NOTES DEL SEMINARI

MONOGRÀFIC SOBRE TREBALLS DE KENNETH RIBET

Barcelona 2010

19

Notes del Seminari de Teoria de Nombres
(UB-UAB-UPC)

MONOGRÀFIC SOBRE TREBALLS DE KENNETH RIBET

Edició a cura de

M. Alsina N. Vila

Amb contribucions de

X. Guitart L. Terracini B. Plans N. Freitas

M. Alsina
Dept. Matemàtica Aplicada III
E P Superior d'Enginyeria de Manresa
Universitat Politècnica de Catalunya
Agda Bases de Manresa, 61-73
08242 Manresa
montserrat.alsina@upc.edu

N. Vila
Facultat de Matemàtiques,
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007 Barcelona
nuriavila@ub.edu

Classificació AMS
Primària: 11G18, 11F33
Secundària: 11D41, 11G05, 11G30, 14G35, 14H25, 14H52

Barcelona, 2010
Amb suport parcial de MTM2006-04895 i MTM2009-07024.
ISBN: 978-84-934244-9-7

Prefaci

Aquest volum *Monogràfic sobre treballs de Kenneth Ribet* conté notes redactades a partir de les exposicions presentades en l'edició 23a del Seminari de Teoria de Nombres (UB-UAB-UPC), que tinguè lloc del 26 al 30 de gener de 2010, a la Facultat de Matemàtiques de la Universitat de Barcelona. El programa fou elaborat per M. Alsina i N. Vila, i les sessions foren dutes a terme per persones del seminari. La seva gentilesa en redactar el contingut de les exposicions ha fet possible l'edició d'aquest volum.

Ribet és un investigador ben conegut en l'àmbit de la Teoria de Nombres, en relació a les formes modulars, varietat abelianes i representacions de Galois. Els seus resultats van ser cabdals en la demostració del teorema de Fermat. Al final del volum trobareu les dades bibliogràfiques dels seus treballs.

En el seminari es van tractar només alguns articles, de manera que no tots els resultats fonamentals de la producció d'en Ribet hi són reflectits. En la selecció dels temes es va optar per donar protagonisme als expositors de manera que escollissin aquell article més proper a la seva producció científica o aquell que els semblés més interessant per ser exposat.

L'objectiu és que amb aquests escrits feu un tast de l'obra d'en Ribet, i alguns dels seus co-autors, com ara M. Baker i S. Takahashi.

M. Alsina i N. Vila

Barcelona, març de 2010

Conferenciants

Xavier Guitart
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya
Jordi Girona 1-3, 08034 Barcelona
xevi.guitart@gmail.com

Lea Terracini
Dipartimento di Matematica
Università de Torino
Via Carlo Alberto 10, 10123 Torino
lea.terracini@unito.it

Bernat Plans
Departament de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Jordi Girona 1-3, 08034 Barcelona
bernat.plans@upc.edu

Luis Dieulofait i Nuno Freitas
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran via de les Corts Catalanes 585, 08007 Barcelona
ldieulefait@ub.edu, **nunobfreitas@gmail.com**

Índex

Capítol 1

Varietats abelianes sobre Q i formes modulars

Xavier Guitart

Aquestes notes són la versió redactada d'una xerrada d'una hora dedicada a explicar l'article [Ri92]. L'objectiu de la presentació era enunciar els dos teoremes més rellevants de l'article i donar una noció de les idees que utilitza Ribet per a demostrar aquests resultats principals, fent a la vegada un sumari de la teoria necessària per tal de fer l'exposició el més autocontinguda possible. Aquest és, també, l'objectiu d'aquest text; òbviament, la millor referència per a una demostració completa, rigurosa i elegant dels resultats que descriurem (a part de molts altres) és l'article original de Ribet.

1.1 Introducció

La conjectura de Shimura-Taniyama, també coneguda com a Teorema de Modularitat des de la seva demostració completa l'any 2001, admet diversos enunciats equivalents. Per exemple, considerem $X_1(N)/\mathbf{Q}$ la corba modular associada a la classificació de parells (E, P), on E és una corba el·líptica i P és un punt de E d'ordre N. Denotem per

Amb el suport parcial de MTM2009-13060-C02-01.

$J_1(N)$ la jacobiana de $X_1(N)$. Aleshores podem enunciar Shimura-Taniyama de la manera següent:

1.1.1 Teorema *Sigui C una corba el·líptica definida sobre $\mathbf{Q}$. Aleshores existeix un morfisme exhaustiu $J_1(N) \to C$ definit sobre $\mathbf{Q}$ per a algun $N \geqslant 1$. És a dir, C és un quocient de $J_1(N)$.*

Una possible interpretació d'aquest enunciat és com a una caracterització de les varietats abelianes de dimensió 1 que són quocient d'alguna $J_1(N)$: són totes les corbes el·líptiques definides sobre $\mathbf{Q}$. En vista d'aquesta interpretació, dues preguntes apareixen de manera molt natural portant a possibles generalitzacions de Shimura-Taniyama en dues direccions diferents. La primera elimina la restricció de considerar quocients de dimensió 1; és a dir, ens podem preguntar per quines són les varietats abelianes sobre $\mathbf{Q}$ que apareixen com a quocient de les varietats $J_1(N)$. La segona, considera quocients no necessàriament sobre $\mathbf{Q}$; més concretament, ens podem preguntar sobre quines són les corbes el·líptiques sobre $\overline{\mathbf{Q}}$ que apareixen com a quocients de les diferents $J_1(N)_{\overline{\mathbf{Q}}}$.

A l'article [Ri92] (del qual se'n pot trobar una nova reimpressió a [Ri04]), Ribet utilitza la conjectura de Serre [Se87, 3.2.4?] sobre representacions de Galois per a donar una resposta a les dues qüestions anteriors. La resposta a la primera pregunta són unes varietats que Ribet anomenà *de tipus* GL_2, i la resposta a la segona són les corbes el·líptiques que anomenà (manllevant un terme utilitzat prèviament per Gross) $\mathbf{Q}$*-corbes*. Així doncs, Ribet demostrà que la conjectura de Serre implica els resultats següents, que són als que dediquem les seccions 1.2 i 1.3 respectivament:

1. Una varietat simple $A/\mathbf{Q}$ és quocient d'alguna $J_1(N)$ si i només si és de tipus GL_2; és a dir, si i només si la seva àlgebra d'endomorfismes $\mathbf{Q}$-definits $\mathrm{End}_{\mathbf{Q}}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ és un cos de nombres de grau sobre $\mathbf{Q}$ igual a la dimensió de A.

2. Una corba el·líptica $C/\overline{\mathbf{Q}}$ és quocient d'alguna $J_1(N)_{\overline{\mathbf{Q}}}$ si i només si és una $\mathbf{Q}$-corba; és a dir, si i només si per a tot $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ la corba ${}^{\sigma}C$ és isògena a C.

Observem que en el moment en què Ribet va escriure l'article la conjectura de Serre no estava demostrada i que, per tant, aquests resultats eren conjecturals. Actualment la conjectura de Serre ja ha estat provada, amb la qual cosa 1 i 2 ja són teoremes. Conseqüentment, hem optat per enunciar-los com a tals, i no en la versió conjectural amb què apareixen a [Ri92]. Finalment, remarquem també que l'article de Ribet tingué un cert caràcter fundacional, en el sentit que arran dels seus resultats es va despertar un gran interès per a les varietats de tipus GL_2 i les $\mathbf{Q}$-corbes. Per exemple, al volum que conté [Ri04] s'hi pot trobar un recull d'articles dedicats a l'estudi d'aquestes varietats, amb especial èmfasi en la seva relació amb les formes modulars.

1.2 Varietats de tipus GL_2

Comencem definint les varietats que, com ja hem comentat, acabaran apareixent en la caracterització dels factors simples de les jacobianes de corbes modulars.

1.2.1 Definició *Una varietat abeliana $A/\mathbf{Q}$ es diu que és de tipus GL_2 si la seva àlgebra d'endomorfismes $\mathbf{Q}$-definits, $\mathbf{Q}\otimes_{\mathbf{Z}}\mathrm{End}_{\mathbf{Q}}(A)$, és isomorfa a un cos de nombres de grau sobre $\mathbf{Q}$ igual a la dimensió de A.*

Les varietats abelianes de tipus GL_2 de dimensió 1 són les corbes el·líptiques sobre $\mathbf{Q}$. En efecte, si $C/\mathbf{Q}$ és un corba el·líptica, la seva àlgebra d'endomorfismes $\mathbf{Q}\otimes\mathrm{End}_{\overline{\mathbf{Q}}}(C)$ és isomorfa a $\mathbf{Q}$ o a un cos quadràtic imaginari K. Observem però, que fins i tot en aquest segon cas es compleix que l'àlgebra d'endomorfismes $\mathbf{Q}$-definits $\mathbf{Q}\otimes\mathrm{End}_{\mathbf{Q}}(C)$ és isomorfa a $\mathbf{Q}$: altrament K actuaria en l'espai de vectors tangents $\mathrm{Lie}(C/\mathbf{Q})$, que té dimensió 1 sobre $\mathbf{Q}$.

Una altra font d'exemples de varietats de tipus GL_2 són les associades a formes modulars de pes 2. Sigui $f=\sum a_nq^n$ una forma modular cuspidal de pes 2 per a un subgrup de $\mathrm{SL}_2(\mathbf{Z})$ de la forma $\Gamma_1(N)$, i que és forma pròpia normalitzada pels operadors de Hecke. Aleshores una construcció de Shimura associa a f una varietat abeliana A_f de tipus GL_2. Aquesta A_f és, per construcció, un

quocient de $J_1(N)$, i $\mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A_f)$ és isomorf a $\mathbf{Q}(\dots, a_n, \dots)$ que té grau igual a la dimensió de A_f. Per tant, $J_1(N)$ té quocients que són varietats de tipus GL_2; de fet, Ribet provà a [Ri80] el següent resultat.

1.2.2 Teorema *La varietat $J_1(N)$ és isògena sobre $\mathbf{Q}$ a un producte de varietats de la forma A_f.*

Així doncs, tot quocient simple de $J_1(N)$ sobre $\mathbf{Q}$ és isogen a una varietat de tipus GL_2. Un dels teoremes principals de [Ri92] és el recíproc d'aquest fet.

1.2.3 Teorema *Sigui $A/\mathbf{Q}$ una varietat de tipus GL_2. Aleshores A és isògena sobre $\mathbf{Q}$ a un factor $\mathbf{Q}$-simple de $J_1(N)$ per a algun $N \geqslant 1$.*

En la resta de secció indicarem, sense entrar en els detalls, quins són els passos que condueixen a la prova d'aquest enunciat. Els dos ingredients principals que hi intervenen són, d'una banda la conjectura de Serre, i de l'altra el teorema de la isogènia de Faltings. Abans d'enunciar la conjectura de Serre, fem un breu repàs de les representacions associades a les varietats abelianes i a les formes modulars.

Representacions associades a varietats de tipus GL_2

Sigui A una varietat abeliana de tipus GL_2 i sigui $E = \mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A)$. Fixem un nombre primer ℓ i sigui $T_\ell(A) = \varprojlim A[\ell^n]$ el mòdul de Tate ℓ-àdic de A; considerem també $V_\ell(A) = T_\ell(A) \otimes_{\mathbf{Z}} \mathbf{Q}$, que és un $\mathbf{Q}_\ell$-mòdul lliure de rang $2 \dim A = 2[E : \mathbf{Q}]$. A més, $V_\ell(A)$ és un $E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$-mòdul lliure de rang 2, i com que E actua sobre A com endomorfismes definits sobre $\mathbf{Q}$, el grup de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ actua en $V_\ell(A)$ de manera $E \otimes \mathbf{Q}_\ell$-lineal. Això dóna lloc a la representació ℓ-àdica

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}_{E \otimes \mathbf{Q}_\ell}(V_\ell(A)) \simeq \mathrm{GL}_2(E \otimes \mathbf{Q}_\ell).$$

En general la representació ℓ-àdica associada a una varietat abeliana pren valors en $\mathrm{GL}_{2d}(\mathbf{Q}_\ell)$, on d és la dimensió de la varietat. El fet que les varietats de tipus GL_2 tinguin com a àlgebra d'endomorfismes $\mathbf{Q}$-definits un cos de nombres de grau igual a la dimensió de la varietat

fa que, tal com acabem de veure, aquesta representació es pugui pensar prenent valors a $\mathrm{GL}_2(E \otimes \mathbf{Q}_\ell)$; aquesta és l'explicació de perquè aquestes varietats s'anomenen de tipus GL_2.

L'anell $E \otimes \mathbf{Q}_\ell$ no és un cos en general, sinó un producte de cossos. Tenim que $E \otimes \mathbf{Q}_\ell \simeq \prod_{\lambda|\ell} E_\lambda$, on el producte recorre tots els primers λ de E que divideixen ℓ, i E_λ és el completat de E respecte de la topologia induïda per λ. Així doncs, per a cada primer λ de E dividint ℓ tenim una representació λ-àdica

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(E_\lambda).$$

Una propietat fonamental d'aquesta representació λ-àdica és que si p és un primer diferent de ℓ i en el qual A té bona reducció, aleshores ρ_λ és no ramificada en p. A més, si Frob_p denota un element de Frobenius per p en $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, resulta que el polinomi característic de $\rho_\lambda(\mathrm{Frob}_p)$ té coeficients a E i no depèn de λ.

Per a poder aplicar la conjectura de Serre cal considerar la reducció d'aquestes representacions. Sigui $\mathcal{O}$ l'anell d'enters de E. Sempre existeix una varietat $\mathbf{Q}$-isògena a A que té anell d'endomorfismes $\mathbf{Q}$-definits isomorf a $\mathcal{O}$. Com que l'enunciat del teorema 1.2.3 no canvia si reemplacem A per una varietat $\mathbf{Q}$-isògena, podem suposar (i suposem) que $\mathrm{End}_{\mathbf{Q}}(A) \simeq \mathcal{O}$. Així doncs, amb un argument anàleg a l'anterior podem prensar que les representacions λ-àdiques tenen coeficients a $\mathcal{O}_\lambda$:

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}_{\mathcal{O}\otimes\mathbf{Z}_\ell}(T_\ell(A)) \simeq \mathrm{GL}_2(\mathcal{O} \otimes \mathbf{Z}_\ell) \simeq \prod_{\lambda \mid \ell} \mathrm{GL}_2(\mathcal{O}_\lambda),$$

i per tant podem reduir mòdul λ cada representació λ-àdica, obtenint una representació amb coeficients al cos finit $\mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda \subseteq \overline{\mathbf{F}}_\ell$:

$$\overline{\rho}_\lambda : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda) \subseteq \mathrm{GL}_2(\overline{\mathbf{F}}_\ell).$$

Representacions associades a formes modulars

Hem vist que a cada varietat abeliana de tipus GL_2 li podem associar representacions que prenen valors en $\mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$; tot seguit veiem que també podem associar representacions d'aquest estil a formes modulars. El resultat principal és el següent.

1.2.4 Teorema *Sigui* $f = \sum a_n q^n \in S_k(\Gamma_1(N))$ *una forma pròpia pels operadors de Hecke, i sigui* $E_f = \mathbf{Q}(\dots, a_n, \dots)$ *i* $\mathcal{O}_f$ *l'anell d'enters d'*E_f*. Existeix una representació*

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathcal{O}_f \otimes \mathbf{Z}_\ell) \simeq \prod_{\tilde{\lambda} \mid \ell} \mathrm{GL}_2(\mathcal{O}_{f,\tilde{\lambda}})$$

associada a f*, és a dir, tal que per a tot* $p \nmid \ell N$ *es compleix que*

- ρ_ℓ *és no ramificada en* p*,*
- $\mathrm{tr}(\rho_{f,\ell}(\mathrm{Frob}_p)) = a_p$*,*
- $\det \rho_{f,\ell}(\mathrm{Frob}_p) = \varepsilon(p) \cdot p^{k-1}$*, on* ε *és el caràcter de* f*.*

Per a cada $\tilde{\lambda} \mid \ell$ *tenim la reducció mòdul* $\tilde{\lambda}$*:*

$$\overline{\rho}_{f,\tilde{\lambda}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathcal{O}_{f,\tilde{\lambda}}/\tilde{\lambda}\mathcal{O}_{f,\tilde{\lambda}}) \subseteq \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$$

que és contínua, irreductible (quasi per a tot λ*) i senar.*

En el cas $k = 2$, la representació no és més que l'associada a la varietat A_f pel procediment que hem descrit a 1.2. Per a pes $k \geqslant 2$ l'existència de $\rho_{f,\ell}$ fou provada per Deligne a [De71], i per a pes $k = 1$ ho fou per Deligne i Serre a [DS74].

La conjectura de Serre és en certa manera un recíproc del teorema anterior.

