ACTA ARITHMETICA
114.2 (2004)

The modular degree and the congruence number of a weight 2 cusp form

by

Alina Carmen Cojocaru (Princeton, NJ)
and Ernst Kani (Kingston, Ontario)

1. Introduction. Let f be a weight 2 normalized newform on the congruence subgroup $\Gamma_0(N)$ with integral Fourier coefficients. There are two important numerical invariants attached to f: its congruence number and its modular degree.

By definition, the *congruence number* of f is the largest integer D_f such that there exists a weight 2 cusp form on $\Gamma_0(N)$, with integral coefficients, which is orthogonal to f with respect to the Petersson inner product and is congruent to f modulo D_f. The *modular degree* of f is the degree $\deg \phi_f$ of the minimal parametrization $\phi_f : X_0(N) \to E$ of the strong Weil elliptic curve $E/\mathbb{Q}$ associated to f via the Shimura construction. Here $X_0(N)/\mathbb{Q}$ denotes the modular curve defined by $\Gamma_0(N)$.

It turns out that the two quantities D_f and $\deg \phi_f$ are closely related. On the one hand we have:

Theorem 1.1. *In the above setting*, $\deg \phi_f \mid D_f$.

This theorem appears already in [Za, p. 381] (in the case that N is a prime) and also in [AU, p. 278], but the existing proofs are not complete, as we will point out in more detail in the following section. The purpose of our paper is to give a detailed and complete proof of this result.

In the opposite direction, it has been announced by Mazur and Ribet (cf. [Mur]) that the only primes dividing $D_f/\deg \phi_f$ are prime divisors of N; their proof has not yet been published. Incidentally, the two invariants need not be equal, as has been shown by Agashe and Stein [AS].

The quantities $\deg \phi_f$ and D_f are closely linked to several deep conjectures in number theory. For example, in [Fr1], Frey formulated the *degree conjecture* which asserts that $\deg \phi_f = O(N^{2+\varepsilon})$ for any $\varepsilon > 0$. A striking

2000 *Mathematics Subject Classification*: 11F33, 11F11, 11G18, 14K15.

result due to Frey and Mai-Murty is that the degree conjecture is equivalent to the famous ABC conjecture; cf. [Fr2, p. 544] and [Mur, p. 180].

On the other hand, the prime divisors of D_f, called the *congruence primes of* f, have been studied extensively by Doi, Hida, Mazur, Ribet, and others; cf. e.g. [Ri2] and the references therein. The question of bounding the congruence primes of f is partially related to a question raised by Mazur, which is discussed in [Mur, p. 181]. This, in turn, is related to another conjecture of Frey (Conjecture 5 of [Fr2]), which is equivalent to the Asymptotic Fermat Conjecture; cf. [Fr2, p. 547].

NOTATION. In addition to the above notation, let $S_2(\Gamma_0(N))$ denote the space of cusp forms of weight 2 on $\Gamma_0(N)$. Moreover, if $R \subset \mathbb{C}$ is a subring, then S_R denotes the submodule of $S_2(\Gamma_0(N))$ consisting of the forms $g(z) = \sum_{n\geq 1} a_n(g)e^{2\pi inz}$ whose Fourier coefficients $a_n(g)$ lie in R. As in [DDT], we let $\mathbb{T}_R \subset \mathrm{End}_R(S_R)$ denote the R-Hecke algebra. Recall that $\mathbb{T}_R$ acts on the right on S_R; this action is written as $g|t$ for $g \in S_R$ and $t \in \mathbb{T}_R$.

For two abelian varieties A, B defined over $\mathbb{Q}$, let $\mathrm{Hom}(A,B) = \mathrm{Hom}_{\mathbb{Q}}(A,B)$ denote the group of homomorphisms defined over $\mathbb{Q}$ and let $\mathrm{Hom}^0(A,B) := \mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$. Note that $\mathrm{Hom}^0(A,B)$ is a finite-dimensional $\mathbb{Q}$-vector space which contains $\mathrm{Hom}(A,B)$ as a lattice.

