1,\psi}^d) = GE_{1,\psi}^d + \phi(p)^{-1} p^{1-\frac{k+d}{2}} (GE_{1,\psi}^d)|[W_p]_k|U_p\,.$$

Ja que $E_{1,\psi} \equiv 1 \pmod{\mathfrak{P}}$ i $\phi(p)$ és una unitat $\mathfrak{P}$-àdica, cerquem un enter d tal que

$$p^{1-\frac{k+d}{2}} (GE_{1,\psi}^d)|[W_p]_{k+d}|U_p \equiv 0 \pmod{\mathfrak{P}}\,.$$

De les definicions es desprèn que

$$(GE_{1,\psi}^d)|[W_p]_{k+d} = G|[W_p]_k\, (E_{1,\psi}|[W_p]_1)^d\,.$$

Ocupem-nos ara, per separat, de cada un dels termes de la dreta:

Comencem per $G|[W_p]_k$. El teorema d'Ogg-Li-Asai (cf. [**Og 69**], [**Li 75**], [**As 76**]) ens assegura que la forma nova $G(q) \in S_k(Np, \phi\psi^{-t})$ té

p-èsim coeficient de Fourier B_p amb $|B_p| = p^{(k-1)/2}$; en particular, se satisfà $B_p \neq 0$. Això ens permet reescriure el pseudo-valor propi $\lambda_p(G)$ de W_p en G. Concretament, trobem $G|[W_p]_k = \lambda_p(G)G'$ on

$$\lambda_p(G) = C(\psi^{-t})\overline{B}_p p^{-k/2}$$

i $G'(q) = \sum B'_n q^n$ és la forma nova que té per coeficients de Fourier els enters algebraics determinats pel teorema 4.1 del capítol 1.

Pel que fa a la sèrie d'Eisenstein recordem que, amb les notacions del §4 del capítol 1, tenim

$$G_{1,\psi} = 2\,L(1,\overline{\psi})\,E_{1,\psi} = \sum_{n \bmod p} \overline{\psi}(n) G_1(z;0,n,p)\,.$$

Aleshores calculem l'acció de la transformació per la matriu $\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$:

$$G_{1,\psi}|\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}_1 = p^{-1/2} G_{2,\overline{\psi}}\,.$$

I, per tant, obtenim

$$E_{1,\psi}|[W_p]_1 = E_{1,\psi}|\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}_1 = \frac{\sqrt{p}}{C(\overline{\psi})}\frac{c_\psi}{c_{\overline{\psi}}} E_{1,\overline{\psi}}\,.$$

D'aquesta manera hem aconseguit

$$(GE^d_{1,\psi})|[W_p]_{k+d} = G|[W_p]_k (E_{1,\psi}|[W_p]_1)^d = \lambda_p(G)G'\left(\frac{\sqrt{p}}{C(\overline{\psi})}\frac{c_\psi}{c_{\overline{\psi}}}\right)^d E^d_{1,\overline{\psi}}\,.$$

El teorema de Stickelberger (cf. **[Wa 80]**, **[Ko 76]**) ens permet calcular la valoració p-àdica de la suma de Gauss $C(\psi^{-t})$ i de la constant $\dfrac{\sqrt{p}}{C(\overline{\psi})}\dfrac{c_\psi}{c_{\overline{\psi}}}$. Trobem

$$v_p(C(\psi^{-t})) = 1 - \frac{t}{p-1}\,, \qquad v_p\left(\frac{\sqrt{p}\,c_\psi}{C(\overline{\psi})c_{\overline{\psi}}}\right) = \frac{1}{2} + \frac{1}{p-1}\,.$$

Finalment, calculem

$$v_p\left(p^{1-\frac{k+d}{2}}\lambda_p(G)\left(\frac{\sqrt{p}}{C(\overline{\psi})}\frac{c_\psi}{c_{\overline{\psi}}}\right)^d\right) = 2 - k + \frac{d-t}{p-1} + v_p(\overline{B}_p)\,,$$

i això prova el teorema. □

§2. Torcement de representacions

Sigui donada

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p),$$

una representació contínua, irreductible i senar. Posem N_ρ, k_ρ, ε_ρ els invariants de Serre associats a ρ.

Per a cada enter i , considerem les representacions

$$\rho(i) : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

torçades de ρ pels inversos de les potències i-èsimes del caràcter ciclotòmic $\chi : \mathrm{G}_{\mathbb{Q}} \to \mathbb{F}_p^*$; és a dir,

$$\rho(i) := \rho \otimes \chi^{-i}.$$

Observació 2.1. De fet, sols tenim $p-1$ representacions $\rho(i)$ torçades de ρ. En efecte, $\rho(i)$ depèn de classe de i mòdul $p-1$. D'altra banda, òbviament $\rho(0) = \rho$.

Observació 2.2. Les representacions $\rho(i)$ són també contínues, irreductibles i senars. Notem que $\det \rho(i) = \chi^{-2i} \det \rho$.

Posem $N_{\rho(i)}$, $k_{\rho(i)}$, $\varepsilon_{\rho(i)}$ els invariants de Serre per a la representació torçada $\rho(i)$. Observem que d'entrada, pel fet de ser χ un caràcter no-ramificat fora de p, tenim

$$N_{\rho(i)} = N_\rho \quad \text{i} \quad \varepsilon_{\rho(i)} = \varepsilon_\rho .$$

Tot seguit donem dos resultats que poden proporcionar una estratègia per provar la conjectura de Serre per a la representació ρ. Consisteix en adonar-se que entre les representacions $\rho(i)$ n'hi ha de privilegiades (en un sentit que explicitarem) i que provant la conjectura per a aquestes, queda

provada per a la representació ρ. Aquests criteris seran útils en posteriors aplicacions en el capítol 7.

Notem que els pesos $k_{\rho(i)}$ no resulten invariants en tòrcer; sabem que

$$k_{\rho(i)} \in [2, p^2 - 1]$$

i, si bé és possible donar-los depenent d'una gamma molt extensa de casos i subcasos, resulta més econòmic fer la següent

Definició 2.3. Anomenarem pes minimal de la representació ρ l'enter més petit d'entre els pesos $k_{\rho(i)}$ associats a les representacions torçades $\rho(i)$ de ρ. Si $k_{\rho(m)}$ és el pes minimal de ρ, direm que $\rho(m)$ és la representació minimal associada a ρ.

Proposició 2.4. *Les notacions com abans, més les del §3 del capítol 4. Es té:*

i) *Existeix un enter n tal que la representació torçada $\rho(n)$ de ρ satisfà $k_{\rho(n)} \leq p+1$. En particular, el pes minimal $k_{\rho(m)}$ d'una repesentació ρ és sempre $\leq p+1$.*

ii) *Existeixen, com a molt, dues classes $n \pmod{p-1}$ que donen representació torçada amb pes $\leq p+1$; una d'elles proporciona el pes minimal de ρ. La taula següent conté els valors de $n \pmod{p-1}$ que fan $k_{\rho(n)} \leq p+1$.*

$\rho\|_{D_p}$	condicions		pes k	n	pes $k_{\rho(n)}$	Cas
irreductible	$0 \leq a < b \leq p-1$		$1+pa+b$	a	$1+b-a$	A1
				$b-1$	$2+p+a-b$	A2
reductible completament	$0 \leq a \leq b \leq p-2$		$1+pa+b$	a	$1+b-a$	B1
				b	$p+a-b$	B2
		$a=b=0$	p	0	p	B3
$\begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}$ $a=\min\{\alpha,\beta\}$ $b=\max\{\alpha,\beta\}$	$\beta \neq \alpha+1$	$\beta > \alpha$	$1+pa+b$	α	$1+b-a$	C1
		$\beta \leq \alpha$			$p+a-b$	C2
	$\beta = \alpha+1$	P.R.	$2+\alpha(p+1)$	α	2	C3
		M.R.	$(\alpha+1)(p+1)$		$p+1$	C4

Assignem a cada cas una lletra seguida d'un nombre. En els casos C_i suposem $* \neq 0$; és a dir, $\rho|_{D_p}$ redueix no-completament.

iii) *Quan $\rho|_{D_p}$ redueix no-completament, la representació torçada $\rho(m)$ que dóna pes $\leq p+1$ és única i, per tant, proporciona el pes minimal $k_{\rho(m)}$.*

iv) *Quan $\rho|_{D_p}$ és irreductible o redueix completament, l'ambigüitat que es presenta a l'hora de decidir el pes minimal $k_{\rho(m)}$ es resol en funció dels valors de a i b; concretament, el pes minimal és:*

Si $\rho|_{D_p}$ és irreductible,

$$k_{\rho(m)} = \begin{cases} 1+b-a & si\ b-a \leq \dfrac{p+1}{2}, \\ 2+p+a-b & si\ b-a > \dfrac{p+1}{2}. \end{cases}$$

Si $\rho|_{D_p}$ redueix completament,

$$k_{\rho(m)} = \begin{cases} 1+b-a & si\ b-a \leq \dfrac{p-1}{2}, \\ p+a-b & si\ b-a > \dfrac{p-1}{2}. \end{cases}$$

DEMOSTRACIÓ. La prova consisteix en adonar-se que l'invariant pes, associat a una representació ρ, és $\leq p+1$ si, i només si, se satisfà alguna de les tres condicions següents:

$$\rho|_{D_p} \text{ irreductible i } \rho^{ss}|_{I_t} = \begin{pmatrix} \vartheta^b_{p^2-1} & 0 \\ 0 & \vartheta^{pb}_{p^2-1} \end{pmatrix}, \text{ amb } 1 \leq b \leq p-1,$$

o bé,

$$\rho|_{I_p} = \begin{pmatrix} \vartheta^b_{p-1} & 0 \\ 0 & 1 \end{pmatrix} \text{ amb } 0 \leq b \leq p-2,$$

o bé,

$$\rho|_{I_p} = \begin{pmatrix} \vartheta^\beta_{p-1} & * \\ 0 & 1 \end{pmatrix} \text{ amb } 1 \leq \beta \leq p-1.$$

Aleshores tot es redueix a manipulacions amb els invariants dels caràcters del grup d'inèrcia moderada en p seguides de l'algoritme per a la determinació del pes (cf. capítol 4, §3). □

Definició 2.5. Sigui ρ com abans. Si existeixen dues classes $(\mathrm{mod}\ p-1)$ diferents n_1 i n_2 tals que les representacions torçades $\rho(n_1)$ i $\rho(n_2)$ tenen pesos $k_{\rho(n_1)}$ i $k_{\rho(n_2)}$ més petits o iguals a $p+1$, diem que $\rho(n_1)$ i $\rho(n_2)$ són dues representacions companyes per a ρ.

§3. Criteris per a la validesa de la conjectura

Mantinguem les notacions com abans. Un dels resultats que estem perseguint és el

Teorema 3.1. *Sigui*

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

una representació contínua, irreductible i senar. Admetem que la seva representació minimal $\rho(m)$ satisfà la conjectura de Serre; és a dir, que existeix g una forma parabòlica de Hecke $(\mathrm{mod}\, p)$ de tipus $(N_\rho, k_{\rho(m)}, \varepsilon_\rho)$, tal que $\rho(m) \preceq \rho_g$. Aleshores ρ satisfà la conjectura de Serre.

DEMOSTRACIÓ. Cerquem $f(q) = \sum a_n q^n$ una forma parabòlica de Hecke $(\mathrm{mod}\, p)$, de tipus $(N_\rho, k_\rho, \varepsilon_\rho)$, tal que $\rho_f \preceq \rho$. La demostració es fa distingint els diferents casos segons quina sigui la classe de l'enter m que dóna la representació minimal.

Si la representació minimal es presenta en els casos $A1, B1, B3, C1, C3, C4$. En tots ells $m = a$. Suposem, doncs, en cada cas, que $\rho(a) = \rho \otimes \chi^{-a}$ satisfà la conjectura de Serre. Per tant, existeix $g(q) = \sum b_n q^n$ una forma de Hecke $(\mathrm{mod}\, p)$ de tipus $(N_\rho, k_{\rho(a)}, \varepsilon_\rho)$ amb $\rho_g \preceq \rho \otimes \chi^{-a}$. Mitjançant l'operador θ de Ramanujan-Katz, clarament es té

$$\rho_{\theta^a g} \preceq \rho .$$

D'altra banda, si la filtració de g no és múltiple de p tenim que

$$\theta^a g \in S_{k_{\rho(a)}+a(p+1)}(N_\rho, \varepsilon_\rho)$$

és una forma de Hecke (mod p) no divisible per l'invariant de Hasse A (cf. capítol 1, proposició 3.3). El mateix passa si la filtració de g és p, ja que aleshores ens trobem en el cas $B3$ i tenim $a = 0$, $k_\rho = k_{\rho(a)} = p$.

Per la proposició 2.4 es té que el pes de $\theta^a g$ s'ajusta al que prediu la conjectura,

$$k_\rho = k_{\rho(a)} + a(p+1)\,.$$

D'on ρ satisfà la conjectura prenent $f(q) := \theta^a g(q)$.

Si la representació minimal es presenta en els casos B2,C2. En aquests casos $m = b$. Suposem que $\rho(b)$ satisfà la conjectura i posem $g(q) = \sum b_n q^n$, la forma parabòlica de Hecke (mod$p$) de tipus $(N_\rho, k_{\rho(b)}, \varepsilon_\rho)$ amb $\rho_g \backsimeq \rho \otimes \chi^{-b}$. Podem admetre que $k_{\rho(b)}$ és la filtració de la forma g.

Podem suposar, a més, que g és nova. Efectivament, en cas contrari tindríem que $\rho(b)$ provindria d'una forma parabòlica amb nivell dividint estrictament $N_{\rho(b)}$ en contradicció amb el teorema 5.6 del capítol 4. Ja que, a més, el pes de g és $\leq p+1$, el corol·lari 2.4 del capítol 3 ens permet assegurar que la forma g és p-ordinària; és a dir, $b_p \not\equiv 0$.

Si $k_{\rho(b)} = 2$, notem que aleshores $b - a = p - 2$; per tant, prenem $f(q) := \theta^b g(q)$. En efecte, $f(q) = \theta^{a-1}\theta^{b-a+1} g(q) = \theta^{a-1}\theta^{p-1} g(q)$ i, ja que la filtració de $\theta^{p-1} g(q)$ és $2p$, aleshores el pes de f és $2p + (a-1)(p+1) = 1 + pa + b = k_\rho$ i es té $\rho_f \backsimeq \rho$.

Si $k_{\rho(b)} \geq 3$, en aplicar el teorema 3.7 del capítol 1 obtenim

$$G(q) = \sum B_n q^n$$

una forma de nova de tipus $(N_\rho p, 2, \varepsilon \chi_p^{k_{\rho(b)}-2})$, amb coeficients a $\overline{\mathbb{Z}}_p$, tal que per reducció mòdul $\mathfrak{P}$ dóna la forma parabòlica g. (Aquí el caràcter ε és l'aixecament multiplicatiu de ε_ρ.)

Ja que $b_p \not\equiv 0$, trobem que $|B_p| = \sqrt{p}$ (cf. **[Og 69]**, **[Li 75]**, **[As 76]**). Per tant, si v_p denota la valoració p-àdica normalitzada estesa a $\overline{\mathbb{Q}}_p$ segons $\mathfrak{P}$, obtenim $v_p(B_p) = 0$ i $v_p(\overline{B}_p) = 1$.

Considerem ara la forma nova

$$G'(q) = \sum B_n' q^n \in S_2(N_\rho p, \varepsilon \overline{\chi}_p^{k_{\rho(b)}-2})\,,$$

múltiple de $G|w_\zeta$, on w_ζ denota la involució de Weil. Pel teorema 4.1 del capítol 1, es té $B_p^{'} \cdot B_p = p\,\varepsilon(p)$; d'on $v_p(B_p^{'}) = 1$ i $v_p(\overline{B'}_p) = 0$.

Estem en condicions d'aplicar el teorema 1.2 per a la forma G'. Normalitzant el caràcter obtenim

$$\overline{\chi}_p^{k_{\rho(b)}-2} = \psi^{-(2-k_{\rho(b)})} = \psi^{-(2-k_{\rho(b)}+p-1)},$$

d'on l'exponent $t = p+1-k_{\rho(b)}$. Ja que $v_p(\overline{B'}_p) = 0$ i G' té pes 2, el mínim enter positiu d que satisfà la congruència

$$\mathrm{Tr}\,(G' E_{1,\psi}^{d}) \equiv G' \pmod{\mathfrak{P}}$$

és $d = p+1-k_{\rho(b)}+p-1 = 2p-k_{\rho(b)}$.