1.2.5 Teorema (Conjectura de Serre) *Sigui* $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ *una representació contínua, irreductible i senar. Aleshores existeix una forma modular* $f \in S_k(\Gamma_1(N))$ *i un primer* $\tilde{\lambda} \subseteq \mathcal{O}_f$ *tal que*

$$\rho \simeq \overline{\rho}_{f,\tilde{\lambda}}.$$

A més, la conjectura dóna una fórmula per a calcular a partir de la representació un pes $k = k(\rho)$ *i un nivell* $N = N(\rho)$ *per a una forma* f *que resol el problema.*

Demostració del teorema 1.2.3

Sigui $A/\mathbf{Q}$ una varietat abeliana de tipus GL_2. Per a poder aplicar la conjectura de Serre a les representacions $\overline{\rho}_\lambda$, Ribet prova que $\overline{\rho}_\lambda$ és senar i absolutament irreductible quasi per a tot λ. Per a aquests λ la conjectura de Serre implica doncs que $\overline{\rho}_\lambda$ és modular. Així doncs, existeixen enters k_λ i N_λ, una forma modular $f_\lambda \in S_{k_\lambda}(N_\lambda)$ i un primer $\tilde{\lambda}$ de $\mathcal{O}_{f_\lambda}$ tal que

$$\overline{\rho}_\lambda \simeq \overline{\rho}_{f_\lambda,\tilde{\lambda}}.$$

El que es vol demostrar és que existeix una forma f de pes 2 tal que A és $\mathbf{Q}$-isògena a A_f. El següent pas que fa Ribet és trobar una forma f candidata a complir que A_f sigui isògena a A. Per a fer-ho, considera Λ el conjunt *infinit* de primers λ tals que $\overline{\rho}_\lambda$ és absolutament irreductible i tals que A té bona reducció en el primer racional que hi ha per sota de λ. Per a tot primer $\lambda \in \Lambda$, es té que $k_\lambda = 2$; això ho dedueix de certes propietats del determinant de $\overline{\rho}_\lambda$ que ha demostrat prèviament, i que li permeten aplicar un teorema de Serre que directament implica $k_\lambda = 2$. En segon lloc, els nivells N_λ estan acotats quan λ recorre Λ. Això és perquè en la definició de N_λ que apareix en la conjectura de Serre s'observa que N_λ divideix el conductor de ρ_λ, i aquest és un divisor del conductor de ρ_ℓ; però el conductor de ρ_ℓ no depèn de ℓ (i és per definició el conductor de A). Com que k_λ sempre és igual a 2 i hi ha un nombre finit de possibles N_λ, es dedueix que hi ha un nombre finit de formes modulars de pes 2 que donen lloc a infinites representacions ρ_λ. Per tant, existeix almenys una forma f de pes 2 que dóna lloc a infinites de les ρ_λ. Aquesta és la forma f candidata, i ara només falta provar que A_f és isògena sobre $\mathbf{Q}$ a A. És en aquest punt on apareix el segon ingredient important de la demostració, el teorema de la isogènia de Faltings.

Sigui $B/\mathbf{Q}$ una varietat abeliana i fixem ℓ un primer de bona reducció; si $p \neq \ell$ és un primer de bona reducció aleshores denotem per $L_p(B,s) = \det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(B))^{-1}$ el factor local en p de la seva L-sèrie.

1.2.6 Teorema (Faltings) *Dues varietats abelianes $B/\mathbf{Q}$ i $C/\mathbf{Q}$ són isògenes sobre $\mathbf{Q}$ si i només si $L_p(B,s) = L_p(C,s)$ quasi per a tot primer p.*

Continuant amb la demostració, veiem ara que A i A_f són $\mathbf{Q}$-isògenes. Sigui $\lambda \in \Lambda$ i p un primer de bona reducció de A. Sabem que existeix un primer $\tilde{\lambda}$ de $\mathcal{O}_\lambda$ tal que $\overline{\rho}_\lambda \simeq \overline{\rho}_{A_f,\tilde{\lambda}}$. En particular, el polinomi característic de $\overline{\rho}_\lambda(\mathrm{Frob}_p)$, que és

$$\det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A)) \bmod \lambda, \tag{1.1}$$

coincideix amb el polinomi característic de $\overline{\rho}_{A_f,\tilde{\lambda}}(\mathrm{Frob}_p)$, que és

$$\det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A_f)) \bmod \tilde{\lambda}. \tag{1.2}$$

Podem pensar que els polinomis $\det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A))$ i $\det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A_f))$ tenen coeficients a la composició $E \cdot E_f$. La igualtat entre (1.1) i (1.2) implica que existeix un primer λ' de $E \cdot E_f$ que divideix λ i tal que

$$\det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A)) \equiv \det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A_f)) \mod \lambda'.$$

Com que aquest raonament és vàlid per a tot $\lambda \in \Lambda$, veiem que $\det(1-p^{-s}\cdot\mathrm{Frob_p} \mid T_\ell(A))$ i $\det(1-p^{-s}\cdot\mathrm{Frob_p} \mid T_\ell(A_f))$ són congruents mòdul *infinits* primers. Però dos polinomis amb coeficients en un cos de nombres que són congruents mòdul infinits primers necessàriament són iguals, i per tant

$$\det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A)) = \det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A_f)).$$

En definitiva, hem vist que $L_p(A, s) = L_p(A_f, s)$ quasi per a tot p, i pel teorema de Faltings això implica que A i A_f efectivament són $\mathbf{Q}$-isògenes.

1.3 Q-corbes

En aquesta secció descriurem la caracterització dels quocients de dimensió 1 del conjunt de varietats de la forma $J_1(N)_{\overline{\mathbf{Q}}}$.

1.3.1 Definició *Una corba el·líptica $C/\overline{\mathbf{Q}}$ és una* $\mathbf{Q}$*-corba si és isògena a cadascuna de les seves conjugades de Galois ${}^\sigma C$ amb $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.*

El segon teorema principal de l'article de Ribet és el següent.

1.3.2 Teorema *Una corba el·líptica $C/\overline{\mathbf{Q}}$ és un quocient de $J_1(N)_{\overline{\mathbf{Q}}}$ per a algun $N \geqslant 1$ si i només si C és una* **Q***-corba.*

Fixem-nos que gràcies als teoremes 1.2.2 i 1.2.3 n'hi ha prou amb caracteritzar els quocients de dimensió 1 sobre $\overline{\mathbf{Q}}$ de les varietats de tipus GL_2. I encara més, gràcies al resultat següent de Shimura n'hi ha prou amb considerar varietats de tipus GL_2 sense CM (multiplicació complexa).

1.3.3 Teorema (Shimura) *Sigui $A/\mathbf{Q}$ una varietat abeliana de tipus GL_2 i suposem que $A_{\overline{\mathbf{Q}}}$ té alguna subvarietat amb CM. Aleshores $A_{\overline{\mathbf{Q}}}$ és isògena a una potència d'una corba el·líptica amb CM.*

És un fet conegut que les corbes el·líptiques amb CM són **Q**-corbes, i a més Shimura també havia demostrat que tota corba el·líptica amb CM és quocient d'alguna $J_1(N)_{\overline{\mathbf{Q}}}$. Així doncs, el resultat que de fet va provar Ribet a [Ri92] i que implica el teorema 1.3.2 és el següent.

1.3.4 Teorema *Una corba el·líptica $C/\overline{\mathbf{Q}}$ sense CM és un quocient d'una varietat de tipus GL_2 si i només si C és una* **Q***-corba.*

En el que queda de secció indicarem els passos principals que duen a la demostració de 1.3.4. Notem que 1.3.2 era conjectural en el moment en què Ribet publicà l'article (ja que 1.2.3 depenia de la conjectura de Serre), però en canvi 1.3.4 no era conjectural, sinó un teorema pròpiament dit.

Prenem $A/\mathbf{Q}$ una varietat abeliana de tipus GL_2 i sigui E la seva àlgebra d'endomorfismes **Q**-definits. Una de les implicacions de 1.3.4 es dedueix de la següent

1.3.5 Proposició *Si $A_{\overline{\mathbf{Q}}}$ no té cap subvarietat amb CM, aleshores $A_{\overline{\mathbf{Q}}}$ és isògena a la potència d'una varietat $\overline{\mathbf{Q}}$-simple.*

Prova: En principi sabem que $A_{\overline{\mathbf{Q}}}$ té una descomposició en producte de varietats absolutament simples de la forma $A_{\overline{\mathbf{Q}}} \sim B_1^{n_1} \times \cdots \times B_r^{n_r}$. Com que E és un cos que actua en $A_{\overline{\mathbf{Q}}}$, de fet actua en cada

factor $B_i^{n_i}$, i per tant actua en $H_1(B_i^{n_i}(\mathbf{C}), \mathbf{Q})$ que és un $\mathbf{Q}$-espai vectorial de dimensió $2\dim B_i^{n_i}$. Així doncs $[E : \mathbf{Q}]$ ha de dividir $2\dim B_i^{n_i}$. Però d'altra banda $[E : \mathbf{Q}] = \dim(A) \geqslant \dim B_i^{n_i}$, i això només deixa lloc a dues opcions: o bé $[E : \mathbf{Q}] = \dim B_i^{n_i}$ o bé $[E : \mathbf{Q}] = 2\dim B_i^{n_i}$. Aquesta darrera no és possible, ja que aleshores $A_{\overline{\mathbf{Q}}}$ tindria una subvarietat amb CM. Per tant ha de ser $[E : \mathbf{Q}] = \dim B_i^{n_i}$, la qual cosa implica que $\dim(A) = \dim(B_i^{n_i})$ i per tant $A_{\overline{\mathbf{Q}}} \sim B_i^{n_i}$. □

Si una corba el·líptica $C/\overline{\mathbf{Q}}$ és un quocient de $A_{\overline{\mathbf{Q}}}$, necessàriament la descomposició de $A_{\overline{\mathbf{Q}}}$ és doncs de la forma $A_{\overline{\mathbf{Q}}} \sim C^n$. Per $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ tenim que ${}^{\sigma}C^n \sim {}^{\sigma}A_{\overline{\mathbf{Q}}} = A_{\overline{\mathbf{Q}}} \sim C^n$. Ara, per la unicitat de la descomposició de varietats abelianes com a producte de varietats simples forçosament ${}^{\sigma}C \sim C$, amb la qual cosa veiem que C és una $\mathbf{Q}$-corba.

Veiem ara com es prova l'altra implicació de 1.3.4. Sigui doncs $C/\overline{\mathbf{Q}}$ una $\mathbf{Q}$-corba sense multiplicació complexa. Hem de veure que existeix una varietat abeliana $A/\mathbf{Q}$ de tipus GL_2 tal que $A_{\overline{\mathbf{Q}}} \sim C^n$. En particular, si això és cert, una certa potència de C serà de fet isògena a una varietat definida sobre $\mathbf{Q}$. El problema d'identificar quan una varietat sobre $\overline{\mathbf{Q}}$ és isògena a una varietat definida sobre $\mathbf{Q}$, és anàleg al problema de descens del cos de definició de varietats algebraiques. La solució d'aquest problema per al cas de varietats algebraiques quasiprojectives és un teorema clàssic de Weil.

1.3.6 Teorema (Teorema del descens de Weil) *Sigui L/K una extensió de de Galois i B/L una varietat algebraica quasiprojectiva. Existeix una varietat A/K isomorfa a B sobre L si i només si per a tot $\sigma \in \mathrm{Gal}(L/K)$ existeix un isomorfisme $\phi_\sigma : {}^{\sigma}B \to B$ i es satisfà que*

$$\phi_\sigma \circ {}^{\sigma}\phi_\tau \circ \phi_{\sigma\tau}^{-1} = 1.$$

Ribet prova, com un dels passos en la seva demostració de 1.3.4, l'anàleg d'aquest teorema en la categoria de varietats abelianes llevat d'isogènia, i de fet l'enuncia a [Ri92, teorema 8.2] de la forma següent.

1.3.7 Teorema *Sigui B/L una varietat abeliana. Existeix una varietat A/K isògena a B sobre L si i només si per a tot $\sigma \in \mathrm{Gal}(L/K)$*

existeix un isomorfisme de la categoria de varietats abelianes llevat d'isogènia $\nu_\sigma : {}^\sigma B \to B$ *i es satisfà que*

$$\nu_\sigma \circ {}^\sigma\nu_\tau \circ \nu_{\sigma\tau}^{-1} = 1.$$

Per a cada $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, sigui $\mu_\sigma : {}^\sigma C \to C$ una isogènia, que sabem que existeix pel fet que C és $\mathbf{Q}$-corba. Per a cada parella d'elements $\sigma, \tau \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ la composició $\mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}$ és un element no nul de $\mathbf{Q}\otimes\mathrm{End}_{\overline{\mathbf{Q}}}(C) \simeq \mathbf{Q}$ (aquest isomorfisme és degut a que estem suposant que C no té CM). Una senzilla comprovació ens mostra que l'aplicació

$$\begin{array}{rccc} c: & \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \times \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) & \longrightarrow & \mathbf{Q}^\times \\ & (\sigma,\tau) & \longmapsto & c(\sigma,\tau) = \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1} \end{array}$$

satisfà la condició de 2-cocicle (considerant $\mathbf{Q}^\times$ com un $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-mòdul amb l'acció trivial). La seva classe de cohomologia $[c]$ és un element de $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathbf{Q}^\times)$ que no depèn de la classe d'isogènia de C, i 1.3.7 ens diu que C és isògena a una varietat definida sobre $\mathbf{Q}$ si i només si $[c] = 1$. En general $[c] \neq 1$, però recordem que el que cal veure no és que C és isògena a una varietat definida sobre $\mathbf{Q}$, sinó que una certa potència de C ho és. El punt clau per a veure-ho és el teorema següent:

1.3.8 Teorema (Tate) *Si considerem* $\overline{\mathbf{Q}}^\times$ *com un* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-mòdul amb l'acció trivial, aleshores* $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \overline{\mathbf{Q}}^\times) = \{1\}$.

Per tant, la imatge de $[c]$ en $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \overline{\mathbf{Q}}^\times)$ és trivial; és a dir, existeix una aplicació contínua $\alpha : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{Q}}^\times$ tal que

$$c(\sigma,\tau) = \alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}.$$

Sigui E el cos que obtenim adjuntant a $\mathbf{Q}$ els valors de α. Observem que $E/\mathbf{Q}$ és finita ja que α és contínua, i posem $n = [E : \mathbf{Q}]$. Fixant una immersió

$$E \hookrightarrow \mathrm{M}_n(\mathbf{Q}) \simeq \mathbf{Q} \otimes \mathrm{End}_{\overline{\mathbf{Q}}}(C^n)$$

podem identificar els $\alpha(\sigma)$ amb endomorfismes de C^n llevat d'isogènia. Denotem per $\hat{\mu}_\sigma$ la isogènia ${}^\sigma C^n \to C^n$ que és μ_σ en cada coordenada,

i definim $\nu_\sigma = \alpha(\sigma)\circ\mu_\sigma \in \mathbf{Q}\otimes \mathrm{Hom}_{\overline{\mathbf{Q}}}({}^\sigma C^n, C^n)$. El càlcul

$$\begin{aligned}\nu_\sigma \circ {}^\sigma\nu_\tau \circ \nu_{\sigma\tau}^{-1} &= \alpha(\sigma)^{-1}\circ\hat\mu_\sigma\circ{}^\sigma\alpha(\tau)^{-1}\circ{}^\sigma\hat\mu_\tau\circ\hat\mu_{\sigma\tau}^{-1}\circ\alpha(\sigma\tau)\\ &= \alpha(\sigma)^{-1}\circ\alpha(\tau)^{-1}\circ\alpha(\sigma\tau)\circ\hat\mu_\sigma\circ{}^\sigma\hat\mu_\tau\circ\hat\mu_{\sigma\tau}^{-1}\\ &= c(\sigma,\tau)^{-1}\circ c(\sigma,\tau) = 1,\end{aligned}$$

juntament amb 1.3.7 ens diu que existeix una varietat abeliana $A/\mathbf{Q}$ definida sobre $\mathbf{Q}$ tal que $A_{\overline{\mathbf{Q}}}\sim C^n$. Així doncs, hi ha un isomorfisme

$$\mathbf{Q}\otimes \mathrm{End}_{\overline{\mathbf{Q}}}(A) \simeq \mathrm{M}_n(\mathbf{Q}).$$

Amb una versió una mica més refinada de 1.3.7 es pot veure que sota aquest isomorfisme, si $\varphi\in\mathbf{Q}\otimes\mathrm{End}_{\overline{\mathbf{Q}}}(A)$ es correspon amb una matriu $X\in\mathrm{M}_n(\mathbf{Q})$, aleshores ${}^\sigma\varphi$ es correspon amb la matriu $\alpha(\sigma)X\alpha(\sigma)^{-1}$ (on identifiquem $\alpha(\sigma)$ amb una matriu via la immersió $E\hookrightarrow\mathrm{M}_n(\mathbf{Q})$). Els elements φ de $\mathbf{Q}\otimes\mathrm{End}_{\mathbf{Q}}(A)$ són aquells que ${}^\sigma\varphi=\varphi$, i per tant es corresponen amb les matrius X tals que $\alpha(\sigma)X\alpha(\sigma)^{-1}=X$. Com que les matrius $\alpha(\sigma)$ generen la imatge de E dins $\mathrm{M}_n(\mathbf{Q})$, això ens diu que $\mathbf{Q}\otimes\mathrm{End}_{\mathbf{Q}}(A)$ es correspon amb el centralitzador de E en $\mathrm{M}_n(\mathbf{Q})$. Com que $[E:\mathbf{Q}]=n$ i $\mathrm{M}_n(\mathbf{Q})$ és una $\mathbf{Q}$-àlgebra central simple de dimensió n^2 sobre $\mathbf{Q}$, resulta que E és un subcòs maximal de $\mathrm{M}_n(\mathbf{Q})$ i és el seu propi centralitzador. Per tant $\mathbf{Q}\otimes\mathrm{End}_{\mathbf{Q}}(A)\simeq E$, i la igualtat $[E:\mathbf{Q}]=n=\dim A$ ens diu que efectivament A és de tipus GL_2.

Bibliografia

[De71] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Sém. Bourbaki, Lecture Notes in Math., vol. 355, 1971, pp. 136–172.

[DS74] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) 7 (1974), 507–530 (1975).

[Ri92] K. A. Ribet, *Abelian varieties over Q and modular forms.* Algebra and topology 1992 (Taejo(n), 53–79, Korea Adv. Inst. Sci. Tech., Taejo(n, 1992.

