Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 86 (2011)

Artikel: Modular elliptic directions with complex multiplication (with an application to Gross's elliptic curves)

Autor: González, Josep / Lario, Joan-C.

DOI: https://doi.org/10.5169/seals-283452

Comment. Math. Helv. 86 (2011), 317–351
DOI 10.4171/CMH/225

Commentarii Mathematici Helvetici

Modular elliptic directions with complex multiplication (with an application to Gross's elliptic curves)

Josep González and Joan-C. Lario*

Abstract. Let A_f be the abelian variety attached by Shimura to a normalized newform $f \in S_2(\Gamma_1(N))$ and assume that A_f has elliptic quotients. The paper deals with the determination of the one dimensional subspaces (elliptic directions) in $S_2(\Gamma_1(N))$ corresponding to the pullbacks of the regular differentials of all elliptic quotients of A_f. For modular elliptic curves over number fields without complex multiplication (CM), the directions were studied by the authors in [8]. The main goal of the present paper is to characterize the directions corresponding to elliptic curves with CM. Then we apply the results obtained to the case $N = p^2$, for primes $p > 3$ and $p \equiv 3 \bmod 4$. For this case we prove that if f has CM, then all optimal elliptic quotients of A_f are also optimal in the sense that its endomorphism ring is the maximal order of $\mathbb{Q}(\sqrt{-p})$. Moreover, if f has trivial Nebentypus then all optimal quotients are Gross's elliptic curve $A(p)$ and its Galois conjugates. Among all modular parametrizations $J_0(p^2) \to A(p)$, we describe a canonical one and discuss some of its properties.

Mathematics Subject Classification (2010). 11G18, 14K22, 11R37, 11F11.

Keywords. Modular abelian varieties, complex multiplication, Grössencharacter, optimal elliptic quotient.

1. Introduction

Let $\mathbb{Q}^{\text{alg}}$ be a fixed algebraic closure of $\mathbb{Q}$. An elliptic curve C defined over $\mathbb{Q}^{\text{alg}}$ is said to be modular if there is a non-constant homomorphism $\pi\colon J_1(N) \to C$, where $J_1(N)$ denotes the jacobian of the modular curve $X_1(N)$. Every modular elliptic curve over $\mathbb{Q}^{\text{alg}}$ is a quotient of some modular abelian variety A_f attached by Shimura to a normalized newform f. From now on, we shall always consider parametrizations $\pi\colon J_1(N) \to C$ which factorize through such abelian varieties A_f, called in this paper modular abelian varieties of *elliptic type*.

A modular parametrization $\pi\colon J_1(N) \to C$ defined over a number field $L \subseteq \mathbb{Q}^{\text{alg}}$ induces an injection $\pi^*\colon \Omega^1(C_{/L}) \hookrightarrow \Omega^1(J_1(N)_{/L})$. In what follows, we shall

*The first author is partially supported by DGICYT Grant BFM MTM2009-13060-C02-02, and the second author by DGICYT Grant BFM MTM2009-13060-C02-01.

identify $\Omega^1(J_1(N)_{/L})$ with the subspace of cusp forms in $S_2(\Gamma_1(N))$ whose q-expansion lies in $L[[q]]$, via $h\, dq/q \mapsto h$ where $q = \exp(2\pi i z)$.

The determination of the normalized cusp forms in $S_2(\Gamma_1(N))$ associated with the pullbacks $\pi^*(\Omega^1(C))$ was discussed by the authors in [8] for elliptic curves without complex multiplication. In this paper, we shall deal with the complex multiplication case that needs techniques *ad hoc*. The present case is substantially richer since it requires the intervention of class field theory as well as the main theorem of complex multiplication.

Shimura shows in [16] that all elliptic curves with complex multiplication (CM) are modular. Due to Ribet [12], we know that A_f has an elliptic quotient with CM by an imaginary quadratic field $K \subset \mathbb{Q}^{\mathrm{alg}}$ if and only if $f = f \otimes \chi$, where χ is the quadratic Dirichlet character attached to K. In this case, there is a primitive Hecke character $\psi\colon I(\mathfrak{m}) \to \mathbb{Q}^{\mathrm{alg}}$ of conductor an ideal $\mathfrak{m}$ of K such that the q-expansion of the CM normalized newform f is given by

$$f = \sum_{(\mathfrak{a},\mathfrak{m})=1} \psi(\mathfrak{a}) q^{\mathrm{N}(\mathfrak{a})} = \sum_{n=1}^{\infty} a_n q^n .$$

Here, $I(\mathfrak{m})$ denotes the multiplicative group of fractional ideals of K relatively prime to $\mathfrak{m}$, and the first summation is over integral ideals. The level of f is $N = \mathrm{N}(\mathfrak{m})\,|\Delta_K|$, the norm of $\mathfrak{m}$ times the absolute value of the discriminant of K. We consider the number fields $E_f = \mathbb{Q}(\{a_n\})$ and $E = \mathbb{Q}(\{\psi(\mathfrak{a})\})$, generated by the images of ψ. One has $E = E_f \cdot K$, and we shall denote by Φ the set of its K-embeddings $E \hookrightarrow \mathbb{Q}^{\mathrm{alg}}$. The number field E is a CM field. Through the paper, for all CM fields we shall denote by bar $\bar{\ }$ the canonical complex conjugation.

For future use, we recall that an abelian variety Y is called an optimal quotient of an abelian variety X over a field k if there is a surjective morphism $\pi\colon X \to Y$ defined over k whose kernel is an abelian variety. In this case, every endomorphism of X which leaves stable $\ker \pi$ induces an endomorphism of Y. The property of being an optimal quotient is transitive. Hereafter, every A_f is taken to be an optimal quotient of $J_1(N)$.

The plan of the paper is as follows. In Section 2, we study the decomposition of A_f over the quadratic field K for f with CM as before. This is an intermediate step necessary to determine the elliptic directions we are interested in. We shall prove

Theorem 1.1. *Let $f \in S_2(\Gamma_1(N))$ be a newform with CM and keep the above notations. There is an abelian variety (A,ι) of CM type Φ defined over K, with $\iota\colon E \hookrightarrow \mathrm{End}^0_K(A)$, satisfying the following properties:*

(i) *A is an optimal quotient of A_f over K and the pullback of $\Omega^1(A)$ corresponds with the subspace generated by $\{{}^{\sigma}f : \sigma \in \Phi\}$;*

(ii) *$\iota(\psi(\mathfrak{a}))^*({}^{\sigma}f) = {}^{\sigma}\psi(\mathfrak{a}){}^{\sigma}f$, for all $\mathfrak{a} \in I(\mathfrak{m})$ and $\sigma \in \Phi$;*

(iii) *ι is an isomorphism;*

(iv) *if $\mathfrak{p}$ is a prime ideal of K with $\mathfrak{p} \nmid N$, then the lifting of the Frobenius endomorphism acting on the reduction of A mod $\mathfrak{p}$ is $\iota(\psi(\mathfrak{p}))$ or $\iota(\overline{\psi(\bar{\mathfrak{p}})})$ depending on $K \not\subseteq E_f$ or $K \subseteq E_f$, respectively.*

We remark that the above abelian variety A is simple over K, and that A is A_f over K when $K \not\subseteq E_f$, while A_f is isogenous over K to $A \times \bar{A}$ when $K \subseteq E_f$. To encode both cases of part (iv) in Theorem 1.1, we shall denote by ψ' the primitive Hecke character mod $\bar{\mathfrak{m}}$ defined as

$$\psi'(\mathfrak{a}) = \begin{cases} \psi(\mathfrak{a}) & \text{if } K \not\subseteq E_f; \\ \overline{\psi(\bar{\mathfrak{a}})} & \text{if } K \subseteq E_f. \end{cases}$$

As it will be shown, one has $\mathfrak{m} = \bar{\mathfrak{m}}$ in the first case.

Then we study the splitting field of A; that is, the smallest number field where all endomorphisms of A are defined. We make use of class field theory to build a certain abelian extension L/K attached to the Hecke character ψ'; the field L is a cyclic extension of the Hilbert class field of K and it is contained in the ray class field mod $\bar{\mathfrak{m}}$. To simplify notation, the Artin automorphism $\left(\frac{L/K}{\mathfrak{a}}\right)$ in $\mathrm{Gal}(L/K)$ will be often denoted by the same symbol representing the ideal $\mathfrak{a}$. In particular, one has

$$^{\mathfrak{p}}\beta \equiv \beta^{\mathrm{N}(\mathfrak{p})} \pmod{\mathfrak{P}}$$

for all $\beta \in \mathcal{O}_L$, where $\mathfrak{P}$ is an unramified prime ideal of L over a prime ideal $\mathfrak{p}$ of K. The extension L/K is characterized by the property that $\mathfrak{a}$ viewed in $\mathrm{Gal}(L/K)$ is trivial if and only if $\psi'(\mathfrak{a}) \in K^*$. The main result of Section 3 is the following

Theorem 1.2. *Let A be as above. Then the following holds:*

(i) *There is an elliptic curve C defined over L with complex multiplication by the ring of integers $\mathcal{O}_K$ and such that A is isogenous over L to $C^{\dim A}$.*

(ii) *The field L is the smallest number field satisfying* $\mathrm{End}^0_{\mathbb{Q}^{\mathrm{alg}}}(A) = \mathrm{End}^0_L(A)$.

(iii) *There is a one-cocycle $\lambda\colon I(\bar{\mathfrak{m}}) \to L^*$ satisfying $\lambda(\mathfrak{a}) = \psi'(\mathfrak{a})$ for all $\mathfrak{a} \in I(\bar{\mathfrak{m}})$ with $\left(\frac{L/K}{\mathfrak{a}}\right) = \mathrm{id}$ in $\mathrm{Gal}(L/K)$. The class of λ in $H^1(I(\bar{\mathfrak{m}}), L^*)$ is uniquely determined by this condition.*

In view of (iii), the cohomology class of λ depends intrinsically on A, and we shall denote it by $[A] \in H^1(I(\bar{\mathfrak{m}}), L^*)$. Section 4 is devoted to determining the elliptic directions in $\Omega^1(A)$ in terms of $[A]$. To this end, for each one-cocycle $\lambda \in [A]$ and $\sigma \in \Phi$, we introduce the sums

$$g_\sigma(\lambda) := \sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} \frac{^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})}{^{\sigma}\psi'(\mathfrak{a})} \in {}^{\sigma}E \cdot L,$$

and also its Φ-trace

$$\operatorname{tr}_\Phi(\lambda) := \sum_{\sigma\in\Phi} g_\sigma(\lambda) \in L.$$

Theorem 1.3. *With the above notations, the following holds.*

(1) *If* $\sum_{n\geq 1} \gamma_n q^n \in S_2(\Gamma_1(N))$ *corresponds to an elliptic direction attached to a modular parametrization* $\pi \in \operatorname{Hom}_L(A, C)$, *then* $\gamma_1 \neq 0$.

(2) *The following statements are equivalent:*

(i) *the normalized cusp form*

$$h = q + \sum_{n\geq 2} \gamma_n q^n \in S_2(\Gamma_1(N))$$

gives an elliptic direction attached to some $\pi \in \operatorname{Hom}_L(A, C)$;

(ii) *there is a one-cocycle* $\lambda \in [A]$ *with* $\operatorname{tr}_\Phi(\lambda) = [L\colon K]$ *and such that*

$$h = \frac{1}{[L:K]} \sum_{\sigma\in\Phi} g_\sigma(\lambda)\cdot {}^\sigma f.$$

The q*-expansion of this elliptic direction is then given by*

$$h = \begin{cases} \displaystyle\sum_{(\mathfrak{a},\mathfrak{m})=1} {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})\, q^{\mathrm{N}(\mathfrak{a})} & \textit{if } K \not\subseteq E_f; \\ \displaystyle\sum_{(\mathfrak{a},\mathfrak{m})=1} \frac{\mathrm{N}(\mathfrak{a})}{\lambda(\bar{\mathfrak{a}})}\, q^{\mathrm{N}(\mathfrak{a})} & \textit{if } K \subseteq E_f. \end{cases}$$

Moreover, all other elliptic directions are $\iota(a)^*(h)$, *for* $a \in E^*$, *and the equality* $\iota(\psi'(\mathfrak{a}))^* h = {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})^{\mathfrak{a}^{-1}} h$ *holds for every* $\mathfrak{a} \in I(\bar{\mathfrak{m}})$.

We shall say that a one-cocycle $\lambda \in [A]$ is *modular* if one has $\operatorname{tr}_\Phi(\lambda) = [L\colon K]$. According to Theorem 1.3, these are precisely the one-cocycles that provide the elliptic directions. In Section 3, we also describe how to obtain all modular one-cocycles in $[A]$ explicitly way by means of a K-linear projector, and close the section by raising some open questions.

In the last three sections, we deal with the particular case concerning the level $N = p^2$ where $p > 3$ is a prime with $p \equiv 3 \bmod 4$. The relevance of this case is in connection with the elliptic curves $A(p)$ studied by Gross in [9] and [10]. For convenience of the reader, we recall here its definition. Let $K = \mathbb{Q}(\sqrt{-p})$ and let $\mathcal{O}_K$ be its ring of integers. Let H denote the Hilbert class field of K, and let

$H_0 = \mathbb{Q}(j(\mathcal{O}_K))$ be its maximal real subfield. The elliptic curve $A(p)$ is defined over H_0 and given by the Weierstrass equation

$$y^2 = x^3 + \frac{mp}{2^4 \cdot 3} x - \frac{np^2}{2^5 \cdot 3^3},$$

where m and n are the real numbers satisfying

$$m^3 = j(\mathcal{O}_K), \quad n^2 = \frac{j(\mathcal{O}_K) - 1728}{-p}, \quad \operatorname{sgn} n = \left(\frac{2}{p}\right).$$

The elliptic curve $A(p)$ admits a global minimal model over H_0 with discriminant $-p^3$ and whose invariants are $c_4 = -mp$ and $c_6 = np^2$.

Given any intermediate modular subgroup Γ between $\Gamma_1(p^2)$ and $\Gamma_0(p^2)$ and a normalized newform $f \in S_2(\Gamma)$, we denote by $A_f^{(\Gamma)}$ its associated optimal quotient of $\operatorname{Jac}(X_\Gamma)$, where X_Γ denotes the modular curve over $\mathbb{Q}$ attached to Γ. According to this terminology, we have $A_f^{(\Gamma_1(p^2))} = A_f$. In Section 5, we prove:

Theorem 1.4. *With the above notations, the following holds.*

(i) *For every positive divisor d of $(p-1)/2$ there is a unique abelian variety A_f of CM elliptic type in $J_1(p^2)$ such that the Nebentypus of f has order d; one has $K \not\subseteq E_f$, $\dim A_f = [H : K]\varphi(d)$, where φ is the Euler function, and the splitting field of A_f is the intermediate field between H and $H \cdot \mathbb{Q}(e^{2\pi i/p})$ of degree d.*

(ii) *Let f be a CM normalized newform in $S_2(\Gamma_1(p^2))$ and let Γ satisfy*

$$\Gamma_1(p^2) \subseteq \Gamma \subseteq \Gamma_\varepsilon := \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^2) \colon \varepsilon(d) = 1\right\},$$

where ε is the Nebentypus of f. Then all optimal elliptic quotients of $A_f^{(\Gamma)}$ have complex multiplication by $\mathcal{O}_K$. Moreover, if f belongs to $S_2(\Gamma_0(p^2))$, then all optimal quotients of $A_f^{(\Gamma)}$ are defined over H and are precisely the elliptic curve $A(p)$ and its Galois conjugates.

Among all modular parametrizations $J_0(p^2) \to A(p)$ one stands out. In Section 6, we discuss this canonical parametrization and give some of its arithmetical properties.

Theorem 1.5. *Set $\mathfrak{p} = \sqrt{-p}\,\mathcal{O}_K$. Let $\delta \colon I(\mathfrak{p}) \to H$ be the unique map defined by the conditions $\delta(\mathfrak{a})^{12} = \Delta(\mathcal{O}_K)/\Delta(\mathfrak{a})$ and $\left(\frac{\mathrm{N}_{H/K}(\delta(\mathfrak{a}))}{\mathfrak{p}}\right) = 1$. Let ω denote a Néron differential of $A(p)$, and let ψ be any Hecke character attached to $A(p)$. Then:*

(i) *There is an optimal quotient* $\pi\colon J_0(p^2)\to A(p)$ *such that* $\pi^*(\omega)=c\,g(q)\,dq/q$ *where the elliptic direction is given by*

$$g(q)=\sum_{(\mathfrak{a},\mathfrak{p})=1}\delta(\mathfrak{a})q^{\mathrm{N}(\mathfrak{a})}\in S_2(\Gamma_0(p^2)),$$

and $c\in\mathbb{Z}$ *is a unit in* $\mathbb{Z}[\frac{1}{2p}]$.

