Modular endomorphism algebras

Modular forms: Arithmetic and Computation
June 3-8, 2007

Víctor Rotger
Universitat Politècnica de Catalunya

Let

$$f = q + \sum_{n \geq 2} a_n q^n$$

be a (non-CM) newform for $\Gamma_1(N)$ of weight two and character ε.

- $E_f = \mathbb{Q}(a_2, a_3, a_4, a_5, \ldots)$, a number field.
- $F_f = \mathbb{Q}(\{a_p^2/\varepsilon(p)\} : p \nmid N)$, a totally real subfield of E_f.
- $B_f = \oplus E_f \cdot \beta_\chi$ where χ are the inner-twists of f, a central simple algebra over F_f, with E_f as maximal subfield.

A Dirichlet character χ is an *inner-twist* of f if $\chi(p)a_p = \sigma(a_p)$ for all $p \nmid N$, for some $\sigma \in \mathrm{Hom}(E_f, \mathbb{C})$.

CONJECTURE: *There exist only finitely many isomorphism classes of algebras E_f and B_f of given degree over $\mathbb{Q}$.*

Let $A_f\,/\,\mathbb{Q}$ be the factor of $J_1(N)$ attached to f.

- $\mathrm{End}_{\mathbb{Q}}(A_f)$ is an order in E_f.
- $\mathrm{End}_{\bar{\mathbb{Q}}}(A_f)$ is an order in B_f.

CONJECTURE: For any $g \geq 1$, there exist only finitely many isomorphism classes of endomorphism rings $\mathrm{End}_K(A)$ of modular abelian varieties $A/\mathbb{Q}$ of dimension g.

Here, $K/\mathbb{Q}$ is an arbitrary algebraic extension.

For $g = 1$, $\mathrm{End}_{\bar{\mathbb{Q}}}(A) = \mathbb{Z}$ or $R \subset \mathbb{Q}(\sqrt{-d})$, $h(R) = 1$.

In $g = 2$: Let $A = E_1 \times E_2$ with E_1, E_2 elliptic curves over $\mathbb{Q}$.

$$\mathrm{End}_{\mathbb{Q}}(A) = \begin{cases} \mathbb{Z} \times \mathbb{Z} & \text{if } E_1, E_2 \text{ are not isogenous} \\ M_0(N) & \text{if there is a cyclic isogeny of degree } N. \end{cases}$$

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

Mazur: *There are finitely many possibilities for* $\mathrm{End}_{\mathbb{Q}}(A)$.

Let $E \,/\, K$ be a $\mathbb{Q}$-curve completely defined over a quadratic $K/\mathbb{Q}$.
Let $A = \mathrm{Res}_{K/\mathbb{Q}}(E)$.

$$\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{\pm d}),\ d = d(E) = \min(\deg \Phi : E^{\sigma} \to E).$$

Conjecture: *$d(E) \leq C$ for some constant $C \geq 1$.*

AIM:

Focus on the case

$$E_f \subsetneq B_f$$

where B_f is a division algebra.

For a general newform $f \in S_2(\Gamma_1(N))$ without CM
(or an abelian variety A of GL_2-type over $\mathbb{Q}$ without CM):

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

- $B = E$ or a totally indefinite quaternion algebra over F.
- A is isogenous over $\bar{\mathbb{Q}}$ to A_0^n, where $A_0/\bar{\mathbb{Q}}$ is absolutely simple and $\mathrm{End}_{\bar{\mathbb{Q}}}(A_0) \otimes \mathbb{Q} \simeq B$: **a building block**.

We thus focus on abelian varieties
A of GL_2-type over $\mathbb{Q}$ such that:

- $\mathcal{O} = \mathrm{End}_{\bar{\mathbb{Q}}}(A)$ is an order in a totally indefinite division quaternion algebra B over F

By the work of Khare, Wintenbeger and Kisin proving Serre's modularity Conjecture:

$$A \sim A_f \text{ for some newform } f \in S_2\left(\Gamma_1(N)\right),\ N \geq 1.$$

By the work of Ribet,

- There exists a (single) non-trivial inner-twist χ of f.
- $\varepsilon = 1$ and $E = F(\sqrt{m})$ for $m \in F^* \setminus F^{*2}$ totally positive.
- $\mathcal{O} = \mathrm{End}_K(A)$, where $K = \bar{\mathbb{Q}}^{\chi} \simeq \mathbb{Q}(\sqrt{-d})$, $d \geq 1$.
- $B \simeq (\frac{-d,m}{F})$. Set $\mathfrak{D} = \wp_1 \cdot \ldots \cdot \wp_{2r}$ where $B \otimes F_{\wp_i} \not\simeq \mathrm{M}_2(F_{\wp_i})$.

