Variedades de Shimura, formas modulares y puntos racionales

Consejo Superior de Investigaciones Científicas
28 de Junio de 2007

Víctor Rotger
Universitat Politècnica de Catalunya

Sea

$$f = q + \sum_{n \geq 2} a_n q^n \in S_2(N)$$

una forma modular por $\Gamma_0(N)$ de peso 2 y nivel $N \geq 1$.
Asumamos que:

- $T_p(f) = a_p \cdot f$ para $p \nmid N$, $w_p(f) = \pm f$ para $p \mid N$.
- f es *nueva*: ortogonal a toda forma *vieja* $g(dz)$, $g \in S_2(M)$, $M \mid N$, $d \mid \frac{N}{M}$.
- f no tiene multiplicación compleja: No existe ningún caracter $\chi \neq 1$ tal que $\chi(a_p) = a_p$ para $p \nmid N$.

- $E_f = \mathbb{Q}(a_2, a_3, a_4, a_5, ...)$ es un cuerpo de números.
- $F_f = \mathbb{Q}(\{a_2^2, a_3^2, ...)$ es un subcuerpo totalmente real de E_f.
- $B_f = \oplus_\chi E_f \cdot \beta_\chi$ es una álgebra central simple sobre F_f, con E_f como subcuerpo maximal.

Aquí, χ recorre los *inner-twist* de f: caracteres de Dirichlet tales que $\chi(p)a_p = \sigma(a_p)$ para todo $p \nmid N$, para algún $\sigma \in \mathrm{Hom}(E_f, \mathbb{C})$.

CONJETURA: *El número de clases de isomorfismo de álgebras E_f y B_f de grado dado sobre $\mathbb{Q}$ es finito.*

Sea A_f / $\mathbb{Q}$ el factor de $J_0(N)$ asociado a f.

- $\mathrm{End}_{\mathbb{Q}}(A_f)$ es un orden en E_f y $[E_f : \mathbb{Q}] = \dim(A)$.
- $\mathrm{End}_{\bar{\mathbb{Q}}}(A_f)$ es un orden en B_f y $[B_f : \mathbb{Q}] = 2\dim(A)$.

CONJETURA: Sea $g \geq 1$. Existe sólo un número finito de anillos de endomorfismos $\mathrm{End}_K(A)$ de variedades abelianas modulares $A/\mathbb{Q}$ de dimension g.

Aquí, $K/\mathbb{Q}$ es una extensión algebraica arbitraria.

Cuando $g = 1$, $\mathrm{End}_{\bar{\mathbb{Q}}}(A) = \begin{cases} \mathbb{Z} \\ R \subset \mathbb{Q}(\sqrt{-d}), h(R) = 1 \end{cases}$

En $g = 2$: Sea $A = E_1 \times E_2$ con E_1, E_2 curvas elípticas sobre $\mathbb{Q}$.

$$\mathrm{End}_{\mathbb{Q}}(A) = \begin{cases} \mathbb{Z} \times \mathbb{Z} & \text{si } E_1, E_2 \text{ no son isógenas} \\ M_0(N) & \text{si existe una isogenia cíclica de grado } N. \end{cases}$$

Aquí, $M_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}), N \mid c\}$.

Mazur: *Hay un número finito de posibilidades para* $\mathrm{End}_{\mathbb{Q}}(A)$.

OBJETIVO:

Centrarnos en el caso

$$E_f \subsetneq B_f$$

donde B_f es una álgebra de división.

En general, para cualquier $A \overset{\mathbb{Q}}{\sim} A_f$:

$$\mathrm{End}_{\bar{\mathbb{Q}}}(A) \otimes \mathbb{Q} \simeq M_n(B) \text{ donde}$$

- $B = \begin{cases} E \\ \text{Cuaterniones totalmente indefinido sobre } F. \end{cases}$
- A es isógena sobre $\bar{\mathbb{Q}}$ a A_0^n, donde $A_0/\bar{\mathbb{Q}}$ es absolutamente simple y $\mathrm{End}_{\bar{\mathbb{Q}}}(A_0) \otimes \mathbb{Q} \simeq B$: **un building block**.