[Ri04] K. A. Ribet, *Abelian varieties over* $\mathbf{Q}$ *and modular forms.* Modular curves and abelian varieties, 241–261, Progr. Math., 224, Birkhäuser, Basel, 2004. Edited by J. Cremona, J.-C. Lario, J. Quer and K. Ribet.

[Ri80] K. A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. 253 (1980), 43–62.

[Se87] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J., 54 (1987), 179–230.

Xavier Guitart
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya
Jordi Girona 1-3, 08034 Barcelona
xevi.guitart@gmail.com

Capítol 2

Parametrizations of elliptic curves by Shimura curves and by classical modular curves

Lea Terracini

Introduction

This is an expository paper following Kenneth Ribet and Shuzo Takahashi, cf. [9]. Let $N = DM$, where D is a product of an even number of distinct primes and M is an integer prime to D. Let f be a newform in $S_2(\Gamma_0(N), \mathbb{Q})$. By Jacquet-Langlands correspondence, f corresponds to a newform f' in $S_2(\Phi_0^D(M))$, where $\Phi_0^D(M)$ is the group of norm 1 elements in an Eichler order of the quaternion algebra over $\mathbb{Q}$ of discriminant D (see for example [5]). There are elliptic curves A and A', associated to f and f' respectively, and they are covered by a modular and a Shimura curve respectively. The results in [9] compare the degrees δ and δ' of the two coverings. It is a well-known fact that these degrees have to do with congruences of f in some

Partially supported by MTM2006-04895.

suitable spaces of modular forms. It turns out that the ratio δ/δ' can be described in terms of the orders c_p of the groups of components of the fiber at p of the Néron model of A and A', for p dividing D, and an "error term"(which the authors explicitely describe) whose support consists only of primes ℓ for which the Galois module $A[\ell]$ is reducible.

A partial generalization of this result in the case where A has non-semistable reduction at some prime ℓ has been obtained in [10, see Corollary 4.7 and the discussion below].

2.1 Degree of parametrization

Classical case

Let $f = \sum a_n q^n$ be a newform in $S_2(\Gamma_0(N), \mathbb{Q})$. Shimura associated to f an elliptic curve A over $\mathbb{Q}$, which is a quotient of $J_0(N)$:

$$\xi : J_0(N) \longrightarrow A.$$

By composing with the standard map $X_0(N) \hookrightarrow J_0(N)$ we get a covering

$$\pi : X_0(N) \to A$$

The **degree of parametrization** of A is the degree $\delta = \delta(N)$ of the covering π.

The degree δ can also be viewed in the following way: the map ξ induces on dual varieties a map

$$\check{\xi} : \check{A} \longrightarrow J_0\check{(}N)$$

jacobians of curves are canonically self dual, so that

$$\check{\xi} : A \longrightarrow J_0(N)$$

$\xi \circ \check{\xi} \in \mathrm{End}(A)$ is the multiplication by the integer δ.

Importance of δ for congruences

Primes p dividing $\delta(N)$ are **congruence primes** for f:

$$p|\delta(N) \iff \text{there is a Hecke eigenform } g \in S_2(\Gamma_0(N), \mathbb{Q}) \text{ such that } f \equiv g \mod p.$$

(Ribet [7, 6], Zagier [11], et al. around 1980)

The quaternionic case

Suppose now $N = DM$ with $(D, M) = 1$ and D product of an even number of distinct primes, so that the quaternion algebra B over $\mathbb{Q}$ of discriminant D is undefined.

Let $R(M)$ be an Eichler order of level M in B and let $\Phi_0^D(M)$ be the group of elements of norm 1 in $R(M)$.

By Jacquet-Langlands correspondence there is a Hecke eigenform $f' \in S_2(\Phi_0^D(M))$, M-new, having the same eigenvalues as f for all the Hecke operators.

There is an abelian variety A' associated to f', isogenous to A, and a map

$$\xi' : J_0^D(M) \longrightarrow A'.$$

Then one can define the degree of this parametrization

$$\delta^D(M) = \xi' \circ \check{\xi}' \in \mathbb{Z}.$$

Interpretation of $\delta^D(M)$ in terms of congruences

$$p|\delta^D(M) \iff \text{there is a Hecke eigenform } g \in S_2(\Gamma_0(N), \mathbb{Q})^{D-\text{new}} \text{ such that } f \equiv g \mod p.$$

Let $\Phi(A, p)$ be the group of components of the fiber at p of the Néron model of A, and

$c_p = |\Phi(A, p)| = ord_p(\Delta)$ where δ is the minimal discriminant of A.

It is known (level-lowering results, for example Ribet [8]) that c_p controls congruences between f and p-old forms in $S_2(\Gamma_0(N))$.

2.2 The main result

These considerations yield to the following heuristic formula:

$$\delta^D(M) = \frac{\delta(N)}{\prod_{p|D} c_p}$$

or (recursively), considering a factorization $N = DpqM$

$$\delta^{Dpq}(M) = \frac{\delta^D(pqM)}{c_p c_q}$$

This formula is in general FALSE.

For example consider $M = 1, D = 1, pq = 14$. There is a unique newform f in $S_2(\Gamma_0(14))$. One has $\delta(14) = 1$, $\delta^{14}(1) = 1$, $c_2 = 6$, $c_7 = 3$ (tables of Antwerp IV, [1])

To state the correct version of the formula we need some notations:

$J = J_0^D(Mpq)$	$J' = J_0^{Dpq}(M)$
$\xi : J \to A$	$\xi' : J' \to A'$
$c_p = \lvert\Phi(A, p)\rvert$	$c'_p = \lvert\Phi(A', p)\rvert$

2.2.1 Teorema *1. One has*

$$\delta^{Dpq}(M) = \frac{\delta^D(pqM)}{c'_p c_q}\mathcal{E}(D, p, q, M)^2$$

where the "error term"$\mathcal{E}(D, p, q, M) \in \mathbb{Z}$ is a positive divisor of $c'_p c_q$.

2. *Suppose M is square free but not a prime number and let ℓ be a prime dividing $\mathcal{E}(D, p, q, M)$. Then the* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-module $A[\ell]$ is reducible.*

2.3 Proof of Assertion 1

In order to prove Assertion 1, the authors give an explicit description of $\mathcal{E}(D,p,q,M)$.

If V is an abelian variety over $\mathbb{Q}$ and ℓ is a prime, let

$$\Phi(V,\ell) \quad = \quad \text{group of components of the fiber at } \ell \text{ of the Néron model of } V$$

Then the following facts are known:

- $\Phi(V,\ell)$ is a finite étale group scheme over $Spec(\mathbb{F}_\ell)$, i.e. it is finite abelian with a canonical action of $\mathrm{Gal}(\overline{\mathbb{F}_\ell}/\mathbb{F}_\ell)$;
- if $V = A$ is an elliptic curve with multiplicative reduction at ℓ then $\Phi(A,\ell)$ is cyclic
- the association $V \mapsto \Phi(V,\ell)$ is functorial

The maps $\xi : J \to A$, $\xi' : J' \to A'$ induce

$$\xi_* : \Phi(J,q) \longrightarrow \Phi(A,q) \qquad \xi'_* : \Phi(J',p) \longrightarrow \Phi(A',p).$$

2.3.1 Teorema *One has*

$$\delta^{Dpq}(M) = \frac{\delta^D(pqM)}{c'_p c_q}\mathcal{E}(D,p,q,M)^2$$

where

$$\mathcal{E}(D,p,q,M) = |image(\xi_*)| \cdot |cokernel(\xi'_*)|.$$

Obviously

$$\text{Theorem 2} \Rightarrow \text{Assertion 1 of Theorem 1.}$$

2.4 Proof of Theorem 2

The proof of Theorem 2 relies on comparisons between the character groups of algebraic tori which are functorially associated to $J'_{/\mathbb{F}_p}$ and $J_{/\mathbb{F}_q}$.

General setting

If V is an abelian variety over $\mathbb{Q}$ and ℓ is a prime, let

$$T \quad = \quad \text{toric part of the fiber at } \ell \text{ of the Néron model for } V$$

and let $\mathcal{X}(V,\ell)$ be its character group:

$$\mathcal{X}(V,\ell) \quad = \quad Hom_{\overline{\mathbb{F}_\ell}}(T, \mathbb{G}_m).$$

Then

- $\mathcal{X}(V,\ell)$ is a free abelian group with compatible actions of: $\mathrm{Gal}(\overline{\mathbb{F}_\ell}/\mathbb{F}_\ell)$ and $End_{\mathbb{Q}}(V)$.
- If V has semistable reduction at ℓ then there is a canonical bilinear pairing (**monodromy pairing**), introduced by Grothendieck [3]:
$$u_V : \mathcal{X}(V,\ell) \times \mathcal{X}(\check{V},\ell) \longrightarrow \mathbb{Z}$$
giving rise to a natural exact sequence
$$0 \to \mathcal{X}(V,\ell) \to \mathrm{Hom}(\mathcal{X}(V,\ell),\mathbb{Z}) \to \Phi(V,\ell) \to 0.$$

Steps for proving Theorem 2

Let $\delta = \delta^D(pqM)$ and $\delta' = \delta^{Dpq}(M)$.

- One reduces the claim to show that
$$\frac{\delta' c'_p}{|coker\xi'_*|^2} = \frac{\delta c_q}{|coker\xi_*|^2}$$
- Let
$$\begin{aligned} \mathcal{L} \quad &= \quad \text{the ``f-part'' of } \mathcal{X}(J,q) \\ \mathcal{L}' \quad &= \quad \text{the ``f'-part'' of } \mathcal{X}(J',p) \end{aligned}$$
Then $\mathcal{L}$ (resp. $\mathcal{L}'$) is a no torsion subgroup of $\mathcal{X}(J,q)$ (resp. $\mathcal{X}(J',p)$) containing the image of $\xi^* : \mathcal{X}(A,q) \to \mathcal{X}(J,q)$ (resp. the image of $\xi'^* : \mathcal{X}(A',p) \to \mathcal{X}(J',p)$).

- Consider the diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{X}(A,q) & \to & \mathrm{Hom}(\mathcal{X}(A,q),\mathbb{Z}) & \to & \Phi(A,q) & \to & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \to & \mathcal{X}(J,q) & \to & \mathrm{Hom}(\mathcal{X}(J,q),\mathbb{Z}) & \to & \Phi(J,q) & \to & 0 \end{array}$$

  It is easy to show that

$$\begin{aligned} |coker(\xi_*)| &= [\mathcal{L} : \mathcal{X}(A,q)] \\ |coker(\xi'_*)| &= [\mathcal{L}' : \mathcal{X}(A',p)] \end{aligned}$$

  so that the claim reduces to

$$\frac{\delta' c'_p}{[\mathcal{L}' : \mathcal{X}(A',p)]} = \frac{\delta c_q}{[\mathcal{L} : \mathcal{X}(A,q)]}.$$

- By multiplicity 1, $\mathcal{L}$ (and $\mathcal{L}'$) have rank 1.
  Fix a generator g of $\mathcal{L}$ and a generator x of $\mathcal{X}(A,q)$.

- The maps

$$\begin{aligned} \xi^* : \mathcal{X}(A,q) &\to \mathcal{X}(J,q) \qquad \text{induced by } \xi \\ \xi_* : \mathcal{X}(J,q) &\to \mathcal{X}(A,q) \qquad \text{induced by } \check{\xi} \end{aligned}$$

  are self-adjoint w.r.t. monodromy, and $\xi^* \circ \xi_* = \delta$, so that

$$\begin{aligned} \delta c_q &= \delta u_A(x,x) = u_A(x, \xi^*\xi_* x) = u_J(\xi^* x, \xi^* x) \\ &= [\mathcal{L} : \mathcal{X}(A,q)]^2 u_J(g,g) \end{aligned}$$

  and analogously $\delta' c'_p = [\mathcal{L}' : \mathcal{X}(A',p)]^2 u_{J'}(g',g')$.

  Then the claim reduces to show that

$$u_J(g,g) = u_{J'}(g',g')$$

  where g is a generator of $\mathcal{L}$ and g' is a generator of $\mathcal{L}'$.

- We need to connect in some way g and g',

  Key point (Ribet [8] for $D = 1$, generalized by K. Buzzard [2]):

there is a canonical exact sequence

$$0 \to \mathcal{X}(J', p) \xrightarrow{i} \mathcal{X}(J, q) \to \mathcal{X}(J'', q) \times \mathcal{X}(J'', q) \to 0$$

where $J'' = J_0^D(qM)$.

The sequence is compatible with the Hecke action and monodromy pairing.

- then i embeds $\mathcal{L}'$ in $\mathcal{L}$, and $\mathcal{L}/i(\mathcal{L}')$ is torsion, but since $\mathcal{X}(J'', q)$ has no torsion, i restricts to an isomorphism $\mathcal{L}' \simeq \mathcal{L}$.
- Then we can pick $g = i(g')$ and the claim is proved.

2.5 Proof of Assertion 2

Let ℓ be a prime such that $A[\ell]$ is irreducible.

Then there exists an isogeny $A \to A'$ whose degree is not divisible by ℓ, so that

$$A[\ell] \simeq A'[\ell] \quad \text{as } G_{\mathbb{Q}} - \text{modules.}$$

and $ord_\ell(c_p) = ord_\ell(c'_p)$ for every prime p.

We define e as the ℓ-part of $\mathcal{E}$

$$e(D, p, q, M) = \ell^{ord_\ell \mathcal{E}(D,p,q,M)}.$$

Then $e(D, p, q, M) = e(D, q, p, M)$.

1 Proposition

$$e(D, p, q, M) = |coker(\xi'_* : \Phi(J', p) \to \Phi(A', p))|_\ell.$$

(Notice that q does not appear in the right hand)

Prova:

By Theorem 2 this amounts to prove that the ℓ-part of $Im(\xi_* : \Phi(J, q) \to \Phi(A, q))$ is trivial.

FACT: $\Phi(J,q)$ is Eisenstein. (Ribet [8] for $D=1$ and generalized to Shimura curve by Buzzard [2] and Jordan-Livné [4])

Then $Im(\xi_*)$ is annihilated by $a_r(f)-r-1$ for every prime r.

$\Rightarrow$ its ℓ-part is trivial, otherwise $a_r \equiv r+1 \mod \ell$ for every prime r which is a contradiction, because $A[\ell]$ is irreducible. $\square$

Then we can consider varying decompositions $N = DpqM$.

Put $M = M'rs$. (By hypothesis M' is square-free but not prime!).

Then

$$e(Drs,p,q,M') = e(Dqs,p,r,M')$$

because each one is the order of the ℓ-part of

$$cocker(\xi'_* : \Phi(J^{Dpqrs}(M'),p) \to \Phi(A',p)).$$

By Assertion 1

$$\left(\frac{\delta^{pqrsD}(M')c_pc_qc_rc_s}{\delta^D(pqrsM')}\right)_\ell = \begin{array}{c} e(Drs,p,q,M')^2 e(D,r,s,M'pq)^2 \\ \| \\ e(Dqs,p,r,M')^2 e(D,q,s,M'pr)^2 \end{array}$$

so that $e(D,r,s,M'pq) = e(D,q,s,M'pr)$.

In conclusion, it follows that if ℓ divides $e(D,p,q,M)$ then ℓ divides c_r for every prime r dividing $N = DpqM$.

By a previous result of Ribet [8], then f should be congruent modulo ℓ to a form in $S_2(\mathrm{SL}_2(\mathbb{Z}))$. But $S_2(\mathrm{SL}_2(\mathbb{Z}))$ is zero; therefore $e(D,p,q,M) = 1$.

Bibliografia

[1] Birch, B., and Kuyk, W. e. *Modular Forms of One Variable IV*, vol. 476 of *Lecture Notes in Mathematics*. Springer, 1975.

[2] Buzzard, K. Integral models of certain Shimura curves. *Duke Math. J. 87* (1997), 591–612.

[3] Grothendieck, A. Modelès de Néron et monodromie (exposé IX). In *SGA 7, Lecture Notes in Mathematics 288* (1972), Springer-Verlag, pp. 313–523.

[4] Jordan, B., and Livné, R. Integral Hodge theory and congruences between modular forms. *Duke Math. J. 80* (1995), 419–484.

[5] Mori, A., and Terracini, L. A canonical map between Hecke algebras. *Boll. Un. Mat. Ital. (8) 2-B* (1999), 429–452.

[6] Ribet, K. A. Congruence relations between modular forms. In *Proceedings of the International Congress of Mathematics* (Warsawa, 1983), pp. 503–514.

[7] Ribet, K. A. Mod p Hecke operators and congruences between modular forms. *Invent. Math. 71* (1983), 193–205.

[8] Ribet, K. A. On modular representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math. 100* (1990), 431–476.

[9] Ribet, K. A., and Takahashi, S. Parametrizations of elliptic curves by Shimura curves and by classical modular curves. *Proc. Natl. Acad. Sci. USA 94* (1997), 11110–11114.

[10] Terracini, L. A Taylor-Wiles system for quaternionic Hecke algebras. *Compositio Mathematica*, 137 (2003), 23–47.

[11] Zagier, D. Modular parametrizations of elliptic curves. *Canad. Math. Bull. 28* (1985), 372–384.

Lea Terracini
Dipartimento di Matematica
Università de Torino
Via Carlo Alberto 10, 10123 Torino
lea.terracini@unito.it

Capítol 3

Galois theory and torsion points on curves

Bernat Plans

Introducció

Aquest capítol és la versió escrita d'una xerrada pronunciada durant el STNB 2008-2009, en la qual vam exposar alguns dels resultats (no tots!) de M. Baker, K. Ribet i A. Tamagawa continguts en [3].