Question. Given E, B, K, does there exist a modular abelian variety $A/\mathbb{Q}$ such that

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

Or a normalized newform $f \in S_2(\Gamma_1(N))$ with $E \simeq E_f$, $B \simeq B_f$ and $\chi = (\frac{K}{})$ as inner twist?

Numerical data

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

Data for $N \leq 5500$ and $F = \mathbb{Q}$.

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

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

Two approaches:

- Moduli interpretation in terms of Shimura varieties.
  - Local methods: rigid analytic uniformization at $\wp \mid \mathfrak{D}$.
  - Global methods: Descent.
  - Brute force: Computation of equations.

- Galois representation on $T_{\wp}(A)$ for some $\wp \mid \mathfrak{D}$.

Shimura varieties: Fix $\mathcal{O} \subset B$.

- $G = \mathrm{Res}_{F/\mathbb{Q}}(B^*)$ reductive algebraic over $\mathbb{Q}$:

$$G(H) = (B \otimes_{\mathbb{Q}} H)^* \text{ for any algebra } H \text{ over } \mathbb{Q}.$$

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

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

Define the Shimura variety

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

where

- $\mathcal{H}_{\pm} = \mathbb{P}^1(\mathbb{C}) \setminus \mathbb{P}^1(\mathbb{R})$.
- $\Gamma_i = \mathcal{O}_i^{*}$, where each $\mathcal{O}_i$ is locally isomorphic to $\mathcal{O}$.

Let $X_{\mathcal{O}}$ be Shimura's canonical model of $X_{\mathcal{O},\mathbb{C}}$ over F.

- If $F = \mathbb{Q}$ and $\mathcal{O} = \mathrm{M}_0(N) \rightsquigarrow X_0(N)$.
- If $\mathcal{O} \subseteq B = M_2(F) \rightsquigarrow$ Hilbert-Blumenthal variety.
- If B is a division totally indefinite quaternion algebra:

$$X_{\mathcal{O}} \text{ is a compact Shimura variety, } \dim(X_{\mathcal{O}}) = [F : \mathbb{Q}].$$

Let $\mathcal{O} \subset B$ be a maximal order.

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

- A is an abelian variety of dimension $g = 2[F : \mathbb{Q}]$,
- $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$,

For $K/\mathbb{Q}$, since $X_{\mathcal{O}}$ is only a *coarse* moduli scheme:

$$X_{\mathcal{O}}(K) = \{ [A, \iota] \}, \ K = \text{field of moduli of } (A, \iota).$$

- Let $A/\mathbb{Q}$ be a modular abelian variety with $\mathcal{O} \stackrel{\iota}{\simeq} \mathrm{End}_K(A) \subset B$:

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

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

- $\omega_m \in B^*$ induces an *Atkin-Lehner involution* on $X_{\mathcal{O}}$:

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

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

Can we prove $X_{\mathcal{O}}/\langle\omega_m\rangle(\mathbb{Q}) = \emptyset$?

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

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

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

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

where $\Gamma = \mathcal{O}'[\frac{1}{p}]^*_1$, $\mathrm{disc}(\mathcal{O}') = D/p$ and $\mathcal{T}_p$ is Bruhat-Tits tree.

- (Zink, Rapoport, Varshavsky) Higher-dimensional analogue.

When $F = \mathbb{Q}$, write X_D for $X_{\mathcal{O}}$ with $\mathrm{disc}(\mathcal{O}) = (D)$.

- **(R.-Skorobogatov-Yafaev)**
  - $m \mid D$.
  - If $m \neq D, D/p$, $X_D/\langle\omega_m\rangle(\mathbb{Q}) \subset X_D/\langle\omega_m\rangle(\mathbb{A}) = \emptyset$.
  - $X_D/\langle\omega_D\rangle(\mathbb{Q}_p) \neq \emptyset$ for all $p \leq \infty$.
  - Explicit criteria for $X_D/\langle\omega_m\rangle(\mathbb{A}) = \emptyset$, where $D = pm$ is any factorization with p prime.
- **(R.)** If $D > 546$, $X_D/\langle\omega_m\rangle(\mathbb{Q})$ is a finite set.