Recíprocamente, sea $A/\mathbb{Q}$ es una variedad abeliana tal que:

- $\mathrm{End}_{\mathbb{Q}}(A)$ es un orden en un cuerpo de números E de grado $[E:\mathbb{Q}] = \dim(A)$.
- $\mathcal{O} = \mathrm{End}_{\bar{\mathbb{Q}}}(A)$ es un orden en una álgebra de cuaterniones totalmente indefinido sobre F.

Por los trabajos de Khare, Wintenbeger, Dieulefait y Kisin que demuestran la Conjetura de Modularidad de Serre:

$$A \sim A_f \text{ para alguna } f \in S_2(N).$$

Por los trabajos de Ribet,

- Existe un (único) inner-twist no-trivial χ de f.
- $E = F(\sqrt{m})$ para algún $m \in F^* \setminus F^{*2}$ totalmente positivo.
- $\mathcal{O} = \mathrm{End}_K(A)$, donde $K = \bar{\mathbb{Q}}^{\chi} \simeq \mathbb{Q}(\sqrt{-d})$, $d \geq 1$.
- $B \simeq (\frac{-d,m}{F})$.

Sea $\mathfrak{D} = \wp_1 \cdot \ldots \cdot \wp_{2r}$ donde $B \otimes F_{\wp_i} \not\simeq \mathrm{M}_2(F_{\wp_i})$.

Problema. Dados E, B, K, existe una variedad abeliana (modular) $A/\mathbb{Q}$ tal que

- $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q} \simeq E$
- $\mathrm{End}_{K}(A) \otimes \mathbb{Q} \simeq B$?

O una $f \in S_2(N)$ tal que $E \simeq E_f$, $B \simeq B_f$ y $\chi = (\frac{K}{\cdot})$ como inner twist?

Encuesta.

N	$\mathfrak{D}$	m	$\mathrm{disc}(K)$
675	6	2	-3
1568	6	3	-4
243	6	6	-3
2700	10	10	-3
1568	14	7	-4
3969	15	15	-7
5408	22	11	-4

$N \leq 5500,\ F = \mathbb{Q}.$

N	$[F:\mathbb{Q}]$	$\mathrm{disc}(F)$	$\mathfrak{D}$	$\mathrm{N}_{F/\mathbb{Q}}(m)$	$\mathrm{disc}(K)$
1089	2	5	$[9,11]$	11	-3
2592	2	33	$[2,3]$	27	-4
3872	2	5	$[4,11]$	11	-4
3872	2	5	$[4,11]$	55	-4
4356	2	5	$[5,11]$	55	-3
4761	2	41	$[2,5]$	10	-3
2187	3	81	$[3,17]$	51	-3
2187	3	81	$[3,8]$	24	-3
3969	3	321	$[3,3]$	81	-7
4563	3	1436	$[2,3]$	6	-3
3267	4	5725	$[9,11]$	11	-3
3267	4	13525	$[5,9]$	5	-3

$N \leq 5500,\ 2 \leq [F:\mathbb{Q}] \leq 4$ (J. Quer).

Dos puntos de vista:

- Interpretación de móduli: variedades de Shimura.
  - Métodos locales: análisis no-arquimediano en $\wp \mid \mathfrak{D}$.
  - Métodos globales: Descenso.
  - Métodos brutales: Cálculo y inspección de ecuaciones.

- Representaciones de Galois en $T_{\wp}(A)$ en $\wp \mid \mathfrak{D}$.

Variedades de Shimura: Fijemos $\mathcal{O} \subset B$.

- $G = \mathrm{Res}_{F/\mathbb{Q}}(B^*)$ algebraico reductivo sobre $\mathbb{Q}$:

$$G(H) = (B \otimes_{\mathbb{Q}} H)^* \text{ para toda álgebra } H \text{ sobre } \mathbb{Q}.$$

- $G(\mathbb{Q}) = B^*$.
- $G(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{R}) \times \overset{(n)}{\cdots} \times \mathrm{GL}_2(\mathbb{R})$.
- $\hat{\mathcal{O}}^* = \prod_{\wp} \mathcal{O}_{\wp}^* \subset G(\mathbb{A}_f)$, un subgrupo compacto abierto.