(ii) *The complex lattice* $\{2\pi\, i\int_\gamma g(z)dz\colon\gamma\in H_1(X_0(p^2),\mathbb{Z})\}$ *is*

$$\frac{1}{c}\cdot i^{(p+1)/4}\cdot\sqrt[h]{\rho\cdot(2\pi)^{(2h+1-p)/4}\cdot\sqrt{p}^{(1-3h)/2}\cdot\prod_{\substack{1\le m<p\\ \chi(m)=1}}\Gamma\Big(\frac{m}{p}\Big)}\cdot\mathcal{O}_K$$

where h *is the class number of* K*, the* h*-th root is taken to be real,* Γ *is the Gamma function, and* $\rho=\prod_{\mathfrak{a}\in\mathrm{Gal}(H/K)}\frac{\delta(\mathfrak{a})}{\psi(\mathfrak{a})}$ *is a positive unit of* H_0.

Finally, in Section 7 we discuss how to compute the modular elliptic directions for A_f when $f\in S_2(\Gamma_1(p^2))$ has CM and its Nebentypus is nontrivial.

2. The abelian variety A

We shall adhere to the notations in the Introduction and prove Theorem 1.1. Let $\psi\colon I(\mathfrak{m})\to\mathbb{Q}^{\mathrm{alg}}$ be the fixed primitive Hecke character, and let

$$f=\sum_{(\mathfrak{a},\mathfrak{m})=1}\psi(\mathfrak{a})q^{\mathrm{N}(\mathfrak{a})}=\sum_{n=1}^{\infty}a_nq^n$$

be its associated CM newform in $S_2(\Gamma_1(N))$. The optimal quotient A_f of $J_1(N)$ is defined over $\mathbb{Q}$ by $A_f=J_1(N)/I_f(J_1(N))$, where $I_f(J_1(N)$ is the annihilator of f in the Hecke algebra acting on $J_1(N)$. In particular, the pullback of $\Omega^1(A_{f\,/\mathbb{Q}^{\mathrm{alg}}})$ is $\langle\{^\sigma f\}\rangle$ where σ runs over $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$. Recall that $E_f=\mathbb{Q}(\{a_n\})$ and $E=\mathbb{Q}(\{\psi(\mathfrak{a})\})$. We fix an isomorphism

$$\iota\colon E_f\hookrightarrow\mathrm{End}^0_{\mathbb{Q}}(A_f),$$

in such a way that $\iota(a_n)$ corresponds to the Hecke operator T_n acting on A_f. The Nebentypus of f is the mod N Dirichlet character $\varepsilon(d)=\chi(d)\psi((d))/d$, where χ is the quadratic character attached to K. We recall that $\iota(\varepsilon(d))$ is the diamond operator $\langle d\rangle$ acting on A_f. One has

$$\dim A_f=[E_f:\mathbb{Q}]=\begin{cases}[E:K] & \text{if } K\not\subseteq E_f;\\ 2[E:K] & \text{if } K\subseteq E_f.\end{cases}$$

Notice that $E = K \cdot E_f$. Now, we proceed to construct the abelian variety A over K of dimension $[E : K]$ with the properties required in Theorem 1.1. According to Shimura's Proposition 8 in [17], there exists $u \in \operatorname{End}^0_K(A_f)$ such that

$$u^*({}^{\sigma} f) = \sqrt{\Delta_K} \cdot {}^{\sigma} f$$

for all σ in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$. Here, the choice of the square root $\sqrt{\Delta_K}$ fixes u up to a sign. For the case $K \not\subseteq E_f$, we let $A = A_f$ and extend ι to E,

$$\iota\colon E \hookrightarrow \operatorname{End}^0_K(A_f),$$

via $\iota(\sqrt{\Delta_K}) = u$. For the second case, we proceed as follows. Since now $K \subseteq E_f$, there is $\alpha \in E_f$ such that $\iota(\alpha) \in \operatorname{End}^0_{\mathbb{Q}}(A_f)$ acts as

$$\iota(\alpha)^*({}^{\sigma} f) = {}^{\sigma}\sqrt{\Delta_K} \cdot {}^{\sigma} f$$

for all σ in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$. Then consider the involution $w := \iota(\alpha)u^{-1} \in \operatorname{End}^0_K(A_f)$. Let A be the optimal quotient of $J_1(N)$ defined by A_f/B, where $B = (1-w)A_f$. Clearly, the abelian variety A is defined over K, and $\Omega^1(A_{/K})$ is identified with $\langle {}^{\sigma} f\rangle_{\sigma\in\Phi}$. Since B is stable by $\iota(E)$, the isomorphism $\iota\colon E \hookrightarrow \operatorname{End}^0_{\mathbb{Q}}(A_f)$ induces in a natural way an embedding still denoted by the same letter

$$\iota\colon E \hookrightarrow \operatorname{End}^0_K(A)$$

such that $\iota(\gamma)^*({}^{\sigma} f) = {}^{\sigma}\gamma \cdot {}^{\sigma} f$ for all γ in E and all K-embeddings σ in Φ. From the equality $\bar{w} = -w$, it follows that $\bar{B} = (1+w)A_f$. Note that $\bar{B}$ is K-isogenous to A.

A case-by-case argument, employing that $\operatorname{End}^0_K(X) \hookrightarrow \operatorname{End}^0_{\mathbb{Q}}(\mathrm{Res}_{K/\mathbb{Q}}(X))$ for any abelian variety $X_{/K}$, shows that the abelian variety A is K-simple in both cases. Therefore, it follows that ι is an isomorphism. In both cases, A is an abelian variety of CM type Φ and satisfies (i), (ii), and (iii) of Theorem 1.1.

To conclude the proof, it remains to check the property (iv) relative to the Frobenius liftings. To this end, let p be a prime such that $p \nmid N$ and denote by Frob_p and Ver_p the Frobenius and the Verschiebung acting on the reduction of A_f modulo p, which satisfy $\mathrm{Frob}_p \cdot \mathrm{Ver}_p = p$. By the Eichler–Shimura congruence, we know that

$$\widetilde{T_p} = \mathrm{Frob}_p + \mathrm{Ver}_p \cdot \widetilde{\langle p\rangle},$$

where $\widetilde{T_p}$ and $\widetilde{\langle p\rangle}$ denote the reductions of the Hecke operator T_p and the diamond operator $\langle p\rangle$ acting on A_f mod p. Let us consider the two cases separately.

Case $K \not\subseteq E_f$: first, assume that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ splits in K. Since

$$\iota(a_p) = \iota(\psi(\mathfrak{p})) + \iota(\psi(\bar{\mathfrak{p}})), \quad \iota(\psi(\mathfrak{p})) \cdot \iota(\psi(\bar{\mathfrak{p}})) = p\,\langle p\rangle,$$

and $\widetilde{T_p} = \widetilde{\iota(a_p)}$, it follows that the lifting of Frob_p is either $\iota(\psi(\mathfrak{p}))$ or $\iota(\psi(\bar{\mathfrak{p}}))$. Since a certain power of $\psi(\mathfrak{p})$ belongs to $\mathfrak{p}$, one concludes that the lifting of $\mathrm{Frob}_{\mathfrak{p}} = \mathrm{Frob}_p$ is $\iota(\psi(\mathfrak{p}))$. A similar argument works when $p\mathcal{O}_K = \mathfrak{p}$ is inert in K, taking into account that $\mathrm{Frob}_{\mathfrak{p}} = \mathrm{Frob}_p^2 = -p\,\widetilde{\langle p\rangle} = \widetilde{\iota(\psi((p)))}$.

Case $K \subseteq E_f$: since $\iota(E)$ leaves the abelian subvariety B stable, applying the same arguments as before, it follows that $\iota(\psi(\mathfrak{p}))$ is the lifting of $\mathrm{Frob}_{\mathfrak{p}}$ acting on the reduction of B mod $\mathfrak{p}$. Since A is K-isogenous to $\overline{B}$, the statement (iv) holds in this case as well. This completes the proof of Theorem 1.1.

The following lemma will be used in the next sections.

Lemma 2.1. *If $K \not\subseteq E_f$, then* $\mathfrak{m} = \bar{\mathfrak{m}}$.

Proof. Since $K \not\subseteq E_f$, there is σ in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/K)$ such that ${}^\sigma f = \bar{f}$. First, we prove that the Hecke characters ${}^\sigma\psi$ and ψ_c given by ${}^\sigma\psi(\mathfrak{a}) = {}^\sigma(\psi(\mathfrak{a}))$ and $\psi_c(\mathfrak{a}) = \overline{\psi(\bar{\mathfrak{a}})}$ coincide on $I(\mathfrak{m}\,\bar{\mathfrak{m}})$. Indeed, since ${}^\sigma\varepsilon = \varepsilon^{-1}$ the assertion is immediate for prime ideals $\mathfrak{p} \mid p$ when p is inert. For the case that p splits completely in K, from the equalities ${}^\sigma a_p = \overline{a_p}$ and ${}^\sigma\varepsilon(p) = \varepsilon^{-1}(p)$, that is,

$$ {}^\sigma\psi(\mathfrak{p}) + {}^\sigma\psi(\bar{\mathfrak{p}}) = \psi_c(\mathfrak{p}) + \psi_c(\bar{\mathfrak{p}}) \quad \text{and} \quad {}^\sigma\psi(\mathfrak{p}) \cdot {}^\sigma\psi(\bar{\mathfrak{p}}) = \psi_c(\mathfrak{p}) \cdot \psi_c(\bar{\mathfrak{p}}), $$

it follows that ${}^\sigma\psi(\mathfrak{p})$ is either $\psi_c(\mathfrak{p})$ or $\psi_c(\bar{\mathfrak{p}})$. Again, we obtain that ${}^\sigma\psi(\mathfrak{p})$ and $\psi_c(\mathfrak{p})$ are equal because a certain power of them lie in $\mathfrak{p}$. Both Hecke characters being primitive of conductor $\mathfrak{m}$ and $\bar{\mathfrak{m}}$ respectively, we must have $\mathfrak{m} = \bar{\mathfrak{m}}$. □

3. Splitting field of A

We first introduce an abelian extension L/K that will play a key role in the splitting of the abelian variety A over $\mathbb{Q}^{\mathrm{alg}}$. Let ψ' be the primitive Hecke character mod $\bar{\mathfrak{m}}$,

$$ \psi'\colon I(\bar{\mathfrak{m}}) \to \mathbb{Q}^{\mathrm{alg}}, $$

given by $\psi'(\mathfrak{a}) = \psi(\mathfrak{a})$ if $K \not\subseteq E_f$ or $\psi'(\mathfrak{a}) = \overline{\psi(\bar{\mathfrak{a}})}$ otherwise. We consider the character $\eta\colon (\mathcal{O}_K/\bar{\mathfrak{m}})^* \to \mathbb{Q}^{\mathrm{alg}}$ defined by

$$ \eta(a) = \frac{\psi'((a))}{a}, \qquad \text{for all } a \in \mathcal{O}_K \text{ with } (a, \bar{\mathfrak{m}}) = 1. $$

One easily checks that η is well defined. Recall that the existence of a Hecke character mod $\bar{\mathfrak{m}}$ is equivalent to the condition that the composition $\mathcal{O}_K^* \hookrightarrow \mathcal{O}_K \to \mathcal{O}_K/\bar{\mathfrak{m}}$ is a group monomorphism (see [16]) and thus $\ker \eta \cap \mathcal{O}_K^* = \{1\}$. By class field theory, to the congruence subgroup

$$ P_\eta(\bar{\mathfrak{m}}) = \{(a) \in I(\bar{\mathfrak{m}})\colon\ a \bmod \bar{\mathfrak{m}} \in \ker(\eta)\} $$

there corresponds an abelian extension L/K. It is easy to check that, for $\mathfrak{a} \in I(\bar{\mathfrak{m}})$, one has $\mathfrak{a} \in P_\eta(\bar{\mathfrak{m}})$ if and only if $\psi'(\mathfrak{a}) \in K$. Let $K_{\bar{\mathfrak{m}}}$ denote the ray class field of K mod $\bar{\mathfrak{m}}$. Since the map $a \mapsto a\mathcal{O}_K$ provides an isomorphism between $\ker \eta$ and $P_\eta(\bar{\mathfrak{m}})/P_1(\bar{\mathfrak{m}})$, by using the exact sequence

$$1 \to \mathcal{O}_K^* \to (\mathcal{O}_K/\bar{\mathfrak{m}})^* \to I(\bar{\mathfrak{m}})/P_1(\bar{\mathfrak{m}}) \to I(\mathcal{O}_K)/P(\mathcal{O}_K) \to 1,$$

one readily shows that $L = K_{\bar{\mathfrak{m}}}^{\ker \eta}$ and $\mathrm{Gal}(L/H)$ is isomorphic to the cyclic group $\mathrm{im}(\eta)/\mathcal{O}_K^*$. Recall that here H denotes the Hilbert class field of K and, as usual, for any integral ideal $\mathfrak{n}$ we denote by $P(\mathfrak{n})$ the subgroup of $I(\mathfrak{n})$ formed by principal ideals and the subscript 1 is for the subgroup of principal ideals with a generator congruent to one mod $\mathfrak{n}$. An alternate route to define the extension L/K is as follows. For every $\sigma \in \Phi$, the character

$$\chi_\sigma \colon \mathrm{Gal}(K_{\bar{\mathfrak{m}}}/K) \to \mathbb{Q}^{\mathrm{alg}*}, \qquad \chi_\sigma(\mathfrak{a}) = \frac{{}^\sigma\psi'(\mathfrak{a})}{\psi'(\mathfrak{a})}$$

is well defined via the Artin isomorphism $\mathrm{Gal}(K_{\bar{\mathfrak{m}}}/K) \simeq I(\bar{\mathfrak{m}})/P_1(\bar{\mathfrak{m}})$. Due to the fact that $\bigcap_{\sigma\in\Phi} \ker \chi_\sigma = P_\eta(\bar{\mathfrak{m}})/P_1(\bar{\mathfrak{m}})$, it follows that

$$L = K_{\bar{\mathfrak{m}}}^{\bigcap_{\sigma\in\Phi} \ker \chi_\sigma}.$$

Notice that $L/\mathbb{Q}$ is not necessarily a normal extension; in fact, this is so if and only if $L = \bar{L}$.

Proposition 3.1. *There is an elliptic curve C defined over L such that:*

(i) $\mathrm{End}_L(C) \simeq \mathcal{O}_K$;

(ii) *its Grössencharacter ψ_C coincides with $\psi' \circ \mathrm{N}_{L/K}$;*

(iii) *C is isogenous over L to all its $\mathrm{Gal}(L/K)$-conjugates;*

(iv) *the abelian variety A is isogenous over L to the power $C^{[E:K]}$.*

Proof. The extreme cases $L = H$ and $L = K_{\bar{\mathfrak{m}}}$ are proved by Gross in [9] and by de Shalit in [6], respectively. For the general case, one can follow the same arguments. Let C_1 be any elliptic curve over L such that $\mathrm{End}_L(C) \simeq \mathcal{O}_K$. Let $\mathfrak{n}$ be its conductor. Once we fix an isomorphism $\theta \colon K \to \mathrm{End}_L^0(C_1)$, we can consider the Grössencharacter $\psi_{C_1} \colon I_L(\mathfrak{n}) \to K^*$ attached to the pair (C_1, θ). For a prime ideal $\mathfrak{P}$ of L relatively prime to $\mathfrak{n}$, we know that $\theta(\psi_{C_1}(\mathfrak{P}))$ is the lifting of the $\mathfrak{P}$-Frobenius acting on the reduction of C_1 mod $\mathfrak{P}$. Recall also that if $\mathfrak{P} \in P_{1,L}(\mathfrak{n})$ then $\psi_{C_1}(\mathfrak{P}) = \mathrm{N}_{L/K}(\beta)$, where $\mathfrak{P} = (\beta)$ with $\beta \equiv 1 \pmod{\mathfrak{P}}$.

By class field theory, the composition $\psi' \circ \mathrm{N}_{L/K}$ takes values in K^* and the equality $\psi' \circ \mathrm{N}_{L/K}(\mathfrak{P}) = \mathrm{N}_{L/K}(\beta)$ holds for every $\mathfrak{P} = (\beta)$ with $\beta \equiv 1 \pmod{\bar{\mathfrak{m}}\mathcal{O}_L}$. Hence the quotient $(\psi' \circ \mathrm{N}_{L/K})/\psi_{C_1}$ defines a character $\delta\colon I_L(\mathfrak{n}\bar{\mathfrak{m}}\mathcal{O}_L)/P_{1,L}(\mathfrak{n}\bar{\mathfrak{m}}\mathcal{O}_L) \to \mathcal{O}_K^*$ of finite order. The twist $C := C_1 \otimes \delta$ satisfies (i) and (ii). Now, (iii) follows from the fact that $\psi_C = \psi_{{}^\alpha C}$ for all $\alpha \in \mathrm{Gal}(L/K)$ due to (ii).

