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
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 $S_2^0(N)$ denote the space of cusp forms of weight 2 on $\Gamma_0(N)$. Moreover, if $R \subseteq \mathbb{C}$ is a subring, then $S_R$ denotes the submodule of $S_2^0(N)$ consisting of the forms $g(z) = \sum_{n \geq 1} a_n(g) e^{2\pi i n z}$ whose Fourier coefficients $a_n(g)$ lie in $R$. As in [DDT], we let $T_R \subseteq \text{End}_R(S_R)$ denote the $R$-Hecke algebra. Recall that $T_R$ acts on the right on $S_R$; this action is written as $g|_t$ for $g \in S_R$ and $t \in T_R$.

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

As usual, the dual abelian variety of $A$ is denoted by $\widehat{A}$. Recall that for each $\alpha \in \text{Hom}(A, B)$ 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 $\text{Hom}^0(A, B) \simeq \text{Hom}^0(\widehat{B}, \widehat{A})$.

If $L \subseteq V$ is a lattice in a $\mathbb{Q}$-vector space $V$, then the denominator $\text{den} \alpha = \text{den}_L \alpha$ 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 $\text{den} \alpha \mid n$.) In particular, if $\alpha \in \text{Hom}^0(A, B)$, then $\text{den}(\alpha)$ denotes the denominator of $\alpha$ with respect to the lattice $\text{Hom}(A, B)$.

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 $\text{End}^0(J_0(N))$, where $J_0(N)$ denotes the Jacobian of $X_0(N)$, satisfying the following three properties: (i) the denominator of $e$ in $\text{End}_\mathbb{Q}(J_0(N))$ is $\deg \phi$; (ii) $e \in T_\mathbb{Q}$; (iii) the denominator of $e$ with respect to $T_\mathbb{Z}$ divides $D_f$. Since $T_\mathbb{Q} \subseteq \text{End}_\mathbb{Q}(J_0(N))$, 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, $T_\mathbb{Q}$ is isomorphic to $\text{End}_\mathbb{Q}(J_0(N))$, 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 \( P \mapsto \text{cl}(P - (\infty)) \),
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 holo-
morphic 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
\( \text{Ker}(p) \) 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 \( \tau = \tau_f : K_f := \mathbb{Q}(\{a_n(f)\}_{n \geq 1}) \hookrightarrow
\text{End}^0(E) := \text{End}_\mathbb{Q}(E) \otimes \mathbb{Q} \) such that
\[
\tau(\chi_f(t)) \circ p = p \circ t \quad \text{for all } t \in \mathbb{T}_\mathbb{Q} \subset \text{End}^0(J_0(N)),
\]
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) \textit{modular parametrization} of the
elliptic curve \( E \). By functoriality, \( \phi \) 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 \( \varrho : E \isom J_E \).) In addition, by duality we have a
homomorphism \( \phi_* : J_0(N) \to J_E \), given by the formula
\[
\phi_* = \theta^{-1}_E \circ (\phi^*)^\wedge \circ \theta,
\]
where \( \theta : J_0(N) \to \hat{J}_0(N) \) and \( \theta_E : J_E \to \hat{J}_E \) are the canonical polarizations
on \( J_0(N) \) and on \( J_E \), respectively, and \( (\phi^*)^\wedge : \hat{J}_0(N) \to \hat{J}_E \) denotes the dual
map of \( \phi^* \). Note that \( \phi^* \) is also the “dual” of \( \phi_* \) in the sense that we have
\[
\phi^* = \theta^{-1} \circ (\phi_*)^\wedge \circ \theta_E;
\]
\( \text{cf. e.g. [Ka1, p. 46]. By the autoduality property of the Jacobian, the map }
\phi_* : J_0(N) \to J_E \text{ is related to } p : J_0(N) \to E \text{ via the formula}
\]
\[
\varrho \circ p = \phi_*.
\]
In particular, the kernel $\text{Ker}(\phi_*) = \text{Ker}(p)$ of $\phi_*$ is connected and hence $\phi^*$ is injective; cf. e.g. [Ka1, pp. 47–48]. Furthermore, we have

$$\phi_* \circ \phi^* = \text{deg}(\phi) \text{id}_{J_E};$$

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

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

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 $f \mapsto f' := \theta^{-1} \circ \hat{f} \circ \theta$ of $\text{End}^0(J_0(N))$ (cf. [Mu, p. 189]); indeed, by (2) and (3) we have

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

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

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

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

$$\text{den}(\hat{\alpha}) = \text{den}(\alpha);$$

$$\text{den}(\beta \circ \alpha) = \text{den}(\alpha) \quad \text{if } \beta \text{ is injective;}$$

$$\text{den}(\alpha \circ \gamma) = \text{den}(\alpha) \quad \text{if } \hat{\gamma} \text{ is injective.}$$