Descent on $\pi: X_{\mathcal{O}} \to X_{\mathcal{O}}/\langle\omega_m\rangle$.

- Let $\Delta \in \mathbb{Z}$ be the product of $p \mid \mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(\mathcal{O})) \cdot \mathrm{disc}(F/\mathbb{Q})$.

- $\pi : \mathcal{X}_{\mathcal{O}} \to \mathcal{X}_{\mathcal{O}}/\langle\omega_m\rangle$ extends to a smooth morphism over $\mathbb{Z}[\Delta^{-1}]$.

- Assume mR_f is square-free and $\tau(m) > 4$ for some $\tau : F \hookrightarrow \mathbb{R}$. Then π is étale if some prime $\wp \mid \mathfrak{D}$ splits in $F(\sqrt{-m})$.

- $X_{\mathcal{O}}/\langle\omega_m\rangle\,(\mathbb{Q}) = \bigcup_d {}^d\pi\,({}^dX_{\mathcal{O}}(\mathbb{Q}))$.

- ${}^dX_{\mathcal{O}}$ is the quadratic twist associated with $\mathbb{Q}(\sqrt{d})$. It suffices to take $d < 0$ and unramified away from Δ.

- $X_{23\cdot 107}/\langle\omega_{107}\rangle$ violates the Hasse principle over $\mathbb{Q}$.

Explicit approaches: equations and point-counting.

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	$2y^2=-x^6-39x^4-431x^2-841$	$(-x,-y)$	$(x,-y)$

Write $Y = X_D/\langle \omega_q \rangle$ for $D = pq$.

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

Theorem. Let $\pi : X_D \to X_D/\langle \omega_m \rangle$ for some $m \mid D$.
The obstruction in $\mathrm{Br}(\mathbb{Q})$ for a point $P \in X_D/\langle \omega_m \rangle(\mathbb{Q})$ to correspond to

$$(A, i : \mathbb{Q}(\sqrt{q}) \hookrightarrow \mathrm{End}^0(A))$$

is

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

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

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	$Y^2 = -16X^6 - 7X^4 + 38X^2 + 1$	$(0,\pm 1), (\pm 1, \pm 4)$

Rational points on genus 2 curves $X_D/\langle\omega_D\rangle$ (Bruin-Flynn-Gonzalez-R.)

Conclusion. Let $f \in S_2(\Gamma_1(N))$ be a non-CM newform with an inner-twist $(\frac{-d}{\cdot})$ such that $E_f = \mathbb{Q}(\sqrt{m})$ and $\mathrm{disc}(\frac{-d,m}{\mathbb{Q}}) = D > 1$.

- **Local methods:** $m \mid D$, $m = D$ or D/p with p prime satisfying explicit congruence conditions.
- **Descent:**
  - $d \mid 2D$
  - $(D, m) \neq (23, 107)$ and similar examples, always explained by the Brauer-Manin obstruction.
- **Brute force:** $(D, m) \neq (91, 91), (123, 123), (155, 155),$ $(158, 158)$, $(326, 326)$, $(446, 446)$.

Main Theorem (R.) Let $f \in S_2(\Gamma_1(N))$ be a newform with an inner-twist by $\chi = (\frac{-d}{\cdot})$. Let $E_f = F_f(\sqrt{m})$ and $\mathfrak{D} = \mathrm{disc}(B_f)$.

Assume B_f is division[1].

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

(ii) $\wp \mid p \equiv 3 \bmod 4$ for any $\wp \mid \mathfrak{D}$, $\wp \nmid 2m$.

(iii) Assume $\mathfrak{D} \nmid 2m$ and $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \not\subset F$ for $n \neq 1, 2, 3, 4, 6$. For any ℓ such that $\sqrt{\ell}$, $\sqrt{2\ell}$, $\sqrt{3\ell}$, $\sqrt{2\ell \pm \sqrt{3}\ell} \notin F$ and $(\frac{K}{\ell}) \neq -1$, either

[1] We also assume that we can choose A_f in its $\mathbb{Q}$-isogeny class such that $\mathcal{O} = \mathrm{End}_K(A)$ is maximal in B_f. See the preprint for a more general version.

- $\left(\frac{-\ell}{\wp}\right) \neq 1$ for all $\wp \mid \mathfrak{D}$, or
- $\wp \in \mathcal{P}_\ell$ for all $\wp \mid \mathfrak{D}$, $\wp \nmid 2m$, where

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

for $0 \leq s \leq 4$ and $a \in R_F$, $a \neq \sqrt{s\ell}$, $|\tau(a)| \leq 2\sqrt{\ell} \quad \forall \tau : F \hookrightarrow \mathbb{R}$.