Now we check (iv). By Faltings's criterion (for instance, see §2, Corollary 2, of [3]), it suffices to prove that for every prime $\mathfrak{P}$ of L not dividing N nor the conductor of C, the reductions of the abelian varieties A and $C^{\dim A}$ modulo $\mathfrak{P}$ are isogenous over the residue field $\mathcal{O}_L/\mathfrak{P}$. We write $\mathfrak{p}^f = \mathrm{N}_{L/K}\mathfrak{P}$, where with no risk of confusion now f is the residue degree of $\mathfrak{P}$ over K. On the one hand, the characteristic polynomial of the endomorphism $\mathrm{Frob}_{\mathfrak{P}}$ acting on the l-adic Tate module of the reduction of A/L modulo $\mathfrak{P}$, for a prime $l \neq p$, is the characteristic polynomial of the complex representation of $\iota(\psi'(\mathfrak{p}^f))$:

$$P_{A,\mathfrak{P}}(x) = \prod_{\sigma \in \Phi} (x - {}^\sigma\psi'(\mathfrak{p}^f))(x - \overline{{}^\sigma\psi'(\mathfrak{p}^f)}).$$

On the other hand, the corresponding Frobenius characteristic polynomial for C at $\mathfrak{P}$ is

$$P_{C,\mathfrak{P}}(x) = (x - \psi_C(\mathfrak{P}))(x - \overline{\psi_C(\mathfrak{P})}\,) = (x - \psi'(\mathfrak{p}^f))(x - \overline{\psi'(\mathfrak{p}^f)}).$$

Since $\psi'(\mathfrak{p}^f)$ belongs to K, we obtain $P_{A,\mathfrak{P}}(x) = P_{C,\mathfrak{P}}(x)^{\dim A}$. Thus, A is isogenous over L to $C^{\dim A}$. □

Proposition 3.2. *The field L is the smallest number field satisfying* $\mathrm{End}^0_{\mathbb{Q}^{\mathrm{alg}}}(A) = \mathrm{End}^0_L(A)$.

Proof. Since A is isogenous over L to the $[E : K]$-th power of the elliptic curve C, we have $\mathrm{End}^0_{\mathbb{Q}^{\mathrm{alg}}}(A) = \mathrm{End}^0_L(A)$. That L is the smallest number field with this property can be deduced from the following fact. For every $\varphi \in \mathrm{End}^0_L(A)$, one has the explicit version of the Skolem–Noether theorem:

$${}^{\mathfrak{p}}\varphi = \iota(\psi'(\mathfrak{p})) \cdot \varphi \cdot \iota(\psi'(\mathfrak{p}))^{-1},$$

for all $\mathfrak{p} \in I(\bar{\mathfrak{m}})$ not dividing N. To check this equality, it is enough to verify that it holds reduced modulo a prime ideal $\mathfrak{P}$ of L over $\mathfrak{p}$. The smallest field of definition for all endomorphisms of A is the fixed field L^G, where

$$G = \{\nu \in \mathrm{Gal}(L/K) : {}^\nu\phi = \phi \quad \text{for all } \phi \in \mathrm{End}^0_L(A)\}.$$

By the Čebotarev density theorem, every ν in $\mathrm{Gal}(L/K)$ can be written as $\nu = (\frac{L/K}{\mathfrak{p}})$ for some prime ideal $\mathfrak{p}$ relatively prime to N. We have that $\nu \in G$ if and only if $\iota(\psi'(\mathfrak{p}))$ is in the center of $\mathrm{End}^0_L(A)$; that is, when $\psi'(\mathfrak{p}) \in K$ and this fact implies that $\mathfrak{p}$ splits completely in L, so that $\nu = \mathrm{id}$. □

Let C be an elliptic curve defined over L as in Proposition 3.1. The main theorem of complex multiplication (Theorem 5.4 in [15]) implies the existence of a system of isogenies $\{\mu_{\mathfrak{a}}\colon C \to {}^{\mathfrak{a}}C\}$ over L, $(\mathfrak{a}, \bar{\mathfrak{m}}) = 1$, satisfying the following properties:

(i) $\mu_{\mathfrak{a}\mathfrak{b}} = {}^{\mathfrak{a}}\mu_{\mathfrak{b}}\,\mu_{\mathfrak{a}}$;

(ii) if C has good reduction at a prime ideal $\mathfrak{P} \mid \mathfrak{p}$, then $\mu_{\mathfrak{p}}$ is the lifting of the Frobenius map between the reductions of C and ${}^{\mathfrak{p}}C$ mod $\mathfrak{P}$.

Attached to the system of isogenies $\{\mu_{\mathfrak{a}}\}$, a one-cocycle can be defined as follows (see also [7]). For a non-zero regular differential ω in $\Omega^1(C_{/L})$, let $\lambda_\omega\colon I(\bar{\mathfrak{m}}) \to L^*$ be the map given by

$$\mu_{\mathfrak{a}}^*({}^{\mathfrak{a}}\omega) = \lambda_\omega(\mathfrak{a})\omega,$$

where ${}^{\mathfrak{a}}\omega$ denotes the differential in ${}^{\mathfrak{a}}C$ corresponding to ω by conjugation. It follows that λ_ω is a one-cocycle, and for all $u \in L^*$ one has

$$\lambda_{u\omega}(\mathfrak{a}) = \lambda_\omega(\mathfrak{a})^{\mathfrak{a}}u/u.$$

Clearly, the class of λ_ω in $H^1(I(\bar{\mathfrak{m}}), L^*)$ does not depend on the particular choice of ω. Note that if $\mathfrak{a} \in P_\eta(\bar{\mathfrak{m}})$, then we have $\lambda_\omega(\mathfrak{a}) = \psi'(\mathfrak{a})$. The class λ_ω in $H^1(I(\bar{\mathfrak{m}}), L^*)$ can be characterized from ψ' as follows:

Proposition 3.3. *Let* $\lambda\colon I(\bar{\mathfrak{m}}) \to L^*$ *be any one-cocycle satisfying* $\lambda(\mathfrak{a}) = \psi'(\mathfrak{a})$ *for all* $\mathfrak{a} \in I(\bar{\mathfrak{m}})$ *with* $(\frac{L/K}{\mathfrak{a}}) = \mathrm{id}$ *in* $\mathrm{Gal}(L/K)$. *Then* $[\lambda] = [\lambda_\omega]$.

Proof. Assume that $\lambda \in H^1(I(\bar{\mathfrak{m}}), L^*)$ satisfies $\lambda(\mathfrak{a}) = \psi'(\mathfrak{a})$ for all $\mathfrak{a} \in P_\eta(\bar{\mathfrak{m}})$. The quotient λ/λ_ω defines a one-cocycle in $H^1(\mathrm{Gal}(L/K), L^*)$. By Hilbert's 90 theorem, we know that there is $u \in L^*$ such that $\lambda(\mathfrak{a})/\lambda_\omega(\mathfrak{a}) = {}^{\mathfrak{a}}u/u$ for all $\mathfrak{a} \in I(\bar{\mathfrak{m}})$. Thus, we have $[\lambda] = [\lambda_\omega]$. □

This completes the proof of Theorem 1.2 in the Introduction. From now on, we shall denote by $[A]$ in $H^1(I(\bar{\mathfrak{m}}), L^*)$ the cohomology class of λ_ω.

4. Modular one-cocycles and elliptic directions

In this section we keep the notations as above and tackle the problem of determining the elliptic directions in $\Omega^1(A)$. The goal is to prove Theorem 1.3 that will be deduced from the next three Propositions after the following

Lemma 4.1. *Let* $\pi \in \mathrm{Hom}_L(A, C)$ *be a non-constant modular parametrization, and let* $\omega \in \Omega^1(C_{/L})$ *be any non-zero regular differential. Denote by*

$$h = \sum_{n \geq 1} \gamma_n q^n \in S_2(\Gamma_1(N))$$

the cusp form associated with the pullback $\pi^*(\omega)$. Then:

(i) $\gamma_1 \in L^*$;

(ii) *for all* $\mathfrak{a} \in I(\bar{\mathfrak{m}})$ *relatively prime to* N, *one has* $\iota(\psi'(\mathfrak{a}))^* h = {}^{\mathfrak{a}^{-1}}\lambda_\omega(\mathfrak{a})^{\mathfrak{a}^{-1}} h$;

(iii) *we have the identity* $h = \frac{1}{[L:K]} \sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} \sum_{\sigma \in \Phi} \frac{{}^{\mathfrak{a}^{-1}}\lambda_\omega(\mathfrak{a})}{{}^{\sigma}\psi'(\mathfrak{a})} {}^{\mathfrak{a}^{-1}} h$;

(iv) $\{\psi'(\mathfrak{a}_i)\}$ *is a* K*-basis of* E *if and only if* $\{{}^{\mathfrak{a}_i^{-1}} h\}$ *is an* L*-basis of* $\Omega^1(A_{/L})$.

Proof. (i) Since π and ω are defined over L, the cusp form h associated with $\pi^*(\omega)$ has q-expansion $\sum_{n \geq 1} \gamma_n q^n$ with coefficients in L. Since the abelian variety A is simple over K, we have that A is a K-factor of the Weil restriction $\mathrm{Res}_{L/K}(C)$. Thus, the set $\{{}^{\mathfrak{a}} h \colon \mathfrak{a} \in \mathrm{Gal}(L/K)\}$ generates $\Omega^1(A_{/L})$. This implies $\gamma_1 \neq 0$.

(ii) It is enough to consider the case when $\mathfrak{a} = \mathfrak{p}$ is a prime ideal not dividing N. Then the claim follows from the commutativity of the diagram

$$\begin{tikzcd}
A \arrow[r, "\iota(\psi'(\mathfrak{a}))"] \arrow[d, "{}^{\mathfrak{a}^{-1}}\pi"'] & A \arrow[d, "\pi"] \\
{}^{\mathfrak{a}^{-1}}C \arrow[r, "{}^{\mathfrak{a}^{-1}}\mu_{\mathfrak{a}}"] & C
\end{tikzcd}$$

due to the fact that $\iota(\psi'(\mathfrak{p}))$ and ${}^{\mathfrak{p}^{-1}}\mu_{\mathfrak{p}}$ are liftings of the corresponding $\mathfrak{p}$-Frobenius morphisms at a prime ideal $\mathfrak{P} \mid \mathfrak{p}$ of L.

(iii) Write $h = \sum_{\nu \in \Phi} c_\nu {}^{\nu} f$, with $c_\nu \in \mathbb{Q}^{\mathrm{alg}}$. By applying (ii), for all $\sigma \in \Phi$ and $\mathfrak{a} \in \mathrm{Gal}(L/K)$, one has

$$\frac{{}^{\mathfrak{a}^{-1}}\lambda_\omega(\mathfrak{a})}{{}^{\sigma}\psi'(\mathfrak{a})} {}^{\mathfrak{a}^{-1}} h = \frac{1}{{}^{\sigma}\psi'(\mathfrak{a})} \Big(\sum_{\nu \in \Phi} c_\nu {}^{\nu}\psi'(\mathfrak{a}) {}^{\nu} f \Big) = \sum_{\nu \in \Phi} c_\nu (\chi_\nu \cdot \chi_\sigma{}^{-1})(\mathfrak{a}) {}^{\nu} f.$$

Thus, it holds

$$\begin{aligned}
\sum_{\mathfrak{a}} \sum_{\sigma} \frac{{}^{\mathfrak{a}^{-1}}\lambda_\omega(\mathfrak{a})}{{}^{\sigma}\psi'(\mathfrak{a})} {}^{\mathfrak{a}^{-1}} h &= \sum_{\sigma,\nu} \sum_{\mathfrak{a}} c_\nu (\chi_\nu \cdot \chi_\sigma{}^{-1})(\mathfrak{a}) {}^{\nu} f \\
&= [L:K] \sum_{\nu} c_\nu {}^{\nu} f = [L:K] h.
\end{aligned}$$

(iv) If $\{\psi'(\mathfrak{a}_1), \dots, \psi'(\mathfrak{a}_r)\}$ is a K-basis of E, then for every $\mathfrak{a} \in I(\bar{\mathfrak{m}})$ we can write $\psi'(\mathfrak{a}) = \sum_{i=1}^{r} \alpha_i \psi'(\mathfrak{a}_i)$ with $\alpha_i \in K$. Thus, we obtain

$${}^{\mathfrak{a}^{-1}}\lambda_\omega(\mathfrak{a})^{\mathfrak{a}^{-1}} h = \iota(\psi'(\mathfrak{a}))^*(h) = \sum_{i=1}^{r} \alpha_i \iota(\psi'(\mathfrak{a}_i))^* h = \sum_{i=1}^{r} \alpha_i {}^{\mathfrak{a}_i^{-1}}\lambda_\omega(\mathfrak{a}_i)^{\mathfrak{a}_i^{-1}} h.$$

Since $\{{}^{\mathfrak{a}}h\colon \mathfrak{a} \in \mathrm{Gal}(L/K)\}$ generates $\Omega^1(A_{/L})$ and $\dim(A) = [E : K]$, it follows that $\{{}^{\mathfrak{a}_1^{-1}}h, \dots, {}^{\mathfrak{a}_r^{-1}}h\}$ is a L-basis of $\Omega^1(A_{/L})$.

Conversely, assume that $\{{}^{\mathfrak{a}_1^{-1}}h, \dots, {}^{\mathfrak{a}_r^{-1}}h\}$ is a L-basis of $\Omega^1(A_{/L})$. By using part (ii), if $\sum_{i=1}^r \alpha_i \psi'(\mathfrak{a}_i) = 0$ for some $\alpha_i \in K$, then $\sum_{i=1}^r \alpha_i {}^{\mathfrak{a}_i^{-1}} \lambda_\omega(\mathfrak{a}_i)^{\mathfrak{a}_i^{-1}}h = 0$. This implies that all $\alpha_i = 0$. Since $\dim(A) = [E : K] = r$, the proof is done. □

Due to part (i) in the above Lemma 4.1, there is a unique $\omega \in \Omega^1(C_{/L})$ such that the pullback $\pi^*(\omega)$ gives a normalized cusp form, say

$$h = q + \sum_{n \geq 2} \gamma_n q^n.$$

This particular λ_ω will be called *modular with respect to* π or, simply, π*-modular*. For every 1-cocycle $\lambda \in [A]$, we consider the following sums. Let $\sigma \in \Phi$, and set

$$g_\sigma(\lambda) := \sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} \frac{{}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})}{{}^{\sigma}\psi'(\mathfrak{a})}.$$

Notice that $g_\sigma(\lambda)$ is well defined and $g_\sigma(\lambda) \in {}^{\sigma}E \cdot L$.

Remark 4.1. The sum $g_\sigma(\lambda)$ can be interpreted as a sort of Gauss sum, in the sense that we have

$$g_\sigma(\lambda) = \sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} \chi_\sigma^{-1}(\mathfrak{a}) u_{\mathfrak{a}}$$

where $u_{\mathfrak{a}} = {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})/\psi'(\mathfrak{a})$. If C admits a global minimal Weierstrass equation over L, then the one-cocycle λ attached to a Néron differential satisfies the capitulation property $\lambda(\mathfrak{a})\mathcal{O}_L = \mathfrak{a}\mathcal{O}_L$ (see Remark 10.3 in [7]). Then $u_{\mathfrak{a}}^e$ is an unit in $\mathcal{O}_L^*$ where e is the order of $\mathfrak{a}$ in $\mathrm{Gal}(L/K)$.

We shall denote the Φ-trace of $g_\sigma(\lambda)$ by

$$\mathrm{tr}_\Phi(\lambda) = \sum_{\sigma \in \Phi} g_\sigma(\lambda) \in L.$$

Remark 4.2. Recall that we have defined $\lambda \in [A]$ to be modular if $\mathrm{tr}_\Phi(\lambda) = [L\colon K]$ in the Introduction. As it will be shown, both terms (modular and π-modular) turn out to be equivalent.

For every $\gamma \in L^*$ and $\lambda \in [A]$, let λ_γ denote the twisted one-cocycle in $[A]$ given by $\lambda_\gamma(\mathfrak{a}) = \lambda(\mathfrak{a})\gamma/{}^{\mathfrak{a}}\gamma$. Writing $\lambda = \lambda_\omega$ with some $\omega \in \Omega^1(C_{/L})$, then $\lambda_\gamma = \lambda_{\frac{1}{\gamma}\omega}$. We shall need the following lemma.

Lemma 4.2. *For all* $\mathfrak{a} \in I(\bar{\mathfrak{m}})$ *and* $\sigma \in \Phi$, *one has*

(i) $g_\sigma(\lambda_{{}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})}) \cdot {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a}) = g_\sigma(\lambda) \cdot {}^{\sigma}\psi'(\mathfrak{a})$;

(ii) $\mathrm{tr}_\Phi(\lambda_{{}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})}) = {}^{\mathfrak{a}^{-1}}\,\mathrm{tr}_\Phi(\lambda)$.

