The Modular Degree, Congruence Primes and Multiplicity One

Amod Agashe   Kenneth A. Ribet   William A. Stein

Abstract.

The modular degree and congruence number are two fundamental invariants of an elliptic curve over the rational field. Frey and Müller have asked whether these invariants coincide. Although this question has a negative answer, we prove a theorem about the relation between the two invariants: one divides the other, and the ratio is divisible only by primes whose squares divide the conductor of the elliptic curve. We discuss the ratio even in the case where the square of a prime does divide the conductor, and we study analogues of the two invariants for modular abelian varieties of arbitrary dimension.

1 Introduction

Let E be an elliptic curve over $\mathbf{Q}$. By [BCDT01], we may view E as an abelian variety quotient over $\mathbf{Q}$ of the modular Jacobian $J_0(N)$, where N is the conductor of E. After possibly replacing E by an isogenous curve, we may assume that the kernel of the map $J_0(N) \to E$ is connected, i.e., that E is an *optimal quotient* of $J_0(N)$.

Let $f_E = \sum a_n q^n \in S_2(\Gamma_0(N))$ be the newform attached to E. The *congruence number* r_E of E is the largest integer such that there is an element $g = \sum b_n q^n \in S_2(\Gamma_0(N))$ with integer Fourier coefficients b_n that is orthogonal to f_E with respect to the Peterson innner product, and congruent to f_E modulo r_E (i.e., $a_n \equiv b_n \pmod{r_E}$ for all n). The *modular degree* m_E is the degree of the composite map $X_0(N) \to J_0(N) \to E$, where we map $X_0(N)$ to $J_0(N)$ by sending $P \in X_0(N)$ to $[P] - [\infty] \in J_0(N)$.

Section 2 is about relations between r_E and m_E. For example, $m_E \mid r_E$. In [FM99, Q. 4.4], Frey and Müller asked whether $r_E = m_E$. We give examples in which $r_E \neq m_E$, then conjecture that for any prime p, $\mathrm{ord}_p(r_E/m_E) \leq \frac{1}{2}\mathrm{ord}_p(N)$. We prove this conjecture when $\mathrm{ord}_p(N) \leq 1$.

In Section 3, we consider analogues of congruence primes and the modular degree for optimal quotients that are not necessarily elliptic curves; these are quotients of $J_0(N)$ and $J_1(N)$ of any dimension associated to ideals of the relevant Hecke algebras. In Section 4 we prove the main theorem of this paper, and in Section 5 we give some new examples of failure of multiplicity one motivated by the arguments in Section 4.

Acknowledgment. The authors are grateful to A. Abbes, R. Coleman, B. Conrad, J. Cremona, H. Lenstra, E. de Shalit, B. Edixhoven, L. Merel, and R. Taylor for several discussions and advice regarding this paper.

2 Congruence Primes and the Modular Degree

Let N be a positive integer and let $X_0(N)$ be the modular curve over $\mathbf{Q}$ that classifies isomorphism classes of elliptic curves with a cyclic subgroup of order N. The Hecke algebra $\mathbf{T}$ of level N is the subring of the ring of endomorphisms of $J_0(N) = \mathrm{Jac}(X_0(N))$ generated by the Hecke operators T_n for all $n \geq 1$. Let f be a newform of weight 2 for $\Gamma_0(N)$ with integer Fourier coefficients, and let I_f be kernel of the homomorphism $\mathbf{T} \to \mathbf{Z}[\ldots, a_n(f), \ldots]$ that sends T_n to a_n. Then the quotient $E = J_0(N)/I_f J_0(N)$ is an elliptic curve over $\mathbf{Q}$. We call E the *optimal quotient* associated to f. Composing the embedding $X_0(N) \hookrightarrow J_0(N)$ that sends ∞ to 0 with the quotient map $J_0(N) \to E$, we obtain a surjective morphism of curves $\phi_{\scriptscriptstyle E} : X_0(N) \to E$.

Definition 2.1. The *modular degree* $m_{\scriptscriptstyle E}$ of E is the degree of $\phi_{\scriptscriptstyle E}$.