L'objectiu principal és veure com aprofitar el concepte de *punts gairebé racionals* de varietats abelianes, introduït per Ribet anys enrere, per a obtenir noves demostracions de les (ex)conjectures de Manin-Mumford i de Coleman-Kaskel-Ribet.

Aquestes conjectures parlen dels punts de torsió en una corba X de gènere $g \geqslant 2$; un punt de X és "de torsió" si ho és en la jacobiana $J := Jac(X)$, via una immersió d'Albanese $X \hookrightarrow J$. Els *punts gairebé racionals* intervenen perquè, per a un punt de J, "ser gairebé racional" (respecte un cos K) és una condició genèricament necessària per tal de provenir d'un punt de X per alguna $X \hookrightarrow J$ (definida sobre K).

Amb el suport parcial de MTM2006-04895.

3.1 Punts de torsió gairebé racionals en varietats abelianes

L'objectiu d'aquesta secció és provar els Teoremes 3.1.1 i 3.1.4, que seran essencials en les demostracions de les conjectures de Manin-Mumford i de Coleman-Kaskel-Ribet, respectivament.

K sempre denotarà un *cos* i G_K el seu grup de Galois absolut $\mathrm{Gal}(\overline{K}/K)$.

Definició. Donada una varietat abeliana A/K, direm que un punt $a \in A(\overline{K})$ és *gairebé racional* si, per a tot parell $\sigma, \tau \in G_K$, es satisfà:

$$[\sigma a + \tau a = 2a \implies \sigma a = \tau a = a].$$

A partir d'ara abreujarem *gairebé racional(s)* per g.r..

Observació. El subconjunt de $A(\overline{K})$ format pels punts g.r. no és necessàriament un subgrup de $A(\overline{K})$.

3.1.1 Finitud

En tot aquest apartat suposarem que K és de *característica* 0 *amb grau de transcendència finit sobre* $\mathbb{Q}$. L'objectiu és provar el

3.1.1 Teorema. *Si A/K és una varietat abeliana, aleshores només un nombre finit de punts de torsió de $A(\overline{K})$ són g.r..*

Recordem, primer, un resultat enunciat a [18, no. 136] (veure també [18, no. 138]).

3.1.2 Teorema. (Serre) *Sigui A/K una varietat abeliana de dimensió g. Sigui $\rho : G_K \longrightarrow \mathrm{Aut}(\widehat{T}A) \cong \mathrm{GL}_{2g}(\widehat{\mathbb{Z}})$ la representació de Galois en el mòdul de Tate adèlic de A. Si $\widehat{\mathbb{Z}}^* \subset \mathrm{Aut}(\widehat{T}A)$ denota el subgrup d'homotècies, aleshores el grup $\widehat{\mathbb{Z}}^*/(\rho(G_K) \cap \widehat{\mathbb{Z}}^*)$ té exponent finit.*

Observació. Una conjectura (no provada) de Lang prediu que, de fet, aquest grup és finit.

Demostració del Teorema 3.1.1:

Sigui $a \in A(\overline{K})^{tors}$ un punt d'ordre m. Veurem que, si m és prou gran, aleshores a no pot ser g.r..

Si e denota l'exponent del grup $\widehat{\mathbb{Z}}^*/(\rho(G_K) \cap \widehat{\mathbb{Z}}^*)$, aleshores

$$((\mathbb{Z}/m\mathbb{Z})^*)^e \subset \rho_m(G_K),$$

on $\rho_m : G_K \to \mathrm{Aut}(A[m])$ és la representació en la m-torsió $A[m]$.

Per tant, donats $x, y \in (\mathbb{Z}/m\mathbb{Z})^*$, existeixen $\sigma, \tau \in G_K$ que actuen en $A[m]$ com les homotècies x^e, y^e. Així, si existeixen x, y satisfent

(i) $x^e + y^e = 2$

(ii) $x^e \neq 1 \neq y^e$,

aleshores a no pot ser g.r., donat que $\sigma a + \tau a = 2a$ i $\sigma a \neq a \neq \tau a$. Això acaba la demostració, gràcies al següent

Lema *Si m és prou gran, aleshores existeixen $x, y \in (\mathbb{Z}/m\mathbb{Z})^*$ que satisfan (i), (ii).*

Demostració: Pel Teorema xinès del residu, si λ és coprimer amb m i la conclusió és vàlida per a m, aleshores també ho és per a $m' = \lambda m$; només cal triar $x' \equiv x \pmod m$ i $y' \equiv y \pmod m$ tals que $x' \equiv y' \equiv 1 \pmod \lambda$. Per tant, és suficient provar el Lema per a $m = p^n$, amb p primer. Recordem que e està fixat.

Cas $n = 1$. Per a $p > e$, l'equació $X^e + Y^e - 2Z^e = 0$ defineix una corba projectiva sobre $\mathbb{F}_p$ que és llisa i de gènere $(e-1)(e-2)/2$. Per les fites de Weil, el nombre de punts sobre $\mathbb{F}_p$ d'aquesta corba és més gran que $p + 1 - (e-1)(e-2)\sqrt{p}$. Per tant, l'equació $x^e + y^e = 2$ té més de $(p + 1 - (e-1)(e-2)\sqrt{p} - e)$ solucions en $\mathbb{F}_p^2$. D'aquestes, menys de $(e+1)^2$ tenen x^e o y^e igual a 0 o 1. La conclusió del Lema es satisfà, doncs, per a $m = p$ prou gran.

Cas $n > 1$. Podem suposar $n > 2r+1$, on r denota la valoració p-àdica de e (això només exclou un nombre finit de casos). En particular, $n - r - 1 > 0$ i $2(n - r - 1) \geqslant n$. En aquest cas, els elements $x := 1 + p^{n-r-1}$, $y := 1 - p^{n-r-1}$ són invertibles en $(\mathbb{Z}/p^n\mathbb{Z})$ i és immediat comprovar que satisfan (i), (ii). □

3.1.2 Acció de la inèrcia en primers de reducció ordinària semiestable

En tot aquest apartat prendrem $K = \mathbb{Q}$ i suposarem/notarem:

- l és un nombre primer fixat.
- $A/\mathbb{Q}$ és una varietat abeliana.
- $I = I_l \subset G_{\mathbb{Q}}$ és "el" subgrup d'inèrcia en l.
- $I(n) := \{\sigma \in I \mid \chi(\sigma) \equiv 1 \pmod{l^n}\}$, on $\chi : G_{\mathbb{Q}} \twoheadrightarrow \mathbb{Z}_l^*$ denota el caràcter ciclotòmic l-àdic.

El punt de partida d'aquesta secció és el següent resultat conegut:

3.1.3 Teorema. (SGA7) *Suposem que $A/\mathbb{Q}$ té reducció ordinària semiestable en l. Sigui M un sub-$\mathbb{Z}[I]$-mòdul finit de $A(\overline{\mathbb{Q}})^{tors}$.*

(a') *Si l no divideix l'ordre de M, aleshores $(\sigma-1)^2 M = 0$, $\forall \sigma \in I$.*

(b') *Sempre existeix $0 \to M' \to M \to M'' \to 0$, successió exacta de $\mathbb{Z}[I]$-mòduls, on M' és I-ciclotòmic i M'' és I-trivial.*

(c') *Si A té bona reducció en l, aleshores M_{non-l} és I-trivial.*

Remarques: 1) M_{non-l} és la part l'-primària de M; és a dir, $M = M_l \oplus M_{non-l}$ on M_l és un l-grup i M_{non-l} té ordre coprimer amb l.

2) Que M' sigui I-ciclotòmic vol dir que I actua via $\chi_{|I} : I \twoheadrightarrow \mathbb{Z}_l^*$, a través de l'acció natural de $\mathbb{Z}_l^*$ (trivial en M'_{non-l} i via $\mathbb{Z}_l^* \twoheadrightarrow (\mathbb{Z}/l^n\mathbb{Z})^*$ en M'_l, si l^n és l'exponent de M'_l).

3) (b') s'obté dels resultats de [7]. Veure la prova de [19, Prop. 2.1].

4) (a') és [7, Prop. 3.5] i es pot enunciar dient que l'acció de I en M és *unipotent de rang* 2 (quan $l \nmid \sharp M$). A més, s'obté com a conseqüència directa de (b'): $l \nmid \sharp M \Rightarrow M'$ és I-trivial (remarca 2); com que M'' és I-trivial, es té $(\sigma-1)M \subseteq M'$ i, per tant, $(\sigma-1)^2 M = 0$, $\forall \sigma \in I$.

5) (c') és [7, Cor. 2.2.9] (Criteri de Néron-Ogg-Shafarevich).

L'objectiu d'aquest apartat és combinar el Teorema 3.1.3 amb la condició "g. r.". Després, en la secció 3.3.2, ho aplicarem en situacions en les que alguna de les conclusions del Teorema 3.1.3 és certa, encara que no tinguem "reducció ordinària". Per això introduïm les

Definicions. Direm que un $\mathbb{Z}[I]$-mòdul finit M és *ordinari semiestable* (resp. *ordinari bo*) si es satisfà la conclusió de l'apartat (b') (resp. (b') i (c')) del Teorema 3.1.3.

Observació. Si M és ordinari semiestable (resp. bo), aleshores també ho és tot subquocient de M.

3.1.4 Teorema. (Tamagawa) *Sigui M un sub-$\mathbb{Z}[I]$-mòdul finit de $A(\overline{\mathbb{Q}})^{tors}$. Suposem que M és ordinari semiestable i que està generat per punts g.r..*

(a) Si l no divideix l'ordre de M, aleshores M és I-trivial.

(b) Si $l > 2$, aleshores M és $I(1)$-trivial.

(c) Si $l \geqslant 5$ i M és ordinari bo, aleshores M és I-trivial.

Observació. És immediat comprovar que els conjugats galoisians d'un punt g.r. també són g.r.. Així, si M està generat per punts g.r. com a $\mathbb{Z}[I]$-mòdul, aleshores també ho està com a $\mathbb{Z}$-mòdul.

Demostració del Teorema 3.1.4:

(a) Siguin $\sigma \in I$, $a \in M$. Per la remarca 4, que M sigui ordinari semiestable d'ordre coprimer amb l implica $(\sigma - 1)^2 a = 0$ i, per tant, $0 = \sigma^{-1}(\sigma - 1)^2 a = \sigma a + \sigma^{-1} a - 2a$. Així, si a és g.r., aleshores $\sigma a = a$. Com que estem suposant que M està generat per punts g.r., haurà de ser I-trivial.

(b) Considerem la successió exacta de (b'). Per la remarca 2, que M' sigui I-ciclotòmic (d'exponent finit) fa que sigui $I(n)$-trivial per a n prou gran. Com que M'' també és $I(n)$-trivial, obtenim $(\sigma - 1)^2 M = 0$, $\forall \sigma \in I(n)$, com a la remarca 4. Per tant, M és $I(n)$-trivial, com en la demostració de (a).

D'altra banda, $I(1)/I(n) \cong \mathbb{Z}/l^{n-1}\mathbb{Z}$ i, per tant, haurà de ser $(\sigma^{l^{n-1}} - 1)M = 0$, $\forall \sigma \in I(1)$. Com abans, $(\sigma - 1)^2 M_{non-l} = 0$ per la remarca 4. Com que $\sigma^{l^{n-1}} - 1 \equiv l^{n-1}(\sigma - 1) \pmod{(\sigma-1)^2}$, obtenim $(\sigma - 1)M_{non-l} = 0$. (No podem aplicar directament (a) perquè no sabem que M_{non-l} es pugui generar per punts g.r.; només per múltiples de punts g.r..) En resum, M_{non-l} és $I(1)$-trivial.

Suposem fixat $\sigma \in I(1)$, és a dir, $\sigma \in I$ tal que $\chi(\sigma) \equiv 1 \pmod{l}$. Volem concloure $(\sigma - 1)M = 0$.

Com que $\sigma \in I(1)$ i la restricció $\chi_{|I} : I \to \mathbb{Z}_l^*$ és exhaustiva, existeix $\tau \in I$ tal que $\chi(\sigma) + \chi(\tau) = 2$. Per força $\chi(\tau) \equiv 1 \pmod{l}$, és a dir, $\tau \in I(1)$.

Observem que, si $(\sigma + \tau - 2)M_l = 0$, aleshores $(\sigma + \tau - 2)M = 0$ perquè M_{non-l} és $I(1)$-trivial. Això implicaria $(\sigma - 1)M = 0$ perquè, per hipòtesi, M està generat per punts g.r.. Haurem acabat, doncs, si veiem $(\sigma + \tau - 2)M_l = 0$.

I actua en M a través del grup *abelià* $I/I(n)$. En particular, $(\rho - 1)(\sigma + \tau - 2)M_l = (\sigma + \tau - 2)(\rho - 1)M_l$, per a tot $\rho \in I$. Però $(\rho - 1)M_l \subseteq M_l'$, perquè M_l'' és I-trivial. A més, $(\sigma + \tau - 2)M_l' = 0$, perquè $\chi(\sigma) + \chi(\tau) = 2$ i M_l' és I-ciclotòmic. Per tant, $\forall \rho \in I$, $(\rho - 1)(\sigma + \tau - 2)M_l = 0$. És a dir, $(\sigma + \tau - 2)M_l \subseteq (M_l)^I$.

D'altra banda, $(\sigma + \tau - 2)M_l \subseteq M_l'$ perquè $(\sigma + \tau - 2)M_l'' = 0$. Així, haurà de ser $(\sigma + \tau - 2)M_l \subseteq (M_l')^I$. Però l'acció de I en M_l' és ciclotòmica (l-àdica) i, per tant, els únics elements de I que fixen un element d'ordre l són els de $I(1)$. Com que $I(1) \neq I$ (perquè $l \neq 2$) i M_l' és un l-grup, obtenim $(M_l')^I = 0$.

En resum, $(\sigma + \tau - 2)M_l = 0$ tal com volíem.

(c) Per hipòtesi, M_{non-l} és I-trivial i, per (b), M és $I(1)$-trivial.

Raonant com en la demostració de (b) veiem que, si $\sigma, \tau \in I$ satisfan $\chi(\sigma) + \chi(\tau) = 2$, aleshores $(\sigma - 1)M = 0$. Per tant, haurem acabat si $I/I(1)$ es pot generar per algun $\bar{\sigma}$ amb $\chi(\sigma) \neq 2 \pmod{l}$. Però això és clarament cert perquè $I/I(1) \cong (\mathbb{Z}/l\mathbb{Z})^*$ i estem suposant $l > 3$ (si $\bar{2}$ genera, també ho fa $\bar{2}^{-1} \neq \bar{2}$).

3.2 La (ex)conjectura de Manin-Mumford

En aquesta secció, sempre que no es digui una altra cosa, seran vàlides les següents

Hipòtesis i notacions:

- K és un cos de nombres; $G_K := \mathrm{Gal}(\overline{K}/K)$.
- X és una corba (completa, no singular i geomètricament irreductible) sobre K de gènere $g \geqslant 2$.
- J és la Jacobiana de X i $J(\overline{K})^{tors}$ és el subgrup de torsió de $J(\overline{K})$.
- $P \in X(K)$ és un punt K-racional.
- $i_P : X \to J$ és el morfisme d'Albanese (K-racional) amb punt base P, que envia $Q \in X(\overline{K})$ a la classe del divisor $(Q)-(P)$; es tracta d'una immersió tancada (per ser $g \geqslant 1$).

3.2.1 L'enunciat

Manin i Mumford van conjecturar, de forma independent, el següent resultat que Lang [8] va batejar com la *conjectura de Manin-Mumford* i que finalment Raynaud va demostrar [15].

Teorema MM. *El conjunt $i_P(X(\overline{K})) \cap J(\overline{K})^{tors}$ és finit.*

3.2.2 La demostració

Introduïm primer la següent

Definició. Un punt $Q \in X(\overline{K})$ és *excepcional* si la corba X és hiperel.líptica i Q és punt de ramificació hiperel.líptic.

Com que el conjunt de punts excepcionals és finit, el Teorema MM s'obté com a conseqüència directa del Teorema 3.1.1 i del següent resultat que, en gran part, motiva el concepte de punts g.r..

3.2.1 Lema. *Si un punt $Q \in X(\overline{K})$ no és excepcional, aleshores $i_P(Q)$ és g.r..*

DEMOSTRACIÓ: Com que P és fix per G_K, que $i_P(Q)$ NO sigui g.r. vol dir que existeixen $\sigma, \tau \in G_K$ tals que $Q \notin \{\sigma Q, \tau Q\}$ i

$$(\sigma Q) + (\tau Q) \sim 2(Q).$$

En aquest cas, existeix una funció racional $f \in \overline{K}(X)$ amb zeros en $\{\sigma Q, \tau Q\}$ i un pol doble en Q. Per tant, Q és excepcional (el morfisme no constant $f : X \to \mathbb{P}^1$ és de grau 2 i ramificat en Q). □

3.2.3 Comentaris addicionals

1. El Teorema MM diu que, quan veiem $X(\overline{K})$ dins de $J(\overline{K})$ via la immersió fixada i_P, només un nombre finit de punts de X són de torsió. Quan fem variar el punt base P, però, pot ser que obtinguem infinits *paquets de torsió* $i_P(X(\overline{K})) \cap J(\overline{K})^{tors}$ diferents (i no trivials, és a dir, amb més d'un punt). És conegut que això només pot passar per a $g \leqslant 3$ i, en qualsevol cas (sempre amb $g \geqslant 2$), existeix una fita uniforme per al cardinal de tots els paquets de torsió que només depèn de X. Cf. [2].