As usual, the dual abelian variety of A is denoted by $\widehat{A}$. Recall that for each $\alpha \in \mathrm{Hom}(A,B)$ we have a dual map $\widehat{\alpha} : \widehat{B} \to \widehat{A}$ between the dual abelian varieties and that the assignment $\alpha \mapsto \widehat{\alpha}$ extends to an isomorphism $\mathrm{Hom}^0(A,B) \simeq \mathrm{Hom}^0(\widehat{B},\widehat{A})$.

If $L \subset V$ is a lattice in a $\mathbb{Q}$-vector space V, then the *denominator* $\mathrm{den}\,\alpha = \mathrm{den}_L\,\alpha$ of $\alpha \in V$ with respect to L is the smallest positive integer d such that $d\alpha \in L$. (Thus, if n is an integer such that $n\alpha \in L$, then $\mathrm{den}\,\alpha \mid n$.) In particular, if $\alpha \in \mathrm{Hom}^0(A,B)$, then $\mathrm{den}(\alpha)$ denotes the denominator of α with respect to the lattice $\mathrm{Hom}(A,B)$.

2. Proof of Theorem 1.1

2.1. *The idea of proof.* The basic idea of the proof of Theorem 1.1, due to Hida, Ribet and others (cf. [Za, p. 381]) is to construct an idempotent e of the ring $\mathrm{End}^0(J_0(N))$, where $J_0(N)$ denotes the Jacobian of $X_0(N)$, satisfying the following three properties: (i) the denominator of e in $\mathrm{End}_{\mathbb{Q}}(J_0(N))$ is $\deg\phi$; (ii) $e \in \mathbb{T}_{\mathbb{Q}}$; (iii) the denominator of e with respect to $\mathbb{T}_{\mathbb{Z}}$ divides D_f. Since $\mathbb{T}_{\mathbb{Q}} \subseteq \mathrm{End}_{\mathbb{Q}}(J_0(N))$, the theorem follows.

A proof of Theorem 1.1 based on the above idea appears first in [Za, pp. 381–382], but only for the case N a prime. Since in this case, by strong results of Mazur, $\mathbb{T}_{\mathbb{Q}}$ is isomorphic to $\mathrm{End}_{\mathbb{Q}}(J_0(N))$, one actually has $\deg\phi = D_f$. Zagier's parenthetic generalization of the result to arbitrary N is

stated incorrectly and the suggested proofs of (ii) and (iii) have gaps. A more detailed proof of Theorem 1.1 appears in [AU, pp. 278–279]. This proof does not provide an explanation for why property (ii) holds (cf. Remark 2.2) and, also, the proof of (iii) has some gaps. In this exposition we shall unravel the details behind these properties and thus present complete proofs.

2.2. *Review of the Shimura construction.* Let $j : X_0(N) \to J_0(N)$ denote the injection of $X_0(N)$ into $J_0(N)$ induced by the map $P \mapsto \mathrm{cl}(P - (\infty))$, where $(\infty) \in X_0(N)(\mathbb{Q})$ is the rational point corresponding to the cusp at infinity. Then, if $\Omega_X = H^0(X, \Omega^1_X)$ denotes the $\mathbb{Q}$-vector space of holomorphic differentials on a variety $X/\mathbb{Q}$, the pullback j^* induces a canonical identification $\Omega_{J_0(N)} \simeq \Omega_{X_0(N)} \simeq S_{\mathbb{Q}}$.

Since $f = \sum_{n\geq 1} a_n(f)q^n \in S_{\mathbb{Z}}$ is a normalized newform and hence a $\mathbb{T}_{\mathbb{Q}}$-eigenform, there exists by the Shimura construction an (essentially unique) abelian quotient $p = p_f : J_0(N) \to A_f = E$ (defined over $\mathbb{Q}$) such that $\mathrm{Ker}(p)$ is connected and such that $p^*\Omega_E = W := \mathbb{Q}f \subset \Omega_{J_0(N)}$ (via the above identifications); cf. [Sh2, Theorem 1] and/or [Ka2, Example 5.2]. In particular, $\dim E = \dim_{\mathbb{Q}} W = 1$, i.e. E is an elliptic curve over $\mathbb{Q}$. Moreover, there is an injective ring homomorphism $\tau = \tau_f : K_f := \mathbb{Q}(\{a_n(f)\}_{n\geq 1}) \hookrightarrow \mathrm{End}^0(E) := \mathrm{End}_{\mathbb{Q}}(E) \otimes \mathbb{Q}$ such that

$$\tau(\chi_f(t)) \circ p = p \circ t \quad \text{for all } t \in \mathbb{T}_{\mathbb{Q}} \subset \mathrm{End}^0(J_0(N)), \tag{1}$$

where $\chi_f : \mathbb{T}_{\mathbb{Q}} \to K_f = \mathbb{Q}$ is the character defined by f, i.e. $f|t = \chi_f(t)f$ for all $t \in \mathbb{T}_{\mathbb{Q}}$.