Congruence primes have been studied by Doi, Hida, Ribet, Mazur and others (see, e.g., [Rib83, §1]), and played an important role in Wiles's work [Wil95] on Fermat's last theorem. Frey and Mai-Murty have observed that an appropriate asymptotic bound on the modular degree is equivalent to the *abc*-conjecture (see [Fre97, p.544] and [Mur99, p.180]). Thus, results that relate congruence primes and the modular degree are of great interest.

Theorem 2.2. *Let E be an elliptic curve over $\mathbf{Q}$ of conductor N, with modular degree $m_{\scriptscriptstyle E}$ and congruence number $r_{\scriptscriptstyle E}$. Then $m_{\scriptscriptstyle E} \mid r_{\scriptscriptstyle E}$ and if $\mathrm{ord}_p(N) \leq 1$ then $\mathrm{ord}_p(r_{\scriptscriptstyle E}) = \mathrm{ord}_p(m_{\scriptscriptstyle E})$.*

We will prove a generalization of Theorem 2.2 in Section 4 below.

The divisibility $m_{\scriptscriptstyle E} \mid r_{\scriptscriptstyle E}$ was first discussed in [Zag85, Th. 3], where it is attributed to the second author (Ribet); however in [Zag85] the divisibility was mistakenly written in the opposite direction. For some other expositions of the proof, see [AU96, Lem 3.2] and [CK04]. We generalize this divisibility in Proposition 4.5. The second part of Theorem 2.2, i.e., that if $\mathrm{ord}_p(N) \leq 1$ then $\mathrm{ord}_p(r_{\scriptscriptstyle E}) = \mathrm{ord}_p(m_{\scriptscriptstyle E})$, follows from the more general Theorem 3.7 below. Note that [AU96, Prop. 3.3–3.4] implies the weaker statement that if $p \nmid N$ then $\mathrm{ord}_p(r_{\scriptscriptstyle E}) = \mathrm{ord}_p(m_{\scriptscriptstyle E})$, since [AU96, Prop. 3.3] implies

$$\mathrm{ord}_p(r_{\scriptscriptstyle E}) - \mathrm{ord}_p(m_{\scriptscriptstyle E}) = \mathrm{ord}_p(\#\mathcal{C}) - \mathrm{ord}_p(c_{\scriptscriptstyle E}) - \mathrm{ord}_p(\#\mathcal{D}),$$

Table 1: Differing Modular Degree and Congruence Number

Curve	m_E	r_E	Curve	m_E	r_E	Curve	m_E	r_E
54B1	2	6	99A1	4	12	128A1	4	32
64A1	2	4	108A1	6	18	128B1	8	32
72A1	4	8	112A1	8	16	128C1	4	32
80A1	4	8	112B1	4	8	128D1	8	32
88A1	8	16	112C1	8	16	135A1	12	36
92B1	6	12	120A1	8	16	144A1	4	8
96A1	4	8	124A1	6	12	144B1	8	16
96B1	4	8	126A1	8	24			

and by [AU96, Prop. 3.4] $\mathrm{ord}_p(\#\mathcal{C}) = 0$. (Here c_E is the Manin constant of E, which is an integer by results of Edixhoven and Katz-Mazur; see e.g., [ARS06] for more details.)

Frey and Müller [FM99, Ques. 4.4] asked whether $r_E = m_E$ in general. After implementing an algorithm to compute r_E in Magma [BCP97], we quickly found that the answer is no. The counterexamples at conductor $N \leq 144$ are given in Table 1, where the curve is given using the notation of [Cre97]:

For example, the elliptic curve 54B1, given by the equation $y^2 + xy + y = x^3 - x^2 + x - 1$, has $r_E = 6$ and $m_E = 2$. To see explicitly that $3 \mid r_E$, observe that the newform corresponding to E is $f = q + q^2 + q^4 - 3q^5 - q^7 + \cdots$ and the newform corresponding to $X_0(27)$ if $g = q - 2q^4 - q^7 + \cdots$, so $g(q) + g(q^2)$ appears to be congruent to f modulo 3. To prove this congruence, we checked it for 18 Fourier coefficients, where the sufficiency of precision to degree 18 was determined using [Stu87].