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

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

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

From the above lemma it follows easily that

$$\text{den}(e_\phi) = \text{deg}(\phi).$$
Indeed, since $\phi^*$ is injective, we deduce by (7) that
\[ \text{den}(\epsilon_{\phi}) = \text{den}\left(\frac{1}{\deg \phi} \phi_*\right). \]
Moreover, since $(\phi_*)^\wedge$ is also injective by (3), it follows from (8) that
\[ \text{den}\left(\frac{1}{\deg \phi} \phi_*\right) = \text{den}\left(\frac{1}{\deg \phi} \text{id}_{J_E}\right) = \deg \phi, \]
and so (9) follows.

2.5. Proof that $e \in T_Q$. To prove that $e \in T_Q$, we shall use Atkin–Lehner theory to construct another idempotent $\varepsilon \in T_Q$ 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 $A = \text{Ker}(\phi_*)$) induces a splitting
\[ \text{End}^0(J_0(N)) \simeq \text{End}^0(E) \times \text{End}^0(A). \]
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 $f \in S_Z$ is a $T_Q$-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 $f \in S_Q$ is a newform, we have (by Atkin–Lehner theory) a $T_Q$-module decomposition $S_Q = W \oplus W'$, where (as before) $W = Qf$. Let $e_W \in \text{End}_{T_Q}(S_Q)$ denote the projector onto $W$; in particular, $\text{Im}(e_W) = W$ and $\ker(e_W) = W'$. Now since $S_Q$ is a free $T_Q$-module of rank 1 (cf. [DDT, p. 36]), it follows that $\text{End}_{T_Q}(S_Q) = \text{End}_{T_Q}(T_Q) = T_Q$ and hence there is a unique $\varepsilon \in T_Q$ such that $g|\varepsilon = e_W(g)$ for all $g \in S_Q$. Note that $\varepsilon$ is necessarily an idempotent and that $T_Q \varepsilon = \text{Ann}_{T_Q}(W')$; cf. Bourbaki [Bo, Prop. 1(d) of §VIII.1, p. 8]. Thus,
\[ \varepsilon t = \chi_f(t)\varepsilon, \]
for if $g = cf + w' \in S_Q$ with $c \in Q, w' \in W'$, then $g|\varepsilon t = cf|\varepsilon t = cf|t = \chi_f(t)cf = \chi_f(t)\varepsilon t = \chi_f(t)g|\varepsilon$, 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 $T_Q$ as a subring of $\text{End}^0(J_0(N))$. Now $T_Q$ is (in general) not preserved under the Rosati involution, i.e. $T_Q' \not\subset T_Q$. However, we shall see presently that $\varepsilon' \in T_Q$ and that in fact $\varepsilon' = \varepsilon$. As a first step
towards this we show
\begin{equation}
  f | t' = \chi_f(t)f \quad \text{for all } t \in \mathbb{T}_Q.
\end{equation}
To see this, recall that the newform $f$ is also a $\mathbb{T}_Q'$-eigenform (cf. [Mi, p. 165]) and so (since $\mathbb{T}_Q$ is commutative) there is a character $\chi_f' : \mathbb{T}_Q \to \mathbb{Q}$ such that $f | t' = \chi_f'(t)f$ for all $t \in \mathbb{T}_Q$. Thus, since $t'$ (viewed as an endomorphism of $S_Q$) is the adjoint of $t$ with respect to the Petersson inner product $\langle \cdot, \cdot \rangle$ on $S_Q$ (cf. Shimura [Sh1, p. 76 and p. 171]), we have
\begin{equation}
  \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,
\end{equation}
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
\begin{equation}
  \epsilon t' = \chi_f(t)\epsilon, \quad t\epsilon' = \chi_f(t)\epsilon' \quad \text{for all } t \in \mathbb{T}_Q.
\end{equation}
Indeed, if $g = cf + w' \in S_Q$ with $c \in \mathbb{Q}, w' \in W'$, then by (12) we have $g|\epsilon t' = \chi_f(t)|c\epsilon t' = c\chi_f(t)c|\epsilon = \chi_f(t)g|\epsilon$, 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 $\epsilon$ is symmetric. Indeed, by taking $t = \epsilon$ in (13) we obtain $\epsilon \epsilon' = \epsilon$ and $\epsilon \epsilon' = \epsilon'$ (recall that $\chi_f(\epsilon) = 1$) and so $\epsilon = \epsilon'$ is symmetric.