2. El Teorema MM és vàlid sobre qualsevol cos K finitament generat de característica 0, donat que el Teorema 3.1.1 ho és. També ho és la següent versió més general provada per Raynaud en [15]:

Teorema. *Per a qualsevol K-immersió tancada $i : X \to A$ en una K-varietat abeliana A, el conjunt $i(X(\overline{K})) \cap A(\overline{K})^{tors}$ és finit.*

Dit d'una altra manera: "dins" d'una varietat abeliana A/K, les úniques corbes X/K que es poden fer passar per infinits punts de torsió són les de gènere 1, és a dir, les traslladades de subvarietats abelianes de dimensió 1 (per un punt de torsió).

Actualment es coneixen diverses demostracions i generalitzacions d'aquest resultat que admeten $\dim X > 1$, A/K varietat semiabeliana, K qualsevol cos de característica 0, ... Veure [20] i les seves referències.

3. Una de les generalitzacions del resultat anterior és l'anomenada *Conjectura de Mordell-Lang*, conjecturada per Lang i finalment

provada per McQuillan [12]. Un cas particular d'aquesta conjectura és el següent:

Teorema. *Sigui $i : X \to A$ una K-immersió tancada en una K-varietat abeliana A. Si Γ és un subgrup finitament generat de $A(\overline{K})$ i $\Gamma' := \{a \in A(\overline{K}) \mid na \in \Gamma$ per algun $n \geqslant 1\}$ és el seu grup de divisió, aleshores el conjunt $i(X(\overline{K})) \cap \Gamma'$ és finit.*

Aquest resultat conté, a la vegada, les conjectures de Manin-Mumford i de Mordell. La primera s'obté amb $\Gamma = \{0\}$ i, per tant, $\Gamma' = A(\overline{K})^{tors}$. La segona s'obté amb $\Gamma = A(K)$ donat que, en aquest cas, $i(X(K)) = i(X(\overline{K})) \cap \Gamma \subseteq i(X(\overline{K})) \cap \Gamma'$.

3.3 La (ex)conjectura de Coleman, Kaskel i Ribet

En tota aquesta secció seran vàlides les següents

Hipòtesis i notacions:

- $X/\mathbb{Q}$ és la corba modular $X := X_0(p)$, amb p primer.
- g és el gènere de X i suposarem $g \geqslant 2$, és a dir, $p \geqslant 23$.
- $0, \infty \in X(\mathbb{Q})$ són les puntes de X.
- $J/\mathbb{Q}$ és la jacobiana $J := J_0(p)$ de X.
- $i := i_\infty : X \hookrightarrow J$ és la immersió standard cuspidal (=Albanese amb punt base $\infty \in X(\mathbb{Q})$).
- $T_\infty := i(X(\overline{\mathbb{Q}})) \cap J(\overline{\mathbb{Q}})^{tors}$.
- w_p és la involució d'Atkin-Lehner de X (permuta 0, ∞). w_p també denota l'endomorfisme induït (functor d'Albanese) en J que envia $[\sum n_i(P_i)]$ a $[\sum n_i(w_p(P_i))]$.
- g^+ és el gènere de $X^+ := X/w_p$.

3.3.1 L'enunciat

La conjectura de Coleman-Kaskel-Ribet [4], demostrada independentment per Baker [1] i Tamagawa [19], afirma:

Teorema CKR.

$$T_\infty = \begin{cases} \{i(0), i(\infty)\} & \text{si } g^+ > 0 \\ \{i(0), i(\infty)\} \cup i(\{\text{punts excepcionals}\}) & \text{si } g^+ = 0 \end{cases}$$

Comentari. Aquest resultat és una versió efectiva de la conjectura de Manin-Mumford per a $X = X_0(p)$. També es coneixen resultats efectius per a d'altres corbes X, incloent-hi les corbes de Fermat. Veure, per exemple, [1], [14], [21].

El que provarem en l'apartat 3.3.2 és:

Teorema CKRbis. *Tot punt gairebé racional de T_∞ és $\mathbb{Q}$-racional. És a dir, el conjunt de punts g.r. en T_∞ és $i(X(\mathbb{Q})) \cap J(\mathbb{Q})^{tors}$.*

Que el Teorema CKR és equivalent al Teorema CKRbis és clar pel Lema 3.2.1 i pels fets següents:

• $\underline{\{i(0), i(\infty)\} \subseteq T_\infty}$, donat que $i(0)$ és de torsió pel Teorema de Manin-Drinfel'd [6].

• $\underline{P \in X(\overline{\mathbb{Q}}) \text{ excepcional} \Rightarrow [i(P) \in T_\infty \Leftrightarrow g^+ = 0]}$.

Això és [4, Prop. 1.1] i és conseqüència de:
· Per un resultat d'Ogg [13], X hiperel.líptica $\Leftrightarrow g^+ = 0$ o bé $p = 37$.
· $g^+ = 0 \Rightarrow w_p = -1$ en J (w_p coincideix amb la inv. hiper.) $\Rightarrow w_p(i(P)) = -i(P), \forall P \in X(\overline{\mathbb{Q}})$. Però $w_p(i(P)) = i(w_p(P)) - i(0)$. Per tant, P excepcional (i $g^+ = 0$) $\Rightarrow 2i(P) = i(0) \in T_\infty \Rightarrow i(P) \in T_\infty$.
· $P \in X_0(37)(\overline{\mathbb{Q}})$ excepcional $\Rightarrow i(P)$ no és de torsió. Veure [11, §5].

• $\underline{i(X(\mathbb{Q})) \cap J(\mathbb{Q})^{tors} = \{i(0), i(\infty)\}}$.

Si $p \notin \{37, 43, 67, 163\}$, aleshores $X(\mathbb{Q}) = \{0, \infty\}$ per un resultat de Mazur [10, Thm. 7.1]. Per als quatre casos restants, veure la prova de [4, Prop. 1.2].

3.3.2 La demostració

A les hipòtesis i notacions anteriors afegim:

- Operadors de Hecke: $T_l \in \mathrm{End}(J)$
- Àlgebra de Hecke: $\mathbf{T} := \mathbb{Z}[\{T_l\}_{l \neq p}, w_p]$
- Ideal d'Eisenstein: $\mathfrak{J} := (\{T_l - (l+1)\}_{l \neq p}, w_p + 1) \subset \mathbf{T}$
- $J[\mathfrak{J}] := \{a \in J(\overline{\mathbb{Q}}) | ta = 0, \forall t \in \mathfrak{J}\}$
- $n := (p-1)/m.c.d(p-1, 12)$

La demostració del Teorema CKRbis combina el Teorema 3.1.4 amb els resultats següents.

Resultat 1. El morfisme $\mathbb{Z} \hookrightarrow \mathbf{T} \twoheadrightarrow \mathbf{T}/\mathfrak{J}$ indueix un isomorfisme $\mathbf{T}/\mathfrak{J} \cong \mathbb{Z}/n\mathbb{Z}$; el $\mathbf{T}/\mathfrak{J}$-mòdul $J[\mathfrak{J}]$ és lliure de rang 2 i, per tant, $J[\mathfrak{J}] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ com a $\mathbb{Z}$-mòduls. Cf. [9, II] i veure [3, p. 26].

Resultat 2. J té reducció ordinària semiestable en p (veure, per exemple, [3, p. 26] o [19, p. 307]). Així, pel Teorema 3.1.3 (b'), tot $\mathbb{Z}[I_p]$-submòdul finit de $J(\overline{\mathbb{Q}})^{tors}$ és ordinari semiestable.

Resultat 3. Si p divideix l'ordre d'un $\mathbf{T}[G_{\mathbb{Q}}]$-submòdul finit $\mathcal{M}$ de $J(\overline{\mathbb{Q}})^{tors}$, aleshores l'acció de I_p en $\mathcal{M}$ és *NO-abeliana*. Cf. [3, pp. 26-27].

Comentari (sobre la dem.): Tot subquocient simple del $\mathbf{T}[G_{\mathbb{Q}}]$-mòdul $J[p]$ és isomorf a un subquocient de $J[\mathfrak{m}]$, per algun ideal maximal $\mathfrak{m} \in Max(\mathbf{T})$ amb $p \in \mathfrak{m}$. Com que $p \nmid n$, $\mathfrak{m}$ és *no-Eisenstein*, i.e. no conté $\mathfrak{J}$. En aquest cas, com a representació de $G_{\mathbb{Q}}$ sobre el cos finit $\mathbf{T}/\mathfrak{m}$ (de característica p), $J[\mathfrak{m}]$ és irreductible i és isomorf a la *representació standard* $\rho_{\mathfrak{m}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbf{T}/\mathfrak{m})$. Cf. [9, Prop. 14.2].

Notem $M := J[\mathfrak{m}]$.
Pel Resultat 2, M és un $\mathbb{Z}[I_p]$-mòdul ordinari semiestable, és a dir, existeix un $\mathbb{Z}[I_p]$-submòdul M' de M tal que M' és I_p-ciclotòmic i $M'' := M/M'$ és I_p-trivial.
Fixem ara un element $\sigma \in I_p$ tal que $\chi_p(\sigma) \equiv 2 \pmod{p}$, on χ_p denota el caràcter ciclotòmic p-àdic; notem que σ existeix perquè $p \neq 2$ i $\chi_{p|I_p} : I_p \to \mathbb{Z}_p^*$ és exhaustiu. Com que p anul.la $M \subseteq J[p]$, resulta que $(\sigma - 1)$ és la identitat en M' i és 0 en M''. Així, $(\sigma - 1)M = M'$ i $(\sigma - 1)^2 = (\sigma - 1)$ en M. D'aquesta manera, com a $\mathbf{T}/\mathfrak{m}$-espai vectorial, $M = M' \oplus M^\sigma$.
Si $\rho_{\mathfrak{m}}(I_p)$ fos abelià, aleshores M^σ seria estable per I_p i, per força, isomorf a M'' com a I_p-mòdul, és a dir, trivial (i, de fet, igual a M^{I_p}). Tindríem, doncs, $M \cong M' \oplus M''$ com a $(\mathbf{T}/\mathfrak{m})[I_p]$-mòduls. Això implicaria que $\rho_{\mathfrak{m}}$ *és finita en* p en el sentit de Serre (veure [19, pp. 307-308]). És conegut, però, que $\rho_{\mathfrak{m}}$ no és finita en p quan $\mathfrak{m}$ és no-Eisenstein. Cf. [17, Prop. 2.2]. En resum, $\rho_{\mathfrak{m}}(I_p)$ és no abelià i això prova el Resultat 3.

Resultat 4. El conjunt de punts de $J(\overline{\mathbb{Q}})^{tors}$ no ramificats en p és $J[\mathfrak{J}]$. Cf. [17, Prop. 3.3].

Resultat 5. $J[\mathfrak{J}]$ admet un subgrup $G_{\mathbb{Q}}$-estable Σ tal que, com a $\mathbb{Z}[G_{\mathbb{Q}}]$-mòduls, $\Sigma \cong \mu_n$ (ciclotòmic) i $J[\mathfrak{J}]/\Sigma \cong \mathbb{Z}/n\mathbb{Z}$ (trivial). Cf. [17, Prop. 3.2]. En particular, per a tot primer l, el $\mathbb{Z}[I_l]$-mòdul $J[\mathfrak{J}]$ és ordinari semiestable.

Observació: $\Sigma := \ker(J \to J_1(p))$ és el *subgrup de Shimura* de J.
Per a n senar, el *subgrup de torsió* $C := \langle i(0) \rangle$ és un complement de Σ en $J[\mathfrak{J}]$, és a dir, $J[\mathfrak{J}] \cong \mu_n \oplus \mathbb{Z}/n\mathbb{Z}$ com a $\mathbb{Z}[G_{\mathbb{Q}}]$-mòduls.
Per a una descripció explícita del $\mathbb{Z}[G_{\mathbb{Q}}]$-mòdul $J[\mathfrak{J}]$ quan n és parell, veure [5].

Resultat 6. Per a tot primer $l \mid n$, el $\mathbb{Z}[I_l]$-mòdul $J[\mathfrak{J}]$ és ordinari bo. Veure [3, pp. 26-27].

Demostració del Teorema CKRbis:

Sigui $P \in X(\overline{\mathbb{Q}})$ i suposem/notem:

- $a := i(P) \in J(\overline{\mathbb{Q}})$ és de torsió.
- a és g.r..
- M és el $\mathbb{Z}[G_{\mathbb{Q}}]$-submòdul de $J(\overline{\mathbb{Q}})^{tors}$ generat per a.

Clarament, M és finit ($M \subseteq J[m]$ si a és d'ordre m).

Objectiu: I_l actua trivialment en M per a tot primer l. Equivalentment, $a \in J(\mathbb{Q})$.

$l = p$

Pel Resultat 2, M és ordinari semiestable com a $\mathbb{Z}[I_p]$-mòdul. Pel Teorema 3.1.4 (b), M és $I_p(1)$-trivial i, per tant, també ho és el $\mathbf{T}[G_{\mathbb{Q}}]$-mòdul $\mathcal{M}$ generat per a (els elements de $\mathbf{T}$ estan definits sobre $\mathbb{Q}$, i.e., commuten amb els de $G_{\mathbb{Q}}$). Així, I_p actua en $\mathcal{M}$ a través del grup abelià $I_p/I_p(1) \cong (\mathbb{Z}/p\mathbb{Z})^*$. Pel Resultat 3, p ha de ser coprimer amb l'ordre de $\mathcal{M}$ (i de M). Aplicant el Teorema 3.1.4 (a), concloem que I_p actua trivialment en M.

Observació: I_p també actuarà trivialment en $\mathcal{M}$. Pel Resultat 4, $\mathcal{M} \subseteq J[\mathfrak{J}]$. En particular, tot element de $\mathbf{T}$ opera en $\mathcal{M}$ com un enter (per definició de $\mathfrak{J}$) i, per tant, $M = \mathcal{M}$.

$l \nmid n, l \neq p$

Pel Resultat 5, el $\mathbb{Z}[I_l]$-mòdul $J[\mathfrak{J}]$ és ordinari semiestable i, per tant, també ho és el $\mathbb{Z}[I_l]$-submòdul $M \subseteq J[\mathfrak{J}]$. Com que l'exponent de M divideix n i estem en el cas $l \nmid n$, el Teorema 3.1.4 (a) garanteix que I_l actua trivialment en M.

$\boxed{l \mid n}$

En aquest cas, el $\mathbb{Z}[I_l]$-mòdul $J[\mathfrak{J}]$ és ordinari bo pel Resultat 6. Per tant, el $\mathbb{Z}[I_l]$-submòdul $M \subseteq J[\mathfrak{J}]$ també és ordinari bo.

Si $l \geqslant 5$, aleshores M és I_l-trivial pel Teorema 3.1.4 (c).

Si $l \in \{2, 3\}$, distingirem dos casos.

⋆ Cas $g^+ = 0$, i.e. $p \in \{23, 29, 31, 41, 47, 59, 71\}$. Tindrem algun $l \in \{2, 3\}$ tal que $l \mid n$ només si $p = 41$, $l = 2$ (i $n = 10$).

Ja hem comentat que el $\mathbb{Z}[I_2]$-mòdul M és ordinari semiestable (de fet, bo), és a dir, tenim una successió exacta de $\mathbb{Z}[I_2]$-mòduls $0 \to M' \to M \to M'' \to 0$, on M' és I_2-ciclotòmic i M'' és I_2-trivial. En la nostra situació, l'exponent de M' divideix $n = 10$ pel Resultat 1. En particular, aquest exponent no és divisible per 4 i, per tant, l'acció ciclotòmica de $I_2 = I_2(1)$ en M' també és trivial. Així, $(\sigma - 1)^2 M = 0$ per a tot $\sigma \in I_2$. Com que M es pot generar amb punts g.r., raonant com a la demostració del Teorema 3.1.4 (a) concloem que M és I_2-trivial.

⋆ Cas $g^+ > 0$. Provarem directament $P \in \{0, \infty\}$.

Considerem l'aplicació $\pi : X \to X^+ = X/w_p$ i notem $\infty^+ := \pi(0) = \pi(\infty)$ (l'única punta de X^+). Per functorialitat d'Albanese, tenim un morfisme $\pi_* : J \to J^+$ tal que $\pi_* \circ i = i^+ \circ \pi$, on $i^+ : X^+ \to J^+$ denota l'aplicació d'Albanese amb punt base ∞^+. Tenint en compte que i^+ és una immersió (perquè $g^+ > 0$), el que volem veure equival a $i(P) \in \ker(\pi_*)$.

Com que $i(P) \in J[\mathfrak{J}] \subset J[1 + w_p]$, existeix una funció racional $g \in \overline{\mathbb{Q}}(X)$ tal que $(g) = (1 + w_p)((P) - (\infty)) = (P) + (w_p(P)) - (\infty) - (0)$. Per tant, o bé $P \in \{0, \infty\}$ o bé X^+ és hiperel.líptica.

Podem suposar, doncs, que X^+ és hiperel.líptica.

Com que estem en el cas $g^+ > 0$, haurà de ser $p = 37$ (cf. [13]). En particular, $i(P) \in J[\mathfrak{J}] \subset J[n] = J[3]$.

D'altra banda, és clar que $\pi_* \circ (1 + w_p) = 2 \circ \pi_*$. Per tant, $\pi_*(i(P)) \in \pi_*(J[1 + w_p]) \subseteq J^+[2]$.

En conclusió, $i(P) \in \ker(\pi_*)$ tal com volíem.