The set $\mathcal{P}_\ell$ is meant to be a small set of small exceptional primes. When $F = \mathbb{Q}$,

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

Theorem. Let $F_f = \mathbb{Q}$, $E_f = \mathbb{Q}(\sqrt{m})$, $\chi = (\frac{-d}{})$ and $D = \mathrm{disc}(\frac{-d,m}{\mathbb{Q}}) = pm$ with p, m odd primes. Then

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

(ii) If $m \equiv 3 \bmod 4$, then $d = p$ and $(\frac{-\ell}{m}) = -1$ for any odd ℓ such that $(\frac{\ell}{p}) = 1$ and $p \notin \mathcal{P}_\ell$.

(iii) If $m \equiv 1 \bmod 4$, then $d = p$ or pm.

- If $d = p$, then $(\frac{-\ell}{p}) = -1$ provided $(\frac{\ell}{p}) = 1$ and $p \notin \mathcal{P}_\ell$.
- If $d = pm$, then $p \equiv 3 \bmod 8$ and $p \in \mathcal{P}_\ell$ for any odd prime ℓ such that $(\frac{-pm}{\ell}) = 1$.

Idea of the proof. Let $r_\wp : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(E_\wp)$ at $\wp \mid \mathfrak{D}$, $\wp \nmid 2m$.

- $A_f/\mathbb{Q}$ has potential good reduction at any $\ell \overset{S-T}{\rightsquigarrow} \tilde{A}_f/\mathbb{F}_\ell$.
- $P_{\varphi_\ell} = T^2 - a_\ell T + \ell$, $a_\ell \in R_E$, $|\tau(a_\ell)| \leq 2\sqrt{\ell}$ for any $\tau : E \hookrightarrow \mathbb{R}$.

Lemma. There is a character $\alpha_\wp : G_\mathbb{Q} \longrightarrow k_\wp^* = \mathbb{F}_q^*$ such that

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

Idea: $\alpha_\wp$ is the restriction of $\bar{r}_\wp$ to certain $A_f[I_\wp] \subset A_f[\wp] \subset A[p]$.

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

Proposition. There is an even positive integer κ such that $\alpha_\wp(\varphi_\ell^\kappa) = \ell^{\kappa/2} \in \mathbb{F}_p^*$ for $\ell \neq p$.

- $\kappa = \kappa(F)$, but can be made smaller for given B_f or $(f, \wp)$.
- If $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \not\subset F$ for $n = 5$ and $n \geq 7$, $\kappa = 24$.

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

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

We defined the finite set $\mathcal{P}_\ell$ so that

$$a_\ell = \sqrt{\ell} \cdot (\zeta + \zeta^{-1}) = 0, \sqrt{\ell},\ \sqrt{2\ell}, \sqrt{3\ell},\ 2\sqrt{\ell} \in F.$$

- Because $(\frac{K}{\ell}) = -1$, $\mathbb{Q} \otimes \mathrm{End}_K(A) \hookrightarrow \mathbb{Q} \otimes \mathrm{End}_{\mathbb{F}_\ell}(\tilde{A}) = \mathrm{M}_{2r}(\tilde{F})$.

- $\tilde{F} = \mathbb{Q}(\sqrt{-\ell})$, $\mathbb{Q}(\sqrt{\ell},\ \sqrt{-3})$, $\mathbb{Q}(\sqrt{2\ell},\ \sqrt{-1})$, $\mathbb{Q}(\sqrt{3\ell}, \sqrt{-3})$ and $r = 2[F : \mathbb{Q}]/[\tilde{F} : \mathbb{Q}]$, by Honda-Tate.

Lemma. $F \cdot \tilde{F}$ splits B, that is, no prime $\wp \mid \mathfrak{D}$ splits in $F \cdot \tilde{F}/F$.

Idea. B acts $F\tilde{F} \otimes \mathbb{Q}_p$-linearly on $V_p(A)$, because
$B \subset \mathbb{Q} \otimes \mathrm{End}_{\mathbb{F}_\ell}(\tilde{A})$, whose center is $\tilde{F}$.
Since $\dim_{F\tilde{F}\otimes\mathbb{Q}_p} V_p(A) = 2$, $B \subset M_2(F\tilde{F} \otimes \mathbb{Q}_p)$.

This proves the Main Theorem.