2.3. *Construction of the idempotent e.* Let $\phi = \phi_f := p_f \circ j : X_0(N) \to E$, which is the associated (minimal) *modular parametrization* of the elliptic curve E. By functoriality, ϕ induces a homomorphism $\phi^* : J_E \to J_0(N)$, where J_E denotes the Jacobian of E. (Note that the polarization on E induces an isomorphism $\varrho : E \xrightarrow{\sim} J_E$.) In addition, by duality we have a homomorphism $\phi_* : J_0(N) \to J_E$, given by the formula

$$\phi_* = \theta_E^{-1} \circ (\phi^*)^\wedge \circ \theta, \tag{2}$$

where $\theta : J_0(N) \to \widehat{J}_0(N)$ and $\theta_E : J_E \to \widehat{J}_E$ are the canonical polarizations on $J_0(N)$ and on J_E, respectively, and $(\phi^*)^\wedge : \widehat{J}_0(N) \to \widehat{J}_E$ denotes the dual map of ϕ^*. Note that ϕ^* is also the "dual" of ϕ_* in the sense that we have

$$\phi^* = \theta^{-1} \circ (\phi_*)^\wedge \circ \theta_E; \tag{3}$$

cf. e.g. [Ka1, p. 46]. By the autoduality property of the Jacobian, the map $\phi_* : J_0(N) \to J_E$ is related to $p : J_0(N) \to E$ via the formula

$$\varrho \circ p = \phi_*. \tag{4}$$

In particular, the kernel $\mathrm{Ker}(\phi_*) = \mathrm{Ker}(p)$ of ϕ_* is connected and hence ϕ^* is injective; cf. e.g. [Ka1, pp. 47–48]. Furthermore, we have

$$\phi_* \circ \phi^* = \deg(\phi)\,\mathrm{id}_{J_E}; \tag{5}$$

cf. e.g. [Ka2, p. 46]. From this it is immediate that the element

$$e = e_\phi := \frac{1}{\deg \phi}\,\phi^* \circ \phi_* \in \mathrm{End}^0(J_0(N))$$

is an *idempotent*, i.e. satisfies the equation $e^2 = e$. For later purposes it is useful to note that e is *symmetric* with respect to the *Rosati involution* $f \mapsto f' := \theta^{-1} \circ \widehat{f} \circ \theta$ of $\mathrm{End}^0(J_0(N))$ (cf. [Mu, p. 189]); indeed, by (2) and (3) we have

$$e' = \frac{1}{\deg \phi}\,\theta^{-1} \circ (\phi_* \circ \phi^*)^\wedge \circ \theta = \frac{1}{\deg \phi}\,\theta^{-1} \circ (\phi^*)^\wedge \circ (\phi_*)^\wedge \circ \theta = e.$$

In addition, we observe that its trace on the space $\Omega_{J_0(N)}$ is $\mathrm{tr}(e^*|\Omega_{J_0(N)}) = \dim \phi^* \Omega_{J_E} = 1$.

2.4. *Calculation of the denominator of e in* $\mathrm{End}(J_0(N))$. We shall use the following simple facts about denominators of elements in $\mathrm{Hom}^0(A, B)$, where A and B are abelian varieties.