In our computations, there appears to be no absolute bound on the p that occur. For example, for the curve 242B1 of conductor $N = 2 \cdot 11^2$ we have[1]

$$m_E = 2^4 \neq r_E = 2^4 \cdot 11.$$

We propose the following replacement for Question 4.4 of [FM99]:

Conjecture 2.3. *Let E be an optimal elliptic curve of conductor N and p be any prime. Then*

$$\mathrm{ord}_p\left(\frac{r_E}{m_E}\right) \leq \frac{1}{2}\,\mathrm{ord}_p(N).$$

We verified Conjecture 2.3 using Magma for every optimal elliptic curve quotient of $J_0(N)$, with $N \leq 539$.

If $p \geq 5$ then $\mathrm{ord}_p(N) \leq 2$, so a special case of the conjecture is

$$\mathrm{ord}_p\left(\frac{r_E}{m_E}\right) \leq 1 \qquad \text{for any } p \geq 5.$$

[1] The curve 242a1 in "modern notation."

Remark 2.4. It is often productive to parametrize elliptic curves by $X_1(N)$ instead of $X_0(N)$ (see, e.g., [Ste89] and [Vat05]). Suppose E is an optimal quotient of $X_1(N)$, let m'_E be the degree of the modular parametrization, and let r'_E be the $\Gamma_1(N)$-congruence number, which is defined as above but with $S_2(\Gamma_0(N))$ replaced by $S_2(\Gamma_1(N))$. For the optimal quotient of $X_1(N)$ isogenous to 54B1, we find using Magma that $m'_E = 18$ and $r'_E = 6$. Thus the equality $m'_E = r'_E$ fails, and the analogous divisibility $m'_E \mid r'_E$ no longer holds. Also, for a curve of conductor 38 we have $m'_E = 18$ and $r'_E = 6$, so equality need not hold even if the level is square free. We hope to investigate this in a future paper.

3 Modular abelian varieties of arbitrary dimension

For $N \geq 4$, let Γ be a fixed choice of either $\Gamma_0(N)$ or $\Gamma_1(N)$, let X be the modular curve over $\mathbf{Q}$ associated to Γ, and let J be the Jacobian of X. Let I be a *saturated* ideal of the corresponding Hecke algebra $\mathbf{T} \subset \mathrm{End}(J)$, so $\mathbf{T}/I$ is torsion free. Then $A = A_I = J/IJ$ is an optimal quotient of J since IJ is an abelian subvariety.

Definition 3.1. If $f = \sum a_n(f)q^n \in S_2(\Gamma)$ and $I_f = \ker(\mathbf{T} \to \mathbf{Z}[\ldots, a_n(f), \ldots])$, then $A = A_f = J/I_fJ$ is the *newform quotient* associated to f. It is an abelian variety over $\mathbf{Q}$ of dimension equal to the degree of the field $\mathbf{Q}(\ldots, a_n(f), \ldots)$.

In this section, we generalize the notions of the congruence number and the modular degree to quotients $A = A_I$, and state a theorem relating the two numbers, which we prove in Sections 4.1–4.2.

Let ϕ_2 denote the quotient map $J \to A$. By Poincare reducibility over $\mathbf{Q}$ there is a unique abelian subvariety $A^\vee$ of J that projects isogenously to the quotient A (equivalently, which has finite intersection with $\ker(\phi_2)$), and so by Hecke equivariance of $J \to A$ it follows that $A^\vee$ is $\mathbf{T}$-stable. Let ϕ be the composite isogeny

$$\phi : A^\vee \xrightarrow{\phi_1} J \xrightarrow{\phi_2} A.$$

Remark 3.2. Note that $A^\vee$ is the dual abelian variety of A. More generally, if C is any abelian variety, let $C^\vee$ denote the dual of C. There is a canonical principal polarization $J \cong J^\vee$, and dualizing ϕ_2, we obtain a map $\phi_2^\vee : A^\vee \to J^\vee$, which we compose with $\theta^{-1} : J^\vee \cong J$ to obtain a map $\phi_1 : A^\vee \to J$. Note also that φ is a polarization (induced by pullback of the theta divisor).