Proof. It follows straightforward from the definitions and by using the cocycle relations for λ. □

Proposition 4.3. *Assume that* $\lambda \in [A]$ *is modular with respect to* $\pi \in \mathrm{Hom}_L(A, C)$. *Then* $\mathrm{tr}_\Phi(\lambda) = [L : K]$ *and*

$$h = \frac{1}{[L:K]} \sum_{\sigma \in \Phi} g_\sigma(\lambda) \cdot {}^{\sigma} f$$

is the normalized elliptic direction in $\pi^*(\Omega^1(C_{/L}))$.

Proof. Since λ is π-modular, there is a non-zero regular differential $\omega \in \Omega^1(C_{/L})$ such that $\pi^*(\omega)$ is a normalized cusp form $h = q + \sum_{n \geq 2} \gamma_n q^n$ and $\lambda = \lambda_\omega$. By comparing the first Fourier coefficient in the equality at Lemma 4.1 (iii), we have that $\mathrm{tr}_\Phi(\lambda) = [L : K]$. For every $\sigma \in \Phi$, set

$$F_\sigma = \sum_{\mathfrak{b} \in \mathrm{Gal}(L/K)} \frac{{}^{\mathfrak{b}^{-1}}\lambda(\mathfrak{b})}{{}^{\sigma}\psi'(\mathfrak{b})}\, {}^{\mathfrak{b}^{-1}}h.$$

Also by Lemma 4.1 (iii), we know that $\sum_{\sigma \in \Phi} F_\sigma = [L : K]\, h$. From the equality $\iota(\psi'(\mathfrak{a}))^*({}^{\mathfrak{b}^{-1}}h) = {}^{(\mathfrak{b}\cdot\mathfrak{a})^{-1}}\lambda(\mathfrak{a})\, {}^{(\mathfrak{b}\cdot\mathfrak{a})^{-1}}h$, one obtains

$$\begin{aligned}
\iota(\psi'(\mathfrak{a}))^*(F_\sigma) &= \sum_{\mathfrak{b} \in \mathrm{Gal}(L/K)} \frac{{}^{\mathfrak{b}^{-1}}\lambda(\mathfrak{b})}{{}^{\sigma}\psi'(\mathfrak{b})}\, {}^{(\mathfrak{b}\cdot\mathfrak{a})^{-1}}\lambda(\mathfrak{a})\, {}^{(\mathfrak{b}\cdot\mathfrak{a})^{-1}}h \\
&= \sum_{\mathfrak{b} \in \mathrm{Gal}(L/K)} \frac{{}^{(\mathfrak{b}\cdot\mathfrak{a})^{-1}}\lambda(\mathfrak{b}\cdot\mathfrak{a})}{{}^{\sigma}\psi'(\mathfrak{b})}\, {}^{(\mathfrak{b}\cdot\mathfrak{a})^{-1}}h = {}^{\sigma}\psi'(\mathfrak{a})\, F_\sigma.
\end{aligned}$$

Hence F_σ and ${}^{\sigma}f$ differ by a scalar multiple. Since the q-expansion of F_σ begins as $g_\sigma(\lambda)\, q + \cdots$, it follows that $F_\sigma = g_\sigma(\lambda) \cdot {}^{\sigma}f$, and then $h = \frac{1}{[L:K]} \sum_{\sigma \in \Phi} g_\sigma(\lambda) \cdot {}^{\sigma} f$. □

Now, we shall prove that the modular one-cocycles λ in $[A]$ with respect to some modular parametrization π are precisely those that satisfy the trace condition $\mathrm{tr}_\Phi(\lambda) = [L : K]$. To this end, for a given one-cocycle $\lambda \in [A]$ (not necessarily modular), let us consider the K-linear map $\mathrm{pr}\colon L \to L$,

$$\mathrm{pr}(u) := \sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} \Big(\sum_{\sigma \in \Phi} \frac{1}{{}^{\sigma}\psi'(\mathfrak{a})} \Big)^{\mathfrak{a}^{-1}} \lambda(\mathfrak{a})^{\mathfrak{a}^{-1}} u = \begin{cases} u \cdot \mathrm{tr}_\Phi(\lambda_u) & \text{if } u \neq 0; \\ 0 & \text{otherwise.} \end{cases}$$

Consider the eigenspace $\mathcal{M} = \{u \in L\colon \operatorname{pr}(u) = [L:K]\cdot u\}$. Notice that λ_u is modular if and only if $u \in \mathcal{M}\backslash\{0\}$. In particular, we know that $\dim_K(\mathcal{M}) > 0$ and it does not depend on the particular choice of $\lambda \in [A]$ used to define the K-linear map pr.

Proposition 4.4. *One has*

(i) $\operatorname{pr}^2 = [L:K]\operatorname{pr}$*;*

(ii) $\dim_K(\mathcal{M}) = [E:K]$*;*

(iii) *if* λ *is modular, then* $\mathcal{M} = \langle\{{}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})\}\rangle_K$ *where* $\mathfrak{a}$ *runs over* $\mathrm{Gal}(L/K)$.

Proof. The first claim comes from the computation:

$$
\begin{aligned}
\operatorname{pr}^2(u) &= \sum_{\mathfrak{a}}\Big(\sum_{\sigma}\frac{1}{{}^{\sigma}\psi'(\mathfrak{a})}\Big)^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})\;{}^{\mathfrak{a}^{-1}}\Big[\sum_{\mathfrak{b}}\Big(\sum_{\tau}\frac{1}{{}^{\tau}\psi'(\mathfrak{b})}\Big)^{\mathfrak{b}^{-1}}\lambda(\mathfrak{b})^{\mathfrak{b}^{-1}}u\Big]\\
&= \sum_{\mathfrak{a}}\sum_{\mathfrak{b}}\Big(\sum_{\sigma}\frac{1}{{}^{\sigma}\psi'(\mathfrak{a})}\Big)\Big(\sum_{\tau}\frac{1}{{}^{\tau}\psi'(\mathfrak{b})}\Big)^{(\mathfrak{a}\mathfrak{b})^{-1}}\lambda(\mathfrak{a}\mathfrak{b})^{(\mathfrak{a}\mathfrak{b})^{-1}}u\\
&= \sum_{\mathfrak{a}}\sum_{\mathfrak{b}}\Big(\sum_{\sigma}\frac{1}{{}^{\sigma}\psi'(\mathfrak{a})}\Big)\Big(\sum_{\tau}\frac{1}{{}^{\tau}\psi'(\mathfrak{a}^{-1}\mathfrak{b})}\Big)^{\mathfrak{b}^{-1}}\lambda(\mathfrak{b})^{\mathfrak{b}^{-1}}u\\
&= \sum_{\mathfrak{b}}\sum_{\mathfrak{a}}\Big(\sum_{\sigma,\tau}(\chi_\sigma\chi_\tau^{-1})(\mathfrak{a})\Big)\frac{{}^{\mathfrak{b}^{-1}}\lambda(\mathfrak{b})}{{}^{\tau}\psi'(\mathfrak{b})}{}^{\mathfrak{b}^{-1}}u\\
&= [L:K]\operatorname{pr}(u).
\end{aligned}
$$

Let us prove (ii) and (iii) simultaneously. Since $\dim_K(\mathcal{M})$ is independent of the one-cocycle λ chosen in $[A]$, we can (and do) assume that λ is modular. Set

$$
h = \frac{1}{[L:K]}\sum_{\sigma\in\Phi} g_\sigma(\lambda)\cdot{}^{\sigma}f = 1 + \sum_{n>1}\gamma_n q^n.
$$

Let $W = \langle\{{}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})\}\rangle_K$ where $\mathfrak{a}$ runs over $\mathrm{Gal}(L/K)$. We need to show that $W = \mathcal{M}$ and $\dim_K(W) = [E:K]$. Choose $\mathfrak{a}_1,\dots,\mathfrak{a}_r \in I(\bar{\mathfrak{m}})$ such that $\{\psi'(\mathfrak{a}_1),\dots,\psi'(\mathfrak{a}_r)\}$ is a K-basis of E. We claim that $\{{}^{\mathfrak{a}_1^{-1}}\lambda(\mathfrak{a}_1),\dots,{}^{\mathfrak{a}_r^{-1}}\lambda(\mathfrak{a}_r)\}$ is a K-basis of W. Indeed, if $\sum_{i=1}^r \alpha_i\,{}^{\mathfrak{a}_i^{-1}}\lambda(\mathfrak{a}_i) = 0$ for some α_i in K, then consider $\alpha := \sum_{i=1}^r \alpha_i\psi'(\mathfrak{a}_i) \in E$. It is easy to check that $\iota(\alpha)^*(h) = \sum_{n\geq 1}\gamma'_n q^n$ with $\gamma'_1 = 0$. This forces $\alpha = 0$, since otherwise we get a contradiction from Lemma 4.1 (i) applied to $\iota(\alpha)^*(h)$. Therefore, all $\alpha_i = 0$ which implies that ${}^{\mathfrak{a}_1^{-1}}\lambda(\mathfrak{a}_1), \dots, {}^{\mathfrak{a}_r^{-1}}\lambda(\mathfrak{a}_r)$ are linearly independent. Now, for every ideal $\mathfrak{a} \in I(\bar{\mathfrak{m}})$, one has $\psi'(\mathfrak{a}) = \sum_{i=1}^r \alpha_i \psi'(\mathfrak{a}_i)$ for some $\alpha_i \in K$. By taking q-expansions in the equality

$$ {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})^{\mathfrak{a}^{-1}}h = \sum_{i=1}^{r} \alpha_i \, {}^{\mathfrak{a}_i^{-1}}\lambda(\mathfrak{a}_i)^{\,\mathfrak{a}_i^{-1}}h, $$

we obtain ${}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a}) = \sum_{i=1}^r \alpha_i \, {}^{\mathfrak{a}_i^{-1}}\lambda(\mathfrak{a}_i)$. So far, we have $\dim_K(W) = [E : K]$ and the inclusion $W \subseteq \mathcal{M}$ follows from Lemma 4.2 (ii).

To easy notation, set $u_i = {}^{\mathfrak{a}_i^{-1}}\lambda(\mathfrak{a}_i)$ for $1 \le i \le r$ and let us show that they generate $\mathcal{M}$. For any nonzero $u \in \mathcal{M}$, consider the normalized cusp form

$$ h_u = \frac{1}{[L : K]} \sum_{\sigma \in \Phi} g_\sigma(\lambda_u) \cdot {}^\sigma f. $$

Since $\{h_{u_1}, \dots, h_{u_n}\}$ is a L-basis of $\Omega^1(A_{/L})$ by Lemma 4.1 (iv), there are $\gamma_i \in L$ such that $h_u = \sum_{i=1}^r \gamma_i \, h_{u_i}$. Notice that $\sum_{i=1}^r \gamma_i = 1$. By applying $\iota(\psi'(\mathfrak{a}))^*$ to h_u, and then conjugate by $\mathfrak{a}$, we obtain

$$ \lambda_u(\mathfrak{a}) h_u = \sum_{i=1}^{r} {}^{\mathfrak{a}}\gamma_i \, \lambda_{u_i}(\mathfrak{a}) \, h_{u_i}. $$

Therefore, we have

$$ \gamma_i = {}^{\mathfrak{a}}\gamma_i \frac{\lambda_{u_i}(\mathfrak{a})}{\lambda_u(\mathfrak{a})} = {}^{\mathfrak{a}}\gamma_i \frac{{}^{\mathfrak{a}}u}{{}^{\mathfrak{a}}u_i} \frac{u_i}{u} $$

for all $\mathfrak{a}$ and $1 \le i \le r$. That is, $\beta_i := \gamma_i \, u/u_i \in K$. Then $u = \sum_{i=1}^r \beta_i \, u_i$ since $\sum_{i=1}^r \gamma_i = 1$. The statement (iii) follows. □

Proposition 4.5. *Let $\lambda' \in [A]$ such that $\mathrm{tr}_\Phi(\lambda') = [L : K]$. Then λ' is modular with respect to some $\pi' \in \mathrm{Hom}_L(A, C)$.*

Proof. We shall prove that there is $\pi' \in \mathrm{Hom}_L(A, C)$ and $\omega' \in \Omega^1(C_{/L})$ such that $\pi'^*(\omega')$ corresponds to the normalized cusp form

$$ h' = \frac{1}{[L : K]} \sum_{\sigma \in \Phi} \sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} \frac{{}^{\mathfrak{a}^{-1}}\lambda'(\mathfrak{a})}{{}^{\sigma}\psi'(\mathfrak{a})} \cdot {}^\sigma f. $$

Consider any non-constant $\pi \in \mathrm{Hom}_L(A, C)$ and take $\omega \in \Omega^1(C_{/L})$ such that $\pi^*(\omega)$ corresponds to the normalized cusp form

$$ h = \frac{1}{[L : K]} \sum_{\sigma \in \Phi} g_\sigma(\lambda) \cdot {}^\sigma f, $$

where $\lambda = \lambda_\omega$. Let $L = \ker(\mathrm{pr}) \oplus \mathcal{M}$ be the decomposition corresponding to the projector pr attached to λ. Now, there is $\gamma \in \mathcal{M}$ such that $\lambda' = \lambda_\gamma$ and

$$h' = \frac{1}{[L:K]} \sum_{\sigma \in \Phi} g_\sigma(\lambda_\gamma) \cdot {}^\sigma f$$

with $\gamma = \sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} {r_\mathfrak{a}}^{\mathfrak{a}^{-1}} \lambda(\mathfrak{a})$ for some $r_\mathfrak{a} \in K$ due to Proposition 4.4 (iii). We claim that

$$\Big(\sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} {r_\mathfrak{a}}^{\mathfrak{a}^{-1}} \lambda(\mathfrak{a}) \Big) h' = \iota \Big(\sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} r_\mathfrak{a} \psi'(\mathfrak{a}) \Big)^* h. \tag{1}$$

Letting $\Psi = \iota\big(\sum_{\mathfrak{a} \in \mathrm{Gal}(L/K)} r_\mathfrak{a} \psi'(\mathfrak{a})\big) \in \mathrm{End}_K^0(A)$, then it follows

$$h' = \Psi^* \Big(\pi^* \Big(\frac{1}{\gamma} \omega \Big) \Big) = (\pi \circ \Psi)^* \Big(\frac{1}{\gamma} \omega \Big),$$

which implies that λ' is modular. To check (1), we use Lemma 4.2 (i):

$$\begin{aligned} \gamma\, h' &= \frac{1}{[L:K]} \sum_\sigma \sum_\mathfrak{b} \frac{{}^{\mathfrak{b}^{-1}} \lambda(\mathfrak{b})^{\mathfrak{b}^{-1}} \gamma}{{}^\sigma \psi'(\mathfrak{b})} {}^\sigma f \\ &= \frac{1}{[L:K]} \sum_\sigma \sum_\mathfrak{b} \sum_\mathfrak{a} \frac{{}^{\mathfrak{b}^{-1}} \lambda(\mathfrak{b}) {r_\mathfrak{a}}^{(\mathfrak{a}\mathfrak{b})^{-1}} \lambda(\mathfrak{a})}{{}^\sigma \psi'(\mathfrak{b})} {}^\sigma f \\ &= \frac{1}{[L:K]} \sum_\sigma \sum_\mathfrak{a} r_\mathfrak{a} g_\sigma(\lambda_{\mathfrak{a}^{-1} \lambda(\mathfrak{a})})^{\mathfrak{a}^{-1}} \lambda(\mathfrak{a})\, {}^\sigma f \\ &= \frac{1}{[L:K]} \sum_\sigma \sum_\mathfrak{a} {r_\mathfrak{a}}^\sigma \psi'(\mathfrak{a}) g_\sigma(\lambda)\, {}^\sigma f \\ &= \frac{1}{[L:K]} \Psi^* \Big(\sum_\sigma g_\sigma(\lambda)\, {}^\sigma f \Big) = \Psi^*(h). \end{aligned}$$

□

The transitivity of the action of $\iota(E^*)$ on the set of elliptic directions follows from the equality (1). To finish the proof of Theorem 1.3, it remains to determine the q-expansions of the normalized elliptic directions. For it, first we need a technical lemma.