Notem que, per aquest valor de d i per les propietats de l'operador traça (cf. teorema 1.2),

$$\mathrm{Tr}\,(G' E_{1,\psi}^{2p-k_{\rho(b)}}) \in S_{2(p+1)-k_{\rho(b)}}(N_\rho, \varepsilon).$$

Prenem

$$f := \theta^{a-1}\,\mathrm{Tr}\,(G' E_{1,\psi}^{2p-k_{\rho(b)}}).$$

Degut a que estem en els casos $B2$ i $C2$, trobem

$$2(p+1)-k_{\rho(b)}+(a-1)(p+1) = 2+p+b-a+ap+a-p-1 = 1+pa+b = k_\rho.$$

D'aquesta manera el tipus de la forma f és $(N_\rho, k_\rho, \varepsilon_\rho)$; així doncs, es correspon als invariants de Serre per a ρ i només ens cal comprovar que $\rho_f \simeq \rho$. Observem primer que, pel teorema 4.1 del capítol 1, es té

$$B_n^{'} = B_n \cdot \psi^{a-b+p-2}, \qquad \text{per a tot } n \text{ primer amb } p.$$

Aleshores la representació residual

$$\rho \otimes \chi^{-b} \otimes \chi^{-(a-b+p-2)} = \rho \otimes \chi^{-a-p+2} = \rho \otimes \chi^{-a+1} = \rho \otimes \chi^{-(a-1)} = \rho(a-1)$$

és la reducció de la representació $\rho_{G'}$ associada a G' i, per tant, veiem que efectivament ρ prové de la forma f.

Si la representació minimal es presenta en el cas A2. Ara es té que $m = b-1$. Posem $g(q) = \sum b_n q^n$ la forma parabòlica de Hecke (mod p) de tipus $(N_\rho, k_{\rho(b-1)}, \varepsilon_\rho)$ tal que fa $\rho(b-1) \simeq \rho_g$.

Pel corol·lari 2.4 del capítol 3 sabem que la forma g és p-supersingular; és a dir, $b_p = 0$. Observem que $k_{\rho(b-1)} = 2 + p + a - b$ satisfà $3 \leq k_{\rho(b-1)} \leq (p+3)/2$ (cf. proposició 2.4). Ara, podem aplicar la proposició 3.3 del capítol 1 que ens assegura que $\theta^{b-1-a}g$ té filtració $1 + b - a$. Per tant, la forma $f(q) := \theta^{b-1-a}\theta^a g(q)$ satisfà les condicions en aquest cas. □

Observació 3.2. La demostració en el cas $B2$ s'hauria pogut reduir a la del cas $B1$ en fer ús de la teoria de Serre sobre les formes companyes (cf. capítol 4, teorema 5.7).

Acabem aquest capítol donant el

Teorema 3.3. *Sigui*

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

una representació contínua, irreductible i senar. Suposem que ρ admet representacions companyes $\rho(n_1)$ i $\rho(n_2)$. Aleshores es té:

$\rho(n_1)$ satisfà la conject. de Serre $\iff$ $\rho(n_2)$ satisfà la conject. de Serre.

DEMOSTRACIÓ. Intercanviant les companyes, si és necessari, podem suposar que $\rho(n_1) = \rho(m)$ és la representació minimal associada a ρ i, per tant, també és la minimal associada a $\rho(n_2)$. Si $\rho(n_1)$ satisfà la conjectura de Serre, el teorema 3.1 ens assegura que el mateix passa per a $\rho(n_2)$.

Veiem ara el recíproc. Posem

$$g(q) = \sum b_n q^n$$

la forma parabòlica de Hecke (mod p), de tipus $(N_\rho, k_{\rho(n_2)}, \varepsilon_\rho)$, tal que $\rho_g \simeq \rho(n_2)$. De la proposició 2.4 se segueix que

$$k_{\rho(n_1)} + k_{\rho(n_2)} = \begin{cases} p+1 & \text{si } \rho|_{D_p} \text{ redueix,} \\ p+3 & \text{si } \rho|_{D_p} \text{ és irreductible.} \end{cases}$$

A més, si $\rho|_{D_p}$ redueix ho fa completament. Per tant, en aquest cas, podem aplicar el teorema 5.7 del capítol 4 i obtenim l'existència d'una forma f, companya de g, tal que f és parabòlica de Hecke (mod$p$), de tipus $(N_\rho, k_{\rho(n_1)}, \varepsilon_\rho)$, i

$$\rho_f(1-k_{\rho(n_2)}) \preceq \rho_g\,.$$

Aleshores,

$$\rho_f(1-k_{\rho(n_2)}) \preceq \rho(n_2)$$

i, ja que $k_{\rho(n_2)} \equiv 1+n_1+n_2 \pmod{p-1}$ (cf. proposició 2.4), obtenim

$$\rho_f \preceq \rho(n_2+k_{\rho(n_2)}-1) \preceq \rho(n_1)\,.$$

Suposem ara que estem en el cas $\rho|_{D_p}$ irreductible. Considerem la forma parabòlica de Hecke (mod$p$), g, de tipus $(N_\rho, k_{\rho(n_2)}, \varepsilon_\rho)$, i tal que $\rho_g \preceq \rho(n_2)$. Ara el corol·lari 2.4 del capítol 3 ens assegura que g és p-supersingular. De la proposició 2.4 se segueix que sempre es té $k_{\rho(n_2)} \equiv 2+n_1+n_2 \pmod{p-1}$. Notem que $p+1-k_{\rho(n_2)} = k_{\rho(n_1)}-2$ i, per tant, tenim que

$$f(q) := \theta^{k_{\rho(n_1)}-2}g(q) \in S_{k_{\rho(n_1)}+(p-1)(k_{\rho(n_1)}-1)}(N_\rho, \varepsilon_\rho)$$

té filtració $< p-1+k_{\rho(n_1)}$ (cf. [**Jo 82**] i capítol 1, proposició 3.3). D'on $f(q)$ té filtració $k_{\rho(n_1)}$, ja que $k_{\rho(n_1)} \leq p+1$. Arribem a que $f(q)$ és una forma parabòlica de Hecke (mod$p$), de tipus $(N_\rho, k_{\rho(n_1)}, \varepsilon_\rho)$, i satisfà

$$\rho_f \preceq \rho_g(-k_{\rho(n_2)}+2) \preceq \rho(n_2-k_{\rho(n_2)}+2) \preceq \rho(n_1)\,,$$

com voliem trobar. □

Com a conseqüència dels resultats anteriors obtenim el

Corol·lari 3.4. *Sigui*

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

una representació contínua, irreductible i senar. Posem que la torçada $\rho(\hat{m})$ sigui la representació minimal o bé la seva companya (si existeix). Aleshores es té que si $\rho(\hat{m})$ satisfà la conjectura de Serre, el mateix passa per a ρ.

CAPÍTOL 6

Càlcul dels invariants de Serre associats a les corbes el·líptiques

Sigui E una corba el·líptica sobre $\mathbb{Q}$. Per a cada primer p, l'acció del grup de Galois $G_{\mathbb{Q}}$ sobre els punts de p-torsió E_p de $E(\overline{\mathbb{Q}})$ defineix una representació contínua

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E_p) \backsimeq \mathrm{GL}_2(\mathbb{F}_p),$$

que és sempre senar i absolutament irreductible si $p > 163$ **[Ma 78]**, **[Se 87]**.

Depenent de l'aritmètica de la corba el·líptica E, anem a trobar els invariants de Serre associats a ρ: conductor N_ρ, pes k_ρ i caràcter ε_ρ.

§1. Invariants associats a la p-torsió

L'aparellament de Weil proporciona un isomorfisme canònic entre $\Lambda^2 E_p$ i μ_p. D'on $\det\rho$ és el p-èsim caràcter ciclotòmic χ i, per tant, el caràcter ε_ρ és trivial.

Pel que fa al conductor N_ρ, considerem l'acció de $G_{\mathbb{Q}}$ sobre el $\mathbb{Q}_p$-mòdul de Tate $V_p(E) = T_p(E) \otimes \mathbb{Q}_p$. Aquesta acció proporciona una representació p-àdica

$$\rho_0 : G_{\mathbb{Q}} \to \mathrm{Aut}(V_p(E)) \backsimeq \mathrm{GL}_2(\mathbb{Q}_p),$$

que és un aixecament de la representació ρ. Posem

$$N_0 = \prod_{\ell \neq p} \ell^{n(\ell,\rho_0)}$$

el conductor d'Artin de ρ_0; és a dir, el producte dels conductors d'Artin locals en cada primer $\ell \neq p$. Els exponents de ramificació venen donats per

$$n(\ell, \rho_0) = \mathrm{codim}_{\mathbb{Q}_p} V_p(E)^{I_\ell} + b(V_p(E)),$$

on I_ℓ denota un grup d'inèrcia en ℓ i $b(V_p(E))$ l'exponent de Swan. Escrivim

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

el conductor de ρ, amb exponents de ramificació

$$n(\ell, \rho) = \mathrm{codim}_{\overline{\mathbb{F}}_p} E_p{}^{I_\ell} + b(E_p),$$

com en el capítol 4. Ja que els grups de ramificació salvatge són pro-ℓ-grups i $\ell \neq p$, resulta que $b(V_p(E)) = b(E_p)$. D'altra banda, és immediat que

$$\mathrm{codim}_{\mathbb{Q}_p} V_p(E)^{I_\ell} \geq \mathrm{codim}_{\overline{\mathbb{F}}_p} E_p{}^{I_\ell}.$$

Arribem a que $N_\rho | N_0$ i, si v_ℓ és la valoració ℓ-àdica de $\mathbb{Q}$ normalitzada per $v_\ell(\ell) = 1$, tenim

$$v_\ell(N_0/N_\rho) = \mathrm{codim}_{\mathbb{Q}_p} V_p(E)^{I_\ell} - \mathrm{codim}_{\overline{\mathbb{F}}_p} E_p{}^{I_\ell}.$$

Sigui ara $\mathcal{E}_{|\mathbb{F}_\ell}$ la fibra especial del model de Néron de E en ℓ i considerem la successió exacta

$$0 \to \mathcal{E}^0_{|\mathbb{F}_\ell} \to \mathcal{E}_{|\mathbb{F}_\ell} \to \Phi_\ell \to 0,$$

on $\mathcal{E}^0_{|\mathbb{F}_\ell}$, Φ_ℓ són la component connexa de l'element neutre i el grup de components de $\mathcal{E}_{|\mathbb{F}_\ell}$, respectivament. Recordem que

$$\mathcal{E}^0_{|\mathbb{F}_\ell} \simeq \begin{cases} \mathcal{E}_{|\mathbb{F}_\ell} & \text{si } E \text{ té bona reducció en } \ell, \\ \mathbb{G}_{m,\overline{\mathbb{F}}_\ell} \text{ (sobre } \overline{\mathbb{F}}_\ell) & \text{si } E \text{ té reducció multiplicativa en } \ell, \\ \mathbb{G}_{a,\mathbb{F}_\ell} & \text{si } E \text{ té reducció additiva en } \ell. \end{cases}$$

Per calcular $\mathrm{codim}_{\mathbb{F}_p} E_p^{I_\ell}$, usem l'isomorfisme

$$E(\overline{\mathbb{Q}}_\ell)[p]^{I_\ell} \simeq \mathcal{E}_{|\mathbb{F}_\ell}(\overline{\mathbb{F}}_\ell)[p]$$

obtingut per reducció [**Se-Ta 68**]; es comprova que

$$\dim \mathcal{E}_{|\mathbb{F}_\ell}(\overline{\mathbb{F}}_\ell)[p] = \begin{cases} 2 & \text{si } E \text{ té bona reducció en } \ell, \\ 1+\dim \Phi_\ell(\overline{\mathbb{F}}_\ell)[p] & \text{si } E \text{ té reducció multiplicativa en } \ell, \\ \dim \Phi_\ell(\overline{\mathbb{F}}_\ell)[p] & \text{si } E \text{ té reducció additiva en } \ell. \end{cases}$$

D'altra banda, es té

$$\dim V_p(E)^{I_\ell} = \begin{cases} 2 & \text{si } E \text{ té bona reducció en } \ell, \\ 1 & \text{si } E \text{ té reducció multiplicativa en } \ell, \\ 0 & \text{si } E \text{ té reducció additiva en } \ell. \end{cases}$$

De tot l'anterior deduïm el següent

Teorema 1.1. *La fórmula per a l'abaixament entre els conductors és*

$$v_\ell(N_0) - v_\ell(N_\rho) = p\text{-}rang\, \Phi_\ell,$$

per a cada $\ell \neq p$. En termes dels 10 símbols de Kodaria, les taules següents contenen el valor exacte de l'abaixament $v_\ell(N_0/N_\rho)$ segons el tipus de reducció del model de Néron en ℓ.

Si $p = 2$,

$v_\ell(N_0/N_\rho)$	ℓ-*tipus*(E)
2	$I_{2\nu}^*$
1	$I_{2\nu}, I_{2\nu+1}^*, III, III^*$
0	$I_0, I_{2\nu+1}, II, II^*, IV, IV^*$

Si $p = 3$,

$v_\ell(N_0/N_\rho)$	ℓ-*tipus*(E)
1	I_ν *si* $3 \mid \nu, IV, IV^*$
0	*altrament*

Si $p \geq 5$,

$v_\ell(N_0/N_\rho)$	ℓ-*tipus*(E)
1	I_ν *si* $p \mid \nu$
0	*altrament*

Observació 1.2. La fórmula dels conductors permet el càlcul efectiu de l'invariant N_ρ, associat a ρ, a condició de conèixer el valor de N_0. Ara bé, el conductor d'Artin N_0 pot ser calculat, per exemple, amb l'algoritme de Tate [**Ta 75**] a partir d'una equació de Weierstraß per a la corba el·líptica E o bé, si E és una corba de Weil, aleshores N_0 és el divisor maximal primer amb p del conductor analític de E. En cas d'optar per la primera possibiltat (ús de l'algoritme de Tate), cal advertir que s'obté un valor per a l'exponent de ramificació de N_0 en el primer 2 que depèn d'una igualtat d'Ogg no comprovada en aquest cas (cf. [**Og 67**]).

Passem al càlcul de l'invariant pes k_ρ, associat a la representació ρ. Fixem $D_p \backsimeq \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ un subgrup de $\mathrm{G}_\mathbb{Q}$. Després d'estendre escalars, cosiderem la restricció de ρ al grup de descomposició en p

$$\rho_p : D_p \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)\,.$$

Sigui ρ_p^{ss} la semisimplificada de ρ_p. Sabem que l'acció del grup d'inèrcia moderada I_t en p, que correspon a D_p, diagonalitza segons

$$\rho_p^{\mathrm{ss}}|_{I_t} = \begin{pmatrix} \phi & 0 \\ 0 & \phi' \end{pmatrix},$$

on ϕ, ϕ' són caràcters de I_t de nivell 1, o bé 2. El pes k_ρ és funció de $\mathrm{inv}\,(\phi)$, $\mathrm{inv}\,(\phi')$, els invariants de ϕ i ϕ', respectivament (cf. capítol 4, §3). El lema següent mostra que ens podem limitar a calcular-ne un d'ells.

Lema 1.3. *Sigui $\rho : \mathrm{G}_\mathbb{Q} \to \mathrm{Aut}(E_p)$ la representació associada als punts de p-torsió de la corba el·líptica $E_{|\mathbb{Q}}$. Amb les notacions d'abans, a $(\mathbb{Q}/\mathbb{Z})'$ es té*

$$inv(\phi) + inv(\phi') = \frac{p}{p-1}\,.$$

A més, l'invariant pes k_ρ satisfà

$$k_\rho \equiv 2 \pmod{p-1}\,.$$

DEMOSTRACIÓ. Ja que $\det\rho : \mathrm{G}_\mathbb{Q} \to \overline{\mathbb{F}}_p^*$ és el caràcter ciclotòmic χ, trobem que la restricció de $\det\rho_p^{\mathrm{ss}}$ a I_t és el caràcter fonamental ϑ_{p-1} de nivell 1. Per tant, tenim la igualtat

$$\mathrm{inv}\,(\phi) + \mathrm{inv}\,(\phi') = \frac{p}{p-1}\,,$$

a $(\mathbb{Q}/\mathbb{Z})'$.