The *exponent* of a finite group G is the smallest positive integer n such that every element of G has order dividing n.

Definition 3.3. The *modular exponent* of A is the exponent of the kernel of the isogeny ϕ, and the *modular number* of A is the degree of ϕ.

We denote the modular exponent of A by $\tilde{n}_A$ and the modular number by n_A. When A is an elliptic curve, the modular exponent is equal to the modular degree of A, and the modular number is the square of the modular degree (see, e.g., [AU96, p. 278]).

If R is a subring of $\mathbf{C}$, let $S_2(R) = S_2(\Gamma; R)$ denote the subgroup of $S_2(\Gamma)$ consisting of cups forms whose Fourier expansions at the cusp ∞ have coefficients in R. (Note that Γ is fixed for this whole section.) Let $S_2(\Gamma; \mathbf{Z})[I]^\perp$ denote the orthogonal complement of $S_2(\Gamma; \mathbf{Z})[I]$ in $S_2(\Gamma; \mathbf{Z})$ with respect to the Petersson inner product.

The following is well known, but we had difficulty finding a good reference.

Proposition 3.4. *The group $S_2(\Gamma; \mathbf{Z})$ is of finite rank as a $\mathbf{Z}$-module.*

Proof. Using the standard pairing between $\mathbf{T}$ and $S_2(\Gamma, \mathbf{Z})$ (see also [Rib83, Theorem 2.2]) we see that $S_2(\Gamma, \mathbf{Z}) \cong \mathrm{Hom}(\mathbf{T}, \mathbf{Z})$. Thus $S_2(\Gamma, \mathbf{Z})$ is finitely generated over $\mathbf{Z}$ if and only if $\mathbf{T}$ is finitely generated over $\mathbf{Z}$. But the action of $\mathbf{T}$ on $\mathrm{H}_1(J, \mathbf{Z})$ is a faithful representation that embeds $\mathbf{T}$ into $\mathrm{Mat}_{2d}(\mathbf{Z}) \cong \mathbf{Z}^{(2d)^2}$. But $\mathbf{Z}$ is Noetherian, so $\mathbf{T}$ is finitely generated over $\mathbf{Z}$. □

Definition 3.5. The exponent of the quotient group

$$\frac{S_2(\Gamma; \mathbf{Z})}{S_2(\Gamma; \mathbf{Z})[I] + S_2(\Gamma; \mathbf{Z})[I]^\perp} \tag{1}$$

is the *congruence exponent* $\tilde{r}_A$ of A and its order is the *congruence number* r_A.

Remark 3.6. Note that $S_2(\Gamma, \mathbf{Z}) \otimes_{\mathbf{Z}} R = S_2(\Gamma, R)$; see, e.g., the discussion in [DI95, §12]. Thus the analogue of Definition 3.5 with $\mathbf{Z}$ replaced by an algebraic integer ring (or even $\overline{\mathbf{Z}}$) gives a torsion module whose annihilator ideal meets $\mathbf{Z}$ in the ideal generated by the congruence exponent.

Our definition of r_A generalizes the definition in Section 2 when A is an elliptic curve (see [AU96, p. 276]), and the following generalizes Theorem 2.2:

Theorem 3.7. *If $f \in S_2(\mathbf{C})$ is a newform, then*

(a) We have $\tilde{n}_{A_f} \mid \tilde{r}_{A_f}$, and

(b) If $p^2 \nmid N$, then $\mathrm{ord}_p(\tilde{r}_{A_f}) = \mathrm{ord}_p(\tilde{n}_{A_f})$.

Remark 3.8. When A_f is an elliptic curve, Theorem 3.7 implies that the modular degree divides the congruence number (since for an elliptic curve the modular degree and modular exponent are the same), i.e., $\sqrt{n_{A_f}} \mid r_{A_f}$. In general, the divisibility $n_{A_f} \mid r_{A_f}^2$ need not hold. For example, there is a newform of degree 24 in $S_2(\Gamma_0(431))$ such that

$$n_{A_f} = (2^{11} \cdot 6947)^2 \nmid r_{A_f}^2 = (2^{10} \cdot 6947)^2.$$

Note that 431 is prime and mod 2 multiplicity one fails for $J_0(431)$ (see [Kil02]).