Lemma 4.6. *Let* $\ell\colon I(\mathfrak{m}) \to L^*$ *be a map such that* $\ell(\mathfrak{a}) = \psi(\mathfrak{a})$ *for all* $\mathfrak{a} = \mathrm{id}$ *in* $\mathrm{Gal}(\bar{L}/K)$. *Let* $\tau\colon \mathrm{Gal}(\bar{L}/K) \to \mathrm{Gal}(L/K)$ *be a map such that* $\ell(\mathfrak{a}\mathfrak{b}) =$

$\ell(\mathfrak{a})^{\tau(\mathfrak{a})}\ell(\mathfrak{b})$ for all $\mathfrak{a} \in I(\mathfrak{m})$. Then the identity

$$\frac{1}{[L:K]}\sum_{\sigma\in\Phi}\beta_\sigma{}^\sigma\psi(\mathfrak{c}) = \ell(\mathfrak{c}) \tag{2}$$

holds for all $\mathfrak{c} \in I(\mathfrak{m})$ if and only if

$$\beta_\sigma = \sum_{\mathfrak{a}\in\mathrm{Gal}(\bar{L}/K)} \frac{\ell(\mathfrak{a})}{{}^\sigma\psi(\mathfrak{a})} \quad \text{and} \quad \sum_{\sigma\in\Phi}\beta_\sigma = [L:K]. \tag{3}$$

Proof. Assume (3). For every $\mathfrak{c} \in I(\mathfrak{m})$, we have

$$\begin{aligned}
\sum_{\sigma\in\Phi}\Big(\sum_{\mathfrak{a}\in\mathrm{Gal}(\bar{L}/K)}\frac{\ell(\mathfrak{a})}{{}^\sigma\psi(\mathfrak{a})}\Big)^\sigma\psi(\mathfrak{c}) &= \sum_{\sigma\in\Phi}\Big(\sum_{\mathfrak{a}\in\mathrm{Gal}(\bar{L}/K)}\frac{\ell(\mathfrak{a}\mathfrak{c})}{{}^\sigma\psi(\mathfrak{a}\mathfrak{c})}\Big)^\sigma\psi(\mathfrak{c})\\
&= \ell(\mathfrak{c})\sum_{\sigma\in\Phi}\Big(\sum_{\mathfrak{a}\in\mathrm{Gal}(\bar{L}/K)}\frac{{}^{\tau(\mathfrak{c})}\ell(\mathfrak{a})}{{}^\sigma\psi(\mathfrak{a})}\Big)\\
&= \ell(\mathfrak{c})\,{}^{\tau(\mathfrak{c})}\Big(\sum_{\mathfrak{a}\in\mathrm{Gal}(\bar{L}/K)}\ell(\mathfrak{a})\Big(\sum_{\sigma\in\Phi}\frac{1}{{}^\sigma\psi(\mathfrak{a})}\Big)\Big)\\
&= \ell(\mathfrak{c})\,{}^{\tau(\mathfrak{c})}\Big(\sum_{\sigma\in\Phi}\beta_\sigma\Big) = \ell(\mathfrak{c})\,[L:K].
\end{aligned}$$

Now, suppose (2). Fix $\nu \in \Phi$. Note that for $\sigma \in \Phi$, the characters χ_σ and χ_ν are equal if and only if $\sigma = \nu$. For every $\mathfrak{a} \in \mathrm{Gal}(\bar{L}/K)$, one has

$$\begin{aligned}
\frac{\ell(\mathfrak{a})}{{}^\nu\psi(\mathfrak{a})} &= \frac{1}{[L:K]}\Big(\beta_\nu + \sum_{\sigma\in\Phi\setminus\{\nu\}}\beta_\sigma\frac{{}^\sigma\psi(\mathfrak{a})}{{}^\nu\psi(\mathfrak{a})}\Big)\\
&= \frac{1}{[L:K]}\Big(\beta_\nu + \sum_{\sigma\in\Phi\setminus\{\nu\}}\beta_\sigma(\chi_\sigma\chi_\nu^{-1})(\mathfrak{a})\Big).
\end{aligned}$$

Summing over all $\mathfrak{a}$, then

$$\sum_{\mathfrak{a}\in\mathrm{Gal}(\bar{L}/K)}\frac{\ell(\mathfrak{a})}{{}^\nu\psi'(\mathfrak{a})} = \beta_\nu + \frac{1}{[L:K]}\Big(\sum_{\sigma\in\Phi\setminus\{\nu\}}\beta_\sigma\sum_{\mathfrak{a}\in\mathrm{Gal}(\bar{L}/K)}(\chi_\sigma\chi_\nu^{-1})(\mathfrak{a})\Big) = \beta_\nu.$$

The condition $\sum_{\sigma\in\Phi}\beta_\sigma = [L:K]$ is obtained by replacing $\mathfrak{a}$ with $\mathcal{O}$ in (2). □

Proposition 4.7. *Assume that* $\lambda \in [A]$ *satisfies* $\mathrm{tr}_\Phi(\lambda) = [L : K]$. *Consider the normalized cusp form*

$$h = \frac{1}{[L:K]} \sum_{\sigma \in \Phi} g_\sigma(\lambda) \cdot {}^\sigma f.$$

Then:

(i) *one has*

$$h = \begin{cases} \displaystyle\sum_{(\mathfrak{a},\mathfrak{m})=1} {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})\, q^{\mathrm{N}(\mathfrak{a})} & \text{if } K \not\subseteq E_f; \\ \displaystyle\sum_{(\mathfrak{a},\mathfrak{m})=1} \frac{\mathrm{N}(\mathfrak{a})}{\lambda(\bar{\mathfrak{a}})} q^{\mathrm{N}(\mathfrak{a})} & \text{if } K \subseteq E_f; \end{cases}$$

(ii) *for all* $\mathfrak{c} \in I(\bar{\mathfrak{m}})$, *we have* $\iota(\psi'(\mathfrak{c}))^*(h) = {}^{\mathfrak{c}^{-1}}\lambda(\mathfrak{c})^{\mathfrak{c}^{-1}} h$.

Proof. For all $\mathfrak{a} \in I(\mathfrak{m})$, set

$$\ell(\mathfrak{a}) = \begin{cases} {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a}) & \text{if } K \not\subseteq E_f; \\ \dfrac{\mathrm{N}(\mathfrak{a})}{\lambda(\bar{\mathfrak{a}})} & \text{if } K \subseteq E_f. \end{cases}$$

It is clear that $\ell(\mathfrak{a}\mathfrak{b})$ is $\ell(\mathfrak{a})^{\mathfrak{a}^{-1}}\ell(\mathfrak{b})$ or $\ell(\mathfrak{a})^{\bar{\mathfrak{a}}}\ell(\mathfrak{b})$ depending on whether $K \not\subseteq E_f$ or not, respectively. Since for the case $K \subseteq E_f$ one has

$$\frac{\ell(\mathfrak{a}^{-1})}{{}^\sigma\psi(\mathfrak{a}^{-1})} = \frac{{}^{\bar{\mathfrak{a}}^{-1}}(1/\ell(\mathfrak{a}))}{{}^\sigma\psi(\mathfrak{a}^{-1})} = \frac{{}^{\bar{\mathfrak{a}}^{-1}}(\mathrm{N}(\mathfrak{a})/\ell(\mathfrak{a}))}{\mathrm{N}(\mathfrak{a})/{}^\sigma\psi(\mathfrak{a})} = \frac{{}^{\bar{\mathfrak{a}}^{-1}}\lambda(\bar{\mathfrak{a}})}{{}^\sigma\psi'(\bar{\mathfrak{a}})},$$

for all $\sigma \in \Phi$, then in both cases it follows that $g_\sigma(\lambda) = \sum_{\mathfrak{a} \in \mathrm{Gal}(\bar{L}/K)} \ell(\mathfrak{a})/{}^\sigma\psi(\mathfrak{a})$. By using Lemma 4.6, a case-by-case computation shows that for all $\mathfrak{a} \in I(\mathfrak{m})$ and $\mathfrak{c} \in I(\bar{\mathfrak{m}})$ one has

$$\frac{1}{[L:K]} \sum_{\sigma \in \Phi} g_\sigma(\lambda)^\sigma\psi(\mathfrak{a})^\sigma\psi'(\mathfrak{c}) = {}^{\mathfrak{c}^{-1}}\lambda(\mathfrak{c})^{\mathfrak{c}^{-1}}\ell(\mathfrak{a}). \tag{4}$$

Plugging $\mathfrak{c} = 1$ in (4) it follows part (i). Part (ii) follows from part (i) and (4). □

Now, Theorem 1.3 in the Introduction follows from Propositions 4.3, 4.5 and 4.7. Note that due to Proposition 4.4, all one-cocycles in $[A]$ are modular if and only if $[E : K] = [L : K]$; i.e., when A is K-isogenous to $\mathrm{Res}_{L/K}(C)$. In general, in order to determine a modular one-cocycle in $[A]$ a strategy emerges from the previous results. Indeed, first one can build a one-cocycle $\lambda \in [A]$ by solving and combining norm equations. If $\mathrm{tr}_\Phi(\lambda) \neq 0$, then $\lambda_{\mathrm{tr}_\Phi(\lambda)}$ is modular since its Φ-trace equals $[L : K]$.

Alternatively, if $\mathrm{tr}_{\Phi}(\lambda) = 0$ or in any circumstance, the nullspace of the K-linear map $\mathrm{pr} - [L : K]\,\mathrm{Id}$ provides all $u \in L$ such that λ_u is modular.

We also remark that for the case $K \subseteq E_f$, there are elliptic quotients of A_f that do not factor through neither A nor $\bar{A}$. These quotients can be obtained using the above results plus the Weil involution acting on A_f.

We conclude this section with three open questions: one concerning about the isomorphism $\iota\colon E \to \mathrm{End}^0_K(A)$ and the others about the elliptic optimal quotients of A. All the results of the paper hold when we replace $J_1(N)$ with $\mathrm{Jac}(X_\Gamma)$, where Γ is an intermediate congruence subgroup between $\Gamma_1(N)$ and $\Gamma_0(N)$ such that f in $S_2(\Gamma)$ and X_Γ is the modular curve attached to this subgroup. Although the optimal quotient A of $A_f^{(\Gamma)}$ does depend on Γ, it is known that $\iota(T_p) \in \mathrm{End}_{\mathbb{Q}}(A_f^{(\Gamma)})$ and, thus, $\iota(T_p)$ belongs to $\mathrm{End}_K(A)$ for all Γ.

Question 4.8. Is $\iota(\psi(\mathfrak{a})) \in \mathrm{End}_K(A)$ for all integral ideals $\mathfrak{a}$ and all Γ?

We ask ourselves whether the j-invariants of optimal modular parametrizations of CM elliptic curves are not far from being also *optimal* in the sense of having CM by the maximal order of K. Of course, if $\iota(\mathcal{O}_K) \subset \mathrm{End}_K(A)$ all optimal elliptic quotients have multiplication by $\mathcal{O}_K$. If $\iota(\eta(\mathfrak{a})) \in \mathrm{End}_K(A)$ for all integral ideals $\mathfrak{a} \in I(\bar{\mathfrak{m}})$, then the j-invariants of all optimal elliptic quotients are in the Hilbert class field H. From Cremona's tables ($N < 130000$), we have checked that all optimal elliptic quotients over $\mathbb{Q}$ with CM of $J_0(N)$ have complex multiplication by $\mathcal{O}_K$. Also, the same experimental result has been obtained in all examples over $\mathbb{Q}^{\mathrm{alg}}$ collected by the authors.

Question 4.9. Assume that $\pi \in \mathrm{Hom}_L(A, C)$ is optimal. Does C have complex multiplication by $\mathcal{O}_K$?

And the last question is related to the above Remark 4.1.

Question 4.10. Is it true that the existence of an optimal elliptic quotient of A having global minimal model over L is equivalent to the existence of a modular one-cocycle $\lambda \in [A]$ with values $\lambda(\mathfrak{a})$ in the ring of integers $\mathcal{O}_L$ for all integral ideals $\mathfrak{a} \in I(\bar{\mathfrak{m}})$?

In the next sections, we apply the above results and focus our attention on Gross's elliptic curves $A(p)$. We also give a positive answer to the second question mentioned above for the particular case of level $N = p^2$.

5. CM elliptic optimal quotients of $J_1(p^2)$

In the sequel p is a prime > 3 and such that $p \equiv 3 \bmod 4$. The discriminant of $K = \mathbb{Q}(\sqrt{-p})$ is $-p$. Set $\mathfrak{p} = \sqrt{-p}\,\mathcal{O}_K$. Let $\mathcal{X}$ denote the set of Hecke characters mod $\mathfrak{p}$ and let $\mathcal{Y}$ be the set of Dirichlet characters $\eta\colon (\mathcal{O}_K/\mathfrak{p})^* \to \mathbb{C}^*$ such that $\eta(-1) = -1$.

To every Hecke character $\psi \in \mathcal{X}$, we attach its eta-character η in $\mathcal{Y}$ defined as in Section 3 by $\eta(a) = \psi((a))/a$, and it can be easily seen that this map $\mathcal{X} \to \mathcal{Y}$ is surjective. The Nebentypus $\varepsilon\colon (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*$ of the newform $f \in S_2(\Gamma_1(p^2))$ associated with ψ is given by $\varepsilon(n) = \chi(n)\eta(n)$, where χ is the quadratic Dirichlet character associated with K. In this case, we have that $\operatorname{ord}\varepsilon = (\operatorname{ord}\eta)/2$.

By the results in Section 3, we know that the elliptic optimal quotients of the abelian variety A_f are defined over a number field L, which is a cyclic extension of H of degree $\operatorname{ord}\varepsilon$ contained in $K_{\mathfrak{p}}$.

Proposition 5.1. *The ray class field $K_{\mathfrak{p}}$ satisfies $[K_{\mathfrak{p}} : H] = (p-1)/2$ and we have $K_{\mathfrak{p}} = H \cdot \mathbb{Q}(\zeta_p)$, where $\zeta_p = e^{2\pi i/p}$.*

Proof. From the exact sequence

$$1 \longrightarrow (\mathcal{O}_K/\mathfrak{p})^*/\mathcal{O}_K{}^* \longrightarrow I(\mathfrak{p})/P_1(\mathfrak{p}) \longrightarrow I(\mathcal{O}_K)/P(\mathcal{O}_K) \longrightarrow 1,$$

we know that the Galois group $\mathrm{Gal}(K_{\mathfrak{p}}/H)$ is isomorphic to $(\mathcal{O}_K/\mathfrak{p})^*/\mathcal{O}_K{}^*$ and, thus, one has $[K_{\mathfrak{p}} : H] = (p-1)/2$. Consider the morphism $\Phi_{\mathfrak{p}}\colon I(\mathfrak{p}) \to \mathrm{Gal}(H \cdot \mathbb{Q}(\zeta_p)/K)$ given by the Artin symbol. We claim that Φ_p has kernel $P_1(\mathfrak{p})$, which implies that $K_{\mathfrak{p}} \subseteq H \cdot \mathbb{Q}(\zeta_p)$. Indeed, for any ideal $\mathfrak{a} \in I(\mathfrak{p})$, we have that $\Phi_{\mathfrak{p}}(\mathfrak{a})$ acts trivially on H if and only if $\mathfrak{a} \in P(\mathfrak{p})$, that is $\mathfrak{a} = a\mathcal{O}$. Moreover, $\Phi_p(a\mathcal{O})$ acts trivially on $\mathbb{Q}(\zeta_p)$ if and only if the Artin symbol $\left(\frac{\mathbb{Q}(\zeta_p)/\mathbb{Q}}{\mathrm{N}(a)}\right)$ is the identity; i.e., $\mathrm{N}(a) \equiv 1 \pmod{\mathfrak{p}}$ which is equivalent to $\mathfrak{a} \in P_1(\mathfrak{p})$ since $\mathrm{N}(a) \equiv a^2 \pmod{\mathfrak{p}}$. Finally, for any subfield F of $\mathbb{Q}(\zeta_p)$ which contains K we have that $H \cap F = K$ since either $F = K$ or F/K is ramified at $\mathfrak{p}$. Hence, one has the equality $[H \cdot \mathbb{Q}(\zeta_p) : H] = (p-1)/2 = [K_{\mathfrak{p}} : H]$ and the statement follows. □

We shall need the following lemma.