LEMMA 2.1. *If $\alpha \in \mathrm{Hom}^0(A, B)$ and if $\beta : B \to C$, $\gamma : C \to A$ are homomorphisms of abelian varieties, then*

$$\mathrm{den}(\widehat{\alpha}) = \mathrm{den}(\alpha); \tag{6}$$

$$\mathrm{den}(\beta \circ \alpha) = \mathrm{den}(\alpha) \quad \textit{if } \beta \textit{ is injective}; \tag{7}$$

$$\mathrm{den}(\alpha \circ \gamma) = \mathrm{den}(\alpha) \quad \textit{if } \widehat{\gamma} \textit{ is injective}. \tag{8}$$

Proof. Let $n := \mathrm{den}(\alpha)$. Then $n\alpha \in \mathrm{Hom}(A, B)$ and hence $n\widehat{\alpha} = (n\alpha)^\wedge \in \mathrm{Hom}(\widehat{B}, \widehat{A})$. Thus $\mathrm{den}(\widehat{\alpha})$ divides $n = \mathrm{den}(\alpha)$, and hence also $\mathrm{den}(\widehat{\alpha})$ divides $\mathrm{den}((\widehat{\alpha})^\wedge) = \mathrm{den}(\alpha)$ (because we have a functorial identification $\kappa_A : A \xrightarrow{\sim} (\widehat{A})^\wedge$). This proves (6).

Moreover, since $n(\beta \circ \alpha) = \beta \circ (n\alpha) \in \mathrm{Hom}(A, C)$, we see that $m := \mathrm{den}(\beta \circ \alpha)$ divides $n = \mathrm{den}(\alpha)$. Set $\alpha_1 := n\alpha \in \mathrm{Hom}(A, B)$ and $\alpha_2 := m(\beta \circ \alpha) \in \mathrm{Hom}(A, C)$. Now since $(n/m)\alpha_2 = \beta \circ \alpha_1$, we see that $\mathrm{Ker}((n/m)\,\mathrm{id}_A) \leq \mathrm{Ker}(\beta \circ \alpha_1) = \mathrm{Ker}(\alpha_1)$, the latter because β is injective. Thus $\alpha_1 = \alpha_3 \circ (n/m)\,\mathrm{id}_A$ for some $\alpha_3 \in \mathrm{Hom}(A, B)$, and so $m\alpha = (m/n)\alpha_1 = \alpha_3$. This means that $n = \mathrm{den}(\alpha) \mid m$, and so $m = n$, which verifies (7).

Finally, the last assertion follows immediately from the first two because $\mathrm{den}(\alpha \circ \gamma) = \mathrm{den}(\widehat{\gamma} \circ \widehat{\alpha}) = \mathrm{den}(\widehat{\alpha}) = \mathrm{den}(\alpha)$ by (6), (7) and (6), respectively.

From the above lemma it follows easily that

$$\mathrm{den}(e_\phi) = \deg(\phi). \tag{9}$$

Indeed, since ϕ^* is injective, we deduce by (7) that

$$\operatorname{den}(e_\phi) = \operatorname{den}\left(\frac{1}{\deg\phi}\,\phi_*\right).$$

Moreover, since $(\phi_*)^\wedge$ is also injective by (3), it follows from (8) that

$$\operatorname{den}\left(\frac{1}{\deg\phi}\,\phi_*\right) = \operatorname{den}\left(\frac{1}{\deg\phi}\,\mathrm{id}_{J_E}\right) = \deg\phi,$$

and so (9) follows.

2.5. *Proof that* $e \in \mathbb{T}_\mathbb{Q}$. To prove that $e \in \mathbb{T}_\mathbb{Q}$, we shall use Atkin–Lehner theory to construct another idempotent $\varepsilon \in \mathbb{T}_\mathbb{Q}$ and then show that in fact $\varepsilon = e$.

Remark 2.2. In [AU], the authors deduce this fact (implicitly) from their assertion that an isogeny $J_0(N) \sim E \times A$ (where $A = \operatorname{Ker}(\phi_*)$) induces a splitting

$$\operatorname{End}^0(J_0(N)) \simeq \operatorname{End}^0(E) \times \operatorname{End}^0(A). \tag{10}$$

This statement, which is asserted without proof on p. 278, is in fact *false* in general because A may have a factor isogenous to E. For example, this always happens in the case that $f \in S_\mathbb{Z}$ is a $\mathbb{T}_\mathbb{Q}$-eigenform which is not a newform. (Note that for this case the Shimura construction and the assertions of §§2.2–2.4 apply as well.) If, however, we assume that f is a newform (as we did throughout), then we do have such splitting (10), but the proof of this fact requires the deep results of Ribet [Ri1, Corollary 4.2] and more. The following proof shows that such deep results are not necessary here.