4 Proof of the Main Theorem

In this section we prove Theorem 3.7. We continue using the notation introduced so far.

4.1 Proof of Theorem 3.7 (a)

We begin with a remark about compatibilities. In general, the polarization of J induced by the theta divisor need not be Hecke equivariant, because if T is a Hecke operator on J, then on $J^\vee$ it acts as $W_N T W_N$, where W_N is the Atkin-Lehner involution (see e.g., [DI95, Rem. 10.2.2]). However, on J^{new} the action of the Hecke operators commutes with that of W_N, so if the quotient map $J \to A$ factors through J^{new}, then the Hecke action on $A^\vee$ induced by the embedding $A^\vee \to J^\vee$ and the action on $A^\vee$ induced by $\phi_1 : A^\vee \to J$ are the same. Hence $A^\vee$ is isomorphic to $\phi_1(A^\vee)$ as a $\mathbf{T}$-module.

Recall that f is a newform, $I_f = \mathrm{Ann}_{\mathbf{T}}(f)$, and $J = J_0(N)$. Let $B = I_f J$, so that $A^\vee + B = J$, and $J/B \cong A$. The following lemma is well known, but we prove it here for the convenience of the reader.

Lemma 4.1. $\mathrm{Hom}_{\mathbf{Q}}(A^\vee, B) = 0$.

Proof. Pick a prime ℓ. Then $\overline{\mathbf{Q}}_\ell \otimes V_\ell(J)^{\text{ss}}$ as a $\overline{\mathbf{Q}}_\ell[G_{\mathbf{Q}}]$-module is a direct sum of copies of the representations ρ_g as g ranges through all normalized eigenforms of weight 2 and level N with coefficients in $\overline{\mathbf{Q}}$; by a well-known result of the second author, these representations are absolutely irreducible. Now since f is a newform and $A^\vee \to A$ is an isogeny, $\overline{\mathbf{Q}}_\ell \otimes V_\ell(A^\vee)^{\text{ss}}$ is a direct sum of copies of $\rho_{\sigma(f)}$ as σ ranges over all embeddings of K_f into $\overline{\mathbf{Q}}$. Thus, by the analytic theory of multiplicity one (see [Li75, Cor. 3, pg. 300]), the Galois modules $V_\ell(A^\vee)$ and $V_\ell(B) = V_\ell(J)/V_\ell(A^\vee)$ share no common Jordan-Hölder factors even when coefficients are extended to $\overline{\mathbf{Q}}_\ell$, so $\mathrm{Hom}_{\mathbf{Q}}(A', B) = 0$. □

Let $\mathbf{T}_1$ be the image of $\mathbf{T}$ in $\mathrm{End}(A^\vee)$, and let $\mathbf{T}_2$ be the image of $\mathbf{T}$ in $\mathrm{End}(B)$. We have the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{T} \arrow[r] \arrow[d] & \mathbf{T}_1 \oplus \mathbf{T}_2 \arrow[r] \arrow[d] & \dfrac{\mathbf{T}_1 \oplus \mathbf{T}_2}{\mathbf{T}} \arrow[r] \arrow[d, dotted] & 0 \\
0 \arrow[r] & \mathrm{End}(J) \arrow[r] & \mathrm{End}(A^\vee) \oplus \mathrm{End}(B) \arrow[r] & \dfrac{\mathrm{End}(A^\vee) \oplus \mathrm{End}(B)}{\mathrm{End}(J)} \arrow[r] & 0.
\end{tikzcd} \tag{2}$$

Let

$$e = (1, 0) \in \mathbf{T}_1 \oplus \mathbf{T}_2,$$

and let e_1 and e_2 denote the images of e in the groups $(\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$ and $(\mathrm{End}(A^\vee) \oplus \mathrm{End}(B))/\mathrm{End}(J)$, respectively. It follows from Lemma 4.1 that the two quotient groups on the right hand side of (2) are finite, so e_1 and e_2

have finite order. Note that because e_2 is the image of e_1, the order of e_2 is a divisor of the order of e_1.