We now relate $\epsilon$ to the idempotent $e$ constructed in §2.3. For this, we first observe that by taking $t = \epsilon$ in (1) we obtain $p \circ \epsilon = \text{id}_E \circ p$ because $\chi_f(\epsilon) = 1$ (and $\tau$ is a ring homomorphism). So by (4) we have
\begin{equation}
  \phi_* \circ \epsilon = \phi_* \quad \text{and hence } e \circ \epsilon = e.
\end{equation}
Thus, since $\epsilon$ and $e$ are both symmetric, we also have $e = e' = (e\epsilon)' = \epsilon' = \epsilon\epsilon$, which means that $\epsilon$ and $e$ commute. This in turn implies that $\epsilon - e$ is an idempotent, for $(\epsilon - e)^2 = \epsilon^2 + e^2 - 2\epsilon e = \epsilon + e - 2\epsilon = \epsilon - e$. Thus, its trace is $\text{tr}(\epsilon - e|S_Q) = \dim \text{Im}(\epsilon - e)$. On the other hand, $\text{tr}(\epsilon - e|S_Q) = \text{tr}(\epsilon|S_Q) - \text{tr}(e|S_Q) = \dim \text{Im}(e_\mathbb{W}) - 1 = 0$, and so $\text{Im}(\epsilon - e) = 0$, i.e. $e = \epsilon \in \mathbb{T}_Q$.

2.6. Proof that the denominator of $e$ in $\mathbb{T}_\mathbb{Z}$ divides $D_f$. Let $L_f := \mathbb{Z}f \oplus (S_Q \cap \langle f \rangle^\perp)$. 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 $S_Q/L_f$; 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 $\overline{T}$ to $S_\mathbb{Q}/L_f$ and hence find that the order of $\overline{T}$ divides $D_f$. For this, consider the exact sequence of $\mathbb{Z}$-modules

$$0 \rightarrow \mathbb{Z}_g \rightarrow \mathcal{T} \rightarrow \overline{T} \rightarrow 0,$$

which induces the exact sequence

$$0 \rightarrow \text{Hom}_{\mathbb{Z}}(\overline{T}, \mathbb{Z}) \rightarrow \text{Hom}_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z}) \overset{r}{\rightarrow} \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_g, \mathbb{Z}) \rightarrow \text{Ext}^1_{\mathbb{Z}}(\overline{T}, \mathbb{Z}) \rightarrow \text{Ext}^1_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z}) \rightarrow \text{Ext}^1_{\mathbb{Z}}(\mathbb{Z}_g, \mathbb{Z}) \rightarrow \ldots,$$

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

$$0 \rightarrow \text{Hom}_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z}) \overset{r}{\rightarrow} \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_g, \mathbb{Z}) \rightarrow \mathbb{Z}/d\mathbb{Z} \rightarrow 0,$$

which implies that $\mathcal{H} := \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_g, \mathbb{Z})/r(\text{Hom}_{\mathbb{Z}}(\mathcal{T}, \mathbb{Z}))$ 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 $d \mid D_f$. To see this, recall that we have the perfect pairing $a_C : S_C \times \mathbb{T}_C \rightarrow \mathbb{C}$ given by $a_C(g, t) = a_1(g|t)$, 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])

$$a_\mathbb{Z} : S_\mathbb{Z} \overset{\sim}{\rightarrow} \text{Hom}_{\mathbb{Z}}(\mathbb{T}_\mathbb{Z}, \mathbb{Z}).$$

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

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

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

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

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

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

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

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

$$(15) \quad f = \chi_f(t_f)s|e,$$

$$(16) \quad g = s|(1 - e)t_g.$$  

\(^{(1)}\) 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 $t_f \in T_{\mathbb{Q}}$, and then $f = \chi_f(e)f = f|e = s|t_f e = s|t_f = \chi_f(t_f)s|e$ because $\chi_f(e) = 1$ (cf. (11)). This proves (15). Moreover, by writing $g = s|t_g$ for some $t_g \in T_{\mathbb{Q}}$ and then using (15) in the form

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

we obtain

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

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 $A$ is well defined. Indeed, suppose that $t_1, t_1', t_2, t_2' \in T_{\mathbb{Z}}$ are such that $e t_1 + (1 - e)t_2 = e t_1' + (1 - e)t_2'$. Then $e t_1 = e t_1'$, $(1 - e)t_2 = (1 - e)t_2'$ and hence by using (15), (16) we obtain $f|t_1 = \chi_f(t_f)s|e t_1 = \chi_f(t_f)s|e t_1' = f|t_1'$ and $g|t_2 = s|t_g(1 - e)t_2 = s|t_g(1 - e)t_2'$, and so $A$ is well defined.

References


---

Received on 14.10.2003

---