Aquí, $n = [F : \mathbb{Q}]$ y $g = [E : \mathbb{Q}] = 2n$.

Definamos la variedad de Shimura

$$X_{\mathcal{O},\mathbb{C}} = G(\mathbb{Q})\backslash\mathcal{H}_{\pm}^{n} \times G(\mathbb{A}_f)/\hat{\mathcal{O}}^{*} = \bigsqcup_{i=1}^{h} \Gamma_i\backslash\mathcal{H}_{\pm}^{n},$$

donde

- $\mathcal{H}_{\pm} = \mathbb{P}^1(\mathbb{C}) \setminus \mathbb{P}^1(\mathbb{R})$.
- $\Gamma_i = \mathcal{O}_i^*$, donde cada $\mathcal{O}_i$ es localmente isomorfo a $\mathcal{O}$.

Sea $X_{\mathcal{O}}$ el modelo canónico de Shimura de $X_{\mathcal{O},\mathbb{C}}$ sobre F.

- Si $F = \mathbb{Q}$ y $\mathcal{O} = \mathrm{M}_0(N) \rightsquigarrow X_0(N)$.
- Si $\mathcal{O} \subseteq B = M_2(F) \rightsquigarrow$ variedad de Hilbert-Blumenthal.
- Si B es una álgebra de cuaterniones de división totalmente indefinida:

$X_{\mathcal{O}}$ es una variedad de Shimura compacta, $\dim(X_{\mathcal{O}}) = [F : \mathbb{Q}]$.

Sea $\mathcal{O} \subset B$ un orden maximal.

$$X_{\mathcal{O}}(\mathbb{C}) = \{(A, \iota)\} / \simeq$$

- A es una variedad abeliana de dimensión $g = 2[F : \mathbb{Q}]$,
- $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$,

Para $K/\mathbb{Q}$, como $X_{\mathcal{O}}$ es sólamente un esquema de móduli *grueso*:

$$X_{\mathcal{O}}(K) \supseteq \{A/K, \iota : \mathcal{O} \hookrightarrow \mathrm{End}_K(A)\}.$$

- Sea $A/\mathbb{Q}$ una variedad abeliana modular con $\mathcal{O} \overset{\iota}{\simeq} \mathrm{End}_K(A) \subset B$:

$$[A, \iota] \in X_{\mathcal{O}}(K).$$

- $R \subset E = F(\omega_m) \subset B$ donde $\omega_m^2 = m$ y $R = E \cap \mathcal{O}$.

- $\omega_m \in B^*$ induce una *involución de Atkin-Lehner* en $X_{\mathcal{O}}$:

$$(A, \iota) \mapsto (A, \omega_m^{-1} \iota \omega_m).$$

- $(A, \iota_{|R}) \in X_{\mathcal{O}}/\langle \omega_m \rangle(\mathbb{Q})$, donde $\iota_{|R} : R \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A)$.

Podemos demostrar que $X_{\mathcal{O}}/\langle\omega_m\rangle(\mathbb{Q}) = \emptyset$?

- (Shimura) $X_{\mathcal{O}}(\mathbb{R}) = \emptyset$.

- (Cerednik, Drinfeld) Cuando $F = \mathbb{Q}$ y $p \mid \mathfrak{D} = (D)$:

$$X_{\mathcal{O}}(\mathbb{C}_p) \simeq \Gamma\backslash(\,\mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p)\,) \text{ donde } \Gamma \subset \mathrm{PSL}_2(\mathbb{Q}_p),$$

$$X_{\mathcal{O}} \mod p \quad \leftrightarrow \quad \Gamma\backslash\mathcal{T}_p,$$

donde $\Gamma = \mathcal{O}'[\frac{1}{p}]_1^*$, $\mathrm{disc}(\mathcal{O}') = D/p$ y $\mathcal{T}_p$ es el árbol de Bruhat-Tits.

- (Zink, Rapoport, Varshavsky) Teoría análoga en dimensión superior.