Lemma 5.2. *Let $\psi \in \mathcal{X}$ and denote by η and f its eta-character and newform, respectively. Then the following holds:*

(i) *For every ideal $\mathfrak{a} \in I(\mathfrak{p})$, one has*

$$\mathrm{Tr}_{E/K}(\psi(\mathfrak{a})) = \begin{cases} a \displaystyle\sum_{\sigma\in\Phi} {}^{\sigma}\eta(a) & \text{if } \mathfrak{a} = a\mathcal{O}_K, \\ 0 & \text{if } \mathfrak{a} \notin P(\mathfrak{p}). \end{cases}$$

(ii) *Let η' and f' denote the eta-character and newform associated with $\psi' \in \mathcal{X}$. Then $f' = {}^{\sigma}f$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/K)$ if and only if $\ker\eta' = \ker\eta$.*

Proof. First, let us prove (i). When $\mathfrak{a} = a\mathcal{O}_K$, the claim on the trace is clear since ${}^\sigma\psi((a)) = a^\sigma\eta(a)$. Suppose that $\mathfrak{a} \notin P(\mathfrak{p})$, and let n be the order of $\mathfrak{a}$ in $I(\mathfrak{p})/P(\eta)$. Notice that $n > 1$ and $\psi(\mathfrak{a}) \notin K$. For every $\sigma \in \Phi$, we have ${}^\sigma\psi(\mathfrak{a}) = \psi(\mathfrak{a})\zeta_\sigma$ for some $\zeta_\sigma \in \mu_n$, where μ_n denotes the group of n-th roots of unity. Thus, we have

$$\sum_{\sigma\in\Phi} {}^\sigma\psi(\mathfrak{a}) = \psi(\mathfrak{a}) \sum_{\sigma\in\Phi} \zeta_\sigma \in K.$$

Therefore, either $\mathrm{Tr}_{E/K}(\psi(\mathfrak{a})) = 0$ or $\psi(\mathfrak{a}) \in K(\mu_n)$. Let us see that the last possibility does not occur. For it, assume that $\psi(\mathfrak{a}) \in K(\mu_n)$ which implies that the extension $K(\psi(\mathfrak{a}))/K$ is normal. Since n is the minimum positive integer such that $\psi(\mathfrak{a})^n \in K$, it follows that either $\mu_n \subset K$ or $\psi(\mathfrak{a})^{2n} \in K^n$ (see Proposition 2 in [14]). Since $\psi(\mathfrak{a}) \notin K$, we must have that $\psi(\mathfrak{a}^{2n}) = b^n = \psi((b\mathcal{O}_K)^n)$ for some $b \in K$ and, hence, $\mathfrak{a}^2 = b\mathcal{O}_K$. The class number of K being odd, we get a contradiction.

Let us prove (ii). If $f' = {}^\sigma f$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/K)$ then the statement is clear since $\eta' = {}^\sigma\eta$. Now, suppose that $\ker\eta' = \ker\eta$. We claim that

$$\{{}^\sigma f : \sigma \in \Phi\} \cap \{{}^\sigma f' : \sigma \in \Phi'\} \neq \emptyset,$$

where Φ' is the corresponding set of K-embeddings $\mathbb{Q}(\psi') \hookrightarrow \mathbb{C}$. Let us consider the normalized cusp forms

$$h = \frac{1}{|\Phi|}\sum_{\sigma\in\Phi} {}^\sigma f = q + \cdots,$$
$$h' = \frac{1}{|\Phi'|}\sum_{\sigma\in\Phi'} {}^\sigma f' = q + \cdots$$

in $S_2(\Gamma_1(p^2))^{\mathrm{new}}$. Since $K \not\subseteq \mathbb{Q}(\operatorname{im}\eta)$ and $\ker\eta' = \ker\eta$, there is $\tau \in \Phi$ such that ${}^\tau\eta(a) = \eta'(a)$ for all $a \in \mathcal{O}_K$ coprime with $\mathfrak{p}$. By applying (i), we obtain the equality

$$h = \sum_{\mathfrak{a}\in P(\mathfrak{p})} \frac{\mathrm{Tr}_{E/K}(\psi(\mathfrak{a}))}{|\Phi|} q^{\mathrm{N}(\mathfrak{a})} = \sum_{\mathfrak{a}\in P(\mathfrak{p})} \frac{\mathrm{Tr}_{E/K}(\psi'(\mathfrak{a}))}{|\Phi'|} q^{\mathrm{N}(\mathfrak{a})} = h'.$$

Therefore, the $\mathbb{Q}^{\mathrm{alg}}$-vector spaces generated by $\{{}^\sigma f : \sigma \in \Phi\}$ and $\{{}^\sigma f' : \sigma \in \Phi'\}$ have a common non-zero cusp form, which implies that $f' = {}^\sigma f$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ (cf. Proposition 3.2 in [1]). Since $h \in \langle {}^\tau f : \tau \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/K)\rangle \cap \langle {}^\tau f' : \tau \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/K)\rangle$, it follows that $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/K)$. □

Proposition 5.3. *For every positive divisor d of $(p-1)/2$ there is a unique abelian variety A_f of CM elliptic type of level p^2 such that the Nebentypus of f has order d; this abelian variety satisfies that $K \not\subseteq E_f$ and* $\dim A_f = [H : K]\varphi(d)$*, where φ is the Euler function.*

Proof. Let d be a divisor of $(p-1)/2$ and take $\psi \in \mathcal{X}$ such that its eta-character has order $2\,d$. Let us denote by f the newform attached to ψ, whose Nebentypus ε has order d. First, let us show that $K \not\subseteq E_f$. Indeed, let $\psi_c \in \mathcal{X}$ defined by $\psi_c(\mathfrak{a}) = \overline{\psi(\bar{\mathfrak{a}})}$. The eta-character and the normalized newform attached to ψ_c are clearly $\bar{\eta}$ and $\bar{f}$, respectively. Since $\ker\bar{\eta} = \ker\eta$, Lemma 5.2 (ii) ensures that $\bar{f} \in \{{}^\sigma f : \sigma \in \Phi\}$, which implies $K \not\subseteq E_f$. The same argument can be applied to another newform f' obtained from $\psi' \in \mathcal{X}$ whose associated character η' has order $2d$ to show that f' belongs to $\{{}^\sigma f : \sigma \in \Phi\}$, which proves that A_f is unique when the order of ε has been fixed.

Since $K \not\subseteq E_f$, the equality $\dim A_f = [E_f : \mathbb{Q}] = [E : K]$ holds. Now, we have that $[E\colon K] = |\{{}^\sigma f : \sigma \in \Phi\}| = |\{{}^\sigma\psi : \sigma \in \Phi\}|$. Again using part (ii) of Lemma 5.2, we obtain

$$[E : K] = |\{\sigma \in \Phi\colon \eta = {}^\sigma\eta\}| \cdot |\{{}^\sigma\eta\colon \sigma \in \Phi\}| = |\{\sigma \in \Phi\colon \eta = {}^\sigma\eta\}| \cdot \varphi(d).$$

Since the condition ${}^\sigma\eta = \eta$ is equivalent to $\psi/{}^\sigma\psi$ being a character of $\mathrm{Gal}(H/K)$, it follows $\dim A_f = [H : K]\varphi(d)$. □

Remark 5.1. Note that the number of abelian varieties A_f of CM elliptic type of level p^2 is the number of divisors of $(p-1)/2$. Also for every number field L intermediate between H and $H \cdot \mathbb{Q}(\zeta_p)$ there is a unique abelian variety A_f of CM elliptic type and level p^2 for which L is its splitting field as defined in Section 3.

Next, in order to show that the CM elliptic optimal quotients of A_f in $J_1(p^2)$ have endomorphism ring isomorphic to $\mathcal{O}_K$, we shall need to use some auxiliary congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of level p^2. To this end, fix a newform f in $S_2(\Gamma_1(p^2))$ attached to a Hecke character $\psi \in \mathcal{X}$. Let ε denote the Nebentypus of f. Let us consider the following congruence subgroups of level p^2:

$$\Gamma_p = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^2)\colon a \equiv d \equiv 1 \pmod{p}\right\},$$

and Γ_ε as in the introduction; i.e.,

$$\Gamma_\varepsilon = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^2)\colon \varepsilon(d) = 1\right\}.$$

It is clear that $\Gamma_1(p^2) \subseteq \Gamma_p \subseteq \Gamma_\varepsilon$ and $f \in S_2(\Gamma_\varepsilon)$. For any intermediate congruence subgroup Γ of level p^2 satisfying $\Gamma_1(p^2) \subseteq \Gamma \subseteq \Gamma_\varepsilon$, let X_Γ be the modular curve over $\mathbb{Q}$ attached to Γ. We shall denote by $A_f^{(\Gamma)}$ the optimal quotient of the jacobian of X_Γ attached to f by Shimura. More precisely, let I_f be the annihilator of f in the Hecke algebra acting on $\mathrm{Jac}(X_\Gamma)$. Then

$$A_f^{(\Gamma)} = \mathrm{Jac}(X_\Gamma)/I_f\,(\mathrm{Jac}(X_\Gamma))\,.$$

Proposition 5.4. *Let f and Γ be as above. Then all elliptic optimal quotients of $A_f^{(\Gamma)}$ have complex multiplication by $\mathcal{O}_K$.*

Proof. Fix an elliptic direction in $\Omega^1(A_f)$ and let C_Γ be an elliptic optimal quotient attached to this direction. By Proposition 5.3 and Theorem 1.2, we know that $K \not\subseteq E_f$ and thus all endomorphisms of $A_f^{(\Gamma)}$ are defined over its splitting field, say L, that satisfies $L \subseteq K_{\mathfrak{p}}$. Let c_Γ denote the conductor of the order $\mathcal{O}_\Gamma \simeq \operatorname{End}_L(C_\Gamma)$ in $\mathcal{O}_K$. We want to show that $c_\Gamma = 1$, and split the proof in three steps.

Step 1: $c_\Gamma \mid 2$ *for all* Γ. Since $\operatorname{End}(C_\Gamma) = \operatorname{End}_L(C_\Gamma)$, one has that L contains the ring class field of $\mathcal{O}_\Gamma$, say K_Γ. Notice that $K_\Gamma \subseteq L \subseteq K_{\mathfrak{p}}$. But $p \nmid c_\Gamma$, since otherwise p must divide $[L : H]$ (cf. Proposition 7.24 in [4]) and this degree is a divisor of $(p-1)/2$. Hence, K_Γ is an unramified extension of the Hilbert class field and, therefore, it must coincide with H. Again by Proposition 7.24 in [4], we obtain that $c_\Gamma \mid 2$.

Step 2: c_Γ *does not depend on* Γ. We consider the natural projection $\pi\colon X_\Gamma \to X_{\Gamma_\varepsilon}$. The degree of π is odd since it divides $[\Gamma_1(p^2) : \Gamma_0(p^2)/\{\pm 1\}] = p(p-1)/2$ and $p \equiv 3 \bmod 4$.

Let $\pi_{\Gamma,\Gamma_\varepsilon}\colon \operatorname{Jac}(X_\Gamma) \to A_{\Gamma,\Gamma_\varepsilon}$ be the optimal quotient over $\mathbb{Q}$ for which there is an isogeny $\nu\colon A_{\Gamma,\Gamma_\varepsilon} \to \operatorname{Jac}(X_{\Gamma_\varepsilon})$ defined over $\mathbb{Q}$ rending the following diagram

$$\begin{tikzcd}
\operatorname{Jac}(X_\Gamma) \arrow[rr, "\pi_*"] \arrow[dr, "\pi_{\Gamma,\Gamma_\varepsilon}"'] & & \operatorname{Jac}(X_{\Gamma_\varepsilon}) \\
& A_{\Gamma,\Gamma_\varepsilon} \arrow[ur, "\nu"'] &
\end{tikzcd}$$

commutative. Since every element of the group $H_1(X_{\Gamma_\varepsilon}, \mathbb{Z})/\pi_*(H_1(X_\Gamma, \mathbb{Z}))$ has order dividing $\deg \pi$, the cardinality of this group is odd. From the group isomorphism $\ker \nu \simeq H_1(X_{\Gamma_\varepsilon}, \mathbb{Z})/\pi_*(H_1(X_\Gamma, \mathbb{Z}))$, it follows that $\deg \nu$ is odd. Since $A_f^{(\Gamma)}$ is an optimal quotient of $A_{\Gamma,\Gamma_\varepsilon}$, there is an isogeny $\nu_f\colon A_f^{(\Gamma)} \to A_f^{(\Gamma_\varepsilon)}$ whose degree divides $\deg \nu$. Hence, for every optimal elliptic quotient $\pi_\Gamma\colon A_f^{(\Gamma)} \to C_\Gamma$ there is an optimal elliptic quotient $\pi_\varepsilon\colon A_f^{(\Gamma_\varepsilon)} \to C_{\Gamma_\varepsilon}$ and an isogeny $\mu\colon C_\Gamma \to C_{\Gamma_\varepsilon}$ rending the diagram

$$\begin{tikzcd}
A_f^{(\Gamma)} \arrow[r, "\nu_f"] \arrow[d, "\pi_\Gamma"'] & A_f^{(\Gamma_\varepsilon)} \arrow[d, "\pi_\varepsilon"] \\
C_\Gamma \arrow[r, "\mu"] & C_{\Gamma_\varepsilon}
\end{tikzcd}$$

commutative. It is clear that $\deg \mu$ is odd since it divides $\deg \nu_f$. So c_{Γ_ε} and c_Γ can only differ by an odd factor, which implies that c_Γ is independent of the group Γ.

Step 3: $c_\Gamma = 1$ *for all* Γ. Now, it suffices to prove $c_\Gamma = 1$ for a particular subgroup Γ. We consider $\Gamma = \Gamma_p$. Following Shimura in [17], we know that the matrix

$$\begin{pmatrix} 1 & 1/p \\ 0 & 1 \end{pmatrix}$$

lies in the normalizer of Γ_p in $\mathrm{SL}_2(\mathbb{R})$ and provides an automorphism u of X_{Γ_p} of order p. Set

$$G = \sum_{\substack{1 \le i < p \\ \chi(i)=1}} (u^*)^i \in \operatorname{End}\operatorname{Jac}(X_{\Gamma_p}).$$

We claim that G leaves stable the subvariety $I_f(\operatorname{Jac}(X_{\Gamma_p}))$, which is equivalent to saying that G leaves stable the vector space generated by the set of eigenforms in $S_2(\Gamma_p)$ which are not Galois conjugates of f. In fact, the action of G on all eigenforms of $S_2(\Gamma_p)$ can be described as follows. It is well-known that if we denote by New_Γ the set of normalized newforms in $S_2(\Gamma)$, then the set of normalized eigenforms in $S_2(\Gamma_p)$ is the disjoint union of New_{Γ_p}, $\mathcal{S}_1$, and $\mathcal{S}_2$, where $\mathcal{S}_1 = \mathrm{New}_{\Gamma_1(p)} \cap S_2(\Gamma_p)$, $\mathcal{S}_2 = B_p(\mathrm{New}_{\Gamma_1(p)}) \cap S_2(\Gamma_p)$, and B_p is the operator acting as $B_p(h(q)) = h(q^p)$. With $\zeta_p = e^{2\pi i/p}$ and from the equality

$$\sum_{\substack{1 \le i < p \\ \chi(i)=1}} \zeta_p^i = \frac{-1+\sqrt{-p}}{2},$$

it can be easily checked that every eigenform $h(q) = \sum_{n \ge 1} b_n q^n \in S_2(\Gamma_p)$ satisfies:

$$G^*(h) = \begin{cases} \dfrac{-1+\sqrt{-p}}{2} h + \dfrac{p-\sqrt{-p}}{2} b_p\, B_p(h) & \text{if } h \in \mathrm{New}_{\Gamma_p} \cup \mathcal{S}_1, \\ \dfrac{p-1}{2} h & \text{if } h \in \mathcal{S}_2. \end{cases}$$

The claim follows from the fact that all $h \in \mathrm{New}_{\Gamma_p}$ have level p^2 and Nebentypus whose conductor divides p and, thus, $b_p = 0$ (see Subsection 1.8 in [5]).

Since G leaves stable the subvariety $I_f(\operatorname{Jac}(X_{\Gamma_p}))$, then G induces an endomorphism of $A_f^{(\Gamma_p)}$, which we still denote by G. Due to the fact that G acts on $\Omega^1(A_f^{(\Gamma_p)})$ as the multiplication by $(-1+\sqrt{-p})/2$, it follows that G leaves stable all subvarieties of $A^{(\Gamma_p)}$. Thus, $(-1+\sqrt{-p})/2 \in \mathcal{O}_{\Gamma_p}$ and the statement follows. □

As for Gross's elliptic curves, we obtain the following result, which concludes the proof of Theorem 1.4.

Corollary 5.5. *Let f be a CM normalized newform with trivial Nebentypus. The elliptic curve $A(p)$ and its Galois conjugates are the optimal quotients of $A_f^{(\Gamma)}$ over the Hilbert class field H, for all subgroups Γ with $\Gamma_1(p^2) \subseteq \Gamma \subseteq \Gamma_0(p^2)$.*

Proof. By Theorem 20.1 in [9], we know that $A(p)$ is a quotient of $J_0(p^2)$ defined over H, attached to a newform f with trivial Nebentypus. Notice that the corresponding field L coincides with the Hilbert class field H. Since we have $K \not\subseteq E_f$, by Theorems 1.1 and 1.2, every elliptic optimal quotient C_Γ of $A_f^{(\Gamma)}$ is defined over H and the abelian variety $A_f^{(\Gamma)}$ is simple over K. Since dim $A_f^{(\Gamma)} = [H : K]$, it follows that $A_f^{(\Gamma)}$ is K-isogenous to the Weil restriction $\mathrm{Res}_{H/K}\, C_\Gamma$. In [9], Gross shows that $A_f^{(\Gamma)}$ is K-isogenous to $\mathrm{Res}_{H/K}\, A(p)$. Therefore, on the one hand, there is $\sigma \in \mathrm{Gal}(H/K)$ such that $A(p)$ and ${}^{\sigma}C_\Gamma$ are $\mathbb{Q}^{\mathrm{alg}}$-isomorphic. On the other hand, by Theorem 5.4, $A(p)$ and ${}^{\sigma}C_\Gamma$ are H-isogenous. Hence, $A(p)$ is H-isomorphic to ${}^{\sigma}C_\Gamma$ and the claim follows. □

6. Canonical CM elliptic direction for $A(p)$

When the class number of K is greater than one, there are infinitely many elliptic directions in $S_2(\Gamma_0(p^2))$ attached to different parametrizations $J_0(p^2) \to A(p)$. Here, we shall emphasize one of them (we call it canonical) in terms of a particular one-cocycle that can be constructed by means of the Dedekind eta-function.