Comentaris.
1) Al final de la demostració hem vist que $i(X(\overline{\mathbb{Q}})) \cap J[\mathfrak{J}] \subset \ker(\pi_*)$, si $g^+ > 0$. Més generalment, és cert (i també ho és quan $g_+ = 0$) que $J[\mathfrak{J}] \subset \ker(\pi_*)$. Cf. [3, p. 28].
2) Part dels arguments donats només fan servir que a pertany al conjunt $J(\overline{\mathbb{Q}})^{tors}_{g.r.} := \{\text{punts g.r. de } J(\overline{\mathbb{Q}})^{tors}\}$, però no que $a \in i(X(\overline{\mathbb{Q}}))$. Així, per exemple, hem provat que $J(\overline{\mathbb{Q}})^{tors}_{g.r.} \subset J[\mathfrak{J}]$ i que aquest conjunt és I_l-trivial per a tot $l \notin \{2,3\} \cap \{\text{divisors de } n\}$.
De fet, és conegut que $J(\overline{\mathbb{Q}})^{tors}_{g.r.} = C \oplus \Sigma[3]$, on C i Σ són els grups de torsió i de Shimura, respectivament. Cf. [16, Thm. 3]. Això estén un resultat de Mazur [9, Thm. 1], conjecturat per Ogg, que estableix $J(\mathbb{Q})^{tors} = C$.

Bibliografia

[1] *M. Baker*, Torsion points on modular curves, Invent. Math. 140 (2000), num. 3, 487–509.

[2] *M. Baker, B. Poonen*, Torsion packets on curves, Compositio Math. 127 (2001), 109–116.

[3] *M. Baker, K. Ribet*, Galois theory and torsion points on curves, J. Théor. Nombres Bordeaux 15 (2003), num. 1, 11–32.

[4] *R. Coleman, B. Kaskel, K. Ribet*, Torsion points on $X_0(N)$, in Automorphic forms, automorphic representations, and arithmetic (Fort Worth, Texas, 1996), Proc. Sympos. Pure Math. 66, Part 1, Amer. Math. Soc., Providence (1999), 27–49.

[5] *J. Csirik*, The kernel of the Eisenstein ideal, J. Number Theory 92 (2002), num. 2, 348–375.

[6] *V. Drinfel'd*, Two theorems on modular curves, Functional Anal. Appl. 7 (1973), 155–156.

[7] *A. Grothendieck*, Modèles de Néron et monodromie (Exposé IX de SGA 7), LNM 288, Springer, 1972, 313–523.

[8] *S. Lang*, Division points on curves, Ann. Mat. Pura Appl. 70 (1965), 229–234.

[9] *B. Mazur*, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.

[10] *B. Mazur*, Rational isogenies of prime degree, Invent. Math. 44 (1978), 129–162.

[11] *B. Mazur, P. Swinnerton-Dyer*, Arithmetic of Weil curves, Invent. Math. 25 (1974), 1–61.

[12] *M. McQuillan*, Division points on semi-abelian varieties, Invent. Math. 120 (1995), num. 1, 143–159.

[13] *A. Ogg*, Hyperelliptic modular curves, Bull. Soc. Math. France 102 (1974), 449–462.

[14] *B. Poonen*, Computing torsion points on curves, Experiment. Math. 10 (2001), num. 3, 449–465.

[15] *M. Raynaud*, Courbes sur une variété abélienne et points de torsion, Invent. Math. 71 (1983), 207–233.

[16] *K. Ribet, M. Kim*, Torsion points on modular curves and Galois theory, arXiv:math/0305281 (2003).

[17] *K. Ribet*, Torsion points on $J_0(N)$ and Galois representations, in Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math. 1716, Springer, Berlin (1999), 145–166.

[18] *J.-P. Serre*, Œuvres. Collected papers. IV (1985–1998), Springer, 2000.

[19] *A. Tamagawa*, Ramification of torsion points on curves with ordinary semistable Jacobian varieties, Duke Math. J. 106 (2001), 281–319.

[20] *P. Tzermias*, The Manin-Mumford conjecture: a brief survey, Bull. London Math. Soc. 32 (2000), num. 6, 641–652.

[21] *P. Tzermias*, Almost rational torsion points and the cuspidal torsion packet on Fermat quotient curves, Math. Res. Lett. 14 (2007), num. 1, 99–105.

Bernat Plans
Departament de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Av. Diagonal, 647, 08028 Barcelona
bernat.plans@upc.edu

Capítol 4

The Modular Approach to some Generalized Fermat Equations

Nuno Freitas

4.1 Introduction

In the middle of the 17th century, Fermat wrote that for $n \geqslant 3$ the equation $a^n + b^n = c^n$ had no solution in the set of strictly positive integers. This sentence became known as Fermat's Last Theorem (FLT). This problem proved to be unexpectedly difficult and a global solution was not found for 350 years. It was only in the 60's that Hellegouarch noticed that non-trivial solutions of the Fermat equation were related to the existence of torsion points in some elliptic curves. On the other hand in the 50's Taniyama formulated a precise conjecture saying that *All rational elliptic curves arise from modular forms*, and it was only in 1985 that Frey suggested that the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ constructed from a solution of the Fermat equation should not be modular. It was along this ideas and with deep results from Serre, Mazur and Ribet on elliptic curves, Ga-

Under the supervision of Luis Dieulefait

lois representations and modular forms that FLT was reduced to the proof of the Taniyama conjecture. Finally, in 1995 in papers from Wiles and Taylor-Wiles the conjecture was proved for semi-stable elliptic curves, establishing the FLT. Wiles' theorem, now known by Modularity theorem, was improved by Breuil, Conrad, Taylor, and Diamond and states that the Taniyama conjecture is indeed true for all rational elliptic curves.

Among the important consequences of the Modularity theorem and the theory around it is the possibility of using and generalizing some key ideas in the proof of FLT in order to study other Diophantine equations. For example, the generalized Fermat equation $x^p + 2^\alpha y^p = z^p$ has been solved by Ribet, and equations of the form $\phi(x, y) = dz^p$, where ϕ is a degree-3 separable homogeneous form had been extensively studied by Billerey.

The interplay between elliptic curves, modular forms and Galois representations given by the Modularity theorem and the Ribet-Mazur theorem is the central point in the modern strategy to solve Diophantic equations, in particular the FLT. The purpose of this work is to introduce some tools and techniques used to prove the FLT and see how they generalize to other Diophantic equations. Precisely, we study Ribet's paper [6] where he solves the generalized Fermat equation $x^p + 2^\alpha y^p = z^p$.

4.2 Elliptic Curves

In this section we start by recalling some basic facts about Galois representations associated with elliptic curves, then we study some properties of $E_{A,B,C}$ curves and finally we introduce the Tate curve and use it to prove a result due to Hellegouarch.

4.2.1 Galois Representation

Let $\bar{\mathbb{Q}} \subset \mathbb{C}$ be the integral closure of $\mathbb{Q}$. It is known that $\bar{\mathbb{Q}}/\mathbb{Q}$ is a Galois extension and we denote its Galois group by $G_{\mathbb{Q}}$.

Let E be an elliptic curve defined over $\mathbb{Q}$, $n \geqslant 1$ and set $V = E(\bar{\mathbb{Q}})[n]$.

Since V is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2, we see that if P_1, P_2 is a basis of V, we have

$$(\sigma(P_1), \sigma(P_2)) = (P_1, P_2) \begin{bmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{bmatrix}.$$

4.2.1 Theorem *The action of $G_{\mathbb{Q}}$ on $E[n]$ defines a representation*

$$G_{\mathbb{Q}} \xrightarrow{\rho_n} GL_2(\mathbb{Z}/n\mathbb{Z}).$$

The image is isomorphic to the Galois group of the extension: newline $\mathbb{Q}(E[n])/\mathbb{Q}$.

About this representation there are two important theorems due to Serre and Mazur. The version that follows of the theorem from Mazur is simplified and stated as it will be of use later.

4.2.2 Theorem *(Serre) Let E be an elliptic curve defined over $\mathbb{Q}$ which is not isomorphic over $\bar{\mathbb{Q}}$ to any curve having complex multiplication. Then there exists an integer $N \geqslant 1$, depending only on E, such that for every integer n prime to N, the representation ρ_n is surjective.*

4.2.3 Theorem *(Mazur) Let $p \geqslant 5$ be a prime and E a semi-stable elliptic curve over $\mathbb{Q}$. Then, the representation ρ_p as above is irreducible.*

Idea of proof: If ρ_p is reducible, meaning that there exists a subspace invariant for all $\rho_p(\sigma)$, then there exists a subgroup C of order p invariant under $G_{\mathbb{Q}}$. From the semistability hypothesis it is possible to deduce that there exists some curve over $\mathbb{Q}$ isogenous to E with a group of rational points isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2l\mathbb{Z}$. This contradicts a result of Mazur in [4].

□

Now fix a prime l. Considering the action of $G_{\mathbb{Q}}$ on the l^n-torsion for all $n \in \mathbb{N}$ and the asociated representations we can put them together to obtain an action on the Tate module $T_l(E) \cong \mathbb{Z}_l \oplus \mathbb{Z}_l$ and a continuous representation

$$\rho_{E,l} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_l) \subset GL_2(\mathbb{Q}_l).$$

We call $\rho_{E,l}$ the 2-dimensional Galois representation associated to E at l.

4.2.4 Theorem *Let l be a prime and E be an elliptic curve over $\mathbb{Q}$ with conductor N. The Galois representation $\rho_{E,l}$ is unramified at every prime $p \nmid lN$. For any such p let $\mathfrak{p} \subset \bar{\mathbb{Z}}$ be any maximal ideal over p. Then the characteristic equation of $\rho_{E,l}(Frob_{\mathfrak{p}})$ is*

$$x^2 - a_p(E)x + p = 0.$$

The Galois representation $\rho_{E,l}$ is irreducible.

4.2.2 $E_{A,B,C}$ curves

Now we introduce Frey's idea which allowed to relate solutions of the Fermat equation to particular elliptic curves. We want to associate to each point (a, b, c) (with a,b,c relatively prime) on the curve $x^p + y^p = z^p$ a cubic curve $E_{A,B,C}$ such that it is an elliptic curve if and only if the point (a, b, c) is a non-trivial solution ($abc \neq 0$). Going into this direction it is natural to search for curves of the form

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

with the following conditions

$$\beta - \gamma = a^p, \qquad \gamma - \alpha = b^p, \qquad \alpha - \beta = c^p,$$

making the discriminant of the right-hand side is $(abc)^{2p} \neq 0$. Thus, putting $\gamma = 0$ we have

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

More generally, let A, B, C be three relatively prime non-zero integers. We say that the equation $A+B+C = 0$ is an **ABC relation.**

4.2.5 Definition *Given an ABC relation, we set*

$$E_{A,B,C}: \quad y^2 = x(x - A)(x + B)$$

These curves satisfy $\Delta = 2^4(ABC)^2$ and $j(E_{A,B,C}) = 2^8(BC + CA + AB)^3(ABC)^{-2}$. Thus saying that $ABC \neq 0$ is equivalent to saying that $E_{A,B,C}$ is smooth. Also, if we make a circular permutation of (A, B, C), the new curve $E_{B,C,A}$ is isomorphic to $E_{A,B,C}$ over $\mathbb{Q}$. In the case of Fermat equation we have $A = a^p, B = b^p$ and $C = -(a^p + b^p) = -c^p$.

A subset of these curves which is going to be of use in the proof of Fermat's last theorem is that of those curves such that

$$A \equiv 3 \bmod 4 \qquad B \equiv 0 \bmod 32.$$

In this situation the following holds.

4.2.6 Theorem *Let l be a prime.*

1. *If l does not divide ABC, the curve $E_{A,B,C}$ has good reduction modulo l.*
2. *If $l \neq 2$ divides ABC, the reduction of $E_{A,B,C}$ modulo l is a curve of genus zero and multiplicative type.*
3. *If $l = 2$, and if 2 divides ABC, the reduction modulo l of a minimal model of $E_{A,B,C}$ is a curve of genus zero and multiplicative type.*

Proof:(1.)If l does not divide ABC then it does not divide Δ, and the reduced curve modulo l is smooth.

(2.) If an odd prime l divides A or B, the equation of the reduced curve is of the type

$$Y^2 = X^2(X + \tilde{c}), \text{ with } \tilde{c} \in \mathbb{F}_l \text{ different from zero.}$$

Then the tangent lines at $(0, 0)$ are given by

$$Y^2 - \tilde{c}X^2 = (Y - \sqrt{\tilde{c}}X)(Y + \sqrt{\tilde{c}}X).$$

Thus we have distinct tangents over $\bar{\mathbb{F}}_l$ and the reduction is multiplicative. If $l \mid C$ we take a circular permutation and apply the previous case.

(3.) For $l = 2$, we consider the change of variables $X = 4x$ and $Y = 4x + 4y$ leading to the minimal model equation

$$y^2 + xy = x^3 + cx^2 + dx$$

with $c = (B-1-A)/4$ and $d = -AB/16$. It follows that the reduced modulo 2 equation is

$$y^2 + xy = \begin{cases} x^3 \text{ if } A \equiv 7 \bmod 8 \\ x^3 + x^2 \text{ if } A \equiv 3 \bmod 8, \end{cases}$$

Hence we can see that the tangents at $(0, 0)$ are given by

$$\begin{cases} y(x + y) \text{ if } A \equiv 7 \bmod 8 \\ y^2 + xy + x^2 \text{ if } A \equiv 3 \bmod 8, \end{cases}$$

In the first case it is clear that the tangents are distinct; for the second case we need to consider the extension $\mathbb{F}_2[u]$, where u is a root of the polynomial $z^2 - z + 1$, to factorize into two distinct tangents. Hence the reduction is multiplicative.

□

4.2.1 Corol·lari. *When $A \equiv 3$ mod 4 and $B \equiv 0$ mod 32, then $E_{A,B,C}$ is semi-stable and its conductor is $rad(ABC)$, the product of the primes dividing ABC.*

4.2.3 The Tate Curve E_q

To finish with elliptic curves we will introduce two theorems due to Tate. The following theorems are essential in the proof of Hellegouarch Theorem which allow to study the ramification of the Galois representation $\rho_p = \bar{\rho}_{E,p}$, the reduction mod p of the representation in the Tate module at p associated to the curve $E = E_{a^p,b^p,c^p}$.

Let $\mathbb{Q}_p$ be the p-adic integers and $|.|_p$ its p-adic absolute value. It is known that every elliptic curve over $\mathbb{C}$ is of the form $\mathbb{C}/\Lambda$ with Λ a lattice. Although $\mathbb{Q}_p$ is a complete field, a similar result for $\mathbb{Q}_p$ has no chances of success because there are no discrete subgroups in $\mathbb{Q}_p$. However, the multiplicative group $\mathbb{Q}_p^*$ has a lot of discrete subgroups, namely those of the form $q^{\mathbb{Z}}$, for $|q|_p \neq 1$. In fact, Tate has constructed a curve E_q for every $q \in \mathbb{Q}_p^*$ such that $|q|_p < 1$ and achieved to prove an uniformization theorem for all elliptic curves over $\mathbb{Q}_p$ with $|j(E)|_p > 1$. That is the content of the two following theorems.

4.2.7 Theorem *(Tate) Let $q \in \mathbb{Q}_p^*$ satisfy $|q|_p < 1$ and let,*

$$s_k(q) = \sum_{n \geqslant 1} \frac{n^k q^n}{1-q^n}, \qquad a_4(q) = -s_3(q),$$
$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}$$

(a) The series $a_4(q)$ and $a_6(q)$ converge in $\mathbb{Q}_p$ to elements in $\mathbb{Z}_p$ and allow to define the **Tate curve** *E_q over $\mathbb{Q}_p$ by the equation*

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

with discriminant and j-invariant given by

$$\Delta(q) = q\prod_{n \geqslant 1}(1-q^n)^{24} \text{ and } \quad j(E_q) = \frac{1}{q} + 744 + 196884q + \ ...$$

(b) There is an isomorphism $\phi : \bar{\mathbb{Q}}_p^*/\langle q \rangle \xrightarrow{\sim} E_q(\bar{\mathbb{Q}}_p)$ where $\langle q \rangle \subset \mathbb{Q}_p^*$ is the multiplicative subgroup generated by q.

(c) *The map ϕ on (b) is compatible with the action of the Galois group of $\bar{\mathbb{Q}}_p/\mathbb{Q}_p$ in the sense that*

$$\phi(u^\sigma) = \phi(u)^\sigma \text{ for all } u \in \bar{\mathbb{Q}}_p^*,\ \sigma \in G_{\bar{\mathbb{Q}}_p/\mathbb{Q}_p}.$$

In particular, for any algebraic extension L/K ϕ induces an isomorphism

$$\phi : L^*/\langle q \rangle \xrightarrow{\sim} E_q(L)$$

The reduction modulo p of E_q gives the curve

$$\tilde{E}_q : y^2 + xy = x^3$$

and elementary calculus shows that there is a double point at $(0,0)$ and the tangents at this point are $y = 0$ and $x + y = 0$. Thus the Tate curve has multiplicative split reduction at p. Note that $|j(E_q)|_p = 1/|q|_p > 1$ thus the uniformization theorem can not work for curves with $j(E) \in \mathbb{Z}_p$. Fortunately, this is the only constraint.