Since $f \in S_\mathbb{Q}$ is a newform, we have (by Atkin–Lehner theory) a $\mathbb{T}_\mathbb{Q}$-module decomposition $S_\mathbb{Q} = W \oplus W'$, where (as before) $W = \mathbb{Q}f$. Let $e_W \in \operatorname{End}_{\mathbb{T}_\mathbb{Q}}(S_\mathbb{Q})$ denote the projector onto W; in particular, $\operatorname{Im}(e_W) = W$ and $\operatorname{Ker}(e_W) = W'$. Now since $S_\mathbb{Q}$ is a free $\mathbb{T}_\mathbb{Q}$-module of rank 1 (cf. [DDT, p. 36]), it follows that $\operatorname{End}_{\mathbb{T}_\mathbb{Q}}(S_\mathbb{Q}) = \operatorname{End}_{\mathbb{T}_\mathbb{Q}}(\mathbb{T}_\mathbb{Q}) = \mathbb{T}_\mathbb{Q}$ and hence there is a unique $\varepsilon \in \mathbb{T}_\mathbb{Q}$ such that $g|\varepsilon = e_W(g)$ for all $g \in S_\mathbb{Q}$. Note that ε is necessarily an idempotent and that $\mathbb{T}_\mathbb{Q}\varepsilon = \operatorname{Ann}_{\mathbb{T}_\mathbb{Q}}(W')$; cf. Bourbaki [Bo, Prop. 1(d) of §VIII.1, p. 8]. Thus,

$$\varepsilon t = \chi_f(t)\varepsilon, \tag{11}$$

for if $g = cf + w' \in S_\mathbb{Q}$ with $c \in \mathbb{Q}, w' \in W'$, then $g|\varepsilon t = cf|\varepsilon t = cf|t = \chi_f(t)cf = \chi_f(t)cf|\varepsilon = \chi_f(t)g|\varepsilon$, which is (11). In particular, we see that $\chi_f(\varepsilon) = 1$ (because $\varepsilon = \varepsilon^2 = \chi_f(\varepsilon)\varepsilon$).

Recall that we can view $\mathbb{T}_\mathbb{Q}$ as a subring of $\operatorname{End}^0(J_0(N))$. Now $\mathbb{T}_\mathbb{Q}$ is (in general) not preserved under the Rosati involution, i.e. $\mathbb{T}'_\mathbb{Q} \not\subset \mathbb{T}_\mathbb{Q}$. However, we shall see presently that $\varepsilon' \in \mathbb{T}_\mathbb{Q}$ and that in fact $\varepsilon' = \varepsilon$. As a first step

towards this we show

$$f|t' = \chi_f(t)f \quad \text{for all } t \in \mathbb{T}_{\mathbb{Q}}. \tag{12}$$

To see this, recall that the newform f is also a $\mathbb{T}'_{\mathbb{Q}}$-eigenform (cf. [Mi, p. 165]) and so (since $\mathbb{T}_{\mathbb{Q}}$ is commutative) there is a character $\chi'_f : \mathbb{T}_{\mathbb{Q}} \to \mathbb{Q}$ such that $f|t' = \chi'_f(t)f$ for all $t \in \mathbb{T}_{\mathbb{Q}}$. Thus, since t' (viewed as an endomorphism of $S_{\mathbb{Q}}$) is the adjoint of t with respect to the Petersson inner product $\langle \cdot, \cdot \rangle$ on $S_{\mathbb{Q}}$ (cf. Shimura [Sh1, p. 76 and p. 171]), we have

$$\chi'_f(t)\langle f, f\rangle = \langle f|t', f\rangle = \langle f, f|t\rangle = \overline{\chi_f(t)}\langle f, f\rangle,$$

where $\overline{\chi_f(t)}$ denotes the complex conjugate of $\chi_f(t)$. This shows that $\chi'(f) = \overline{\chi_f(t)} = \chi_f(t)$, which proves (12).