Let $\mathcal{O}_H$ be the ring of integers of the Hilbert class field H. For all $a \in K$ coprime with $\mathfrak{p}$, we denote by $(\frac{a}{\mathfrak{p}})$ the Jacobi symbol $(\frac{m}{p})$, where m is an integer such that $a \equiv m \pmod{\mathfrak{p}}$. One has $\eta(a) = (\frac{a}{\mathfrak{p}})$. By [10], we know that there is a unique map $\delta\colon I(\mathfrak{p}) \to H$ with the following two requirements:

(i) $\delta(\mathfrak{a})^{12} = \Delta(\mathcal{O})/\Delta(\mathfrak{a})$,

(ii) $\left(\frac{\mathrm{N}_{H/K}(\delta(\mathfrak{a}))}{\mathfrak{p}}\right) = 1$,

for all $\mathfrak{a} \in I(\mathfrak{p})$. Moreover, this map also satisfies the following conditions:

(iii) $\delta(\mathfrak{a})\mathcal{O}_H = \mathfrak{a}\mathcal{O}_H$,

(iv) $\delta(\mathfrak{a} \cdot \mathfrak{b}) = \delta(\mathfrak{a}) \cdot {}^{\mathfrak{a}^{-1}}\delta(\mathfrak{b})$ for all $\mathfrak{a}, \mathfrak{b} \in I(\mathfrak{p})$,

(v) $\delta(\bar{\mathfrak{a}}) = \overline{\delta(\mathfrak{a})}$ for all $\mathfrak{a} \in I(\mathfrak{p})$.

By taking into account conditions (ii) and (iv), and since $[H : K]$ is odd, we also obtain:

(vi) for all $\mathfrak{a} \in P(\mathfrak{p})$, one has $\delta(\bar{\mathfrak{a}}) \in K$ and $\left(\frac{\delta(\mathfrak{a})}{\mathfrak{p}}\right) = 1$.

For every $\mathfrak{a} \in I(\mathfrak{p})$, we set

$$\lambda(\mathfrak{a}) := {}^{\mathfrak{a}}\delta(\mathfrak{a}) = \frac{\mathrm{N}(\mathfrak{a})}{\delta(\bar{\mathfrak{a}})}. \tag{5}$$

The map $\lambda\colon I(\mathfrak{p}) \to H$ also satisfies conditions (ii), (iii), (v), and (vi). But now conditions (i) and (iv) are replaced with (i′) $\lambda(\mathfrak{a})^{12} = \mathrm{N}(\mathfrak{a})^{12}\frac{\Delta(\bar{\mathfrak{a}})}{\Delta(\mathcal{O}_K)}$,

and the one-cocycle condition:

(iv′) $\lambda(\mathfrak{a}\cdot\mathfrak{b}) = \lambda(\mathfrak{a})\cdot {}^{\mathfrak{a}}\lambda(\mathfrak{b})$, for all $\mathfrak{a}, \mathfrak{b} \in I(\mathfrak{p})$.

Conditions (vi) and (iv′) imply that the one-cocycle λ belongs to $[A_f]$ for all A_f of CM elliptic type and level p^2.

Remark 6.1. Notice that the above one-cycle λ can be effectively computed by using the Dedekind eta-function on ideals (as Rodríguez-Villegas does in [13]), and it coincides with what Hajir denotes ϕ in Definition 2.3 in [11].

Let f denote the normalized newform in $S_2(\Gamma_0(p^2))$ attached to a Hecke character ψ whose eta-character has order 2. By Section 3, the splitting field L of A_f is H. Let $S_2(A_f)$ be the $\mathbb{C}$-vector space generated by the Galois conjugates of the newform f attached to ψ and let ω denote a Néron differential of Gross's elliptic curve $A(p)$.

Proposition 6.1. *Let f be as above. There is an optimal quotient $\pi\colon J_0(p^2) \to A(p)$ such that $\pi^*(\omega) = c\,g(q)\,dq/q$, where*

$$g(q) = \sum_{(\mathfrak{a},\mathfrak{p})=1} \delta(\mathfrak{a})q^{\mathrm{N}(\mathfrak{a})} \in S_2(A_f),$$

and $c \in \mathbb{Z}$ is a unit in $\mathbb{Z}[\frac{1}{2p}]$.

Proof. By Lemma 5.3, we have $[E : K] = [L : K]$ and, thus, all one-cocycles in $[A_f]$ are modular. Therefore, by Theorem 1.3 we have that

$$g(q) = \sum_{(\mathfrak{a},\mathfrak{p})=1} {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})q^{\mathrm{N}(\mathfrak{a})} = \sum_{(\mathfrak{a},\mathfrak{p})=1} \delta(\mathfrak{a})q^{\mathrm{N}(\mathfrak{a})}$$

is a normalized cusp form in $S_2(A_f)$ for which there is an optimal elliptic quotient C_λ given by the lattice

$$\Lambda_g = \left\{2\pi i \int_\gamma g(z)dz\colon \gamma \in H_1(X_0(p^2),\mathbb{Z})\right\}.$$

Since $\delta(\bar{\mathfrak{a}}) = \overline{\delta(\mathfrak{a})}$ for all $\mathfrak{a} \in I(\mathfrak{p})$, it follows that $g(q) \in H_0[[q]]$. Thus, $g(q)\,dq/q \in \Omega^1(X_0(p^2))_{/H_0}$. Hence, the natural morphism $\pi\colon X_0(p^2) \to C_\lambda$ is defined over H_0. Notice that necessarily one has $\Lambda_g = \Omega\cdot\mathcal{O}_K$, for some $\Omega \in \mathbb{C}^*$. Indeed, $\mathcal{O}_K$ is the only ideal $\mathfrak{a}$ such that $j(\mathfrak{a}) = \overline{j(\mathfrak{a})}$ since $[H : K]$ is odd. Thus, we have $j(\Lambda_g) = j(\mathcal{O}_K)$. Since A_f is $\mathbb{Q}$-isogenous to $\mathrm{Res}_{H_0/\mathbb{Q}}(C_\lambda)$ and to $\mathrm{Res}_{H_0/\mathbb{Q}}(A(p))$, it follows that C_λ and $A(p)$ are H_0-isogenous and, therefore, H_0-isomorphic. Therefore, there exists $c \in H_0^*$ such that $\pi^*(\omega) = c\,g(q)\,dq/q$. It is clear that $\Delta(\Lambda_g) = -p^3c^{12}$.

The Manin ideal attached to π is $c\,\mathcal{O}_{H_0}$ (we refer to Section 4 in [8] for more details on the Manin ideal). By Propositions 4.1 and 4.2 in [8], we know that $c\mathcal{O}_{H_0}$ is an integral ideal and it can only be divided by primes lying over 2 or p. Now, we want to prove that $c \in \mathbb{Z}$. Since $\pi^*(\omega/c) = g\,dq/q$, the one-cocycle attached to ω/c is λ. This means that for every $\mathfrak{a} \in I(\mathfrak{p})$ there is an isogeny of degree $\mathrm{N}(\mathfrak{a})$,

$$\mu\colon {}^{\mathfrak{a}^{-1}}C_\lambda \to C_\lambda,$$

such that $\mu^*(\omega/c) = {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a})\cdot{}^{\mathfrak{a}^{-1}}(\omega/c)$. Taking into account that $j(\mathfrak{a}) = {}^{\mathfrak{a}^{-1}}j(\mathcal{O}_K)$, we obtain that the lattice corresponding to ${}^{\mathfrak{a}^{-1}}C_\lambda$ is $\frac{1}{\delta(\mathfrak{a})}\cdot\Omega\mathfrak{a}$. Finally, we have that

$${}^{\mathfrak{a}^{-1}}\Delta(\Omega\mathcal{O}_K) = \Delta\Big(\frac{1}{\delta(\mathfrak{a})}\Omega\mathfrak{a}\Big) = \delta(\mathfrak{a})^{12}\Delta(\Omega\mathfrak{a}) = \frac{\Delta(\mathcal{O}_K)}{\Delta(\mathfrak{a})}\Delta(\Omega\mathfrak{a}) = \Delta(\Omega\mathcal{O}_K).$$

Therefore, $\Delta(\Lambda) \in K \cap H_0 = \mathbb{Q}$ and $c^{12} \in \mathbb{Q}$. Since $\mathbb{Q}(c) \subseteq H$ is unramified outside p and there is not a real quadratic field of discriminant p, it follows that $c^3 \in \mathbb{Q}$. Finally, since H does not contain the 3rd roots of unity (recall $p > 3$), one obtains $c \in \mathbb{Q}$. □

Remark 6.2. Since $c \in K^*$, the one-cocycle attached to ω is also λ. In this sense, we say that the normalized cusp form g is the canonical cusp form attached to $A(p)$.

For when the class number of K is 1 (that is, $p = 7, 11, 19, 43, 67, 163$), one has that π is defined over $\mathbb{Q}$ and c coincides with the (classical) Manin constant. Then $c = \pm 1$ in these cases since Manin's conjecture has been checked for all elliptic curves over $\mathbb{Q}$ with conductor ≤ 130000 in Cremona's tables. We have computed c for the remaining primes $p \leq 100$ (that is, $p = 23, 31, 47, 59, 71, 79, 83$) and we have also obtained that $c = \pm 1$. It seems reasonable to expect $c = \pm 1$ for all $A(p)$.

Remark 6.3. In general, as already mentioned, there are infinitely many normalized cusp forms $g' \in S_2(A_f)$ whose directions are pullbacks of $\Omega^1(A(p))$ under modular parametrizations $\pi'\colon A_f \to A(p)$. For each one of them, there is a one-cocycle λ' (cohomologous to λ) such that

$$g' = \sum_{\mathfrak{a}} {}^{\mathfrak{a}^{-1}}\lambda'(\mathfrak{a})q^{\mathrm{N}(\mathfrak{a})} \in S_2(A_f),$$

and a constant $c' \in H_0$ with $\pi'^*(\omega) = c'g'$. The concern on whether the constant c is ± 1 is already in [9], see Question 23.2.2 on p. 81, but without fixing π'. However, $c' \neq \pm 1$ unless $\pi' = \pi$ (canonical) as in Theorem 6.1, although the Manin ideal attached to any $\pi' \neq \pi$ might still be $\mathcal{O}_K$ as well.

We end this section giving an expression for the transcendental $\Omega \in \mathbb{C}^*$ attached to the lattice Λ of $A(p)$, which generalizes the one given by Gross in [9] for when K has class number one. Keeping the above notations, we set

$$\rho := \prod_{\substack{\mathfrak{b} \in \mathrm{Gal}(H/K) \\ (\mathfrak{b},\mathfrak{p})=1}} \frac{\delta(\mathfrak{b})}{\psi(\mathfrak{b})}.$$

It is clear that ρ is well defined, independent of the Galois conjugate of ψ, and $\rho \in \mathcal{O}_H^*$. Let h denote the class number of K, and consider

$$\{\mathcal{O}_K, \mathfrak{b}_1, \dots, \mathfrak{b}_{(h-1)/2}, \dots, \bar{\mathfrak{b}}_1, \dots, \bar{\mathfrak{b}}_{(h-1)/2}\}$$

a set of representatives of $\mathrm{Gal}(H/K)$ with $(\mathfrak{b}_i, \mathfrak{p}) = 1$. Then we can rewrite

$$\rho = \prod_{i=1}^{(h-1)/2} \frac{\delta(\mathfrak{b}_i)\,\delta(\bar{\mathfrak{b}}_i)}{\mathrm{N}(\mathfrak{b}_i)}. \tag{6}$$

Indeed, since $\delta(\mathfrak{b})/\psi(\mathfrak{b})$ is independent of the class of $\mathfrak{b}$ in $\mathrm{Gal}(H/K)$, it suffices to prove that $\psi(\mathfrak{b}) \cdot \psi(\bar{\mathfrak{b}}) = \mathrm{N}(\mathfrak{b})$. But this is a consequence of

$$\left(\frac{\mathrm{N}(\mathfrak{b})}{p}\right) = \left(\frac{\mathrm{N}(\mathfrak{b})}{p}\right)^h = \left(\frac{\beta}{\mathfrak{p}}\right)\left(\frac{\bar{\beta}}{\mathfrak{p}}\right) = \left(\frac{\beta}{\mathfrak{p}}\right)^2 = 1,$$

where $\beta \in K$ is a generator of $\mathfrak{b}^h$. Observe that ρ is a positive unit in $\mathcal{O}_{H_0}^*$.

Proposition 6.2. *Let $\Lambda = \Omega \cdot \mathcal{O}_K$ be the lattice attached to $A(p)$. Then*

$$\Omega = \pm\, i^{(p+1)/4} \sqrt[h]{\rho \cdot (2\pi)^{(2h+1-p)/4} \cdot \sqrt{p}^{(1-3h)/2} \cdot \prod_{\substack{1 \le m < p \\ \chi(m)=1}} \Gamma\left(\frac{m}{p}\right)},$$

where the h-th root is taken to be real.

Proof. By the Chowla–Selberg formula [2], we know that

$$\prod_{\mathfrak{a} \in \mathrm{Gal}(H/K)} \mathrm{N}(\mathfrak{a})^{-6} \Delta(\tau_{\mathfrak{a}}) = \left(\frac{2\pi}{p}\right)^{6h} \left(\prod_{m=1}^{p-1} \Gamma\left(\frac{m}{p}\right)^{\chi(m)}\right)^6,$$

where $\langle 1, \tau_{\mathfrak{a}} \rangle = \frac{1}{\mathrm{N}(\mathfrak{a})}\mathfrak{a}$. Since λ is the one-cocycle attached to ω, we have that

$$\Delta(\tau_{\mathfrak{a}}) = \mathrm{N}(\mathfrak{a})^{12} \Delta(\mathfrak{a}) = \mathrm{N}(\mathfrak{a})^{12} \Delta\left(\frac{\Omega}{\delta(\mathfrak{a})}\mathfrak{a}\right) \frac{\Omega^{12}}{\delta(\mathfrak{a})^{12}} = -p^3 \frac{\mathrm{N}(\mathfrak{a})^{12}}{\delta(\mathfrak{a})^{12}} \Omega^{12}. \tag{7}$$

Combining (6), (7), and Gauss's identity

$$\prod_{i=1}^{n-1} \Gamma\Big(\frac{i}{n}\Big) = (2\pi)^{(n-1)/2} n^{-1/2},$$

the statement follows by taking into account that Ω lies in $\mathbb{R}$ or $i\,\mathbb{R}$ according to $p \equiv -1 \pmod 8$ or not (cf. [9]). □

As a result, we obtain the following fact, which concludes the proof of Theorem 1.5.

Corollary 6.3. *With the above notations, one has*

$$\left\{2\pi\, i \int_\gamma g(z)dz\colon \gamma \in H_1(X_0(p^2), \mathbb{Z})\right\} = \tfrac{1}{c} \cdot \Omega \cdot \mathcal{O}_K.$$

7. CM elliptic directions for non-trivial Nebentypus

In this section, we shall consider arbitrary Hecke characters mod $\mathfrak{p}$. Let ψ in $\mathcal{X}$ and let η be its eta-character. Let f denote the normalized newform attached to ψ. In order to find the elliptic directions in $S_2(A_f)$, one needs to determine the modular one-cocycles λ_u in $[A_f]$. Then the normalized cusp forms

$$g_u = \sum_{(\mathfrak{a},\mathfrak{p})=1} {}^{\mathfrak{a}^{-1}}\lambda_u(\mathfrak{a})\, q^{\mathrm{N}(\mathfrak{a})}$$

are the elliptic directions in $S_2(A_f)$. Recall that in the particular case $\eta^2 = 1$, all one-cocycles are modular. In general, as explained above, to find the modular one-cocycles amounts to an eigenvector problem. In our particular setting, the following lemma will be useful since it will allow to handle certain linear systems by means of a quotient polynomial ring.