D'altra banda, per la mateixa definició del pes associat a una representació tenim que, si I_p és el grup d'inèrcia en p, $\det \rho|_{I_p} = \chi^{k_\rho - 1}$. □

Podem trobar el pes k_ρ, segons l'aritmètica de la corba el·líptica E. Posem

$$c_4,\, c_6 \in \mathbb{Z}$$

els invariants usuals de E, determinats a menys de p-unitats a partir d'un model p-minimal de Weierstraß. Assumim, per raons de regularitat en les fórmules, que $p > 7$. Aleshores provem el següent

Teorema 1.4. *El pes $k_\rho = 2 + \lambda(p-1)$ i els invariants $inv(\phi)$, $inv(\phi')$ dels caràcters associats a la representació*

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}\,(E_p)$$

es poden llegir en les taules:

$\mathcal{E}_{\mid \mathbb{F}_p}$	*altres condicions*	$inv(\phi)$	λ
I_ν	*si* $p \mid \nu$	$1/(p-1)$	0
	si $p \nmid \nu$	$1/(p-1)$	1
II	$p \equiv 1\ (3)$	$(5p+1)/6(p-1)$	$(p+5)/6$
	$p \equiv 2\ (3)$, $v_p(c_4) = 1$	$(5p-1)/6(p-1)$	$(p+7)/6$
	$p \equiv 2\ (3)$, $v_p(c_4) > 1$	$(5p^2+1)/6(p^2-1)$	$(p+7)/6$
III	$p \equiv 1\ (4)$	$(3p+1)/4(p-1)$	$(p+3)/4$
	$p \equiv 3\ (4)$, $v_p(c_6) = 2$	$(3p-1)/4(p-1)$	$(p+5)/4$
	$p \equiv 3\ (4)$, $v_p(c_6) > 2$	$(3p^2+1)/4(p^2-1)$	$(p+5)/4$
IV	$p \equiv 1\ (3)$	$(2p+1)/3(p-1)$	$(p+2)/3$
	$p \equiv 2\ (3)$, $v_p(c_4) = 2$	$(2p-1)/3(p-1)$	$(p+4)/3$
	$p \equiv 2\ (3)$, $v_p(c_4) > 2$	$(2p^2+1)/3(p^2-1)$	$(p+4)/3$

I_ν^*	$si\ p \mid \nu$	$(p+1)/2(p-1)$	$(p+1)/2$
	$si\ p \nmid \nu$	$(p+1)/2(p-1)$	$(p+3)/2$
II^*	$p \equiv 1\ (3)$	$(p+5)/6(p-1)$	$(p+11)/6$
	$p \equiv 2\ (3)\,,\ v_p(c_4) = 4$	$(p+1)/6(p-1)$	$(p+7)/6$
	$p \equiv 2\ (3)\,,\ v_p(c_4) > 4$	$(p^2+5)/6(p^2-1)$	$(p+1)/6$
III^*	$p \equiv 1\ (4)$	$(p+3)/4(p-1)$	$(p+7)/4$
	$p \equiv 3\ (4)\,,\ v_p(c_6) = 5$	$(p+1)/4(p-1)$	$(p+5)/4$
	$p \equiv 3\ (4)\,,\ v_p(c_6) > 5$	$(p^2+3)/4(p^2-1)$	$(p+1)/4$
IV^*	$p \equiv 1\ (3)$	$(p+2)/3(p-1)$	$(p+5)/3$
	$p \equiv 2\ (3)\,,\ v_p(c_4) = 3$	$(p+1)/3(p-1)$	$(p+4)/3$
	$p \equiv 2\ (3)\,,\ v_p(c_4) > 3$	$(p^2+2)/3(p^2-1)$	$(p+1)/3$

DEMOSTRACIÓ. Els resultats de la segona taula es poden obtenir a partir dels resultats de la primera en tòrcer pel caràcter quadràtic ramificat en p. Quan la corba el·líptica E té reducció de tipus I_ν en p, els valors de $\mathrm{inv}\,(\phi)$ i k_ρ es troben a [**Se 87**]. Per tant, ens cal considerar els casos on E té p-tipus(E) igual a II, III, o bé IV.

Sigui e l'enter mínim comú múltiple de les multiplicitats de les components irreductibles de la fibra especial del model amb creuements normals, associat al model minimal de E, pel procés d'esclatament; és a dir, del model estable de E. Tenim

$$e = \begin{cases} 6 & \text{si } E \text{ és de tipus } II \text{ en } p, \\ 4 & \text{si } E \text{ és de tipus } III \text{ en } p, \\ 3 & \text{si } E \text{ és de tipus } IV \text{ en } p. \end{cases}$$

La corba el·líptica E adquireix bona reducció sobre el cos $L = \mathbb{Q}_p^{\mathrm{nr}}(\pi)$, on $\pi^e = p$. Això es pot veure fàcilment a partir dels possibles models de Weierstraß de E segons el tipus de reducció. Notem $E_{/L}$ la corba el·líptica obtinguda pel canvi de base $E \otimes_{\mathbb{Q}_p^{\mathrm{nr}}} L$ i

$$m : E_{/L}(\overline{\mathbb{Q}}_p) \to E(\overline{\mathbb{Q}}_p)$$

el $\mathrm{Gal}\,(\overline{\mathbb{Q}}_p/L)$-isomorfisme induït pel canvi de base.

Cerquem un subspai 1-dimensional V del $\overline{\mathbb{F}}_p[I_t]$-mòdul $(E_p \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p)^{\mathrm{ss}}$. Per a això, considerem $\widehat{E}$ el grup formal de E_L i posem h la seva altura. La

proposició 10 de [**Se 72**] garanteix que el nucli $\widehat{E}_p$ de la multiplicació per $[p]$ a $\widehat{E}$ conté sempre un $\mathbb{F}_p$-subspai vectorial V_L, no nul, on el grup d'inèrcia moderada $I_{t,L}$ de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$ hi actua. La $\dim_{\mathbb{F}_p} V_L$ i l'acció de $I_{t,L}$ sobre $\mathbb{F}_{p^h} \otimes V_L$ poden ser llegides a partir del polígon de Newton de la sèrie formal de la multiplicació per $[p]$ sobre $\widehat{E}$. Amb una verificació cas per cas obtenim:

h	altres condicions	$\dim_{\mathbb{F}_p} V_L$	$I_{t,L}$ on $\overline{\mathbb{F}}_p \otimes V_L$
1	II , $p \equiv 1\ (3)$ III , $p \equiv 1\ (4)$ IV , $p \equiv 1\ (3)$	1	ϑ_{p-1}^e
2	II , $p \equiv 2\ (3)$, $v_p(c_4) = 1$ III , $p \equiv 3\ (4)$, $v_p(c_6) = 2$ IV , $p \equiv 2\ (3)$, $v_p(c_4) = 2$	1	ϑ_{p-1}^4 ϑ_{p-1}^2 ϑ_{p-1}
2	II , $p \equiv 2\ (3)$, $v_p(c_4) > 1$ III , $p \equiv 3\ (4)$, $v_p(c_6) > 2$ IV , $p \equiv 2\ (3)$, $v_p(c_4) > 2$	2	$\vartheta_{p^2-1}^e$, $\vartheta_{p^2-1}^{pe}$

on ϑ_{p-1}, $\vartheta_{p^2-1} : I_{t,L} \to \overline{\mathbb{F}}_p^*$ són caràcters fonamentals de $I_{t,L}$ de nivell 1 i 2, respectivament.

Finalment, prenem $V := \mathbb{F}_{p^h} \otimes m(V_{E_L})$, on V_{E_L} és la imatge de V_L per la immersió de $\widehat{E}_p$ en el grup dels punts de p-torsió, $E_{L,p}$, de $E_L(\overline{\mathbb{Q}}_p)$. Ara I_t actua sobre V i l'acció es pot controlar a través de m. Per fer-ho, mirem l'acció de $s_m := m^{-1} \circ s \circ m$ sobre $\mathbb{F}_{p^h} \otimes V_L$, per a $s \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{nr}})$. Mostrem tots els càlculs que hem efectuat únicament per al cas on E té reducció de tipus IV en p, amb $p \equiv 2 \pmod 3$, i $v_p(c_4) > 2$:

$$E \ : Y^2 = X^3 - p^2AX + p^2B \quad \text{amb } A,B \in \mathbb{Z},\ (p,B) = 1,$$
$$E_L : Y^2 = X^3 - \pi^2AX + B\,,\ \text{altura}(\widehat{E}) = 2\,,\ \dim_{\mathbb{F}_p} V_L = 2\,,$$

$$m^{-1} : E(\overline{\mathbb{Q}}_p) \to E_L(\overline{\mathbb{Q}}_p), \quad m^{-1}(x,y) = \left(\frac{x}{\pi^2}, \frac{y}{\pi^3}\right),$$

i

$$V_L = \{z = -\pi x/y \,|\, (\frac{x}{\pi^2}, \frac{y}{\pi^3}) \in E_{L,p}\,,\, v_\pi(-\pi x/y) = \frac{3}{p^2-1}\}$$
$$= \{z = -\pi x/y \,|\, (\frac{x}{\pi^2}, \frac{y}{\pi^3}) \in E_{L,p}\,,\, v_p(-x/y) = \frac{-p^2+4}{3(p^2-1)}\}\,,$$
$$V = \mathbb{F}_{p^2} \otimes \{(x,y) \in E_p \,|\, \frac{-\pi x}{y} \in V_L\}.$$

Si $s \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{nr}})$ i $z = -\pi x/y \in V_L$, aleshores

$$s(\frac{x}{y}) = \vartheta_{p^2-1}^{\frac{-p^2+4}{3}}(s)\,\frac{x}{y} = \vartheta_{p^2-1}^{\frac{2p^2+1}{3}}(s)\,\frac{x}{y}\,.$$

Finalment, per a $1 \otimes (x,y) \in V$ aconseguim

$$\begin{aligned} s(1 \otimes (x,y)) &= 1 \otimes (m \circ s_m \circ m^{-1})(x,y) \\ &= 1 \otimes (m \circ s_m)(x/\pi^2, y/\pi^3) \\ &= 1 \otimes m(sx/\pi^2, sy/\pi^3) \\ &= \vartheta_{p^2-1}^{\frac{2p^2+1}{3}}(s) \otimes m(x/\pi^2, y/\pi^3) \\ &= \vartheta_{p^2-1}^{\frac{2p^2+1}{3}}(s)\,(1 \otimes m(x/\pi^2, y/\pi^3)) \\ &= \vartheta_{p^2-1}^{\frac{2p^2+1}{3}}(s)\,(1 \otimes (x,y))\,. \end{aligned}$$

Ara, cas a cas, omplim la taula tenint present la recepta per al pes k_ρ (cf. capítol 4, §3). □

Observació 1.5. En cas que la representació sigui salvatgement ramificada, el caràcter ϕ que apareix a les taules és el que correspon al subspai de dimensió 1 invariant per la inèrcia. Es a dir,

$$\rho|_{I_p} = \begin{pmatrix} \phi & * \\ 0 & \phi' \end{pmatrix}.$$

§2. Invariants minimals. Invariants companys

Acabem aquest capítol inspeccionant amb més detall, d'una banda, els caràcters de la inèrcia moderada associats a la representació

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\,(E_p)\,,$$

i, de l'altra, la representació torçada $\rho(m)$ que proporciona el pes minimal $k_{\rho(m)}$ per a ρ.

En mirar de cara els nostres objectius posteriors, és suficient restringir-nos als casos en què la corba el·líptica E té reducció potencialment bona (ordinària o supersingular) en $p > 7$; és a dir, reducció additiva amb p-tipus(E) diferent de I_ν^*, $\nu > 0$ (cas que tractarem en l'Apèndix 1). Tanmateix, si no s'especifica expressament el contrari, suposarem que el p-tipus de E és diferent de I_0^*, per tractar-se d'un cas aparellat amb la bona reducció I_0 i, per tant, més senzill.

No obstant el que acabem dir, i tenint en compte la notació en la demostració del teorema 1.4, d'ara endavant posem

$\mathcal{E}_{/\mathbf{F}_p}$	I_0	II	III	IV	I_0^*	II^*	III^*	IV^*
e	1	6	4	3	2	6	4	3

.

De les taules que donen les fórmules per al pes k_ρ (cf. teorema 1.4) es poden deduir les proposicions que segueixen.

Proposició 2.1. *Si E té reducció potencialment ordinària en $p > 7$, aleshores $p \equiv 1 \pmod{e}$ i*

$$\rho|_{I_p} = \begin{pmatrix} \phi & * \\ 0 & \phi' \end{pmatrix},$$

on els caràcters ϕ, ϕ', sobre I_t, són de nivell 1 i els seus ordres $ord(\phi)$, $ord(\phi')$ venen donats, segons el p-símbol Kodaira de E, per

$\mathcal{E}_{/\mathbf{F}_p}$	$ord(\phi)$, $ord(\phi')$	condicions	$ord(\phi)$, $ord(\phi')$	$\mathcal{E}_{/\mathbf{F}_p}$
II	$6, p-1$ o $\frac{p-1}{2}$	$p \equiv 1,4\,(9)$	$3, p-1$	IV^*
	$6, \frac{p-1}{3}$ o $\frac{p-1}{6}$	$p \equiv 7\,(9)$	$3, \frac{p-1}{3}$	

$\mathcal{E}_{/\mathbf{F}_p}$	$ord(\phi),\ ord(\phi')$	*condicions*	$ord(\phi),\ ord(\phi')$	$\mathcal{E}_{/\mathbf{F}_p}$
III	$4, p-1$	$p \equiv 1,9\,(16)$	$4, p-1$	*III**
	$4, \frac{p-1}{2}$	$p \equiv 13\,(16)$	$4, \frac{p-1}{4}$	
	$4, \frac{p-1}{4}$	$p \equiv 5\,(16)$	$4, \frac{p-1}{2}$	

$\mathcal{E}_{/\mathbf{F}_p}$	$ord(\phi),\ ord(\phi')$	*condicions*	$ord(\phi),\ ord(\phi')$	$\mathcal{E}_{/\mathbf{F}_p}$
IV	$3, p-1$	$p \equiv 1,7\,(9)$	$6, p-1$ *o* $\frac{p-1}{2}$	*II**
	$3, \frac{p-1}{3}$	$p \equiv 4\,(9)$	$6, \frac{p-1}{3}$ *o* $\frac{p-1}{6}$	

Proposició 2.2. *Si E té reducció potencialment supersingular en $p > 7$, aleshores $p \not\equiv 1 \pmod{e}$ i*

$$\rho|_{I_p} = \begin{cases} \begin{pmatrix} \phi & * \\ 0 & \phi' \end{pmatrix} \text{ o bé,} \\ \text{irreductible diagonalitzant amb } \phi,\ \phi' \text{ sobre } I_t\,, \end{cases}$$

on els caràcters ϕ, ϕ', sobre I_t, són de nivell 1 en el primer cas, i de nivell 2 en el segon. Els seus ordres $ord(\phi)$, $ord(\phi')$ venen donats, segons el p-símbol de Kodaira de E, per:

i) *Si ϕ, ϕ' són de nivell 1,*

$\mathcal{E}_{/\mathbf{F}_p}$	$ord(\phi),\ ord(\phi')$	$ord(\phi),\ ord(\phi')$	$\mathcal{E}_{/\mathbf{F}_p}$
II	$p-1, \frac{p-1}{2}$ *o* $\frac{p-1}{4}$	$\frac{p-1}{2}, p-1$	*IV**

$\mathcal{E}_{/\mathbf{F}_p}$	$ord(\phi),\ ord(\phi')$	*condicions*	$ord(\phi),\ ord(\phi')$	$\mathcal{E}_{/\mathbf{F}_p}$
III	$\frac{p-1}{2}, p-1$	$p \equiv 3,11\,(16)$	$p-1, \frac{p-1}{2}$	*III**
	$p-1, \frac{p-1}{2}$	$p \equiv 7,15\,(16)$	$\frac{p-1}{2}, p-1$	

$\mathcal{E}_{/\mathbb{F}_p}$	$ord(\phi),\ ord(\phi')$	$ord(\phi),\ ord(\phi')$	$\mathcal{E}_{/\mathbb{F}_p}$
IV	$p-1, \frac{p-1}{2}$	$\frac{p-1}{2}$ o $\frac{p-1}{4}, p-1$	II^*

ii) *Si ϕ, ϕ' són de nivell 2,*

$\mathcal{E}_{/\mathbb{F}_p}$	$ord(\phi),\ ord(\phi')$	*condicions*	$ord(\phi),\ ord(\phi')$	$\mathcal{E}_{/\mathbb{F}_p}$
II	$\frac{p^2-1}{3}, \frac{p^2-1}{3}$	$p \equiv 5\,(9)$	$\frac{p^2-1}{3}, \frac{p^2-1}{3}$	IV^*
	p^2-1, p^2-1	$p \equiv 2,8\,(9)$	p^2-1, p^2-1	

$\mathcal{E}_{/\mathbb{F}_p}$	$ord(\phi),\ ord(\phi')$	$ord(\phi),\ ord(\phi')$	$\mathcal{E}_{/\mathbb{F}_p}$
III	p^2-1, p^2-1	p^2-1, p^2-1	III^*

$\mathcal{E}_{/\mathbb{F}_p}$	$ord(\phi),\ ord(\phi')$	*condicions*	$ord(\phi),\ ord(\phi')$	$\mathcal{E}_{/\mathbb{F}_p}$
IV	$\frac{p^2-1}{3}, \frac{p^2-1}{3}$	$p \equiv 2\,(9)$	$\frac{p^2-1}{3}, \frac{p^2-1}{3}$	II^*
	p^2-1, p^2-1	$p \equiv 5,8\,(9)$	p^2-1, p^2-1	

Observació 2.3. Notem que les sentències de les proposicions 2.1 i 2.2 són idependents de què la representació ρ sigui moderadament ramificada o no; és a dir, tan si $\rho|_{D_p}$ és reductible completament com reductible no-completament.

Pel que fa als invariants minimals de la representació

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}\,(E_p)$$

amb $p > 7$, i a la vista del teorema 1.4, obtenim primer els invariants de

$\rho(\hat{m})$, la representació minimal o companya associada a ρ. Posteriorment, desfarem aquesta ambigüitat en donar els invariants minimals de ρ.