4.2.8 Theorem *(Tate) Let $E/\mathbb{Q}_p$ be an elliptic curve with $|j(E)|_p > 1$.*

A. *There is a unique $q \in \mathbb{Q}_p^*$ with $|q|_p < 1$ such that E is isomorphic over $\bar{\mathbb{Q}}_p$ to the Tate curve E_q.*

B. *Furthermore, the isomorphism is over $\mathbb{Q}_p$ if and only if E has split multiplicative reduction at p. If E does not have split multiplicative reduction at p then the isomorphism is over a (unique) quadratic extension of $\mathbb{Q}_p$. This quadratic extension is unramified if and only if E has (non-split) multiplicative reduction.*

Let $E = E_{a^p,b^p,c^p}$ be the ABC curve associated to a solution of the Fermat equation with $p \geqslant 5$. As mentioned in the beginning of this section we want to study the ramification of the representation $\bar{\rho}_{E,p}$. We know that if $\rho_{E,p}$ ramifies at l then there is a $\sigma \in I_\mathfrak{l}$ acting non-trivially in $T_p(E)$. As we will see ramification can disappear when reducing mod p. So we do not know if the action of $I_\mathfrak{l}$ on $E[p]$ is non-trivial, that is if $\bar{\rho}_{E,p}$ ramifies at l. The action of $I_\mathfrak{l}$ on $E[p]$ is

non-trivial if and only if the field extension $K_p = \mathbb{Q}(E[p])/\mathbb{Q}$ has non-trivial inertia subgroup at l, that is K_p ramifies at l. Then we want to understand the ramification of the field K_p. Since ramification is a local property we can suppose for each prime l that E is defined over $\mathbb{Q}_l$ and that $K_p = \mathbb{Q}_l(E[p])$. For l dividing abc we prove the following theorem.

4.2.9 Theorem *(Hellegouarch) Let l be a prime dividing abc. Then the field K_p associated to the curve E_{a^p,b^p,c^p} can be considered as a subfield of $\mathbb{Q}_l(\zeta_p, 2^{1/p})$ (or $\mathbb{Q}_l(\beta^{1/2})(\zeta_p, 2^{1/p})$ with $\mathbb{Q}_l(\beta^{1/2})$ unramified).*

Proof: We start by showing that K_p always contain a primitive p-root of unity ζ_p. One can show that $E[p]$ is equipped with the Weil form

$$e_p : E[p] \times E[p] \to \mu_p(\bar{\mathbb{Q}}),$$

where $\mu_p(\bar{\mathbb{Q}})$ are the p-roots of unity. This form turns out to be bilinear, alternating ($e_p(T,T) = 1$), non-degenerate and compatible with the action of $G_{\bar{\mathbb{Q}}/K}$ in the sense that $e_p(S,T)^\sigma = e_p(S^\sigma, T^\sigma)$ for any extension $K/\mathbb{Q}$ and all $\sigma \in G_{\bar{\mathbb{Q}}/K}$. Now, since $E[p] \subset K_p$ we have for each pair of points (S,T)

$$e_p(S,T)^\sigma = e_p(S^\sigma, T^\sigma) = e_p(S,T) \text{ for all } \sigma \in G_{\bar{\mathbb{Q}}/K_p}$$

Hence $e_p(S,T) \in K_p$ thus $\mu_p(\bar{\mathbb{Q}}) \subset K_p$.

Replacing (A,B,C) by (a^p, b^p, c^p) in the formula for the j-invariant of $E_{A,B,C}$ we get that $j = -2^8(a^pc^p + b^pc^p + a^pb^p)^3(abc)^{-2p}$. Recall that $mdc(a,c) = mdc(a,b) = mdc(b,c) = 1$ and let l be a prime dividing abc. Then $\nu_l(j) = -2p\nu_l(abc)$ if $l \neq 2$ and $\nu_l(j) = 8 - 2p\nu_l(abc)$ if $l = 2$. That is, $|j|_l > 1$ for all l if $p \geqslant 5$. From Tate's uniformization theorem and corollary 4.2.1 we know that E_{a^p,b^p,c^p} is equivalent to the curve E_q over the field $\mathbb{Q}_l$ or over an unramified quadratic extension of $\mathbb{Q}_l$.

Now we suppose that the isomorphism is over $\mathbb{Q}_l$ and let $L = \mathbb{Q}_l(\zeta_p, 2^{1/p})$. From Tate's theorem we have $E_q(L)$ isomorphic to $L^*/\langle q \rangle$. Since j is up to an unit a p-th power in L it follows from the discriminant formula of E_q that the same is true for the parameter q. Hence there exists $q' \in L$ such that $q = unit * (q')^p$. Thus, $\langle \zeta_p, q' \rangle / \langle q \rangle$ is

contained in $L^*/\langle q\rangle$. Since $\langle \zeta_p, q'\rangle/\langle q\rangle$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ we conclude that $L^*/\langle q\rangle \sim E_q(L)$ already contains all the p-torsion, implying $K_p \subset L$. In the case that the isomorphism is over the unramified quadratic extension $\mathbb{Q}_l(\beta^2)$ we take $L = \mathbb{Q}_l(\beta^{1/2})(\zeta_p, 2^{1/p})$ and repeat the reasoning.

□

4.2.10 Theorem *(Néron-Ogg-Shafarevich) Let $E/\mathbb{Q}$ be an elliptic curve. E has good reduction at l if and only if $\rho_{E,p}$ is unramified at l for some prime $p \neq l$ if and only if $\rho_{E,p}$ is unramified at l for all primes $p \neq l$.*

4.2.2 Corol·lari. *For $p \geqslant 5$, the representation $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ is unramified outside $2p$.*

Proof: Let $l \neq p$. If $l \nmid abc$ then $l \nmid \Delta$ and E has good reduction at l. By theorem 4.2.10 $\rho_{E,p}$ is unramified at l, hence $\bar{\rho}_{E,p}$ also is. If $l|abc$ then Hellegouarch theorem implies that K_p does not ramify at l if $l \neq 2, p$. Then $\bar{\rho}_{E,p}$ is unramified outside $2p$.

□

4.3 Modular Representations

In this section we recall results about cusp forms and their associated representations and we will also introduce the definition of modular representation.

Let $\mathcal{S}_k(\Gamma_0(N))$ denote the $\mathbb{C}$-vector space of the weight k cusp forms respect to the congruence subgroup $\Gamma_0(N)$. From the theory surrounding the Riemann-Roch theorem it is possible to derive formulas for the dimension of these spaces. An important corollary that will be of use later is the following.

4.3.1 Corol·lari. *$\mathcal{S}_2(\Gamma_0(2^t)) = \{0\}$ for $t \in \{0,1,2,3,4\}$ and $\mathcal{S}_2(\Gamma_0(32))$ has dimension 1.*

Now we will need some notation. Let K be any number field (i.e. a finite extension of $\mathbb{Q}$) and $\mathcal{O}_K$ its ring of integers. Let l be a prime

number and λ any maximal ideal lying over l. Denote by K_λ the λ-adic field obtained by taking fractions of

$$\mathcal{O}_{K,\lambda} = \varprojlim_n \{\mathcal{O}_K/\lambda^n\}.$$

We may view $\mathbb{Z}_l$ as a subring of $\mathcal{O}_{K,\lambda}$ and $\mathbb{Q}_l$ as a subfield K_λ. For a modular form f denote by $\mathbf{K}_f$ the field generated by its Fourier coefficients. It can be shown that $\mathbf{K}_f$ is a number field.

It is possible to construct from the modular curves $X_1(N)$ an abelian variety $J_1(N)$, the **Jacobian** of the modular curve $X_1(N)$. Similarly to what happen with elliptic curves, to the torsion points of $J_1(N)$ there is an associated Galois representation. This representation decomposes into 2-dimensional representations associated to modular forms. The next theorem is a consequence of the mentioned procedure and says that there are Galois representations arising from weight 2 cusp forms.

4.3.1 Theorem *Let $f \in \mathcal{S}_2(\Gamma_0(N))$ be a normalized eigenform with number field $\boldsymbol{K}_f$. Let l be a prime. For each maximal ideal λ of $\mathcal{O}_{\boldsymbol{K}_f}$ lying over l there is a 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} :\to GL_2(\boldsymbol{K}_{f,\lambda}).$$

This representation is unramified at every prime $p \nmid lN$. For any such p let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over p. Then $\rho_{f,\lambda}(Frob_{\mathfrak{p}})$ satisfies the polynomial equation

$$x^2 - a_p x + p = 0.$$

For the converse phenomenon we make the following definition.

4.3.2 Definition *An irreducible Galois representation*

$$\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_l)$$

such that $det\rho = \chi_l$ is ***modular of weight 2*** *if there exists a newform $f \in \mathcal{S}_2(\Gamma_0(M))$ such that $\boldsymbol{K}_{f,\lambda} = \mathbb{Q}_l$ for some maximal ideal λ of $\mathcal{O}_{K_f}$ lying over l and such that $\rho_{f,\lambda} \sim \rho$.*

4.3.2 Remarca. Note that the representations $\rho_{E,l}$ associated to elliptic curves as in chapter 1 are good candidates to be modular.

We can extend this ideas for mod l representations. Let $f \in \mathcal{S}_2(\Gamma_0(M))$ be a newform and let $\lambda \subset \mathcal{O}_{\mathbf{K}_f}$ lie above l. It can be shown that up to similarity we may assume that the representation $\rho_{f,\lambda}$ maps to $GL_2(\mathcal{O}_{K_f,\lambda})$. So it reduces modulo l to a representation

$$\bar{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{K_f,\lambda}/\lambda\mathcal{O}_{K_f,\lambda}).$$

More generally we consider continuous mod l representations $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_l)$. Since $G_{\mathbb{Q}}$ is compact this means that the image is finite and therefore lies in $GL_2(\mathbb{F}_{l^r})$ for some r. The notion of modularity has a mod l analogous.

4.3.3 Definition *An irreducible representation $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_p)$ is* ***modular of weight*** 2 ***and level*** N *if there exists a newform $f \in \mathcal{S}_2(\Gamma_0(N))$ and a maximal ideal $\lambda \subset \mathcal{O}_{\mathbf{K}_f}$ lying over p such that $\bar{\rho}_{f,\lambda} \sim \bar{\rho}$*

4.3.3 Remarca. Also for $f \in \mathcal{S}_k(\Gamma_0(N))$ a normalized eigenform of weight $k > 2$ there is attached to it (by a result of Deligne) a Galois representations where the trace of Frobenius agree with the values $a_p(f)$. Thus, definitions 4.3.2 and 4.3.3 also generalize to any weight $k > 2$.

4.4 The Big Theorems

In this section we present the final ingredients for the study of the Fermat equation: the Modularity theorem and the Mazur-Ribet theorem.

4.4.1 Wiles' Theorem

Wiles proved that every semi-stable elliptic curve over $\mathbb{Q}$ is modular and later the result was generalized for all elliptic curves. This general version of Wiles Theorem is known as Modularity Theorem and there are several equivalent versions of it. Here we will state three versions: the first one is the more arithmetic and the other two use the Galois representations for elliptic curves and Modular forms. The

last version will directly take part in the proof of Fermat last theorem.

Let E be an elliptic curve defined over $\mathbb{Q}$, and let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be a minimal Weirstrass model for E. For a prime p of good reduction, i.e. primes not dividing the conductor of E, we define the quantities

$$a_p(E) := p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

4.4.1 Theorem *(Modularity Theorem, Version a_p) Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then for some newform $f \in \mathcal{S}_2(\Gamma_0(N_E))$,*

$$a_p(f) = a_p(E) \quad \textit{for all primes } p \nmid N_E.$$

4.4.2 Theorem *(Modularity Theorem, Version R) Let E be an elliptic curve over $\mathbb{Q}$. Then $\rho_{E,l}$ is modular for some l.*

4.4.3 Theorem *(Modularity Theorem, strong Version R) Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. Then for some newform $f \in \mathcal{S}_2(\Gamma_0(N))$ with number field $K_f = \mathbb{Q}$,*

$$\rho_{f,l} \sim \rho_{E,l} \textit{ for all } l.$$

4.4.4 Proposition *Let E be an elliptic curve over $\mathbb{Q}$. Then if $\rho_{E,l}$ is modular for some l then $\rho_{E,l}$ is modular for all l.*

4.4.2 Mazur-Ribet's Theorem

The last ingredient for the proof of the FLT is a deep and technical fact about representations. The Ribet-Mazur theorem allows to lower the level of modularity of representations and we will see that this has powerful consequences.

We will call **odd** to a representation ρ such that $\det \rho(conj) = -1$, where *conj* is the complex conjugation. There is a very important conjecture (now is a theorem) regarding modularity of mod l representations due to Serre. In its formulation Serre gives a recipe for obtain a minimal level $N_{\bar{\rho}}$ in terms of the ramification of $\bar{\rho}$.

1 Conjecture *(Serre) Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$ be irreducible and odd. Then $\bar{\rho}$ is modular of level $N_{\bar{\rho}}$ (the* ***Artin conductor of*** *$\bar{\rho}$) and some weight $k \geqslant 2$. For example, a prime $l \neq p$ divides $N_{\bar{\rho}}$ if and only if $\bar{\rho}$ is ramified at p.*

4.4.1 Remarca. For our purposes, we consider the Artin conductor outside of p, that is $p \nmid N_{\bar{\rho}}$.

4.4.5 Theorem *(Mazur-Ribet) Let $p \geqslant 3$ be a prime. Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ be a representation irreducible over $\bar{\mathbb{F}}_p$ and modular of level N.*

If $\bar{\rho}$ is finite at p then we can take N to be the Artin conductor of the representation and $k = 2$. In other words if $\bar{\rho}$ is modular then it is modular of level $N_{\bar{\rho}}$ predicted by Serre and weight 2.

We will not explain the meaning of '$\bar{\rho}$ is finite at p', because it is too technical. For our considerations it is enough to know that for an elliptic curve E, semi-stable at a prime p such that $p|\nu_p(\Delta)$, then the representation $\rho_p : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ is finite at p. Also, if E has good reduction at p then ρ_p is finite at p. The requirement '$\bar{\rho}$ is finite at p' is only needed to remove the prime p from the level of modularity. The other primes can be removed with less hypothesis.

4.5 The Equation $x^p + 2^\alpha y^p = z^p$

In this section we will use all the machinery from the previous sections to study the equation $x^p + 2^\alpha y^p = z^p$. Although the Modularity theorem will be used three times in this chapter, there are weaker results that would be enough for this equations. We first study the case $\alpha = 0$ which only needs Wiles result on semi-stable elliptic curves; then we proceed to the cases $\alpha > 1$ and $\alpha = 1$. For both cases results due to Diamond on the modularity of $E_{A,B,C}$ curves are enough.

4.5.1 Case $\alpha = 0$

Since we are considering $\alpha = 0$ our equation is the Fermat equation. To a solution (a, b, c) of the equation $x^p + y^p = z^p$ we will call it

primitive if a, b, c are relatively prime and *non-trivial* if $(abc \neq 0)$. Now we state and prove Fermat's Last Theorem.

4.5.1 Theorem *(Fermat-Wiles) Let $p \geqslant 5$ be a prime. There are no non-trivial primitive solutions of*

$$x^p + y^p = z^p.$$

Proof: Let (a, b, c) be a non-trivial primitive solution of Fermat's equation for $p \geqslant 5$. Since the solution is primitive it is easy to see that we can suppose that b is even and a, c are odd and also that $a \equiv -1 \pmod 4$ (if $a \equiv 1 \pmod 4$ we take the solution $(-a, -b, -c)$).

Now consider the curve $E = E_{a^p, b^p, c^p}$ (which is semistable by corollary 4.2.1) and the representation $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ induced by the action of $G_{\mathbb{Q}}$ on $E[p]$. The modularity theorem says that $\rho_{E,p}$ must be modular of level N, hence $\bar{\rho}_{E,p}$ is also modular. This representation is irreducible by theorem 4.2.3 and finite at p, hence it satisfies the hypothesis of Mazur-Ribet theorem. Thus we can take N to be the Artin conductor of $\bar{\rho}_{E,p}$. Since $\bar{\rho}_{E,p}$ only ramifies at $2p$ its Artin conductor equals 2. But $\mathcal{S}_2(\Gamma_0(2)) = \{0\}$ by corollary 4.3.1 so $\bar{\rho}_{E,p}$ is not modular and so $\rho_{E,p}$ is not modular, reaching a contradiction.

□

4.5.2 Case $\alpha > 1$

In this section we solve the equation $x^p + 2^\alpha y^p = z^p$ for the cases $\alpha > 1$ but first we make some considerations which are valid also when $\alpha = 1$.

Suppose that (a, b, c) is a solution of $0 = a^p + 2^\alpha b^p + c^p$, then also $a^p + 2^{\alpha - kp}(2^k b)^p + c^p = 0$ thus there exists a solution for an equation with α satisfying $1 \leqslant \alpha < p$. Let $1 \leqslant \alpha < p$. If the solution is primitive, then it is immediate that a and c are odd, meaning that $A = a^p$, $B = 2^\alpha b^p$ and $C = c^p$ are relatively prime. As before we normalize the solutions to $a \equiv -1 \pmod 4$. Because of the normalization we have $A \equiv -1 \equiv 3 \pmod 4$ and B even. Consider

the Frey curve

$$E : y^2 = x(x - A)(x + B),$$

with minimal discriminant of the form $\Delta_E = 2^s(ABC)^2$ by the proof of part 3 of theorem 4.2.6. Looking at the proof of parts 1 and 2 of the same theorem we see that we only needed the hypothesis $A \equiv 3$, hence E is semi-stable at every prime $p \neq 2$. Moreover, calculations show that the conductor N_E of E has the form $2^t rad'(ABC)$ with $t \in \{0, 1, 3, 5\}$, where $rad'(ABC)$ is the product of the odd primes in $rad(ABC)$. Furthermore, 4 divides B if and only if $t \leqslant 3$; E is semi-stable at 2 ($t = 0, 1$) if and only if $16|B$, more precisely from part 3 of theorem 4.2.6 follows that if 32 divides B then the reduction at 2 is multiplicative ($t = 1$); and $t = 5$ if and only if $ord_2(B) = 1$. Now, keeping $p \geqslant 5$ we will use the same ideas of the previous section to prove the following theorem.