From (12) it follows that

$$\varepsilon t' = \chi_f(t)\varepsilon, \quad t\varepsilon' = \chi_f(t)\varepsilon' \quad \text{for all } t \in \mathbb{T}_{\mathbb{Q}}. \tag{13}$$

Indeed, if $g = cf + w' \in S_{\mathbb{Q}}$ with $c \in \mathbb{Q}, w' \in W'$, then by (12) we have $g|\varepsilon t' = cf|\varepsilon t' = cf|t' = \chi_f(t)cf = \chi_f(t)cf|\varepsilon = \chi_f(t)g|\varepsilon$, which proves the first equation of (13). The second equation follows from the first by applying the Rosati involution to both sides.

From the two equations (13) it follows immediately that ε is symmetric. Indeed, by taking $t = \varepsilon$ in (13) we obtain $\varepsilon\varepsilon' = \varepsilon$ and $\varepsilon\varepsilon' = \varepsilon'$ (recall that $\chi_f(\varepsilon) = 1$) and so $\varepsilon = \varepsilon'$ is symmetric.

We now relate ε to the idempotent e constructed in §2.3. For this, we first observe that by taking $t = \varepsilon$ in (1) we obtain $p \circ \varepsilon = \mathrm{id}_E \circ p$ because $\chi_f(\varepsilon) = 1$ (and τ is a ring homomorphism). So by (4) we have

$$\phi_* \circ \varepsilon = \phi_* \quad \text{and hence} \quad e \circ \varepsilon = e.$$

Thus, since ε and e are both symmetric, we also have $e = e' = (e\varepsilon)' = \varepsilon' e' = \varepsilon e$, which means that ε and e commute. This in turn implies that $\varepsilon - e$ is an idempotent, for $(\varepsilon - e)^2 = e^2 + \varepsilon^2 - 2e\varepsilon = e + \varepsilon - 2e = \varepsilon - e$. Thus, its trace is $\mathrm{tr}(\varepsilon - e|S_{\mathbb{Q}}) = \dim \mathrm{Im}(\varepsilon - e)$. On the other hand, $\mathrm{tr}(\varepsilon - e|S_{\mathbb{Q}}) = \mathrm{tr}(\varepsilon|S_{\mathbb{Q}}) - \mathrm{tr}(e|S_{\mathbb{Q}}) = \dim \mathrm{Im}(e_W) - 1 = 0$, and so $\mathrm{Im}(\varepsilon - e) = 0$, i.e. $e = \varepsilon \in \mathbb{T}_{\mathbb{Q}}$.

2.6. *Proof that the denominator of e in $\mathbb{T}_{\mathbb{Z}}$ divides D_f.* Let $L_f := \mathbb{Z}f \oplus (S_{\mathbb{Z}} \cap \langle f \rangle^{\perp})$. Then it is not difficult to see that the congruence number D_f (as defined in the introduction) is equal to the exponent of the (finite) group $S_{\mathbb{Z}}/L_f$; cf. e.g. [Za, p. 381].

Moreover, put $\mathcal{T} := e\mathbb{T}_{\mathbb{Z}} \oplus (1 - e)\mathbb{T}_{\mathbb{Z}}$ and $\overline{\mathcal{T}} := \mathcal{T}/\mathbb{T}_{\mathbb{Z}}$. Note that $\overline{\mathcal{T}}$ is a cyclic group of order d, where d is the denominator of e in $\mathbb{T}_{\mathbb{Z}}$. Indeed, by using the surjectivity of $\chi_f : \mathbb{T}_{\mathbb{Z}} \to \mathbb{Z}$ and (11), we see that $\mathcal{T} = e\mathbb{T}_{\mathbb{Z}} \oplus (1 - e)\mathbb{T}_{\mathbb{Z}} = e + \mathbb{T}_{\mathbb{Z}}$, and hence $\overline{\mathcal{T}} = (e\mathbb{Z} + \mathbb{T}_{\mathbb{Z}})/\mathbb{T}_{\mathbb{Z}} \simeq \mathbb{Z}/d\mathbb{Z}$.