Proposició 2.4. *Les taules següents contenen la classe* $\hat{m} \pmod{p-1}$ *que proporciona la representació minimal, o bé la companya,* $\rho(\hat{m})$ *associada a* ρ*; la seva restricció al grup d'inèrcia en* p*; i el seu pes* $k_{\rho(\hat{m})}$.

Si E *és potencialment ordinària en* p,

p-tipus$(E) =$ *II, III, IV*	
$\hat{m}$	$\frac{p-1}{e}$
$\rho(\hat{m})\|_{I_p}$	$\begin{pmatrix} \chi^{1-2\hat{m}} & * \\ 0 & 1 \end{pmatrix}$
$k_{\rho(\hat{m})}$	$p+1-2\hat{m}$

p-tipus$(E) =$ *II*, III*, IV**	
$\hat{m}$	$-\frac{p-1}{e}$
$\rho(\hat{m})\|_{I_p}$	$\begin{pmatrix} \chi^{1-2\hat{m}} & * \\ 0 & 1 \end{pmatrix}$
$k_{\rho(\hat{m})}$	$2(1-\hat{m})$

Si E *és potencialment supersingular en* p *amb* $\rho|_{D_p}$ *reductible,*

p-tipus$(E) =$ *II, III, IV*	
$\hat{m}$	$\frac{p+1}{e}$
$\rho(\hat{m})\|_{I_p}$	$\begin{pmatrix} \chi^{1-2\hat{m}} & * \\ 0 & 1 \end{pmatrix}$
$k_{\rho(\hat{m})}$	$\hat{m}(e-2)$

p-tipus$(E) =$ *II*, III*, IV**	
$\hat{m}$	$1-\frac{p+1}{e}$
$\rho(\hat{m})\|_{I_p}$	$\begin{pmatrix} \chi^{1-2\hat{m}} & * \\ 0 & 1 \end{pmatrix}$
$k_{\rho(\hat{m})}$	$2(1-\hat{m})$

Si E *és potencialment supersingular en* p *amb* $\rho|_{D_p}$ *irreductible,*

p-tipus$(E) =$ *II, III, IV*	
$\hat{m}$	$\frac{p+1}{e}$
$\rho(\hat{m})_p^{ss}\|_{I_t}$	$\begin{pmatrix} \vartheta_{p^2-1}^{p-2\hat{m}} & 0 \\ 0 & \vartheta_{p^2-1}^{1-2p\hat{m}} \end{pmatrix}$
$k_{\rho(\hat{m})}$	$p+1-2\hat{m}$

p-tipus$(E) =$ *II*, III*, IV**	
$\hat{m}$	$\frac{p+1}{e}-1$
$\rho(\hat{m})_p^{ss}\|_{I_t}$	$\begin{pmatrix} \vartheta_{p^2-1}^{p-2\hat{m}} & 0 \\ 0 & \vartheta_{p^2-1}^{1-2p\hat{m}} \end{pmatrix}$
$k_{\rho(\hat{m})}$	$p+1-2\hat{m}$

Per distingir quins són els invariants minimals de

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}\,(E_p),$$

observem que ens podem limitar a calcular-los en el cas en què el p-símbol de Kodaira de E sigui II, III, IV. En efecte, trobem el

Lema 2.5. *Sigui ρ com abans. Si p-tipus$(E) = II^*, III^*, IV^*$, aleshores*

$$\rho(\frac{p-1}{2}) : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

és la representació associada als punts de p-torsió de la corba el·líptica E', torçada de E per l'únic caràcter quadràtic ramificat només en p, amb p-tipus$(E') = IV, III, II$, respectivament.

Aleshores, amb les notacions d'abans, obtenim la

Proposició 2.6. *Les taules següents contenen la classe $m \pmod{p-1}$ que proporciona la representació minimal $\rho(m)$ associada a ρ i el seu pes $k_{\rho(m)}$.*

i) *Si E és potencialment ordinària en p,*

p-tipus$(E) = II$	m	$k_{\rho(m)}$
$\rho\|_{D_p}$ red. compl.	$\frac{5p+1}{6}$	$\frac{p-1}{3}$
$\rho\|_{D_p}$ red. no-compl.	$\frac{p-1}{6}$	$2\frac{p+1}{3}$

p-tipus$(E) = III$	m	$k_{\rho(m)}$
$\rho\|_{D_p}$ red. compl.	$\frac{3p+1}{4}$	$\frac{p-1}{2}$
$\rho\|_{D_p}$ red. no-compl.	$\frac{p-1}{4}$	$\frac{p+3}{2}$

p-tipus$(E) = IV$	m	$k_{\rho(m)}$
$\rho\|_{D_p}$ red. compl.	$\frac{p-1}{3}$	$\frac{p+5}{3}$
$\rho\|_{D_p}$ red. no-compl.	$\frac{p-1}{3}$	$\frac{p+5}{3}$

ii) *Si E és potencialment supersingular en p,*

p-tipus $(E) = II$	m	$k_{\rho(m)}$
$\rho\|_{D_p}$ *red. compl.*	$\frac{5p-1}{6}$	$\frac{p+1}{3}$
$\rho\|_{D_p}$ *red. no-compl.*	$\frac{p+1}{6}$	$2\frac{p+1}{3}$
$\rho\|_{D_p}$ *irreductible*	$\frac{5p-7}{6}$	$\frac{p+7}{3}$

p-tipus $(E) = III$	m	$k_{\rho(m)}$
$\rho\|_{D_p}$ *red. compl.*	$\frac{3p-1}{4}$	$\frac{p+1}{2}$
$\rho\|_{D_p}$ *red. no-compl.*	$\frac{p+1}{4}$	$\frac{p+1}{2}$
$\rho\|_{D_p}$ *irreductible*	$\frac{p+1}{4}$	$\frac{p+1}{2}$

p-tipus $(E) = IV$	m	$k_{\rho(m)}$
$\rho\|_{D_p}$ *red. compl.*	$\frac{p+1}{3}$	$\frac{p+1}{3}$
$\rho\|_{D_p}$ *red. no-compl.*	$\frac{p+1}{3}$	$2\frac{p+1}{3}$
$\rho\|_{D_p}$ *irreductible*	$\frac{p+1}{3}$	$\frac{p+1}{3}$

Veieu l'experiment numèric No.1 del capítol 8 on es posen de manifest els avantatges de considerar la representació minimal associada a una representació donada.

CAPÍTOL 7

Prova de la conjectura de Serre per al cas de corbes de Weil potencialment ordinàries

En aquest capítol provem la conjectura de Serre per a les representacions de Galois residuals, ρ, associades als punts de p-torsió de les corbes de Weil potencialment ordinàries en p. Per veure aquest resultat apliquem les tècniques de les representacions torçades exposades en el capítol 5. La dificultat rau en què una tal representació residual no és, d'entrada, modular ja que prové d'una forma parabòlica (en característica 0) amb p^2 dividint el seu nivell. La prova consisteix en tres etapes; en la primera, s'associa a la representació ρ una certa forma nova amb caràcter no trivial i nivell estrictament inferior al conductor de la corba de Weil. En la segona, s'analitzen els *coeficents ocults* d'aquesta forma nova i es determina la p-ordinarietat de la mateixa en funció dels p-símbols de Kodaira. En la tercera, les sèries d'Eisenstein de pes 1 i l'operador traça acompleixen l'efecte d'abaixar el nivell i augmentar el pes, de manera simultània, convertint-los en els invariants conductor i pes predits per la conjectura.

§1. Una forma nova amb Nebentypus associada a E

Sigui E una corba de Weil de conductor analític N_E. Posem F la forma nova de pes 2 associada a E via el morfisme no constant $\phi : X_0(N_E) \to E$ (cf. capítol 1, §5).

De **[Ca 86]** se segueix la igualtat entre el conductor analític i el

geomètric; és a dir, $N_E = N_0$ on N_0 és el conductor d'Artin de la representació de $G_{\mathbb{Q}}$ en els automorfismes del $\mathbb{Q}_\ell$-mòdul de Tate $V_\ell(E)$ amb $\ell \nmid N_E$. De fet, a **[Ca 86]** s'hi troba un resultat més general que assegura que, per a tot primer ℓ, el nivell d'una forma nova qualsevol i el conductor d'Artin de la representació ℓ-àdica associada són iguals en els factors fora de ℓ.

Per tant, essent p un primer ≥ 5, notem que si la corba de Weil E té p-símbol de Kodaira I_0^*, II, III, IV, II^*, III^*, o bé IV^* aleshores $p^2 \| N_E$; és a dir, $N_E = Np^2$ amb N el conductor d'Artin de la represntació p-àdica associada.

Quan la corba de Weil E té potencialment bona reducció ordinària en $p \geq 5$, en la següent proposició associem a E una altra forma nova G, amb caràcter, que ens servirà per provar la conjectura de Serre per a la representació de $G_{\mathbb{Q}}$ definida pels punts de p-torsió de E.

Proposició 1.1. *Sigui $F(q) = \sum A_n q^n \in S_2(Np^2)$ la forma nova associada a una corba de Weil E amb bona reducció potencial ordinària en $p \geq 5$. Aleshores existeix una forma nova*

$$G(q) = \sum B_n q^n \in S_2(Np^a, \psi^{2v}), \qquad q = e^{2\pi i z},$$

amb el mateix sistema de valors propis que la forma torçada $F \otimes \psi^v$, on

$\mathcal{E}_{/\mathbf{F}_p}$	I_0^*	II	III	IV	II^*	III^*	IV^*
a	0	1	1	1	1	1	1

,

el caràcter

$$\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \overline{\mathbb{Q}}^*$$

és l'invers del caràcter de Teichmüller (després d'escollir una immersió $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$), i

$$v = \frac{p-1}{e}.$$

DEMOSTRACIÓ. Observem que la forma $F \otimes \psi^v$ és una funció pròpia per als operadors de Hecke amb sistema de valors propis $\{A_\ell \psi^v(\ell), \psi^{2v}\}_{\ell \nmid Np}$. Per tant, existeix un divisor M de Np^2 i una forma nova $G \in S_2(M, \psi^{2v})$ amb el mateix sistema de valors propis que $F \otimes \psi^v$. De fet,

$$F \otimes \psi^v = G - G|U_p|_p B\,,$$

on U_p és el p-èsim operador de Hecke i ${}_pB$ és l'operador de degeneració (cf. [**At-Li 78**]). Hem de provar que $M = N$ si la corba el·líptica E té p-símbol de Kodaira I_0^*, i $M = Np$ altrament.

Sigui ara ℓ un primer tal que $\ell \nmid Np$. Triem una immersió de $\overline{\mathbb{Q}}$ a $\overline{\mathbb{Q}}_\ell$ i notem per

$$\psi_\ell : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mu_{p-1} \to \overline{\mathbb{Q}}_\ell^*$$

el caràcter galoisià ℓ-àdic deduït de ψ. Per les congruències d'Eichler-Shimura (cf. capítol 2, §1), si

$$\rho_\ell : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell(E) \otimes \overline{\mathbb{Q}}_\ell) \backsimeq \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

denota la representació ℓ-àdica associada a E, aleshores

$$\rho_\ell \otimes \psi_\ell^v : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

és la representació ℓ-àdica associada a $F \otimes \psi^v$. Notem que $\rho_\ell \otimes \psi_\ell^v$ és també la representació ℓ-àdica per a la forma nova G.

Pel teorema de Carayol [**Ca 86**], sabem que el nivell d'una forma nova es pot llegir en la representació ℓ-àdica associada; per tant, tot el que hem de fer és calcular el conductor d'Artin de la representació $\rho_\ell \otimes \psi_\ell^v$. Ara bé, ja que el caràcter ψ_ℓ és no-ramificat fora de p, només cal calcular l'acció de I_p, el grup d'inèrcia de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Ja que E té reducció potencialment ordinària en p, E adquireix bona reducció sobre l'anell d'enters del cos $\mathbb{Q}_p(\pi)$, amb $\pi^e = p$ i $p \equiv 1 \pmod{e}$; per tant, ρ_ℓ restringida a I_p factoritza a través d'un grup cíclic C_e, d'ordre e. En particular, això força que la restricció $\rho_\ell|_{I_p}$ diagonalitzi. Més encara, $\det \rho_\ell(I_p) = 1$ i, per tant,

$$\rho_\ell|_{I_p} = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$$

amb un caràcter $\varepsilon : C_{p-1} \to \mu_e(\overline{\mathbb{Q}}_\ell)$. Podem veure ε com un caràcter galoisià no-ramificat fora de p, denotat encara ε,

$$\varepsilon : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Gal}\,(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \backsimeq C_{p-1} \to C_e \to \mu_e(\overline{\mathbb{Q}}_\ell)\,.$$

Però, ε ha de ser $\psi_\ell^{\pm v}$ ja que, amb $\overline{\mathbb{Q}}_\ell$ fixada, només hi ha dos caràcters de $C_{p-1} \to \mu_{p-1}(\overline{\mathbb{Q}}_\ell)$ d'ordre e quan $e = 3, 4, 6$, i només un quan $e = 2$. Per tant, ara és clar que $\rho_\ell \otimes \psi_\ell^v$ té conductor d'Artin amb exponent 1 en p si $e = 3, 4, 6$, i 0 si $e = 2$. □

Definició 1.2. Anomenem forma nova amb Nebentypus (caràcter no necessàriament trivial) associada a E la forma G obtinguda a partir de la corba de Weil E en la proposició 1.1. D'aquesta manera distingim la forma G de la forma F amb Hauptypus (caràcter trivial) associada a la corba de Weil E.

Veieu l'experiment numèric No.2 del capítol 8 que fou la font per intuir l'enunciat de la proposició 1.1.

§2. Coeficients ocults

Observem que la forma nova amb Nebentypus $G(q) = \sum_{n=1}^{\infty} B_n q^n$, associada a E, satisfà

$$B_\ell = A_\ell\, \psi^v(\ell)\,,$$

per a tot primer $\ell \neq p$. El coeficient de Fourier B_p, que anomenem coeficient ocult, de moment ens és desconegut. En aquesta secció esbrinem les propietats de B_p que necessitarem tot seguit.

Excloem, per ara, el cas en què la corba de Weil E té p-símbol de Kodaira I_0^*; la raó d'aquesta exclusió prové del fet que, en tal cas, la forma nova G correspon a una corba de Weil E' amb bona reducció a p. Més exactament, E' és la corba el·líptica torçada de E per l'únic caràcter quadràtic no-ramificat fora de p. Aleshores el coeficient B_p és un enter i té la mateixa llibertat que tot altre coeficient de Fourier; llibertat que, recordem, està restringida per la desigualtat $|B_p| < 2\sqrt{p}$, conjecturada per E. Artin i provada als anys 30 per Hasse.

Proposició 2.1. *Es mantenen les hipòtesis de la proposició* 1.1 *i assumim* $a = 1$. *Posem* K_G *el cos de nombres generat per tots els coeficients de Fourier* B_n *de la forma nova amb Nebentypus* $G(q) = \sum B_n q^n \in S_2(Np, \psi^{2v})$, *associada a la corba de Weil* E. *Aleshores tenim:*

i) *El cos* K_G *és igual a*

$$\mathbb{Q}(\psi^v) = \begin{cases} \mathbb{Q}(\sqrt{-3}) & si\ e = 3,6, \\ \mathbb{Q}(i) & si\ e = 4. \end{cases}$$

ii) *El coeficient ocult* B_p *satisfà* $|B_p| = \sqrt{p}$.

iii) *Si* v_p *denota la valoració p-àdica normalitzada de* $\overline{\mathbb{Q}}$ *fixada per* $\overline{\mathbb{Q}}_p$, *aleshores*

$$v_p(B_p) \in \{0, 1\}.$$

DEMOSTRACIÓ. Ja que el desenvolupament de Fourier de la forma nova F associada a E té coeficients enters, és clar que B_ℓ pertany al cos $\mathbb{Q}(\psi^v)$ per a tot primer $\ell \neq p$. Per ser G una forma nova es té, pel teorema B de Miyake a [**Mi 71**], que el cos K_G pot ser generat per quasi tots els coeficients B_ℓ llevat d'un nombre finit. Per tant, tots els coeficients de Fourier de G pertanyen a $\mathbb{Q}(\psi^v)$.

D'altra banda, ja que la forma nova G té p-Nebentypus primitiu (en el sentit que coincideixen les valoracions en p del seu nivell i del conductor del seu caràcter), podem aplicar el teorema d'Ogg-Li-Asai que proporciona $|B_p| = \sqrt{p}$ i, per tant, $v_p(B_p) + v_p(\overline{B}_p) = 1$.