Cuando $F = \mathbb{Q}$, denotamos X_D en lugar de $X_{\mathcal{O}}$ con $\mathrm{disc}(\mathcal{O}) = (D)$.

- **(R.-Skorobogatov-Yafaev)**
  - $m \mid D$.
  - Si $m \neq D, D/p$, $X_D/\langle\omega_m\rangle(\mathbb{Q}) \subset X_D/\langle\omega_m\rangle(\mathbb{A}) = \emptyset$.
  - $X_D/\langle\omega_D\rangle(\mathbb{Q}_p) \neq \emptyset$ para todo $p \leq \infty$.
  - Criterios explícitos para $X_D/\langle\omega_m\rangle(\mathbb{A}) = \emptyset$, donde $D = pm$ es una factorización con p primo.
- **(R.)** Si $D > 546$, $X_D/\langle\omega_m\rangle(\mathbb{Q})$ es un conjunto finito.

Descenso en $\pi : X_{\mathcal{O}} \to X_{\mathcal{O}}/\langle \omega_m \rangle$.

- Sea $\Delta \in \mathbb{Z}$ el producto de $p \mid \mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(\mathcal{O})) \cdot \mathrm{disc}(F/\mathbb{Q})$.
- $\pi : \mathcal{X}_{\mathcal{O}} \to \mathcal{X}_{\mathcal{O}}/\langle \omega_m \rangle$ extiende a un morfismo liso sobre $\mathbb{Z}[\Delta^{-1}]$.
- Supongamos que mR_f es libre de cuadrados y $\tau(m) > 4$ para algún $\tau : F \hookrightarrow \mathbb{R}$. Entonces π es étale si algún primo $\wp \mid \mathfrak{D}$ descompone en $F(\sqrt{-m})$.
- $X_{\mathcal{O}}/\langle \omega_m \rangle(\mathbb{Q}) = \bigcup_d {}^d\pi({}^dX_{\mathcal{O}}(\mathbb{Q}))$.
- ${}^dX_{\mathcal{O}}$ es el twist cuádratico asociado a $\mathbb{Q}(\sqrt{d})$. Podemos limitarnos a $d < 0$ y no-ramificados fuera de Δ.
- $X_{23\cdot 107}/\langle \omega_{107} \rangle$ viola el principio de Hasse sobre $\mathbb{Q}$.

Métodos brutales: ecuaciones y conteo de puntos.

D	g	X_D	$\omega_p(x,y)$	$\omega_q(x,y)$
6	0	$x^2+y^2+3=0$	$(-x,-y)$	$(\ \ x,-y)$
10	0	$x^2+y^2+2=0$	$(\ \ x,-y)$	$(-x,-y)$
22	0	$x^2+y^2+11=0$	$(-x,-y)$	$(\ \ x,-y)$
14	1	$(x^2-13)^2+7^3+2y^2=0$	$(-x,\ \ y)$	$(-x,-y)$
15	1	$(x^2+3^5)(x^2+3)+3y^2=0$	$(-x,\ \ y)$	$(-x,-y)$
21	1	$x^4-658x^2+7^6+7y^2=0$	$(-x,-y)$	$(-x,\ \ y)$
33	1	$x^4+30x^2+3^8+3y^2=0$	$(-x,\ \ y)$	$(-x,-y)$
34	1	$3x^4-26x^3+53x^2+26x+3+y^2=0$	$(-\frac{1}{x},\frac{y}{x^2})$	$(-\frac{1}{x},\frac{-y}{x^2})$
46	1	$(x^2-45)^2+23+2y^2=0$	$(-x,\ \ y)$	$(-x,-y)$
26	2	$y^2=-2x^6+19x^4-24x^2-169$	$(-x,-y)$	$(-x,\ \ y)$
38	2	$y^2=-16x^6-59x^4-82x^2-19$	$(-x,-y)$	$(-x,\ \ y)$
58	2	$2y^2=-x^6-39x^4-431x^2-841$	$(-x,-y)$	$(\ \ x,-y)$

Sea $Y = X_D/\langle\omega_q\rangle$, donde $D = pq$.