Next, we shall relate $\overline{\mathcal{T}}$ to $S_{\mathbb{Q}}/L_f$ and hence find that the order of $\overline{\mathcal{T}}$ divides D_f. For this, consider the exact sequence of $\mathbb{Z}$-modules

$$0 \to \mathbb{T}_{\mathbb{Z}} \to \mathcal{T} \to \overline{\mathcal{T}} \to 0,$$

which induces the exact sequence

$$\begin{aligned} 0 \to \mathrm{Hom}_{\mathbb{Z}}(\overline{\mathcal{T}}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z}) \xrightarrow{r} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z}) \\ \to \mathrm{Ext}^1_{\mathbb{Z}}(\overline{\mathcal{T}}, \mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z}) \to \dots, \end{aligned}$$

where r denotes the restriction map defined by $r(f) = f_{|\mathbb{T}_{\mathbb{Z}}}$. Since $\overline{\mathcal{T}}$ is a finite cyclic group, we have $\mathrm{Hom}_{\mathbb{Z}}(\overline{\mathcal{T}}, \mathbb{Z}) = 0$ and $\mathrm{Ext}^1_{\mathbb{Z}}(\overline{\mathcal{T}}, \mathbb{Z}) \simeq \overline{\mathcal{T}} \simeq \mathbb{Z}/d\mathbb{Z}$. Also, since $\mathcal{T}$ is a free (hence projective) $\mathbb{Z}$-module, $\mathrm{Ext}^1_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z}) = 0$. Therefore we are left with the exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z}) \xrightarrow{r} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z}) \to \mathbb{Z}/d\mathbb{Z} \to 0,$$

which implies that $\mathcal{H} := \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z})/r(\mathrm{Hom}_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z}))$ is a finite cyclic group of order d.

Next we show that $\mathcal{H}$ is isomorphic to a quotient of $S_{\mathbb{Z}}/L_f$ and that hence $d \,|\, D_f$. To see this, recall that we have the perfect pairing $a_{\mathbb{C}} : S_{\mathbb{C}} \times \mathbb{T}_{\mathbb{C}} \to \mathbb{C}$ given by $a_{\mathbb{C}}(g, t) = a_1(g|t)$, where $a_1(g|t)$ denotes the first Fourier coefficient of $g|t$, and that this pairing induces the isomorphism (cf. [Ri2, Th. 2.2])

$$a_{\mathbb{Z}} : S_{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z}).$$

To verify the above assertion, it is thus enough to construct a homomorphism

$$\mathcal{A} : L_f = \mathbb{Z}f \oplus (S_{\mathbb{Z}} \cap \langle f \rangle^{\perp}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z})$$

with the property that $r \circ \mathcal{A} = (a_{\mathbb{Z}})_{|L_f}$, for then it follows immediately that

$$\mathcal{H} = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z})/r(\mathrm{Hom}_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z})) \simeq \mathbb{Z}/d\mathbb{Z}$$

is a quotient of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z})/r(\mathrm{Im}(\mathcal{A})) \simeq S_{\mathbb{Z}}/L_f$.

To define $\mathcal{A}$, let $a \in \mathbb{Z}$, $g \in S_{\mathbb{Z}} \cap \langle f \rangle^{\perp}$, $t_1, t_2 \in \mathbb{T}_{\mathbb{Z}}$ and put

$$\mathcal{A}(af + g)(et_1 + (1 - e)t_2) := a_1(af|t_1 + g|t_2). \tag{14}$$

We shall presently see that this is a well defined (injective) group homomorphism ([1]). Note that by taking $t_1 = t_2$ in (14), it then follows that $r \circ \mathcal{A} = (a_{\mathbb{Z}})_{|L_f}$, as desired.

To see that $\mathcal{A}$ is well defined, write $S_{\mathbb{Q}} = s\mathbb{T}_{\mathbb{Q}}$ (recall that $S_{\mathbb{Q}}$ is a free $\mathbb{T}_{\mathbb{Q}}$-module of rank 1) and let $g \in S_{\mathbb{Z}} \cap \langle f \rangle^{\perp}$. Then there exist $t_f, t_g \in \mathbb{T}_{\mathbb{Q}}$ such that

$$f = \chi_f(t_f)s|e, \tag{15}$$

$$g = s|(1 - e)t_g. \tag{16}$$

([1]) One can show that the homomorphism $\mathcal{A}$ is in fact an isomorphism. This implies that $S_{\mathbb{Z}}/L_f \simeq \mathcal{H} \simeq \mathbb{Z}/d\mathbb{Z}$ is a cyclic group of order d.