Finalment, notem que B_p és un enter del cos K_G per ser un valor propi de l'operador de Hecke U_p i que, per tenir E reducció potencialment ordinària en p, el primer p descompon completament a K_G. D'on se segueix que $v_p(B_p) \in \{0, 1\}$. □

Com a conseqüència de l'anterior proposició obtenim el següent

Corol·lari 2.2. *Amb les notacions d'abans,*

i) *Si* $e = 3, 6$, *existeixen dos enters* a, $b \in \mathbb{Z}$ *tals que*

$$B_p = \frac{2a + b}{2} + \frac{b}{2}\sqrt{-3}, \qquad amb \qquad a^2 + ab + b^2 = p.$$

ii) *Si* $e = 4$, *existeixen dos enters* $a, b \in \mathbb{Z}$ *tals que*

$$B_p = a + bi\,, \qquad amb \qquad a^2 + b^2 = p\,.$$

Observació 2.3. Els dos únics cossos quadràtics imaginaris amb grup d'unitats diferent de $\{\pm 1\}$ són, precisament, $\mathbb{Q}(\sqrt{-3})$ i $\mathbb{Q}(i)$. Això fa que al resoldre les equacions diofàntiques $x^2 + xy + x^2 = p$ i $x^2 + y^2 = p$ trobem 6 candidats a coeficient ocult B_p en el primer cas ($e = 3, 6$), i 4 candidats en el segon cas ($e = 4$). Com saber discernir, directament a partir de E, entre els candidats és una qüestió encara no resolta. No obstant, a continuació mostrem un procediment, o enginy numèric, que pot ser útil per al càlcul de B_p.

Sigui $A_{|\mathbb{Q}}$ la varietat abeliana, factor de $J_1(Np)_{|\mathbb{Q}}$, associada a la forma nova G (cf. capítol 2, §1). És clar que $\dim(A_{|\mathbb{Q}}) = 2$. Un exercici senzill (cf. capítol 1, §4) ens mostra que, si W_p és la involució de Fricke en p, aleshores

$$G|W_p = \lambda_p(G)\,\overline{G}$$

on $\lambda_p(G) \neq 0$ és el pseudo-valor propi de W_p en G i $\overline{G}$ és la forma nova conjugada complexa de G; és a dir,

$$\overline{G}(q) = \sum \overline{B}_n q^n\,.$$

Per tant, l'espai $\Omega_{A_{/\mathbb{C}}}$ de les diferenecials invariants s'identifica amb l'espai $< G, \overline{G} >$ generat sobre $\mathbb{C}$ per les formes noves G i $\overline{G}$. D'altra banda, sabem que $G|W_{Np} = \lambda_{Np}(G)\,\overline{G}$ (cf. capítol 1, §4). Aleshores es satisfan les hipòtesis del teorema 1 a **[Sh 73]**. En aplicar-lo obtenim que la funció zeta de la varietat abeliana $A_{|\mathbb{Q}}$ coincideix, llevat pot ser dels factors d'Euler en els primers de mala reducció, amb el producte $G(q)\,\overline{G}(q)$. Posteriors resultats de teoria general donen la igualtat en tots els factors (cf. **[Ca 86]**).

L'obtenció del coeficient ocult B_p es redueix, doncs, a conèixer la funció zeta de la varietat abeliana $A_{|\mathbb{Q}}$ o, equivalentment, a conèixer la forma parabòlica $H = G\overline{G}$ de nivell Np, pes 4 i caràcter trivial. En efecte, tenim que

$$H(q) = \sum C_n q^n \in S_4(Np)\,,$$

amb $C_n = \sum_{i+j=n} B_i \overline{B}_j$ i, amb el coneixement d'una base de l'espai $S_4(Np)$, és possible determinar B_p com a solució d'un sistema d'equacions lineals.

Veieu l'experiment numèric No.3 del capítol 8 que serví per intuir la naturalesa del coeficient ocult.

§3. Ordinarietat

En la secció anterior hem tractat dels coeficients ocults; les seves propietats i les dificultats per obtenir-los. En particular, hem vist que el coeficient ocult B_p és un enter algebraic de valoració p-àdica nul·la o igual a 1. Decidir quan es presenta un cas o l'altre és un punt clau en la prova de la conjectura de Serre per a les representacions que provenen de la p-torsió de les corbes de Weil potencialment ordinàries en p. Ara anem a distingir aquests dos casos en funció del p-símbol de Kodaira de la corba de Weil.

Proposició 3.1. *Sigui E una corba de Weil potencialment ordinària en $p > 7$, amb p-tipus diferent de I_0^*. Posem G la forma nova amb Nebentypus associada a E, i $\overline{G}$ la forma nova múltiple de $G|W_p$. Es té:*

i) *Si el p-símbol de Kodaira de E és II, III, o bé IV, aleshores G és una forma $\mathfrak{P}$-ordinària.*

ii) *Si el p-símbol de Kodaira de E és II^*, III^*, o bé IV^*, aleshores $\overline{G}$ és una forma $\mathfrak{P}$-ordinària.*

DEMOSTRACIÓ. Ja que E té bona reducció potencial ordinària en p, la restricció de $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E_p) \simeq \mathrm{GL}_2(\mathbb{F}_p)$ al grup d'inèrcia I_p redueix. Ve donada per

$$\begin{pmatrix} \chi^{p-v} & * \\ 0 & \chi^v \end{pmatrix} \text{ si el } p\text{-tipus}(E) = II, III, IV, \text{ i}$$

$$\begin{pmatrix} \chi^{v+1} & * \\ 0 & \chi^{v(e-1)} \end{pmatrix} \text{ si el } p\text{-tipus}(E) = II^*, III^*, IV^*$$

(cf. capítol 6, teorema 1.4 i proposició 2.1).

Obtenim

forma	representació	p-tipus$(E) = II, III, IV$	p-tipus$(E) = II^*, III^*, IV^*$
G	$\rho \otimes \chi^{-v}\vert_{I_p}$	$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} * & * \\ 0 & \chi^{(e-2)v} \end{pmatrix}$
$\overline{G}$	$\rho \otimes \chi^{v}\vert_{I_p}$	$\begin{pmatrix} * & * \\ 0 & \chi^{2v} \end{pmatrix}$	$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$

Per tant, pel teorema 1.4 del capítol 3, G no pot ser $\mathfrak{P}$-ordinària quan E és de tipus II^*, III^* o bé IV^* en p, resp. $\overline{G}$ no pot ser $\mathfrak{P}$-ordinària quan E és de tipus II, III o bé IV en p. Ja que, per la proposició 2.1, sabem que una d'ambdues ha de ser ordinària, la proposició queda provada. □

§4. La prova

Ara tot és a punt per provar el

Teorema 4.1. *La conjectura de Serre* [**Se 87**, (3.2.4?)] *és certa per a tota representació irreductible*

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\,(E_p) \backsimeq \mathrm{GL}_2(\mathbb{F}_p)\,,$$

on E és una corba de Weil potencialment ordinària en $p > 7$. És a dir, la representació ρ prové d'una forma parabòlica de Hecke (mod$p$) *de tipus* $(N_\rho, k_\rho, \varepsilon_\rho)$.

DEMOSTRACIÓ. Sigui N_E el conductor geomètric de E. Sabem que $N_E = Np^2$, on N és el conductor d'Artin de la representació p-àdica associada a E. Si utilitzem el corol·lari 3.4 que hem provat en el capítol 5, és suficient veure que la representació minimal associada a ρ, o bé una companya seva en cas d'existir, satisfà la conjectura de Serre.

Seguint la proposició 2.4 que hem obtingut en el capítol 6, trobem la representació minimal (o la companya) $\rho(\hat{m})$, associada a ρ, segons el tipus de reducció de E en p:

$$\rho(\hat{m}) = \begin{cases} \rho(\upsilon) & \text{si } p\text{-tipus}(E) = II,\ III,\ IV\ , \\ \rho(-\upsilon) & \text{si } p\text{-tipus}(E) = II^*,\ III^*,\ IV^*\ , \\ \rho(\upsilon) & \text{si } p\text{-tipus}(E) = I_0^*\ , \end{cases}$$

on $\upsilon = \dfrac{p-1}{e}$.

Posem N_ρ, k_ρ els invariants conductor i pes associats a ρ; els seus valors els hem calculat en els teoremes 1.1 i 1.4 del capítol 6. Recordem que en aquest cas l'invariant ε_ρ és el caràcter trivial. En cada cas, anem a veure que $\rho(\hat{m})$ satisfà la conjectura.

Cas 1. El p-símbol de Kodaira de E és II, III, o bé IV. Els invariants de $\rho(\upsilon)$ són

$$(N_\rho, p+1-2\upsilon, 1)\,.$$

Considerem la forma nova $G(q) = \sum B_n q^n$ amb Nebentypus associada a E. Sabem, per la proposició 3.1, que G és una forma $\mathfrak{P}$-ordinària. Per tant, la valoració p-àdica del coeficient ocult és $v_p(B_p) = 0$. Si normalitzem l'exponent del caràcter $\psi^{2\upsilon}$, d'acord amb el teorema 1.2 que hem provat en el capítol 5, podem prendre $d = \upsilon(e-2)$ i, aleshores, arribem a que

$$\mathrm{Tr}\,(GE_{1,\psi}^{\upsilon(e-2)}) \in S_{p+1-2\upsilon}(N)\,,$$

i

$$\mathrm{Tr}\,(GE_{1,\psi}^{\upsilon(e-2)}) \equiv G \pmod{\mathfrak{P}}\,.$$

Els coeficients de Fourier de g, la reducció $\pmod{\mathfrak{P}}$ de $\mathrm{Tr}\,(GE_{1,\psi}^{\upsilon(e-2)})$, són congrus a $\rho(\upsilon)(\mathrm{Frob}_\ell)$ per a tot $\ell \nmid Np$. D'on g és una forma parabòlica de Hecke $(\bmod p)$ de tipus $(N, p+1-2\upsilon, 1)$ i tal que

$$\rho_g \backsimeq \rho(\upsilon)\,.$$

El pes i el càracter de g són els correctes i el seu nivell N és primer amb p. Només si es presenta la situació d'existir un primer ℓ amb ℓ-tipus$(E) = \mathrm{I}_r$ i $p \mid r$, N no és encara el conductor N_ρ (cf. capítol 6, teorema 1.1); no obstant això, notem que estem en condicions d'aplicar el teorema 5.5 del capítol 4 [**Jor-Liv 89**] i corregir aquest eventual abaixament. Per tant, $\rho(\upsilon)$ satisfà la conjectura de Serre i això acaba la prova en aquest cas.

Cas 2. El p-símbol de Kodaira de E és II^*, III^*, o bé IV^*. La demostració per a aquest cas és simètrica, "respecte la involució W_p", del cas anterior. Ara, els invariants de la representació minimal, o bé de la companya, $\rho(-v)$ són

$$(N_\rho, 2(v+1), 1).$$

Cal considerar la forma nova $\overline{G}(q) = \sum \overline{B}_n q^n$, conjugada complexa de la forma nova amb Nebentypus, G, associada a E. Ara és $\overline{G}$ la forma $\mathfrak{P}$-ordinària. Per tant, la valoració p-àdica del coeficient ocult és $v_p(B_p) = 1$. En normalitzar l'exponent del caràcter ψ^{-2v} de $\overline{G}$, d'acord amb el teorema 1.2 del capítol 5, trobem $d = 2v$ i, aleshores, arribem a que

$$\mathrm{Tr}\,(\overline{G}E_{1,\psi}^{2v}) \in S_{2(v+1)}(N),$$

i

$$\mathrm{Tr}\,(\overline{G}E_{1,\psi}^{2v}) \equiv \overline{G} \pmod{\mathfrak{P}}.$$

Els coeficients de Fourier de $\overline{g}$, la reducció (mod $\mathfrak{P}$) de $\mathrm{Tr}\,(\overline{G}E_{1,\psi}^{2v})$, són congrus a $\rho(-v)(\mathrm{Frob}_\ell)$ per a tot $\ell \nmid Np$. D'on $\overline{g}$ és una forma parabòlica de Hecke (mod p) de tipus $(N, 2(v+1), 1)$ i tal que

$$\rho_{\overline{g}} \backsimeq \rho(-v).$$

El mateix raonament d'abans ens porta a que $\rho(-v)$ satisfà la conjectura de Serre.

Cas 3. El p-símbol de Kodaira de E és I_0^*. Aquest cas és fàcil ja que els invariants de la representació minimal $\rho(m)$ són $(N_\rho, 2, 1)$. La reducció (mod $\mathfrak{P}$) de la forma nova G amb Nebentypus associada a E proporciona una forma parabòlica g de Hecke (mod p) de tipus $(N, 2, 1)$ amb $\rho_g \backsimeq \rho(m)$. En cas necessari (cf. capítol 6, teorema 1.1), notem que estem en condicions d'aplicar el teorema 5.4 del capítol 4 **[Ca 89]** i acabem d'arreglar el nivell. □

CAPÍTOL 8

Experiments numèrics

§1. Experiment No. 1: Avantatges de la representació minimal

Considerem la corba el·líptica E sobre $\mathbb{Q}$ donada pel model de Weierstraß

$$y^2 + xy + y = x^3 + 7x - 15\,;$$

aquesta corba es troba a les taules d'Edixhoven-de Groot-Top [**Ed-Gr-To 90**]. El seu discriminant és potència de primer,

$$\Delta_E = -359^2\,,$$

i el seu conductor

$$N_E = 359^2\,.$$

Implementat l'algoritme de Tate, trobem que el model de Néron sobre l'anell local $\mathbb{Z}_{359}$ té reducció amb símbol de Kodaira *II*. D'altra banda, ja que $359 \equiv 2 \pmod 3$, tenim que $E_{|\mathbb{Q}}$ té bona reducció potencial supersingular en 359.

La representació del grup de Galois absolut

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\,(E_{359})\,,$$

definida per l'acció de $\mathrm{G}_{\mathbb{Q}}$ sobre els punts de 359-torsió de $E_{|\mathbb{Q}}$ és contínua, senar i irreductible (per exemple, ja que $163 < 359$). Els teoremes 1.1 i 1.4 del capítol 6 permeten calcular els invariants per a ρ:

$$N_\rho = 1 \qquad k_\rho = 21840 \qquad \varepsilon_\rho = 1\,.$$

Aleshores, la conjectura de Serre prediu l'existència d'una forma parabòlica de Hecke

$$f \in S_{21840}(1)\,,$$

amb coeficients a_ℓ congrus (mod 359) als de la L-sèrie de Hasse-Weil associada a la corba el·líptica

$$L(E,s) = \sum_{n=1}^{\infty} \frac{A_n}{n^s}\,,$$

per a tot primer $\ell \neq 359$. Calculem els primers coeficients de la L-sèrie:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A_n	1	1	−2	−1	1	−2	−4	−3	1	1	−2	2	3	−4	−2

En calcular la dimensió de l'espai de formes parabòliques, on hem de cercar f, obtenim

$$\dim S_{21840}(1) = 1821\,.$$

Aquesta dimensió és excessiva per realitzar càlculs sobre un ordinador de talla mitjana.

Ara bé, al considerar la representació minimal (o la companya) associada a ρ, podem alleugerir els càlculs i, en conseqüència, el temps d'execució per tal de trobar la forma f que contrasti favorablement la conjectura. En efecte, seguint la proposició 2.4 del capítol 6, trobem que els invariants associats a la representació $\rho(60)$ per a ρ són:

$$N_\rho = 1 \qquad k_{\rho(60)} = 240 \qquad \varepsilon_\rho = 1\,.$$

Ara $\dim S_{240}(1) = 20$ i una base ve donada per

$$S_{240}(1) = < f_i >_{i=1,20} \quad \text{amb } f_i = \Delta^i E_6^{40-2i}\,,$$

on

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24} \in S_{12}(1)$$

i

$$E_6(q) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \in M_6(1),$$

són l'invariant discriminant i la sèrie d'Eisenstein de pes 6, respectivament.

S'ha implementat un programa escrit en codi FORTRAN que obté els vectors propis per a l'operador de Hecke T_2 actuant a $S_k(1)$. Per a $k = 240$, expressat en l'anterior base, trobem els vector propi

$$G = (1, 200, 8, 89, 210, 347, 117, 284, 158, 24,$$
$$242, 6, 264, 238, 190, 233, 238, 320, 303, 281).$$

Els seus primers coeficients de Fourier són:

$$\begin{aligned} G(q) = & q - \\ & 18976\,q^2 + \\ & 174762740\,q^3 - \\ & 1040444733543\,q^4 + \\ & 4499651242530976\,q^5 - \\ & 15060060147344832709\,q^6 + \\ & 40580143460545124102245\,q^7 - \\ & 90415252923989878420327980\,q^8 + \\ & 169773777843010223881644216947\,q^9 - \\ & 272439902993476545159400919943020\,q^{10} + \\ & 377555704481308893617379138488273600\,q^{11} - \\ & 455414178223644406628199528768738304222\,q^{12} + \\ & 480912466381700331716014103399776614240292\,q^{13} - \\ & 446423056402027970479412561736757701070300244\,q^{14} + \\ & 365253275569640340540625846681467784312619400533\,q^{15} - \\ & \ldots \end{aligned}$$

En reduir la forma $G \pmod{359}$ obtenim la forma $g(q) = \sum b_n q^n$,

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
b_n	1	−308	104	−88	47	−81	140	−181	191	−116	279	177	184	−40	221 .