D	$\sharp Y(\mathbb{Q})$	$\sharp\, Y_{CM}(\mathbb{Q})$	$\sharp\{A, i : \mathbb{Q}(\sqrt{q}) \hookrightarrow \mathrm{End}^0(A)\}$
$2 \cdot 3$	∞	1	∞
$2 \cdot 5$	∞	2	∞
$2 \cdot 7$	6	2	4
$2 \cdot 11$	∞	2	∞
$2 \cdot 13$	3	1	0
$2 \cdot 17$	0	0	0
$2 \cdot 19$	3	1	0
$2 \cdot 23$	2	2	0
$2 \cdot 29$	∞	2	> 0
$3 \cdot 5$	4	4	0
$3 \cdot 7$	0	0	0
$3 \cdot 11$	2	2	0

Teorema (González-R.)

Sea $\pi : X_D \to X_D/\langle\omega_m\rangle$ para algún $m \mid D$.
La obstrucción en $\mathrm{Br}(\mathbb{Q})$ para que un punto $P \in X_D/\langle\omega_m\rangle(\mathbb{Q})$ corresponda a

$$(A/\mathbb{Q}, \iota : \mathbb{Z}[\sqrt{q}] \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A))$$

es

$$B \otimes (\frac{-d, m}{\mathbb{Q}}).$$

Aquí, $\pi^{-1}(P) \subset X_D(\,\mathbb{Q}(\sqrt{-d})\,)$.

D	$X_D/\langle\omega_D\rangle$	$X_D/\langle\omega_D\rangle(\mathbb{Q})$
91	$Y^2 = -X^6 + 19X^4 - 3X^2 + 1$	$(0, \pm 1), (\pm 1, \pm 4), (\pm 3, \pm 28)$
123	$Y^2 = -9X^6 + 19X^4 + 5X^2 + 1$	$(0, \pm 1), (\pm 1, \pm 4),$ $(\pm 1/3, \pm \frac{4}{3})$
141	$Y^2 = 27X^6 - 5X^4 - 7X^2 + 1$	$(\pm 1, \pm 4), (\pm \frac{1}{3}, \pm \frac{4}{9}),$ $(0, \pm 1), (\pm \frac{11}{13}, \pm \frac{4012}{2197})$
142	$Y^2 = 16X^6 + 9X^4 - 10X^2 + 1$	$\pm\infty, (0, \pm 1), (\pm 1, \pm 4),$ $(\pm \frac{1}{3}, \pm \frac{4}{27})$
155	$Y^2 = 25X^6 - 19X^4 + 11X^2 - 1$	$\pm\infty, (\pm 1, \pm 4), (\pm \frac{1}{3}, \pm \frac{4}{27})$
158	$Y^2 = -8X^6 + 9X^4 + 14X^2 + 1$	$(\pm 1, \pm 4), (0, \pm 1),$ $(\pm \frac{1}{3}, \pm \frac{44}{27})$
254	$Y^2 = 8X^6 + 25X^4 - 18X^2 + 1$	$(0, \pm 1), (\pm 1, \pm 2), (\pm 2, \pm 29)$
326	$Y^2 = X^6 + 10X^4 - 63X^2 + 4$	$\pm\infty, (0, \pm 2)$
446	$Y^2 = -16X^6 - 7X^4 + 38X^2 + 1$	$(0, \pm 1), (\pm 1, \pm 4)$

Puntos en curvas $X_D/\langle\omega_D\rangle$ de género 2 (Bruin-Flynn-Gonzalez-R.)

Conclusión. Sea $f \in S_2(\Gamma_0(N))$ una forma *nueva* sin CM, con un inner-twist $(\frac{-d}{\cdot})$ tal que $E_f = \mathbb{Q}(\sqrt{m})$ y $\mathrm{disc}(\frac{-d,m}{\mathbb{Q}}) = D > 1$.

- **Métodos locales:** $m \mid D$, $m = D$ o D/p con p primo sujeto a restricciones explícitas dadas por congruencias.
- **Descenso:**
  - $d \mid 2D$
  - $(D, m) \neq (23, 107)$ y ejemplos similares, siempre explicados por la obstrucción de Brauer-Manin.
- **Fuerza bruta:** $(D, m) \neq (91, 91), (123, 123), (155, 155), (158, 158), (326, 326), (446, 446)$.