4.5.2 Theorem *Let $p \geqslant 5$. The equation $a^p + 2^\alpha b^p + c^p = 0$ has no solutions in nonzero integers a, b, c if $\alpha > 1$.*

Proof: By the modularity theorem $\rho_{E,p}$ is modular of level N_E and so $\bar{\rho}_{E,p}$ is also modular of level N_E. It is not possible to apply theorem 4.2.3, because E is not semi-stable at 2. For this case Ribet achieves to prove irreducibility working with information about the conductor of $\bar{\rho}_{E,p}$ for this specific curve. Since every prime $l \neq 2$ is semi-stable and $\Delta(E)$ is a p-th power times a power of 2, $\bar{\rho}_{E,p}$ is finite at p. Hence, by the Mazur-Ribet theorem, $\bar{\rho}_{E,p}$ is modular of level equal to its Artin conductor. With an argument similar to Hellegouarch it is possible to show that the Artin conductor is 2^t. By corollary 4.3.1 we see that $t = 5$, that is $ord_2(B) = 2$. Since $B = 2^\alpha b^p$ we have a contradiction with $\alpha > 1$.

□

4.5.3 Case $\alpha = 1$

In this section we treat the hardest case, $\alpha = 1$. We say it is the hardest not only because we only cover it for values of $p \equiv 1 \bmod 4$, but also because it makes use of tools that have not been introduced so far. In view of this will only give the guideline of the proof by sating new results at each step. We aim to the following theorem.

4.5.3 Theorem *Let $p \geqslant 17$ and $p \equiv 1$ mod 4. Let (a, b, c) be a solution in non-zero integers of the equation $x^p + 2y^p + z^p = 0$. If (a, b, c) are coprime and we use the normalization $a \equiv -1$ mod 4, then the only possible solution is $(a, b, c) = (-1, 1, -1)$.*

Since (a, b, c) are coprime, it is clear that a and c need to be odd. But it is an immediate corollary of the previous section that b must also be odd.

4.5.1 Corol·lari. *The equation $a^p + 2b^p + c^p = 0$ has no integer solutions with b even.*

Proof: From the proof of theorem 4.5.2 we see that we must have $ord_2(B) = 2$. This is not possible when b is even since $B = 2b^p$.

□

Let E_0 be the elliptic curve associated with the trivial solution $(-1, 1, -1)$ (i.e. the elliptic curve with complex multiplication $y^2 = x^3 - x$) and E the elliptic curve associated to a solution (a, b, c). Let also $\bar{\rho}_{E_0,p}$ and $\bar{\rho}_{E,p}$ be the associated 2-dimensional mod p representations. The following holds.

4.5.4 Proposition *The 2-dimensional mod p representations of $G_{\mathbb{Q}}$ defined by E and E_0 are isomorphic.*

Idea of proof: We have seen in the previous section that $\bar{\rho}_{E,p}$ is associated with a eigenform coming from $\Gamma_0(32)$. This is a one dimensional space, that is $J_0(32)$ is an elliptic curve, hence $\bar{\rho}_{E,p}$ arises from $J_0(32)[p]$. In particular, the isomorphism class of $\bar{\rho}_{E,p}$ does not depend on the solution. Then $\bar{\rho}_{E_0,p} \sim \bar{\rho}_{E,p}$.

□

Now we can use information about the elliptic curve E_0.

4.5.5 Proposition *The image of $\bar{\rho}_{E_0,p}$ is contained in the normalizer of a Cartan subgroup of $GL_2(\mathbb{F}_p)$. If $p \equiv 1$ mod 4 (or $p \equiv -1$ mod 4) then it is the normalizer of a Cartan split (or non-split) subgroup of $GL_2(\mathbb{F}_p)$.*

The next theorem puts strong constraints on the set of primes at which E does not have potential good reduction.

4.5.6 Theorem *(Mazur-Momose) Let $p \geqslant 17$. If the image of $\bar{\rho}_{E,p}$ is contained in the normalizer of a Cartan split subgroup of $GL_2(\mathbb{F}_p)$ then E has potential good reduction at all primes $l \neq 2$.*

Finally, we prove theorem 4.5.3. Since $p \equiv 1 \bmod 4$, from the above propositions we see that $\bar{\rho}_{E,p}$ is under the hypothesis of Mazur-Momose theorem. From the previous section we know that E has multiplicative reduction at all odd primes dividing abc, then it can not have potential good reduction at these primes. Then Mazur-Momose theorem imply that there is no such a prime, hence abc is 2^n with $n \geqslant 0$. Since all of them are odd we must have $n = 0$. Hence the only normalized solution is $(-1, 1, -1)$.

□

4.6 More Equations

In this section, in order to illustrate that the techniques of the previous sections also work with curves that are not ABC we will give two more examples of Diophantine equations. In the examples bellow we will make explicit the associated Frey curve, the discriminant Δ, the conductor N and the Artin conductor N_ρ, but we will not solve the equation.

As we already mentioned, Diamond proved without using the full generality of the Modularity theorem (MT) that the curves $E_{A,B,C}$ are modular. Furthermore, he also proved a weaker version of the MT for curves with restricted ramification. In the first of the following two examples modularity of the Frey curve follows from the work of Diamond, but in the second example the full power of the Modularity theorem is needed. Let (a, b, c) denote a non-trivial primitive solution.

Example 1: The equation $a^p + b^p = c^2$. If ab is even, we can assume $c \equiv 1 \pmod 4$ and consider the elliptic curve

$$y^2 + xy = x^3 + \frac{c-1}{4}x^2 + \frac{a^p}{2^6}x.$$

This curves satisfies

$$\Delta = \frac{1}{2^{12}}(a^2b)^p, \quad N = rad(ab), \quad N_\rho = 2.$$

If ab is odd, we can assume $a \equiv -1 \pmod 4$ and consider

$$y^2 = x^3 + 2cx^2 + a^p x$$

which satisfies

$$\Delta = 2^6(a^2b)^p, \quad N = 2^5 rad(ab), \quad N_\rho = 32.$$

Example 2: The equation $a^p + b^p = c^3$. If ab is even consider

$$y^2 = x^3 - 3(a^p + 9b^p)cx - 2(a^{2p} - 18a^pb^p - 27b^{2p})$$

with discriminant $\Delta = 2^{12}3^3(a^3b)^p$. If $c = 2c_0$ is even let

$$y^2 + b^p y = x^3 - 3(c_0^3 + b^p)c_0 x - c_0^3(2c_0^3 - 5b^p)$$

which have discriminant $\Delta = 3^3(a^3b)^p$. In both cases

$$N = rad(ab), \quad N_\rho = 3 \quad \text{if } 3|ab$$

or

$$N = 3^3 rad(ab), \quad N_\rho = 27 \quad \text{if } 3 \nmid ab.$$

Bibliografia

[1] H Darmon and L. Merel. Winding quotients and some variants of fermat's last theorem. *http://people.math.jussieu.fr/ merel/winding.pdf*.

[2] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Springer, 2005.

[3] Y. Hellegouarch. *Invitation to the Mathmatics of Fermat-Wiles*. Academic Press, 2002.

[4] B. Mazur. Rational isogenies of prime degree. *Invent. Math*, 44:129–162, 1978.

[5] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[6] K. Ribet. On the equations $a^p + 2^\alpha b^p + c^p = 0$. *Acta Arithmetica*, LXXIX.1:7–16, 1997.

[7] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[8] J. H. Silverman. *Advances Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.

Nuno Freitas
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran via de les Corts Catalanes 585, 08007 Barcelona
nunobfreitas@gmail.com

Bibliografia

[1] A. Agashe, K. Ribet, and W. A. Stein. The Manin constant. *Pure Appl. Math. Q.*, 2(2, part 2):617–636, 2006.

[2] M. H. Baker and K. A. Ribet. Galois theory and torsion points on curves. *J. Théor. Nombres Bordeaux*, 15(1):11–32, 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[3] N. Boston, H. W. Lenstra, Jr., and K. A. Ribet. Quotients of group rings arising from two-dimensional representations. *C. R. Acad. Sci. Paris Sér. I Math.*, 312(4):323–328, 1991.

[4] J. Coates, R. Greenberg, K. A. Ribet, and K. Rubin. *Arithmetic theory of elliptic curves*, volume 1716 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1999. Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997, Edited by C. Viola.

[5] R. Coleman, B. Kaskel, and K. A. Ribet. Torsion points on $X_0(N)$. In *Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996)*, volume 66 of *Proc. Sympos. Pure Math.*, pages 27–49. Amer. Math. Soc., Providence, RI, 1999.

[6] P. Deligne and K. A. Ribet. Values of abelian L-functions at negative integers over totally real fields. *Invent. Math.*, 59(3):227–286, 1980.

[7] F. Diamond and K. A. Ribet. l-adic modular deformations and Wiles's "main conjecture". In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 357–371. Springer, New York, 1997.

[8] R. N. Gupta, J. Flowers, and K. A. Ribet. Problems and Solutions: Solutions of Elementary Problems: E2463. *Amer. Math. Monthly*, 82(3):305–307, 1975.

[9] W. R. Hearst III and K. A. Ribet. Book Review: Rational points on elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 30(2):248–252, 1994.

[10] O. Jacquinot and K. A. Ribet. Deficient points on extensions of abelian varieties by $\mathbf{G}_m$. *J. Number Theory*, 25(2):133–151, 1987.

[11] B. Mazur and K. A. Ribet. Two-dimensional representations in the arithmetic of modular curves. *Astérisque*, (196-197):6, 215–255 (1992), 1991. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[12] E. Papier and K. A. Ribet. Eisenstein ideals and λ-adic representations. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):651–665 (1982), 1981.

[13] K. Ribet. *Fonctions L p-adiques et théorie d'Iwasawa*, volume 1 of *Publications Mathématiques d'Orsay 79 [Mathematical Publications of Orsay 79]*. Université de Paris-Sud Département de Mathématique, Orsay, 1979. Course notes by Philippe Satgé.

[14] K. Ribet. Sur les variétés abéliennes à multiplications réelles. *C. R. Acad. Sci. Paris Sér. A-B*, 291(2):A121–A123, 1980.

[15] K. A. Ribet. On the component groups and the Shimura subgroup of $J_0(N)$. In *Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988)*, pages Exp. No. 6, 10. Univ. Bordeaux I, Talence, 19??

[16] K. A. Ribet. Endomorphisms of semi-stable abelian varieties over number fields. *Ann. Math. (2)*, 101:555–562, 1975.

[17] K. A. Ribet. On l-adic representations attached to modular forms. *Invent. Math.*, 28:245–275, 1975.

[18] K. A. Ribet. p-adic interpolation via Hilbert modular forms. In *Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Hum-*

boldt State Univ., Arcata, Calif., 1974), pages 581–592. Amer. Math. Soc., Providence, R. I., 1975.

[19] K. A. Ribet. Dividing rational points on Abelian varieties of CM-type. *Compositio Math.*, 33(1):69–74, 1976.

[20] K. A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[21] K. A. Ribet. A modular construction of unramified p-extensions of$Q(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[22] K. A. Ribet. Galois representations attached to eigenforms with Nebentypus. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 17–51. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[23] K. A. Ribet. p-adic L-functions attached to characters of p-power order. In *Séminaire Delange-Pisot-Poitou, 19e année: 1977/78, Théorie des nombres, Fasc. 1*, pages Exp. No. 9, 8. Secrétariat Math., Paris, 1978.

[24] K. A. Ribet. Sur la recherche des p-extensions non ramifiées de $\mathbf{Q}(\mu_p)$. In *Groupe d'Étude d'Algèbre (Marie-Paule Malliavin), 1re année (1975/76)*, pages Exp. No. 2, 3. Secrétariat Math., Paris, 1978.

[25] K. A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46(4):745–761, 1979.

[26] K. A. Ribet. Report on p-adic L-functions over totally real fields. In *Journées Arithmétiques de Luminy (Colloq. Internat. CNRS, Centre Univ. Luminy, Luminy, 1978)*, volume 61 of *Astérisque*, pages 177–192. Soc. Math. France, Paris, 1979.

[27] K. A. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253(1):43–62, 1980.

[28] K. A. Ribet. Division fields of abelian varieties with complex multiplication. *Mém. Soc. Math. France (N.S.)*, (2):75–94, 1980/81. Abelian functions and transcendental numbers (Colloq., Étole Polytech., Palaiseau, 1979).

[29] K. A. Ribet. Endomorphism algebras of abelian varieties attached to newforms of weight 2. In *Seminar on Number Theory, Paris 1979–80*, volume 12 of *Progr. Math.*, pages 263–276. Birkhäuser Boston, Mass., 1981.

[30] K. A. Ribet. Generalization of a theorem of Tankeev. In *Seminar on Number Theory, 1981/1982*, pages Exp. No. 17, 4. Univ. Bordeaux I, Talence, 1982.

[31] K. A. Ribet. Hodge classes on certain types of abelian varieties. *Amer. J. Math.*, 105(2):523–538, 1983.

[32] K. A. Ribet. Mod p Hecke operators and congruences between modular forms. *Invent. Math.*, 71(1):193–205, 1983.

[33] K. A. Ribet. Congruence relations between modular forms. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, pages 503–514, Warsaw, 1984. PWN.

[34] K. A. Ribet. On l-adic representations attached to modular forms. II. *Glasgow Math. J.*, 27:185–194, 1985.

[35] K. A. Ribet. Cohomological realization of a family of 1-motives. *J. Number Theory*, 25(2):152–161, 1987.

[36] K. A. Ribet. Bimodules and abelian surfaces. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 359–407. Academic Press, Boston, MA, 1989.

[37] K. A. Ribet. Book Review: Abelian l-adic representations and elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 22(1):214–218, 1990.

[38] K. A. Ribet. From the Taniyama-Shimura conjecture to Fermat's last theorem. *Ann. Fac. Sci. Toulouse Math. (5)*, 11(1):116–139, 1990.

[39] K. A. Ribet. Multiplicities of Galois representations in Jacobians of Shimura curves. In *Festschrift in honor of I. I. Piatetski-Shapiro on the occasion of his sixtieth birthday, Part II (Ramat Aviv, 1989)*, volume 3 of *Israel Math. Conf. Proc.*, pages 221–236. Weizmann, Jerusalem, 1990.

[40] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[41] K. A. Ribet. Raising the levels of modular representations. In *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 259–271. Birkhäuser Boston, Boston, MA, 1990.

[42] K. A. Ribet. Lowering the levels of modular representations without multiplicity one. *Internat. Math. Res. Notices*, (2):15–19, 1991.

[43] K. A. Ribet. Multiplicities of p-finite mod p Galois representations in $J_0(Np)$. *Bol. Soc. Brasil. Mat. (N.S.)*, 21(2):177–188, 1991.

[44] K. A. Ribet. The old subvariety of $J_0(pq)$. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 293–307. Birkhäuser Boston, Boston, MA, 1991.

[45] K. A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

[46] K. A. Ribet. *Modular elliptic curves and Fermat's last theorem.* Selected Lectures in Mathematics. American Mathematical Society, Providence, RI, 1993. A lecture presented at George Washington University, Washington, DC, August 1993.

[47] K. A. Ribet. Wiles proves Taniyama's conjecture; Fermat's last theorem follows. *Notices Amer. Math. Soc.*, 40(6):575–576, 1993.

[48] K. A. Ribet. Fields of definition of abelian varieties with real multiplication. In *Arithmetic geometry (Tempe, AZ, 1993)*, volume 174 of *Contemp. Math.*, pages 107–118. Amer. Math. Soc., Providence, RI, 1994.

[49] K. A. Ribet. Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 639–676. Amer. Math. Soc., Providence, RI, 1994.

[50] K. A. Ribet. Wiles proves Taniyama's conjecture; Fermat's last theorem follows *Math. Bohem.*, 119(1):75–78, 1994. Translated from the English by Jan Nekovář.

[51] K. A. Ribet. Galois representations and modular forms. *Bull. Amer. Math. Soc. (N.S.)*, 32(4):375–402, 1995.

[52] K. A. Ribet. Irreducible Galois representations arising from component groups of Jacobians. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 131–147. Int. Press, Cambridge, MA, 1995.

[53] K. A. Ribet. Erratum to: "Galois representations and modular forms" [Bull. Amer. Math. Soc. (N.S.) **32** (1995), no. 4, 375–402; MR1322785 (96b:11073)]. *Bull. Amer. Math. Soc. (N.S.)*, 33(1):43, 1996.

[54] K. A. Ribet. Images of semistable Galois representations. *Pacific J. Math.*, (Special Issue):277–297, 1997. Olga Taussky-Todd: in memoriam.

[55] K. A. Ribet. On the equation $a^p + 2^\alpha b^p + c^p = 0$. *Acta Arith.*, 79(1):7–16, 1997.

[56] K. A. Ribet. Torsion points on $J_0(N)$ and Galois representations. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 145–166. Springer, Berlin, 1999.

[57] K. A. Ribet. Modular forms and Diophantine questions. In *Challenges for the 21st century (Singapore, 2000)*, pages 162–182. World Sci. Publ., River Edge, NJ, 2001.

[58] K. A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004.

[59] K. A. Ribet. Bernoulli numbers and ideal classes. *Gaz. Math.*, (118):42–49, 2008.

[60] K. A. Ribet and W. A. Stein. Lectures on Serre's conjectures. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, volume 9

of *IAS/Park City Math. Ser.*, pages 143–232. Amer. Math. Soc., Providence, RI, 2001.

[61] K. A. Ribet and S. Takahashi. Parametrizations of elliptic curves by Shimura curves and by classical modular curves. *Proc. Nat. Acad. Sci. U.S.A.*, 94(21):11110–11114, 1997. Elliptic curves and modular forms (Washington, DC, 1996).