La potència 60 de l'operador de Ramanujan-Katz ens proporciona

$$f(q) := \theta^{60} g(q) = \sum_{n=1}^{\infty} a_n q^n ,$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_n	1	−358	357	−1	1	−2	355	−3	1	−358	357	−357	3	−4	357 .

Notem que els primers coeficients resulten congrus (mod 359) als de la L-sèrie $L(E, s)$. Hem comprovat que ρ satisfà la conjectura en prendre la forma f, al menys per als primers 100 coeficients.

§2. Experiment No. 2: Abaixament de nivells

Considerem

$$F(z) = \sum_{n=1}^{\infty} A_n e^{2\pi i n z}$$

una forma nova de tipus (N, k, ε), definida sobre $\overline{\mathbb{Q}}$. Si

$$\phi : (\mathbb{Z}/M\mathbb{Z})^* \to \mathbb{C}^*$$

és un caràcter de Dirichlet mòdul M, aleshores

$$F \otimes \phi(z) = \sum_{n=1}^{\infty} A_n \, \phi(n) e^{2\pi i n z} \qquad (\phi(n) = 0 \text{ si m.c.d.}(n, M) \neq 1)$$

és una forma de Hecke parabòlica de tipus $(N', k, \varepsilon \, \phi^2)$, on

$$N' = \text{m.c.m.}(N, M \cdot \text{conductor}(\varepsilon), M^2) .$$

Si M és primer amb el nivell N, aleshores $F \otimes \phi$ és una forma nova de tipus $(NM^2, k, \varepsilon\,\phi^2)$; però en cas contrari, la forma $F \otimes \phi$ pot deixar de ser nova! La qüestió és "quan?".

Dels treballs de Li **[Li 75]** s'obté un criteri molt bonic per saber decidir quan una forma és nova o no. Concretament, es consideren els operadors K i H_N definits segons

$$G|H_N = G|\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \quad \text{i} \quad G|K(z) = \overline{G(-\overline{z})}\,,$$

per a tota forma parabòlica $G(z) = \sum_{n=1}^{\infty} B_n e^{2\pi i n z}$ de tipus (N, k, ε), definida sobre $\overline{\mathbb{Q}}$; aquests operadors satisfan les propietats següents:

$$\begin{aligned} H_N^2 &= (-1)^k\,, \\ K^2 &= 1\,, \\ H_N K &= (-1)^k K H_N\,, \\ H_N T_p &= \overline{\varepsilon}(p)\, T_p H_N \quad \text{si } p \nmid N\,, \\ G|K(z) &= \sum \overline{B}_n e^{2\pi i n z}\,. \end{aligned}$$

Es té

Proposició 2.1. (cf. **[Li 75]**). *Sigui $G \in S_k(N, \varepsilon)$ una forma parabòlica de Hecke. Aleshores, la forma G*

és nova de tipus $(N, k, \varepsilon) \iff$ satisfà l'equació funcional $G|K|H_N = \gamma G$,

per a certa constant complexa γ de mòdul 1.

Aleshores, per veure quan $F \otimes \phi$ deixa de ser nova podem aplicar el següent

Corol·lari 2.2. *Les notacions com abans. Si existeix un nombre complex $z \in \mathbb{H}$ tal que*

$$\left| \frac{\sum_{n=1}^{\infty} \overline{A}_n \overline{\phi}(n)\, e^{-2\pi i n/Nz}}{\sqrt{N^k}\, z^k \sum_{n=1}^{\infty} A_n \phi(n)\, e^{2\pi i n z}} \right| - 1 \neq 0\,,$$

aleshores $F \otimes \phi$ no és nova.

La implementació a l'ordinador d'un programa que apliqui l'anterior criteri per a les formes parabòliques de Hecke $F \otimes \phi$, obtingudes en tòrcer la forma nova F associada a una corba de Weil, ha estat el detonant per establir la proposició 1.1 del capítol 7. A continuació, expliquem els detalls d'aquesta implementació.

Considerem E una corba el·líptica sobre $\mathbb{Q}$ amb reducció additiva en un primer $p \geq 5$. Calculem un truncament de la L-sèrie de E:

$$L(E,s) = \sum_{n=1}^{\infty} \frac{A_n}{n^s},$$

a partir d'una equació de Weierstraß minimal. Si E és de Weil, aleshores

$$F(z) = \sum_{n=1}^{\infty} A_n e^{2\pi i n z}$$

és la forma nova de tipus $(N_E, 2, 1)$ associada a E, amb $N_E = Np^2$ i $p \nmid N$.

Es calcula una arrel primitiva ARRPR de $\mathbb{F}_p^*$ i es pren, com a ϕ, el caràcter de Dirichlet $(\bmod p)$, ψ, determinat per

$$\psi(\text{ARRPR}) = e^{2\pi i/(p-1)}.$$

Per a cada enter j, $0 \leq j \leq p-2$, s'esbrina si la forma $F \otimes \psi^j$ sembla ser, o no, nova de tipus $(Np^2, 2, \psi^{2j})$. Per a això, comprovem l'equació funcional de la porposició 2.1 aplicant el corol·lari 2.2 amb $z = 2i/\sqrt{N_E}$.

Heus ací, el programa escrit en codi FORTRAN i un joc de proves obtingut en un VAX 8600 de la Facultat d'Informàtica de Barcelona.

```
      PROGRAM PROPOSICIO 1.1 DEL CAPÍTOL 7
      IMPLICIT INTEGER(A-Z)
      DIMENSION                  AN(100000),P(10000)
      REAL*16                    A1,A2,A3,A4,A6,Q1,Q2,PI,X,A,NN
      COMPLEX*16                 XI(0:4596),F1,F2
-----------------------------------------------------------------
       ENTRADA DE DADES I CÀLCUL DE ARRPR
-----------------------------------------------------------------
      PI = 1
      PI = 4*ATAN(PI)
      P(1) = 2
      READ(104,*) (P(I),I=2,10000)
10    WRITE(5,*) 'ESCRIU NOMBRE DE COEFICIENTS'
      READ(5,*) NAN
```

```
      WRITE(5,*) 'ESCRIU PRIMER DOLENT'
      READ(5,*) PP
      DO I = 0,PP-1
              XI(I) = 0
      ENDDO
      XI(0) = 0
      XI(1) = 1
      DO I = 2,PP-1
              J = I
              DO WHILE(J.NE.1)
                      XI(J) = 1
                      J = MOD(I*J,PP)
              ENDDO
              DO J = 1,PP-1
                      IF(XI(J).EQ.0) GOTO 100
              ENDDO
              GOTO 110
100           CONTINUE
      ENDDO
110   ARRPR = I
      WRITE(5,*)'ARREL PRIMITIVA=',ARRPR
      WRITE(5,*)'ESCRIU COEFICIENTS DE LA C.E.:A1,A2,A3,A4,A6'
      READ(5,*) A1,A2,A3,A4,A6
      WRITE(5,*)'QUIN CONDUCTOR TÉ ?'
      READ(5,*) NN
```

CÀLCUL DE LA L-SÈRIE DE LA CORBA EL·LÍPTICA

```
      AN(2) = 0
      IF(QMOD(A6,QEXT(2)).EQ.0) AN(2)=AN(2)+1
      IF(QABS(QMOD(A6,QEXT(2))).EQ.QABS(QMOD(1+A3,QEXT(2))))
     C AN(2)=AN(2)+1
      IF(QMOD(A6+A4+A2+1,QEXT(2)).EQ.0) AN(2)=AN(2)+1
      IF(QABS(QMOD(A6+A4+A2+1,QEXT(2))).EQ.
     C QABS(QMOD(1+A1+A3,QEXT(2)))) AN(2)=AN(2)+1
      AN(2) = 2-AN(2)
      I=2
      DO WHILE(P(I).LE.NAN)
              AN(P(I)) = 0
              DO X = 0,P(I)-1
                      T = NINT(QMOD((A1*X+A3)**2+4*
     C                (X**3+A2*X**2+A4*X+A6),QEXT(P(I))))
                      IF(T.LT.0) T=T+P(I)
                      AN(P(I)) = AN(P(I))-LEG(T,P(I))
              ENDDO
              I = I+1
      ENDDO
      AN(1) = 1
      DO I = 4,NAN
              II = NINT(SQRT(FLOAT(I)))
              J = 1
              DO WHILE(P(J).LE.II)
                      IF(MOD(I,P(J)).EQ.0) THEN
                              AN(I) = AN(I/P(J))*AN(P(J))
                              IF(MOD(I,P(J)*P(J)).EQ.0.AND.
     C                        QMOD(NN,QEXT(P(J))).NE.0) AN(I)
     C                        = AN(I)-P(J)*AN(I/P(J)/P(J))
                              GOTO 20
                      ENDIF
                      J = J+1
              ENDDO
20    CONTINUE
```

```
      ENDDO
      WRITE(5,*) 'JA HE COMPUTAT LA L--SERIE '
```

TEST DE L'EQUACIÓ FUNCIONAL EN Z= i A/$\sqrt{NN}$

```
      A = 2
      Q1 = EXP(-2*PI/A/SQRT(NN))
      Q2 = EXP(-2*PI*A/SQRT(NN))
      WRITE(5,*) 'ORDRES DE LES CUES:'
      WRITE(5,*) Q1**NAN,Q2**NAN
      DO L = 0,PP-2
              XI(ARRPR) = EXP(2*PI*(0,1)*L/(PP-1))
              J = ARRPR
              DO WHILE(J.NE.1)
                      JJ = J
                      J = MOD(J*ARRPR,PP)
                      XI(J) = XI(JJ)*XI(ARRPR)
              ENDDO
              F1 = (0,0)
              F2 = (0,0)
              DO I = 1,NAN
                      F1 = F1+AN(I)*XI(MOD(I,PP))*Q1**I
                      F2 = F2+AN(I)*XI(MOD(I,PP))*Q2**I
              ENDDO
              WRITE(5,*) 'TEST:'
              WRITE(5,666) L,ABS(1-ABS(A*A*F2/F1))
      ENDDO
```

TORNAR A COMENÇAR AMB UN ALTRE EXEMPLE

```
      GOTO 10
666   FORMAT(I10,F30.10)
      END
```

Per a la corba el·líptica 338 **A1** de les taules de Cremona [**Cre 91**¬], $E : y^2 + xy = x^3 - x^2 + x + 1$ de conductor $N_E = 2 \cdot 13^2$, s'obtenen els resultats següents:

```
ESCRIU NOMBRE DE COEFICIENTS
500
ESCRIU PRIMER DOLENT
13
ARREL PRIMITIVA=  2
ESCRIU COEFICIENTS DE LA C.E.:A1,A2,A3,A4,A6
1,-1,0,1,1
QUIN CONDUCTOR TÉ ?
338
JA HE COMPUTAT LA L--SERIE
ORDRES DE LES CUES:
7.8316798774586411517161891399435 72E-0038
3.7620079493098318152677350009170 55E-0149
TEST:
         0                0.0000000000
         1                0.0000000000
         2                2.6699959395
         3                0.0000000000
         4                0.0000000000
         5                0.0000000000
         6                0.0000000000
         7                0.0000000000
```

```
 8                0.0000000000
 9                0.0000000000
10                2.6699959395
11                0.0000000000
```

Observem que les formes parabòliques de Hecke $F \otimes \psi^2$ i $F \otimes \psi^{10}$ semblen deixar de ser noves.

Per a la corba el·líptica $E : y^2 + xy + y = x^3 - 39x - 27$ de conductor $N_E = 43^2$, extreta de les taules **[Ed-Gr-To 90]**, s'obtenen els resultats següents:

```
ESCRIU NOMBRE DE COEFICIENTS
500
ESCRIU PRIMER DOLENT
43
ARREL PRIMITIVA=  3
ESCRIU COEFICIENTS DE LA C.E.:A1,A2,A3,A4,A6
1,0,1,-39,-27
QUIN CONDUCTOR TÉ ?
1849
JA HE COMPUTAT LA L--SERIE
ORDRES DE LES CUES:
1.36508179939715099004713027397206 1E-0016
3.47243963775299112396157985606635 7E-0064
TEST:
        0                0.0000000000
        1                0.0000000000
        2                0.0000000000
        3                0.0000000000
        4                0.0000000000
        5                0.0000000000
        6                0.0000000000
        7                0.0000000000
        8                0.0000000000
        9                0.0000000000
       10                0.0000000000
       11                0.0000000000
       12                0.0000000000
       13                0.0000000000
       14                5.5513673695
       15                0.0000000000
       16                0.0000000000
       17                0.0000000000
       18                0.0000000000
       19                0.0000000000
       20                0.0000000000
       21                0.0000000000
       22                0.0000000000
       23                0.0000000000
       24                0.0000000000
       25                0.0000000000
       26                0.0000000000
       27                0.0000000000
       28                5.5513673695
       29                0.0000000000
       30                0.0000000000
       31                0.0000000000
       32                0.0000000000
       33                0.0000000000
       34                0.0000000000
       35                0.0000000000
       36                0.0000000000
```

```
37              0.0000000000
38              0.0000000000
39              0.0000000000
40              0.0000000000
41              0.0000000000
```

Ara són les formes parabòliques de Hecke $F \otimes \psi^{14}$ i $F \otimes \psi^{28}$ que semblen deixar de ser noves.

En els dos exemples anteriors la corba el·líptica té reducció potencialment ordinària en $p = 13, 43$, respectivament; en efecte, en ambdos casos tenim $p \equiv 1 \pmod 3$ i, si seguim l'algoritme de Tate, trobem p-símbol de Kodaira igual a II i IV, respectivament. Aleshores, notem que es produeix l'abaixament d'acord amb la proposició 1.1 del capítol 7. No passa així quan la reducció és potencialment supersingular en p; per exemple: la corba el·líptica 605 **A1** de [**Cre 91**¬], E : $y^2+xy = x^3-x^2-1414x-44027$ de conductor $N_E = 5 \cdot 11^2$, té 11-símbol de Kodaira IV^*. Ja que $11 \equiv 2 \pmod 3$, E té reducció potencialment supersingular en 11. En executar el programa, obtenim:

```
ESCRIU NOMBRE DE COEFICIENTS
500
ESCRIU PRIMER DOLENT
11
ARREL PRIMITIVA=  2
ESCRIU COEFICIENTS DE LA C.E.:A1,A2,A3,A4,A6
1,-1,0,-1414,-44027
QUIN CONDUCTOR TÉ ?
605
JA HE COMPUTAT LA L--SERIE
ORDRES DE LES CUES:
1.84122388144332473599560176234758 1E-0038
1.14928144983344485193690092654354 9E-0149
TEST:
        0               0.0000000000
        1               0.0000000000
        2               0.0000000000
        3               0.0000000000
        4               0.0000000000
        5               0.0000000000
        6               0.0000000000
        7               0.0000000000
        8               0.0000000000
        9               0.0000000000
```

Totes les formes torçades $F \otimes \psi^j$ semblen ser noves.

§3. Experiment No. 3: Càlcul de coeficients ocults

Considerem la corba el·líptica $E_{|\mathbb{Q}}$ donada pel model de Weierstraß

$$y^2 + xy + y = x^3 - x^2 + 2x - 2\,;$$

aquesta corba es troba en les taules **[Ed-Gr-To 90]**. El seu conductor és

$$N_E = 37^2\,.$$

Amb l'algoritme de Tate, trobem que el model de Néron sobre $\mathbb{Z}_{37}$ té reducció amb símbol de Kodaira *II*. D'altra banda, ja que $37 \equiv 1 \pmod 3$, $E_{|\mathbb{Q}}$ té bona reducció potencial ordinària en 37.

Admetem que $E_{|\mathbb{Q}}$ és una corba de Weil. Aleshores, $F(q) = \sum A_n q^n$, l'anti-transformada de Mellin de la L sèrie de la corba el·líptica $E_{|\mathbb{Q}}$, és una forma nova de pes 2 i nivell 37^2.

Triem una immersió $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{37}$ de tal sort que el caràcter

$$\psi : (\mathbb{Z}/37\mathbb{Z})^* \to \overline{\mathbb{Q}}\,, \quad \psi(2) = e^{2\pi i/36}\,,$$

satisfaci

$$\psi(2) \equiv 2^{-1} \pmod{\mathfrak{P}_{37}}\,,$$

on $\mathfrak{P}_{37}$ és el primer de $\overline{\mathbb{Q}}$ dividint 37 que la immersió determina. (Notem que 2 és una arrel primitiva de $\mathbb{F}_{37}^*$.)

Considerem ara la forma nova G amb Nebentypus associada a E per la proposició 1.1 del capítol 7. Tenim $v = \dfrac{p-1}{e} = 6$, i

$$G(q) = \sum B_n q^n \in S_2(37, \psi^{12})\,,$$

té el mateix sistema de valors propis que $F \otimes \psi^6$; la forma nova $\overline{G}$ té el mateix sistema de valors propis que $F \otimes \psi^{30}$. Tenim

$$B_n = A_n\, \psi^6(n)\,,$$
$$\overline{B}_n = A_n\, \psi^{30}(n)\,,$$

per a tot $n \geq 1$ tal que $37 \nmid n$.