The *denominator* of any $\varphi \in \mathrm{End}(J) \otimes \mathbf{Q}$ is the smallest positive integer n such that $n\varphi \in \mathrm{End}(J)$.

Let $\pi_{A^\vee}, \pi_B \in \mathrm{End}(J) \otimes \mathbf{Q}$ be projection onto $A^\vee$ and B, respectively. Note that the denominator of $\pi_{A^\vee}$ equals the denominator of π_B, since $\pi_{A^\vee} + \pi_B = 1_J$, so that $\pi_B = 1_J - \pi_{A^\vee}$.

Lemma 4.2. *The element $e_2 \in (\mathrm{End}(A^\vee) \oplus \mathrm{End}(B))/\mathrm{End}(J)$ defined above has order $\tilde{n}_A$.*

Proof. Let n be the order of e_2, so n is the denominator of $\pi_{A^\vee}$, which, as mentioned above, is also the denominator of π_B. We want to show that n is equal to $\tilde{n}_A$, the exponent of $A^\vee \cap B$.

Let $i_{A^\vee}$ and i_B be the embeddings of $A^\vee$ and B into J, respectively. Then

$$\varphi = (n\pi_{A^\vee}, n\pi_B) \in \mathrm{Hom}(J, A^\vee \times B)$$

and $\varphi \circ (i_{A^\vee} + i_B) = [n]_{A^\vee \times B}$. We have an exact sequence

$$0 \to A^\vee \cap B \xrightarrow{x \mapsto (x,-x)} A^\vee \times B \xrightarrow{i_{A^\vee} + i_B} J \to 0.$$

Let Δ be the image of $A^\vee \cap B$. Then by exactness,

$$[n]\Delta = (\varphi \circ (i_{A^\vee} + i_B))(\Delta) = \varphi \circ ((i_{A^\vee} + i_B)(\Delta)) = \varphi(\{0\}) = \{0\},$$

so n is a multiple of the exponent $\tilde{n}_A$ of $A^\vee \cap B$.

To show the opposite divisibility, consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A^\vee \cap B \arrow[r, "x \mapsto (x,-x)"] \arrow[d, "{[\tilde{n}_A]}"] & A^\vee \times B \arrow[r] \arrow[d, "{([\tilde{n}_A],0)}"] & J \arrow[r] \arrow[d, dotted, "\psi"] & 0 \\
0 \arrow[r] & A^\vee \cap B \arrow[r, "x \mapsto (x,-x)"] & A^\vee \times B \arrow[r] & J \arrow[r] & 0,
\end{tikzcd}$$

where the middle vertical map is $(a, b) \mapsto (\tilde{n}_A a, 0)$ and the map ψ exists because $[\tilde{n}_A](A^\vee \cap B) = 0$. But $\psi = \tilde{n}_A \pi_{A^\vee}$ in $\mathrm{End}(J) \otimes \mathbf{Q}$. This shows that $\tilde{n}_A \pi_{A^\vee} \in \mathrm{End}(J)$, i.e., that $\tilde{n}_A$ is a multiple of the denominator n of $\pi_{A^\vee}$.

□

Let $\mathrm{Ext}^1 = \mathrm{Ext}^1_{\mathbf{Z}}$ denote the first Ext functor in the category of $\mathbf{Z}$-modules.