Teorema (R.)[1] Sea $f \in S_2(N)$ una forma nueva con un inner-twist por $\chi = (\frac{-d}{\cdot})$. Sea $E_f = F_f(\sqrt{m})$ y $\mathfrak{D} = \mathrm{disc}(B_f) \neq (1)$.

(i) $mR_F = \mathfrak{m}_0^2 \cdot \mathfrak{m}$ con $\mathfrak{m} \mid \mathfrak{D}$.

(ii) $\wp \mid p \equiv 3 \bmod 4$ para todo $\wp \mid \mathfrak{D}$, $\wp \nmid m$.

(iii) Asumamos que $\mathfrak{D} \nmid m$ y $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \not\subset F$ para $n \neq 1, 2, 3, 4, 6$.

Para todo ℓ tal que $(\mathfrak{D}, \ell) = 1$, $\sqrt{\ell}$, $\sqrt{2\ell}$, $\sqrt{3\ell}$, $\sqrt{2\ell \pm \sqrt{3\ell}} \notin F$ y $(\frac{K}{\ell}) \neq -1$:

[1] Suponemos por simplicidad que $(\mathfrak{D}, 2) = 1$.

- $(\frac{-\ell}{\wp}) = -1$ para todo $\wp \mid \mathfrak{D}$, o
- $\wp \in \mathcal{P}_\ell$ para todo $\wp \mid \mathfrak{D}$, $\wp \nmid m$, donde

$$\mathcal{P}_\ell = \{\wp : \wp \mid \ell,\ a^2 - s\ell,\ \text{ó}\ a^4 - 4a^2\ell + \ell^2\},$$

para
•$0 \leq s \leq 4$ y
•a$\in R_F \setminus \{0\}$, $|\tau(a)| \leq 2\sqrt{\ell} \quad \forall\, \tau : F \hookrightarrow \mathbb{R}$.

$\mathcal{P}_\ell$ es un conjunto pequeño de primos excepcionales pequeños.
Cuando $F = \mathbb{Q}$,

$$\mathcal{P}_2 = \{2, 3, 5, 7\}\ \text{y}\ \mathcal{P}_3 = \{2, 3, 5, 11, 23\}.$$

Teorema. Sea $F_f = \mathbb{Q}$, $E_f = \mathbb{Q}(\sqrt{m})$, $\chi = (\frac{-d}{\cdot})$ y $D = \operatorname{disc}(\frac{-d,m}{\mathbb{Q}}) = pm$ con p, m primos impares. Entonces

(i) $p \equiv 3 \bmod 4$ y $(\frac{-p}{m}) = -1$.

(ii) Si $m \equiv 3 \bmod 4$, entonces $d = p$ y $(\frac{-\ell}{m}) = -1$ para todo $\ell \neq 2$ tal que $(\frac{\ell}{p}) = 1$ y $p \notin \mathcal{P}_\ell$.

(iii) Si $m \equiv 1 \bmod 4$, entonces $d = p$ o pm.

- Si $d = p$, entonces $(\frac{-\ell}{p}) = -1$ para todo ℓ tal que $(\frac{\ell}{p}) = 1$ y $p \notin \mathcal{P}_\ell$.
- Si $d = pm$, entonces $p \equiv 3 \bmod 8$ y $p \in \mathcal{P}_\ell$ para todo primo $\ell \neq 2$ tal que $(\frac{-pm}{\ell}) = 1$.

Idea de la demostración.

La filosofía de la prueba de Fermat es:

- Sea (a, b, c) una solución de $X^p + Y^p = Z^p$, p primo, $p \geq 5$, b par, $a \equiv 3 \bmod 4$.
- Sea $A : y^2 = x(x - a^p)(x + b^p)$. la curva elíptica de Frey.
- Sea $r_\ell : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(A[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$.

Y vemos que tal representación no puede existir.