A continuació trobem el coeficient ocult B_{37}. El producte de les dues formes noves és

$$H(q) = G(q)\,\overline{G}(q) = \sum C_n q^n \in S_4(37)\,,$$

amd $C_n = \sum_{i+j=n} B_i\,\overline{B}_j$.

Ja que H és parabòlica, tenim $C_0 = 0$; també coneixem B_n per a $n < 37$. Això ens permet trobar els primers 37 coeficients de la forma H, alguns d'ells són:

n	1	2	3	4	5	6	7	8	9	10	11	12	...	36	37
C_n	0	1	−1	1	1	0	−1	−1	−10	7	−8	−4	...	−16	0 .

D'altra banda, sabem que $\dim S_4^{\text{noves}}(37) = 9$; una base amb coeficients enters la podem trobar a les taules de Bonn [**Bonn 87¬**]:

$$S_4^{\text{noves}}(37) = < g_1, g_2, g_3, g_4, g_5, f_1, f_2, f_3, f_4 > \,.$$

Trobem

$$H = \frac{1}{8}g_2 + \frac{1}{8}g_3 + \frac{15}{8}g_4 + \frac{39}{8}g_5\,.$$

Per tant, ara coneixem més coeficients de H:

n	1	2	3	4	5	6	7	8	9	10	11	...	37	38	39
C_n	0	1	−1	1	1	0	−1	−1	−10	7	−8	...	0	58	73 .

El coeficient de Fourier C_{38} proporciona l'equació:

$$B_{37} + \overline{B}_{37} = -11\,,$$

i el coeficient C_{39}:

$$(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)\,B_{37} + (-\frac{1}{2} - \frac{\sqrt{3}}{2}i)\,\overline{B}_{37} = 1\,.$$

D'on el coeficient ocult és

$$B_{37} = -\frac{11}{2} - \frac{3\sqrt{3}}{2}i.$$

Notem finalment, d'acord amb la proposició 2.1 del capítol 7, que $|B_{37}| = \sqrt{37}$ i B_{37} és un enter algebraic del cos $\mathbb{Q}(\sqrt{-3})$. A més, ja que

$$e^{2\pi i/36} \equiv 2^{-1} \pmod{\mathfrak{P}_{37}},$$

trobem $\sqrt{-3} \equiv 2^{-5} - 1 \equiv 21 \pmod{\mathfrak{P}_{37}}$; aleshores

$$B_{37} \equiv 26 \not\equiv 0 \pmod{\mathfrak{P}_{37}},$$

d'acord amb el fet que la corba el·líptica $E_{|\mathbb{Q}}$ té reducció potencialment ordinària en 37 amb símbol de Kodaira II (cf. capítol 7, proposició 3.1).

APÈNDIX 1

Cas semistable

En aquest apèndix tractem les representacions irreductibles

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\,(E_p)$$

associades als punts de p-torsió de les corbes el·líptiques amb reducció semistable en $p \geq 5$. Posem N_ρ, k_ρ i $\varepsilon_\rho = 1$ els invariants corresponents a ρ. El conductor geomètric de E és de la forma $N_E = Np$. Sabem (cf. capítol 6, teorema 1.4) que

$$k_\rho = \begin{cases} 2 & \text{si } p \mid \nu \\ p+1 & \text{si } p \nmid \nu, \end{cases}$$

on I_ν és el p-símbol de Kodaira per a E.

§1. El cas semistable finit

Quan la representació ρ és finita en p, tenim $k_\rho = 2$. Del profund treball de Ribet (cf. **[Ri 90]**) es dedueix el

Teorema 1.1. *Suposem que E és una corba de Weil amb reducció multiplicativa en $p \geq 5$. Si ρ és irreductible i finita en p, aleshores ρ satisfà la conjecutra de Serre.*

DEMOSTRACIÓ. Ja que $p \geq 5$, el teorema 1.1 que hem obtingut en el capítol 6 assegura que es produeix un abaixement entre N i N_ρ justament en els primers ℓ on ρ és finita. A més, per ser E de Weil i ρ finita en p, el teorema de Ribet (cf. capítol 4, teorema 5.3) assegura que ρ prové d'una forma parabòlica de Hecke de tipus $(N_\rho, 2, 1) = (N_\rho, k_\rho, \varepsilon_\rho)$. □

Observació 1.2. És així com es pot donar, suposant que les corbes el·líptiques de Frey **[Fr 86]** són de Weil, una prova per al darrer teorema de Fermat. A una hipotètica solució, no trivial, de l'equació de Fermat $a^p + b^p = c^p$, Frey associa una corba el·líptica $E = E(a,b,c,p)$ semistable sobre $\mathbb{Q}$. A més, la representació ρ definida pels punts de p-torsió és irreductible i finita en p, si $p \geq 5$. Per tant, si E és de Weil, ρ satisfà la conjectura de Serre. Però, s'arriba a una contradicció ja que resulta $N_\rho = 2$, $k_\rho = 2$, $\varepsilon_\rho = 1$ i, per ser la corba modular $X_0(2)$ de gènere 0, $\dim S_2(2) = 0$!!!!.

§2. El cas semistable no finit

Veiem ara que, amb lleugeres modificacions, podem aplicar les tècniques del capítol 5 per tal de provar el següent

Teorema 2.1. *Les notacions com a la secció anterior. Admetem que E és una corba de Weil amb reducció multiplicativa en $p \geq 5$. Si ρ és irreductible i no finita en p, aleshores ρ satisfà la conjecutra de Serre.*

DEMOSTRACIÓ. Ara tenim $k_\rho = p + 1$. Sigui $F(q) = \sum A_n q^n \in S_2(Np)$ la forma nova associada a la corba de Weil E. Considerem $E_{1,\psi}$ la sèrie d'Eisenstein de pes 1 que correspon al caràcter ψ, invers del caràcter de Teichmüller segons una immersió $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$. Fem el producte

$$FE_{1,\psi}^{p-1} \in S_{p+1}(Np)\,.$$

És fàcil comprovar que la forma parabòlica de Hecke ($\mathrm{mod}\ p$), g, obtinguda en reduir

$$\mathrm{Tr}\,(FE_{1,\psi}^{p-1}) \in S_{p+1}(N)$$

produeix la forma modular f que prediu la conjectura degut a que té el pes correcte, p no divideix el seu nivell i, ja que $A_p = \pm 1$, se satisfà

$$\mathrm{Tr}\,(FE_{1,\psi}^{p-1}) \equiv F \pmod{\mathfrak{P}}\,,$$

on $\mathfrak{P}$ és el primer de $\overline{\mathbb{Q}}$ que la immersió $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ determina (cf. capítol 5, §1 i **[Jor-Liv 89]**, remarca 2). □

Com a conseqüència obtenim

Corol·lari 2.2. *La conjectura de Serre és certa per a tota representació irreductible*

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E_p)$$

on $p \geq 5$ i E és una corba de Weil amb p-tipus$(E) = I_\nu^*$ $(\nu > 0)$; és a dir, amb reducció potencialment semistable en p.

DEMOSTRACIÓ. Considerem la representació torçada $\rho(\frac{p-1}{2})$ de ρ. Aquesta és la representació associada als punts de p-torsió de la corba E', torçada de E per l'únic caràcter quadràtic ramificat només en p. A més, $\rho(\frac{p-1}{2})$ és la minimal per a ρ. Ja que E' és de Weil, per ser-ho E, i semistable en p, tant si $\rho(\frac{p-1}{2})$ és finita en p com si no, podem aplicar els anteriors teoremes així com els criteris obtinguts en el capítol 5; aleshores trobem que ρ satisfà la conjectura. □

APÈNDIX 2

Cas supersingular

A continuació presentem algunes consideracions finals sobre les representacions

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\,(E_p)$$

definides pels punts de p-torsió de les corbes el·líptiques potencialment supersingulars en p, el darrer cas que queda.

§1. Una conjectura per al cas supersingular

A tota aquesta secció, E és una corba el·líptica sobre $\mathbb{Q}$ potencialment supersingular en $p \geq 5$ i tal que la representació ρ és irreductible. Despreciem el cas on el p-tipus$(E) = I_0^*$, ja que pot ser tractat amb les tècniques exposades en el capítol 7. Posem $N_E = Np^2$ el seu conductor geomètric. Considerem

$$L(E,s) = \sum_{n=1}^{\infty} \frac{A_n}{n^s}$$

la seva L-sèrie de Hasse-Weil. Definim

$$v^{\mathrm{ss}} = \frac{p+1}{e},$$

on e, com d'habitud, és el mínim comú múltiple de les multiplicitats de les components irreductibles de la fibra especial del model estable de E.

Per darrera vegada, escollim una extensió a $\overline{\mathbb{Q}}$ de la valoració p-àdica de $\mathbb{Q}$ i sigui $\mathfrak{P}$ el primer de $\overline{\mathbb{Q}}$, dividint p, que li correspon. Considerem el caràcter

$$\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \overline{\mathbb{Q}}^*$$

que s'identifica amb l'invers del caràcter de Teichmüller (segons $\mathfrak{P}$).

Amb les notacions anteriors, formulem la següent

Conjectura 1.1.$_?$ *Sigui E una corba el·líptica com abans. Existeix una forma nova, definida sobre $\mathbb{C}$,*

$$G(q) = \sum B_n q^n, \text{ de tipus } \begin{cases} (N_\rho p, 2, \psi^{2v^{ss}}) \\ (N_\rho p, 2, \psi^{2(1-v^{ss})}) \\ (N_\rho p, 2, \psi^{-2(1-v^{ss})}), \end{cases}$$

tal que per a tot n primer amb $N_\rho p$ es té

$$B_n \equiv \begin{cases} A_n\, \psi^{v^{ss}}(n) \\ A_n\, \psi^{1-v^{ss}}(n) \\ A_n\, \psi^{v^{ss}-1}(n) \end{cases} \pmod{\mathfrak{P}}$$

$$\text{si } \begin{cases} p\text{-tipus}(E) = II, III, IV \\ \rho|_{D_p} \text{ redueix i } p\text{-tipus}(E) = II^*, III^*, IV^* \\ \rho|_{D_p} \text{ irreductible i } p\text{-tipus}(E) = II^*, III^*, IV^*, \end{cases}$$

respectivament. A més, G és $\mathfrak{P}$-ordinària si, i només si, $\rho|_{D_p}$ redueix.

A la secció següent es mostra amb detall un exemple numèric d'aquesta conjectura; en tots els exemples efectuats s'ha obtingut èxit. Aleshores, es té el

Teorema 1.2. *Admetem la conjectura* 1.1.$_?$ *per a E. S'afirma que la representació*

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\,(E_p)$$

satisfà la conjectura de Serre.

DEMOSTRACIÓ. La prova consisteix en aplicar el corol·lari 3.4 que hem obtingut en el capítol 5. És suficient, doncs, veure que la representació $\rho(\hat{m})$, minimal o companya de ρ, satisfà la conjectura. Per a això, anem a manipular la forma nova G d'acord amb el teorema 1.2 que hem provat en el capítol 5. En normalitzar el caràcter de G, s'obté el valor

$$t = \begin{cases} -2v^{ss} + (p-1) & \text{si } p\text{-tipus}(E) = II, III, IV \\ 2(v^{ss} - 1) & \text{si } \rho|_{D_p} \text{ redueix, } p\text{-tipus}(E) = II^*, III^*, IV^* \\ 2(1 - v^{ss}) + (p-1) & \text{si } \rho|_{D_p} \text{ irred., } p\text{-tipus}(E) = II^*, III^*, IV^*. \end{cases}$$

Si tenim en compte l'ordinarietat en $\mathfrak{P}$ de G, pel teorema 1.2 del capítol 5, trobem que el valor

$$d = \begin{cases} -2v^{ss} + (p-1) & \text{si } p\text{-tipus}(E) = II, III, IV, \ \rho|_{D_p} \text{ redueix} \\ -2v^{ss} + 2(p-1) & \text{si } p\text{-tipus}(E) = II, III, IV, \ \rho|_{D_p} \text{ irred.} \\ 2(v^{ss} - 1) & \text{si } p\text{-tipus}(E) = II^*, III^*, IV^*, \ \rho|_{D_p} \text{redueix} \\ 2(1 - v^{ss}) + 2(p-1) & \text{si } p\text{-tipus}(E) = II^*, III^*, IV^*, \ \rho|_{D_p} \text{ irred.} \end{cases}$$

és tal que se satisfà la congruència

$$\mathrm{Tr}\,(GE_{1,\psi}^d) \equiv G \pmod{\mathfrak{P}}.$$

Per tant, la forma de Hecke g, obtinguda reduïnt $\mathrm{Tr}\,(GE_{1,\psi}^d)$, és de tipus $(N, 2+d, 1)$. Notem que

$$2 + d = \begin{cases} (e-2)\frac{p+1}{e} & \text{si } p\text{-tipus}(E) = II, III, IV, \ \rho|_{D_p} \text{ redueix} \\ 2p - 2\frac{p+1}{e} & \text{si } p\text{-tipus}(E) = II, III, IV, \ \rho|_{D_p} \text{ irred.} \\ 2\frac{p+1}{e} & \text{si } p\text{-tipus}(E) = II^*, III^*, IV^*, \ \rho|_{D_p} \text{ redueix} \\ 2(p+1) - 2\frac{p+1}{e} & \text{si } p\text{-tipus}(E) = II^*, III^*, IV^*, \ \rho|_{D_p} \text{ irred.} \end{cases}$$

Quan $\rho|_{D_p}$ redueix, si comparem amb la proposició 2.4 del capítol 6, trobem que, en cada cas, $(N, 2+d, 1)$ són els invariants minimals o companys associats a la representació ρ. Quan $\rho|_{D_p}$ és irreductible, els teoremes 3.4 del capítol 1 i 2.3 del capítol 3 donen que la filtració de $g(q)$ és $2+d-(p-1)$; per tant, obtenim també els invariants minimals o companys per a aquest cas. D'altra banda, per les hipòtesis sobre els coeficients de Fourier B_n, obtenim en cada cas que la representació $\rho(\hat{m})$ és isomorfa a ρ_g. Una vegada més, si cal, el teorema 5.5 del capítol 4 [**Jor-Liv 89**] permet corregir els eventuals abaixements entre els nivells i així veiem que $\rho(\hat{m})$ satisfà la conjectura. □

§2. Contrastació numèrica de la conjectura 1.1.?

Considerem la corba el·líptica E sobre $\mathbb{Q}$ donada pel model de Weierstraß

$$y^2 + xy = x^3 + 3x + 1\,;$$

aquesta corba el·líptica és la 242 **A1** de les taules [**Cre 91**¬]. El seu conductor és

$$N_E = 2 \cdot 11^2\,.$$

El model de Néron sobre l'anell local $\mathbb{Z}_{11}$ té reducció amb símbol de Kodaira II i, aleshores, E és potencialment supersingular en 11; la corba E només té isogènies $\mathbb{Q}$-racionals de grau 3, per tant

$$\rho:\ \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\,(E_{11}) \backsimeq \mathrm{GL}_2(\mathbb{F}_{11})$$

és irreductible i, ja que $v_{11}(c_4) = 1$, tenim que $\rho|D_{11}$ redueix.

Triem una immersió $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{11}$ de tal sort que el caràcter

$$\psi : (\mathbb{Z}/11\mathbb{Z})^* \to \overline{\mathbb{Q}}^*\,, \quad \psi(2) = e^{2\pi i/10}\,,$$

satisfaci

$$\psi(2) \equiv 2^{-1} \pmod{\mathfrak{P}_{11}}\,,$$

on $\mathfrak{P}_{11}$ és el primer de $\overline{\mathbb{Q}}$, dividint 11, que la immersió determina. (Notem que 2 és una arrel primitiva de $\mathbb{F}_{11}^*$.)

La conjectura 1.1.? prediu l'existència d'una forma parabòlica

$$G(q) = \sum B_n q^n \in S_2(22, \psi^4)$$

que satisfà les congruències

$$B_n \equiv A_n \psi^2(n) \pmod{\mathfrak{P}_{11}}$$

per a tot n senar primer amb 11.

De les taules de Barcelona [**Barna 91**¬] extraiem la informació

$$\dim S_2(22, \psi^4) = 1\,.$$

Com construir una base? La fórmula de les traces d'Eichler-Selberg proporciona la traça de l'operador de Hecke T_ℓ en l'espai de formes parabòliques $S_k(N,\varepsilon)$; quan $k=2$ i ε és un caràcter de Dirichlet de conductor p, pren l'aspecte

$$\text{Traça de } T_\ell \text{ en } S_2(N,\varepsilon) = -\sum_s a(s) \sum_r b(s,r) \prod_{q|N} c'_\varepsilon(s,r,q)\,,$$

on s recorre tots els enters tals que $s^2-4\ell$ és negatiu o un quadrat; és a dir,

$$\begin{cases} s^2-4\ell = t^2\,, \\ s^2-4\ell = t^2 m,\ 0>m\equiv 1 \pmod 4 \text{ i lliure de quadrats}, \\ s^2-4\ell = t^2 4m,\ 0>m\equiv 2,3 \pmod 4 \text{ i lliure de quadrats}. \end{cases}$$

Aleshores,

$$a(s) = \begin{cases} \operatorname{sgn}(x)\dfrac{\min(|x|,|y|)}{|x-y|} & \text{si } s^2-4\ell>0 \\ \dfrac{1}{2} & \text{si } s^2-4\ell<0\,, \end{cases}$$

amb x, y les arrels complexes del polinomi $\Phi(X)=X^2-sX+\ell$.