Lemma 4.3. *The group $(\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$ is isomorphic to the quotient (1) in Definition 3.5, so $r_A = \#((\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T})$ and $\tilde{r}_A$ is the exponent of $(\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$. More precisely, $\mathrm{Ext}^1((\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}, \mathbf{Z})$ is isomorphic as a $\mathbf{T}$-module to the quotient (1).*

Proof. Apply the $\mathrm{Hom}(-,\mathbf{Z})$ functor to the first row of (2) to obtain a three-term exact sequence

$$0 \to \mathrm{Hom}(\mathbf{T}_1 \oplus \mathbf{T}_2, \mathbf{Z}) \to \mathrm{Hom}(\mathbf{T}, \mathbf{Z}) \to \mathrm{Ext}^1((\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}, \mathbf{Z}) \to 0. \qquad (3)$$

There is a $\mathbf{T}$-equivariant bilinear pairing $\mathbf{T} \times S_2(\mathbf{Z}) \to \mathbf{Z}$ given by $(t, g) \mapsto a_1(t(g))$, which is perfect by [AU96, Lemma 2.1] (see also [Rib83, Theorem 2.2]). Using this pairing, we transform (3) into an exact sequence

$$0 \to S_2(\mathbf{Z})[I_f] \oplus S_2(\Gamma; \mathbf{Z})[I_f]^{\perp} \to S_2(\mathbf{Z}) \to \mathrm{Ext}^1((\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}, \mathbf{Z}) \to 0$$

of $\mathbf{T}$-modules. Here we use that $\mathrm{Hom}(\mathbf{T}_2, \mathbf{Z})$ is the unique saturated Hecke-stable complement of $S_2(\mathbf{Z})[I_f]$ in $S_2(\mathbf{Z})$, hence must equal $S_2(\mathbf{Z})[I_f]^{\perp}$. Finally note that if G is any finite abelian group, then $\mathrm{Ext}^1(G, \mathbf{Z}) \approx G$ as groups, which gives the desired result. □

Lemma 4.4. *The element $e_1 \in (\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$ has order $\tilde{r}_A$.*

Proof. By Lemma 4.3, the lemma is equivalent to the assertion that the order r of e_1 equals the exponent of $M = (\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$. Since e_1 is an element of M, the exponent of M is divisible by r.

To obtain the reverse divisibility, consider any element x of M. Let $(a, b) \in \mathbf{T}_1 \oplus \mathbf{T}_2$ be such that its image in M is x. By definition of e_1 and r, we have $(r, 0) \in \mathbf{T}$, and since $1 = (1, 1) \in \mathbf{T}$, we also have $(0, r) \in \mathbf{T}$. Thus $(\mathbf{T}r, 0)$ and $(0, \mathbf{T}r)$ are both subsets of $\mathbf{T}$ (i.e., in the image of $\mathbf{T}$ under the map $\mathbf{T} \to \mathbf{T}_1 \oplus \mathbf{T}_2$), so $r(a, b) = (ra, rb) = (ra, 0) + (0, rb) \in \mathbf{T}$. This implies that the order of x divides r. Since this is true for every $x \in M$, we conclude that the exponent of M divides r. □

Proposition 4.5. *If $f \in S_2(\mathbf{C})$ is a newform, then $\tilde{n}_{A_f} \mid \tilde{r}_{A_f}$.*

Proof. Since e_2 is the image of e_1 under the right-most vertical homomorphism in (2), the order of e_2 divides that of e_1. Now apply Lemmas 4.2 and 4.4. □

This finishes the proof of the first statement in Theorem 3.7.

4.2 Proof of Theorem 3.7 (b)

Let $\mathbf{T}'$ be the saturation of $\mathbf{T} = \mathbf{Z}[\ldots, T_n, \ldots]$ in $\mathrm{End}(J_0(N))$, i.e., the set of elements of $\mathrm{End}(J_0(N)) \otimes \mathbf{Q}$ some positive multiple of which lie in $\mathbf{T}$. The quotient $\mathbf{T}'/\mathbf{T}$ is a finitely generated abelian group because both $\mathbf{T}$ and $\mathrm{End}(J_0(N))$ are finitely generated over $\mathbf{Z}$. Since $\mathbf{T}'/\mathbf{T}$ is also a torsion group, it is finite.

In Section 4.2.1, we will give some conditions under which $\mathbf{T}$ and $\mathbf{T}'$ agree locally at maximal ideal of $\mathbf{T}$. In Section 4.2.2, we will explain how the ratio of the congruence number to the modular degree is closely related to the order of $\mathbf{T}'/\mathbf{T}$, and finally deduce that this ratio is 1 (for quotients associated to newforms) locally at a prime p such that $p^2 \nmid N$.