Lemma 7.1. *Let M/F be a cyclic field extension of degree k. Fix a generator τ of $\mathrm{Gal}(M/F)$, and let μ_k be the group of k-th roots of unity. Let $\mathcal{E} = \mathrm{End}_{F[\mathrm{Gal}(M/F)]}(M)$ be the F-algebra of $\mathrm{Gal}(M/F)$-equivariant F-linear endomorphisms of M. One has*

(i) *the map $\Theta\colon F[X]/(X^k - 1) \to \mathcal{E}$ given by*

$$\Theta\Big(\sum_{i=1}^{k} a_i X^i\Big)(u) = \sum_{i=1}^{k} a_i\, {}^{\tau^i}u, \quad \textit{for all } u \in M,$$

is well defined and an isomorphism of F-algebras.

(ii) *For every $p(X) \in F[X]/(X^k - 1)$, let $\mathcal{Z} = \{\zeta \in \mu_k \colon p(\zeta) = 0\}$. Then the endomorphism $G = \Theta(p(X))$ diagonalizes and its characteristic polynomial is*

$$(-1)^k \prod_{i=1}^{k} \left(X - p(\zeta_k^i)\right),$$

where $\zeta_k = e^{2\pi i/k}$. We have $\dim_F \ker G = |\mathcal{Z}|$, *and*

$$\ker G = \Theta\left(\frac{X^k - 1}{\prod_{\zeta \in \mathcal{Z}}(X - \zeta)}\right)(M). \tag{8}$$

Proof. It is obvious that Θ is well defined and a morphism of F-algebras. Choose $\alpha \in M$ such that $\{\tau^i \alpha\}_{1 \le i \le k}$ is a F-basis of M. The morphism Θ is injective because $\Theta(q(X)) = 0$ implies that $\Theta(q(X))(\alpha) = 0$ and, then, $q(X) = 0$. For a given $G \in \mathcal{E}$, we have that $G(\alpha) = \sum_{i=1}^{k} a_i \tau^i \alpha$ for some $a_i \in F$ and, thus, $G(u) = \sum_{i=1}^{k} a_i \tau^i u$ for all $u \in M$. Therefore, Θ is surjective and part (i) is proved.

We consider the F-algebra monomorphism $\Psi \colon \mathcal{E} \to \operatorname{End}_F F[X]/(X^k - 1)$ defined by $\Psi(G) = \widehat{G}$, where

$$\widehat{G}(q(X)) = \Theta^{-1}(G) \cdot q(X), \quad \text{for all } q(X) \in F[X]/(X^k - 1). \tag{9}$$

Now it suffices to prove part (ii) for $\widehat{G}$. Note that for any field extension F_0/F, the relation (9) allows us to consider $\widehat{G}$ as a F_0-linear endomorphism of $F_0[X]/(X^k - 1)$.

Let $G = \Theta(p(X))$. The set of eigenvalues of $\widehat{G}$ is $\{p(\zeta_k^i) \colon 1 \le i \le k\}$. Indeed, if $\beta \in F_0$ is an eigenvalue of eigenvector $q(X) \in F_0[X]/(X^k - 1)$, then there exists $\zeta \in \mu_k$ such that $q(\zeta) \neq 0$ and, thus, $\beta = p(\zeta)$. Conversely, if $\beta = p(\zeta)$ for some $\zeta \in \mu_k$ then $q(X) = \prod_{\zeta' \in \mu_k \setminus \{\zeta\}}(X - \zeta')$ is an eigenvector with eigenvalue β. Notice that all eigenvalues of $\widehat{G}$ are in $F_0 = F(\mu_k)$.

Now, let $\beta = p(\zeta)$ for some $\zeta \in \mu_k$ and we will prove that

$$\dim_{F_0} \ker(\widehat{G} - \beta \,\mathrm{id}) = |\{\zeta \in \mu_k \colon p(\zeta) = \beta\}|,$$

which implies part (ii) except for the equality (8). Note that by a translation of $\widehat{G}$, we can (and do) assume $\beta = 0$. Then one has

$$\begin{aligned} \ker \widehat{G} &= \{q(X) \in F_0[X]/(X^k - 1) \colon q(\zeta) = 0 \quad \text{for all } \zeta \in \mu_k \setminus \mathcal{Z}\} \\ &= \{q(X) \in F_0[X]/(X^k - 1) \colon q(X) = \prod_{\zeta \in \mu_k \setminus \mathcal{Z}} (X - \zeta)\, r(X),\ \deg r < |\mathcal{Z}|\}. \end{aligned}$$

It follows that $\dim_{F_0} \ker \widehat{G} = |\mathcal{Z}|$ and $\ker \widehat{G} = \ker(\Psi \circ \Theta)(\prod_{\zeta \in \mathcal{Z}}(X - \zeta))$. Finally, the equality (8) is a consequence of the fact that $q(X) = \prod_{\zeta \in \mathcal{Z}}(X - \zeta) \in F[X]$ is coprime with $r(X) = (X^k - 1)/p(X)$ and $q(X) \cdot r(X)$ is zero in $F[X]/(X^k - 1)$. □

Now, we focus our attention on the Hecke character $\psi \in \mathcal{X}$. For the sake of simplicity, let us assume that its eta-character satisfies $\mathrm{ord}(\eta) = p-1$. Since $\ker \eta$ is trivial, the corresponding field L is the ray class field of K mod $\mathfrak{p}$; that is, $L = H \cdot \mathbb{Q}(\zeta_p)$ (cf. Propsition 5.1). The cyclic group $\mathrm{Gal}(L/H)$ has order $k := (p-1)/2$. Also, let $\mathcal{E} = \mathrm{End}_{H[\mathrm{Gal}(L/H)]}(L)$ be the H-algebra of $\mathrm{Gal}(L/H)$-equivariant endomorphisms. After fixing a generator τ of $\mathrm{Gal}(L/H)$, consider Θ as in Lemma 7.1. Finally, let $\lambda\colon I(\mathfrak{p}) \to L^*$ be the one-cocycle in Section 6. To find the elliptic directions in $S_2(A_f)$ turns out to be equivalent to find the twisted one-cocycles $\lambda_u(\mathfrak{a}) = \lambda(\mathfrak{a})\, u/{}^{\mathfrak{a}}u$ which are modular. Note that now λ is not modular in $[A_f]$.

Proposition 7.2. *For all $u \in L^*$, the following conditions are equivalent:*

(i) *the one-cocycle $\lambda_u(\mathfrak{a}) = \lambda(\mathfrak{a})\frac{u}{{}^{\mathfrak{a}}u}$ is modular;*

(ii) $u = \Theta\big(\frac{X^k-1}{\Phi_k(X)}\big)(v)$, *for some $v \notin \ker \Theta\big(\frac{X^k-1}{\Phi_k(X)}\big)$.*

In particular, for $u = \Theta\big(\frac{X^k-1}{\Phi_k(X)}\big)(\zeta_p)$ the one-cocycle λ_u is modular. Here, $\Phi_k(X)$ denotes the k-th cyclotomic polynomial.

Proof. The values $u \in L^*$ for which λ_u is modular are the eigenvectors of the K-linear map

$$\mathrm{pr}(u) = \sum_{\mathfrak{a}\in \mathrm{Gal}(L/K)} {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a}) \Big(\sum_{\sigma\in\Phi} \frac{1}{{}^{\sigma}\psi(\mathfrak{a})}\Big)^{\mathfrak{a}^{-1}} u \tag{10}$$

with eigenvalue equal to $[L:K]$. Also, by Proposition 4.4, we know that $\mathrm{pr}/[L:K]$ is a projector, pr diagonalizes, and its characteristic polynomial is

$$([L:K]-X)^{[E:K]} X^{[L:K]-[E:K]} = \big(([L:K]-X)^{\varphi(k)} X^{k-\varphi(k)}\big)^{[H:K]}.$$

By part (i) of Lemma 5.2, we can rewrite

$$\mathrm{pr}(u) = \sum_{\mathfrak{a}\in \mathrm{Gal}(L/H)} {}^{\mathfrak{a}^{-1}}\lambda(\mathfrak{a}) \Big(\sum_{\sigma\in\Phi} \frac{1}{{}^{\sigma}\psi(\mathfrak{a})}\Big)^{\mathfrak{a}^{-1}} u.$$

Let $g \in \mathbb{Z}$ be a primitive root of $(\mathbb{Z}/p\,\mathbb{Z})^*$ such that $\eta(g) = \zeta$, where $\zeta = e^{\frac{\pi i}{k}}$. Since the set of principal ideals $\{\mathfrak{a}_j = g^{2j}\mathcal{O}_K : 1 \le j \le k\}$ is a set of representatives of $\mathrm{Gal}(L/H)$ and $\lambda(g^{2j}\mathcal{O}_K) = g^{2j}$, we have

$$G(u) := \frac{\mathrm{pr}(u)}{[H:K]} = \frac{1}{[H:K]}\sum_{j=1}^{k}\Big(\sum_{\sigma\in\Phi} {}^{\sigma}\zeta^{-2j}\Big)^{\mathfrak{a}_j^{-1}} u = \sum_{j=1}^{k} \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{-2j})^{\mathfrak{a}_j^{-1}} u.$$

Hence, G belongs to $\mathcal{E}$ and its characteristic polynomial has roots 0 and k with multiplicities $k-\varphi(k)$ and $\varphi(k)$, respectively.

Now, we fix the generator $\tau = g^{-2}\mathcal{O}_K$ of $\mathrm{Gal}(L/H)$ and apply Lemma 7.1 to the endomorphism $G - k\,\mathrm{Id} \in \mathcal{E}$. It follows that the set

$$\mathcal{Z} = \left\{\zeta' \in \mu_k \colon \textstyle\sum_{j=1}^{k} \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{-2j})(\zeta')^{2j} - k = 0\right\}$$

has cardinality $|\mathcal{Z}| = \varphi(k)$. Letting $\zeta_k = \zeta^2$, we claim that

$$\mathcal{Z} = \{\zeta_k^j \colon 1 \le j < k,\ \gcd(j,k) = 1\}.$$

Since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ acts transitively on $\mathcal{Z}$ and $|\mathcal{Z}| = \varphi(k)$, it suffices to prove that $\zeta_k \in \mathcal{Z}$. Indeed, one checks:

$$\sum_{j=1}^{k}\Big(\sum_{i\in(\mathbb{Z}/k\mathbb{Z})^*} \zeta_k^{-j\,i}\Big)\zeta_k^{j} = \sum_{j=1}^{k}\Big(\sum_{i\in(\mathbb{Z}/k\mathbb{Z})^*} \zeta_k^{(1-i)\,j}\Big) = \sum_{j=1}^{k}\Big(\sum_{i\in(\mathbb{Z}/k\mathbb{Z})^*} \zeta_k^{i\,j}\Big) = k.$$

Then, from Lemma 7.1, we obtain

$$\{u \in L \colon \mathrm{pr}(u) = [L:K]\,u\} = \Big\{u = \Theta\Big(\tfrac{X^k-1}{\Phi_k(X)}\Big)(v) \colon v \in L\Big\}.$$

Note that the image of $\Theta\Big(\frac{X^k-1}{\Phi_k(X)}\Big)$ is independent of the choice of the generator τ in $\mathrm{Gal}(L/H)$. It can be easily checked that $\Theta((X^k-1)/\Phi_k(X))$ vanishes on H, which implies that $\Theta((X^k-1)/\Phi_k(X))(\zeta_p)$ is non-zero since the class of the polynomial $(X^k-1)/\Phi_k(X)$ in $L[X]/(X^k-1)$ is non-zero. □

Example. Take $p = 7$, so that $K = \mathbb{Q}(\sqrt{-7})$ has class number one. Let ψ in $\mathcal{X}$ with eta-character satisfying $\eta(3) = e^{2\pi i/6}$. Its corresponding newform $f = \sum \psi((a))q^{\mathrm{N}(a)} \in S_2(\Gamma_1(49))$ has Nebentypus ε of order 3; note that $\psi((a)) = a\eta(a)$ for all $a \in \mathcal{O}_K$. The one-cocyle λ satisfies $\lambda((a)) = a$ with the unique choice of sign for a such that the symbol $(a/\sqrt{-7}) = 1$. This one-cocycle is not modular for ψ (in fact, it is modular for the Hecke character in $\mathcal{X}$ with eta-character of order 2 in which case the (unique) elliptic direction coincides with the rational newform in $S_2(\Gamma_0(49))$ giving rise to the elliptic curve 49A1 in Cremona's notation.) Thus, we need to twist λ by a coboundary in order to get a modular one-cocycle. According to Proposition 7.2, we can take, for instance, $u = \Theta(X-1)(\zeta_7) = \zeta_7^2 - \zeta_7$ and the cuspidal form $g_u = \sum {}^{\mathfrak{a}^{-1}}\lambda_u(\mathfrak{a})q^{\mathrm{N}(\mathfrak{a})} = \sum \lambda((a))^{(a^2)}u/u\, q^{\mathrm{N}(a)} \in S_2(\Gamma_1(49))$ is an elliptic direction of A_f. A computer calculation shows the lattice Λ for the corresponding elliptic optimal quotient from $\mathrm{Jac}(X_{\Gamma_\varepsilon})$ satisfies: $c_4(\Lambda) = c_4(A(7))u^4$, and $c_6(\Lambda) = c_6(A(7))u^6$.

References

[1] M. H. Baker, E. González-Jiménez, J. González, and B. Poonen, Finiteness results for modular curves of genus at least 2. *Amer. J. Math.* **127** (6) (2005), 1325–1387. Zbl 1127.11041 MR 2183527

[2] S. Chowla and A. Selberg, On Epstein's zeta-function. *J. Reine Angew. Math.* **227** (1967), 86–110. Zbl 0166.05204 MR 0215797

[3] G. Cornell and J. H. Silverman (eds.), *Arithmetic geometry*. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984 Springer-Verlag, New York 1986. Zbl 0596.00007 MR 0861969

[4] D. A. Cox, *Primes of the form* $x^2 + ny^2$. John Wiley & Sons Inc., New York 1989. Zbl 0701.11001 MR 1028322

[5] P. Deligne and J.-P. Serre, Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup.* (4) **7** (1974), 507–530. Zbl 0321.10026 MR 0379379

[6] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication. p-adic* L *functions.* Perspect. Math. 3, Academic Press Inc., Boston, Mass., 1987. Zbl 0674.12004 MR 0917944

[7] C. Goldstein and N. Schappacher, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe. *J. Reine Angew. Math.* **327** (1981), 184–218. Zbl 0456.12007 MR 0631315

[8] J. González and J.-C. Lario, **Q**-curves and their Manin ideals. *Amer. J. Math.* **123** (3) (2001), 475–503. Zbl 1035.14009 MR 1833149

[9] B. H. Gross, *Arithmetic on elliptic curves with complex multiplication.* With an appendix by B. Mazur, Lecture Notes in Math. 776, Springer-Verlag, Berlin 1980. Zbl 0433.14032 MR 0563921

[10] B. H. Gross, Minimal models for elliptic curves with complex multiplication. *Compositio Math.* **45** (2) (1982), 155–164. Zbl 0541.14010 MR 0651979

[11] F. Hajir, On units related to the arithmetic of elliptic curves with complex multiplication. *Arch. Math.* (*Basel*) **66** (4) (1996), 280–291. Zbl 0855.11027 MR 1380570

[12] K. A. Ribet, Galois representations attached to eigenforms with Nebentypus. In *Modular functions of one variable, V* (Proc. Second Internat. Conf., Universität Bonn, 1976), Lecture Notes in Math. 601, Springer-Verlag, Berlin 1977, 17–51. Zbl 0363.10015 MR 0453647

[13] F. Rodríguez Villegas, On the square root of special values of certain L-series. *Invent. Math.* **106** (3) (1991), 549–573. Zbl 0773.11034 MR 1134483

[14] D. E. Rohrlich, Galois conjugacy of unramified twists of Hecke characters. *Duke Math. J.* **47** (3) (1980), 695–703. Zbl 0446.12011 MR 0587174

[15] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Kanô Memorial Lectures 1, Publications of the Mathematical Society of Japan 11, Iwanami Shoten, Publishers, Tokyo 1971. Zbl 0221.10029 MR 0314766

[16] G. Shimura, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. *Nagoya Math. J.* **43** (1971), 199–208. Zbl 0225.14015 MR 0296050

[17] G. Shimura, On the factors of the Jacobian variety of a modular function field. *J. Math. Soc. Japan* **25** (1973), 523–544. Zbl 0266.14017 MR 0318162

Received October 24, 2008

Josep González Rovira, Departament Matemàtica Aplicada 4, UPC, Vilanova i la Geltrú,
Av. Víctor Balaguer, s/n., 08800 Vilanova i la Geltrú, Spain

E-mail: josepg@ma4.upc.edu

Joan-Carles Lario, Departament Matemàtica Aplicada 2, UPC, Barcelona, Jordi Girona, 1-3,
08034 Barcelona, Spain

E-mail: joan.carles.lario@upc.edu