Fixat el valor s, r recorre els divisors de t i

$$b(s,r) = \begin{cases} \dfrac{1}{2}\varphi\left(\dfrac{s^2-4\ell}{r}\right) & \text{si } s^2-4\ell>0 \\ h\left(\dfrac{s^2-4\ell}{r^2}\right)/w\left(\dfrac{s^2-4\ell}{r^2}\right) & \text{si } s^2-4\ell<0\,, \end{cases}$$

on φ és la funció d'Euler i $h(d)$ (resp. $w(d)$) és el nombre de classes d'ideals (resp. 1/2 del cardinal del grup d'unitats) del cos quadràtic $\mathbb{Q}(\sqrt{d})$.

Fixat el parell (s,r), per a cada primer q divisor de N es consideren els conjunts

$$A = A(s,r,q) = \left\{x\in\mathbb{Z}/q^{\nu+b}\mathbb{Z}\colon \Phi(x)\equiv 0 \pmod{q^{\nu+2b}},\, 2x\equiv s \pmod{q^b}\right\}$$
$$B = B(s,r,q) = \left\{x\in A\colon \Phi(x)\equiv 0 \pmod{q^{\nu+2b+1}}\right\}$$
$$B' = B'(s,r,q) = \{s-z\colon z\in B\}\,,$$

on $\nu = v_q(N)$ i $b = v_q(r)$. Aleshores

$$c'_\varepsilon(s,r,q) = \begin{cases} \sum_{x\in A} \varepsilon(x) & \text{si } (s^2-4\ell)/r^2 \not\equiv 0 \pmod q \\ \sum_{x\in A} \varepsilon(x) + \sum_{y\in B'} \varepsilon(y) & \text{altrament.} \end{cases}$$

Per a una versió més general de la fórmula de les traces cal consultar [**Hij-Pi-She 90**].

Una implementació de la fórmula de les traces es deu a J. Quer; el seu programa, escrit en UBASIC, trobà els primers coeficients de l'única forma de Hecke $G(q) = \sum_{n\geq 1} B_n q^n$ a $S_2(22, \psi^4)$:

$$\begin{aligned} B_3 &= -\zeta^4 - \zeta^2 - 2\zeta - 2 \\ B_5 &= -2\zeta^3 - 2 \\ B_7 &= -2\zeta^4 - 2\zeta^3 - 4\zeta^2 - 2\zeta \\ B_{13} &= -2\zeta^2 - 2\zeta - 2 \\ B_{17} &= -4\zeta^4 - 4\zeta^3 - 5\zeta^2 - 5\zeta - 4 \\ B_{19} &= -2\zeta^4 - 6\zeta^3 - 2\zeta^2 - 5\zeta - 5 \\ &\cdots \end{aligned}$$

on $\zeta = e^{2\pi i/5}$.

Es poden arreglar els coeficients B_n si es té en compte que $\cos \pi/5$ és l'única arrel positiva (doble) del polinomi $16X^5 - 20X^3 + 5X + 1$ i que

$$i \cos\frac{\pi}{10} = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5} - \frac{\sqrt{5}-1}{4}.$$

D'altra banda, si calculem els primers coeficients de la L-sèrie de la corba el·líptica E, trobem:

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43
A_ℓ	–	−2	−3	−2	–	−5	−3	−2	6	3	2	−7	−3	−8.

Finalment, ja que

$$\sqrt{5} \equiv 4 \pmod{11}$$

i

$$\cos\frac{\pi}{5} + i\sin\frac{\pi}{5} = e^{2\pi i/10} \equiv 2^{-1} \equiv 6 \pmod{\mathfrak{P}_{11}},$$

trobem

ℓ	$\psi^2(\ell)$	B_ℓ	$A_\ell\,\psi^2(\ell) - B_\ell \pmod{\mathfrak{P}_{11}}$
2	$\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$	–	–
3	$\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$	$-\frac{\sqrt{5}+1}{2}(\psi^4(3)+1)$	0
5	$\cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5}$	$(\sqrt{5}-1)(\psi^8(5)+1)-2$	0
7	$\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}$	$-(\sqrt{5}-1)\psi^6(7)+2$	0
11	–	–	–
13	$\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$	$-(\sqrt{5}-1)\psi^2(13)$	0
17	$\cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5}$	$-\frac{\sqrt{5}+1}{2}\psi^8(17)+1$	0
19	$\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$	$(2\sqrt{5}-5)(\psi^4(19)+1)$	0
23	1	$-(\sqrt{5}+1)$	0
29	$\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}$	$(\sqrt{5}-5)\psi^6(29)+2\sqrt{5}$	0
31	$\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$	$2\psi^2(31)$	0
37	$\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}$	$6\psi^6(37)-3(\sqrt{5}+1)$	0
41	$\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$	$\frac{7-5\sqrt{5}}{2}(\psi^4(41)+1)$	0
43	1	$\frac{3}{2}(3\sqrt{5}+1)$	0
47	$\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$	$(2\sqrt{5}-6)(\psi^4(47)+1)$	0

Referències

[**As 76**] Asai, T.: On the Fourier coefficients of automorphic forms at various cusps and some applications to Rankin's convolution, *J. Math. Soc. Japan* **28**, n. 1 (1976), 48–61.

[**Ash-St 86**] Ash, A.; Stevens, G.: Modular forms in characteristic ℓ and special values of their L-functions, *Duke Math. Journal* **53**, n. 3 (1986), 849–868.

[**At-Le 70**] Atkin, A.O.L.; Lehner, J.: Hecke operators for $\Gamma_0(N)$, *Math. Ann.* **185** (1970), 134–160.

[**At-Li 78**] Atkin, A.O.L.; Li, W.: Twists of newforms and pseudo eigenvalues of W-operators, *Invent. Math.* **48** (1978), 221–244.

[**Ba-Fr 91**] Bayer, P.; Frey, G.: Galois representations of octahedral type and 2-coverings of elliptic curves, *Math. Z.* (1991). Per aparèixer.

[**Ba-La 91**] Bayer, P.; Lario, J.-C.: On Galois representations defined by torsion points of modular elliptic curves, *Compositio Math.* (1991). Per aparèixer.

[**Ba-Ne 81**] Bayer, P.; Neukirch, J.: On automorphic forms and Hodge theory, *Math. Ann.* **257**, n. 2 (1981), 137–155.

[**Barna 91¬**] : Corbes modulars (algoritmes i taules), pre-publicació, Seminari Teoria de Nombres de Barcelona (UB-UAB-UPC), 1991.

[**Bonn 87¬**] : Tables of modular froms, pre-publicació, Max-Plank Institut of Bonn, 1987.

[**Ca 86**] Carayol, H.: Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert, *Ann. Sci. École Norm. Sup.* **19** (1986), 409–468.

[Ca 89] Carayol, H.: Sur les représentations Galoisiennes modulo ℓ attachées aux formes modulaires, *Duke Math. Journal* **59**, n. 3 (1989), 785–801.

[Cre 91¬] Cremona, J.E.: Computation of modular elliptic curves and the Birch—Swinnerton-Dyer conjecture, pre-publicació, University of Exeter, 1991.

[Cr 90] Crespo, T.: Explicit construction of $2S_n$ Galois extensions, *J. of Algebra* **129**, n. 2 (1990), 312–319.

[De 71] Deligne, P.: Formes modulaires et représentations ℓ-adiques, *Springer Lectures Notes in Math.* **179** (1971), 136–172.

[De-Ra 73] Deligne, P.; Rapoport, M.: Schémas de modules de courbes elliptiques, *Springer Lectures Notes in Math.* **349** (1973), 143–316.

[De-Se 74] Deligne, P.; Serre, J.-P.: Formes modulaires de poids 1, *Ann. Sci. École Norm. Sup.* **7** (1974), 507–530. (= Serre, J.-P. Œ. 101).

[Ed 91¬] Edixhoven, B.: The weight in Serre's conjectures on modular forms, pre-publicació, University of California, Berkeley, 1991.

[Ed-Gr-To 90] Edixhoven, B.; de Groot, A.; Top, J.: Elliptic curves over the rationals with bad reduction at only one prime, *Math. of Computation* **54**, n. 189 (1990), 413–419.

[Ei 54] Eichler, M.: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, *Arch. Math.* **5** (1954), 355–366.

[Fo 77] Fontaine, J.-M.: Groupes p-divisibles sur les corps locaux, *Astérisque* **47-48** (1977).

[Fre-Ki 88] Freitag, E.; Kiehl, R.: *Etale Cohomology and the Weil Conjecture*, A Series of Modern Surveys in Mathematics, Springer-Verlag, 1988.

[Fr 86] Frey, G.: Links between stable elliptic curves and certain diophantine equations, *Ann. Univ. Saraviensis Math. Ser.* **1** (1986), 1–40.

[Fri 22] Fricke, R.: *Die elliptischen Funktionen und ihre Anwendungen II*, Leipzig, 1922.

[Fri 28] Fricke, R.: *Lehrbuch der Algebra, III*, Vieweg & Sons, 1928.

[Gr 90] Gross, B.H.: A tameness criterion for Galois representations associated to modular forms (mod p), *Duke Math. Journal* **61**, n. 2 (1990), 445–517.

[He 27] Hecke, E.: Theorie der Eisensteinschen Reihen Höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik, *Abh. Math. Sem. Hamburg* **15** (1927), 199–224. (= Werke 24).

[He 37] Hecke, E.: Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung I, *Math. Ann.* **114** (1937), 1–28. (= Werke 35).

[Hi 86] Hida, H.: Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, *Invent. Math.* **85** (1986), 545–613.

[Hij-Pi-She 90] Hijikata, H.; Pizer, A.; Shemanske, T.: Twist of newforms, *J. of Number Theory* **35** (1990), 287–324.

[Jo 82] Jochnowitz, N.: The local components of the Hecke algebra mod ℓ, *Transactions of the AMS* **270** (1982), 253–267.

[Jor-Liv 89] Jordan, B.; Livné, R.: Conjecture "epsilon" for weight $k > 2$, *Bull. (New Series) of the AMS* **21**, n. 1 (1989), 51–56.

[Ka 73] Katz, N.M.: p-adic properties of modular schemes and modular forms, *Springer Lectures Notes in Math.* **350** (1973), 69–190.

[Ka 76] Katz, N.M.: A result on modular forms in characteristic p, *Springer Lectures Notes in Math.* **601** (1976), 53–61.

[Ka-Ma 85] Katz, N.M.; Mazur, B.: *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, Princeton University Press, 1985.

[Ko 76] Koike, M.: Congruences between cusp forms and linear representations of the Galois group, *Nagoya Math. J.* **64** (1976), 63–85.

[Kr 90¬] Kraus, A.: *Sur l'arithmétique des courbes elliptiques.* Tesi, Université Paris VI, 1990.

[Lan 73] Langlands, R.P.: Modular forms and ℓ-adic representations, *Springer Lectures Notes in Math.* **349** (1973), 361–500.

[La-Qu 87¬] Lario, J.C.; Quer, J.: De la solución de un problema de inmersión a la costrucción de formas modulares de peso 1, pre-publicació. Actas de las XIII Jornadas Hispano-Lusas, Valladolid, 1987.

[Li 75] Li, W.: Newforms and functional equations, *Math. Ann.* **212** (1975), 285–315.

[Liv 89] Livné, R.: On the Conductors of (modℓ) Galois Represetnations Coming from Modular Forms, *J. of Number Theory* **31** (1989), 133–141.

[Ma 78] Mazur, B.: Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.

[Ma 85¬] Mazur, B.:. Carta a J.-F. Mestre, 25 d' agost de 1985.

[Ma 90] Mazur, B.: Two-dimensional p-adic Galois representations unramified away from p, *Compositio Math.* **74** (1990), 115–133.

[Ma-Ti 90] Mazur, B.; Tilouine, J.: Représentations galoisiennes, différentielles de Kähler, et "conjectures principales", *Publ. Math. IHES* **71** (1990), 65–103.

[Ma-Wi 84] Mazur, B; Wiles, A.: Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76** (1984), 179–330.

[Ma-Wi 86] Mazur, B; Wiles, A.: On p-adic analytic families of Galois representations, *Compositio Math.* **59** (1986), 231–264.

[Mi 71] Miyake, T.: On automorphic forms of GL_2 and Hecke operators, *Ann. of Math.* **94** (1971), 174–189.

[Mo 17] Mordell, L.J.: On Mr. Ramanujan's empirical expressions of modular functions, *Proc. Cambridge Phil. Soc.* **19** (1917), 117–124.

[Og 67] Ogg, A.P.: Elliptic curves and wild ramification, *Amer. J. Math.* **89** (1967), 1–21.

[Og 69] Ogg, A.P.: On the eigenvalues of Hecke operators, *Math. Ann.* **179** (1969), 101–108.

[Oh 82] Ohta, M.: On ℓ-adic representations attached to automorphic forms, *Japan. J. Math.* **8**, n. 1 (1982), 1–47.

[Ra 16] Ramanujan, S.: On certain arithmetical functions, *Trans. Cambridge Phil. Soc.* **22** (1916), 159–184.

[Ray 70] Raynaud, M.: Variétés abéliennes et géométrie rigide, *Actes, Congrès Intern. Math.* **1** (1970), 473–477.

[Ri 77] Ribet, K.A.: Galois representations attached to eigenforms with Nebentypus, *Springer Lectures Notes in Math.* **601** (1977), 17–52.

[Ri 80] Ribet, K.A.: Twists of modular forms and endomorphisms of abelian varieties, *Math. Ann.* **253** (1980), 43–62.

[Ri 90] Ribet, K.A.: On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431–476.

[Se 67] Serre, J.-P.: Une interprétation des congruences relatives à la fonction τ de Ramanujan, *Séminaire Delange-Pisot-Poitou* **14** (1967/68). (= Œ. 80).

[Se 72] Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331. (= Œ. 94).

[Se 73] Serre, J.-P.: Formes modulaires et fonctions zêta p-adiques, *Springer Lectures Notes in Math.* **350** (1973), 191–268. (= Œ. 97).

[Se 75] Serre, J.-P.: Valeurs propres des opérateurs de Hecke modulo ℓ, Journées Arith. de Bordeaux, *Astérisque* **24-25** (1975), 109–117. (= Œ. 104).

[Se 87] Serre, J.-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. Journal* **54**, n. 1 (1987), 179–230.

[Se 88] Serre, J.-P.: Resumé des Cours de 1987-1988, *Annuaire du Collège de France* (1988).

[Se-Ta 68] Serre, J.-P.; Tate, J.: Good reduction of abelian varieties, *Ann. of Math.* **88**, n. 2 (1968), 492–517. (= Serre, J.-P. Œ. 79).

[Sh 66] Shimura, G.: A reciprocity law in non-solvable extensions, *J. Reine Angew. Math.* **221** (1966), 209–220.

[Sh 71] Shimura, G.: *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.

[**Sh-2 71**] Shimura, G.: On the zeta-function of an abelian variety with complex multiplication, *Ann. of Math.* **94** (1971), 504–533.

[**Sh 73**] Shimura, G.: On the factors of the jacobian variety of a modular function field, *J. Math. Soc. Japan* **25**, n. 3 (1973), 523–544.

[**Sh-2 73**] Shimura, G.: On modular forms of half-integral weight, *Ann. of Math.* **97** (1973), 440–481.

[**Sw 73**] Swinerton-Dyer, H.P.F.: On ℓ-adic representations and congruences for coefficients of modular forms, *Springer Lectures Notes in Math.* **350** (1973), 1–55.

[**Tan 55¬**] Taniyama, Y.: Some unsolved problems of mathematics, No. 12. Tokio-Nikko conference on Number Theory, 1955.

[**Ta 67**] Tate, J.: p-divisible groups, en el llibre *Proceedings of a Conference on Local Fields at Driebergen*, Springer-Verlag, 1967, pp. 158–184.

[**Ta 75**] Tate, J.: Algorithm for determining the type of a singular fibre in an elliptic pencil, *Springer Lectures Notes in Math.* **476** (1975), 33–52.

[**Ti 87**] Tilouine, J.: Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke, *Bull. Soc. Math. France* **115** (1987), 329–360.

[**Ti 88**] Tilouine, J.: Théorie d'Iwasawa classique et de l'algèbra de Hecke ordinaire, *Compositio Math.* **65** (1988), 265–320.

[**Wa 80**] Washington, L.C.: *Introduction to cyclotomic fields*, GTM, Springer, 1980.

[**Wi 86**] Wiles, A.: On p-adic representations for totally real fiels, *Ann. of Math.* **123** (1986), 407–456.