Indeed, since $f \in S_{\mathbb{Q}}$, we can write $f = s|t_f$ for some $t_f \in \mathbb{T}_{\mathbb{Q}}$, and then $f = \chi_f(e)f = f|e = s|t_f e = s|et_f = \chi_f(t_f)s|e$ because $\chi_f(e) = 1$ (cf. (11)). This proves (15). Moreover, by writing $g = s|t_g$ for some $t_g \in \mathbb{T}_{\mathbb{Q}}$ and then using (15) in the form

$$s|e = \frac{1}{\chi_f(t_f)}\, f,$$

we obtain

$$g = s|et_g + s(1-e)t_g = \frac{\chi_f(t_g)}{\chi_f(t_f)}\, f + s|(1-e)t_g.$$

But $g \in \langle f \rangle^{\perp}$, hence

$$0 = \langle g, f\rangle = \frac{\chi_f(t_g)}{\chi_f(t_f)}\, \langle f, f\rangle + \langle s|(1-e)t_g, \chi_f(t_f)s|e\rangle = \frac{\chi_f(t_g)}{\chi_f(t_f)}\, \langle f, f\rangle,$$

where we have also used the fact that e is a symmetric idempotent. This implies that $\chi_f(t_g) = 0$, which, in turn, proves (16).

Now we can check easily that $\mathcal{A}$ is well defined. Indeed, suppose that $t_1, t_1', t_2, t_2' \in \mathbb{T}_{\mathbb{Z}}$ are such that $et_1 + (1-e)t_2 = et_1' + (1-e)t_2'$. Then $et_1 = et_1'$, $(1-e)t_2 = (1-e)t_2'$ and hence by using (15), (16) we obtain $f|t_1 = \chi_f(t_f)s|et_1 = \chi_f(t_f)s|et_1' = f|t_1'$ and $g|t_2 = s|t_g(1-e)t_2 = s|t_g(1-e)t_2' = g|t_2'$, and so $\mathcal{A}$ is well defined.

References

[AU] A. Abbes et E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. 103 (1996), 269–286.

[AS] A. Agashe and W. Stein, *The Manin constant, congruence primes and the modular degree*, preprint.

[Bo] N. Bourbaki, *Algèbre, Ch. VIII*, Hermann, Paris, 1958.

[DDT] H. Darmon, F. Diamond and R. Taylor, *Fermat's last theorem*, in: Current Developments in Mathematics, 1995, R. Bott *et al.* (eds.), Internat. Press, Cambridge, MA, 1995, 1–154.

[Fr1] G. Frey, *Links between elliptic curves and solutions of* $A - B = C$, J. Indian Math. Soc. 51 (1987), 117–145.

[Fr2] —, *On ternary equations of Fermat type and relations with elliptic curves*, in: Modular Forms and Fermat's Last Theorem, G. Cornell, J. H. Silverman and G. Stevens (eds.), Springer, New York, 1997, 527–548.

[Ka1] E. Kani, *Hurwitz spaces of genus* 2 *covers of an elliptic curve*, Collect. Math. 54 (2003), 1–51.

[Ka2] —, *Abelian subvarieties and the Shimura construction*, preprint.

[Mi] T. Miyake, *Modular Forms*, Springer, Berlin, 1989.

[Mu] D. Mumford, *Abelian Varieties*, Oxford Univ. Press, Oxford, 1970.

[Mur] M. R. Murty, *Bounds for congruence primes*, in: Proc. Sympos. Pure Math. 66, Part 1, Amer. Math. Soc., Providence, RI, 1999, 177–192.

[Ri1] K. Ribet, *Twists of newforms and endomorphisms of abelian varieties*, Math. Ann. 253 (1980), 43–62.

[Ri2] K. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. 71 (1983), 193–205.

[Sh1] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten, Tokyo, and Princeton Univ. Press, Princeton, NJ, 1971.

[Sh2] —, *On the factors of the Jacobian variety of a modular function field*, J. Math. Soc. Japan 25 (1973), 523–544.

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

Mathematics Department
Princeton University
Princeton, NJ 08544-1000, U.S.A.
E-mail: cojocaru@math.princeton.edu

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
Canada, K7L 3N6
E-mail: kani@mast.queensu.ca

Received on 14.10.2003 (4646)