- Sea $A_f/\mathbb{Q}$ la variedad abeliana asociada a f
- $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(A_f) \simeq E_f$.
- $r_\wp : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(\, T_\wp(A_f)) \simeq \mathrm{GL}_2(E_{f,\wp})$ con $\wp \mid \mathfrak{D}$, $\wp \nmid 2m$.
- Sea ℓ tal que $\sqrt{\ell}$, $\sqrt{2\ell}$, $\sqrt{3\ell}$, $\sqrt{2\ell \pm \sqrt{3}\ell} \notin F$, $(\frac{K}{\ell}) \neq -1$, $\wp \notin \mathcal{P}_\ell$.

Queremos demostrar que $(\frac{-\ell}{\mathfrak{q}}) = -1$ para todo $\mathfrak{q} \mid \mathfrak{D}$.

- $A_f/\mathbb{Q}$ tiene buena reducción potencial en ℓ :

  $\rightsquigarrow\ \tilde{A}_f/\,\mathbb{F}_\ell$.

- $P_{\varphi_\ell} = T^2 - a_\ell T + \ell,\ a_\ell \in R_F,\ |\tau(a_\ell)| \leq 2\sqrt{\ell}$.

Lema. Existe un caracter $\alpha_\wp : G_\mathbb{Q} \longrightarrow k_\wp^* = \mathbb{F}_q^*$ tal que

$$\bar{r}_\wp : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(k_\wp), \qquad \bar{r}_\wp = \begin{pmatrix} \chi \cdot \alpha_\wp^q & 0 \\ * & \alpha_\wp \end{pmatrix}.$$

Idea: $\alpha_\wp$ es la restricción de $\bar{r}_\wp$ a un cierto $A_f[I_\wp] \subset A_f[\wp] \subset A[p]$.

Corolario. $a_\ell \bmod \wp = \alpha_\wp(\varphi_\ell) + \ell\alpha_\wp(\varphi_\ell^{-1})$.

Proposición. Existe un entero par κ tal que $\alpha_\wp(\varphi_\ell^\kappa) = \ell^{\kappa/2} \in \mathbb{F}_p^*$.

- Si $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \not\subset F$ para $n = 5$ y $n \geq 7$, $\kappa = 24$.

Idea: Para $\ell \neq p$, $\alpha_\wp(I_\ell)^{24} = \{1\}$.

Corolario. $a_\ell \bmod \wp = \sqrt{\ell} \cdot (\zeta + \zeta^{-1})$, $\zeta^{24} = 1$.

- Puesto que $\wp \notin \mathcal{P}_\ell$: $\quad a_\ell = \sqrt{\ell} \cdot (\zeta + \zeta^{-1}) = 0.$
- Puesto que $(\frac{K}{\ell}) = -1$, la teoría de Honda-Tate:
  $B = \mathbb{Q} \otimes \mathrm{End}_K(A) \hookrightarrow \mathbb{Q} \otimes \mathrm{End}_{\mathbb{F}_\ell}(\tilde{A}) = \mathrm{M}_{2n}(\mathbb{Q}(\sqrt{-\ell}))$.
- B actua $F_\mathfrak{q}(\sqrt{-\ell})$-linealmente en $T_\mathfrak{q}(A) = T_\mathfrak{q}(\tilde{A})$.
- Como $\dim_{F_\mathfrak{q}(\sqrt{-\ell})} T_\mathfrak{q}(A) = 2$, $B \subset M_2(F_\mathfrak{q}(\sqrt{-\ell}))$.
- $B \otimes F_\mathfrak{q}$ es álgebra de division $\quad \Rightarrow \quad B \otimes F_\mathfrak{q} \not\simeq \mathrm{M}_2(F_\mathfrak{q})$
  $\Rightarrow \quad \mathfrak{q}$ es inerte en $F(\sqrt{-\ell})$.

Proyecto (con Luis García):

- Formas modulares p-ádicas en $X_{\mathcal{O}}$ para $p \mid \mathfrak{D}$ se construyen como integrales de distribuciones en $\mathbb{P}^1(\mathbb{Q}_p)$ contra un núcleo de Poisson.

- Investigar esta construcción en relación con los haces canónicos de $X_{\mathcal{O}}$, la conjetura de Birch y Swinnerton-Dyer p-ádica, ...