4.2.1 MULTIPLICITY ONE

Fixt an integer N and a prime $p \mid N$. Suppose for a moment that N is prime, so $p = N$. In [Maz77], Mazur proves that $\mathbf{T} = \mathbf{T}'$; he combines this result with the equality

$$\mathbf{T} \otimes \mathbf{Q} = \mathrm{End}(J_0(p)) \otimes \mathbf{Q},$$

to deduce that $\mathbf{T} = \mathrm{End}(J_0(p))$. This result, combined with Ribet's result [Rib75] or [Rib81] to the effect that $\mathbf{T} \otimes \mathbf{Q} = (\mathrm{End}_{\overline{\mathbf{Q}}} J_0(N)) \otimes \mathbf{Q}$, shows that $\mathbf{T}$ is the full ring of endomorphisms of $J_0(N)$ over $\overline{\mathbf{Q}}$. When N is no longer necessarily prime, the method of [Maz77] shows that $\mathbf{T}$ and $\mathbf{T}'$ agree locally at a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ that satisfies a simple condition involving differentials form mod ℓ, where ℓ is the residue characteristic of $\mathfrak{m}$.

For the sake of completeness, we state and prove a lemma that can be easily extracted from [Maz77]. Let m be the largest square dividing N and let $R = \mathbf{Z}[\frac{1}{m}]$. Let $X_0(N)_R$ denote the minimal regular model of $X_0(N)$ over R. Let $\Omega = \Omega_{X_0(N)/R}$ denote the sheaf of regular differentials on $X_0(N)_R$, as in [Maz78, §2(e)]. If ℓ is a prime such that $\ell^2 \nmid N$, then $X_0(N)_{\mathbf{F}_\ell}$ denotes the special fiber of $X_0(N)_R$ at the prime ℓ.

LEMMA 4.6 (Mazur). *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ of residue characteristic ℓ such that $\ell^2 \nmid N$. Suppose that*

$$\dim_{\mathbf{T}/\mathfrak{m}} \mathrm{H}^0(X_0(N)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}] \leq 1.$$

Then $\mathbf{T}$ and $\mathbf{T}'$ agree locally at $\mathfrak{m}$.

Proof. Let M denote the group $H^1(X_0(N)_R, \mathcal{O}_{X_0(N)})$, where $\mathcal{O}_{X_0(N)}$ is the structure sheaf of $X_0(N)$. As explained in [Maz77, p. 95], we have an action of $\mathrm{End}_{\mathbf{Q}} J_0(N)$ on M, and the action of $\mathbf{T}$ on M via the inclusion $\mathbf{T} \subseteq \mathrm{End}_{\mathbf{Q}} J_0(N)$ is faithful, so likewise for the action by $\mathbf{T}'$. Hence we have an injection $\phi : \mathbf{T}' \hookrightarrow \mathrm{End}_{\mathbf{T}} M$. Suppose $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ that satisfies the hypotheses of the lemma. To prove that $\mathbf{T}_{\mathfrak{m}} = \mathbf{T}'_{\mathfrak{m}}$ it suffices to prove the following claim:

Claim: The map $\phi|_{\mathbf{T}}$ is surjective locally at $\mathfrak{m}$.

Proof. By Nakayama's lemma, to show that M is generated as a single element over $\mathbf{T}$ locally at $\mathfrak{m}$, it suffices to check that the dimension of the $\mathbf{T}/\mathfrak{m}$-vector space $M/\mathfrak{m}M$ is at most one. Since $\ell^2 \nmid N$, $M/\mathfrak{m}M$ is dual to $H^0(X_0(N)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$ (see, e.g., [Maz78, §2]). Since we are assuming that $\dim_{\mathbf{T}/\mathfrak{m}} H^0(X_0(N)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}] \leq 1$, we have $\dim_{\mathbf{T}/\mathfrak{m}}(M/\mathfrak{m}M) \leq 1$, which proves the claim. □

□

If $\mathfrak{m}$ is a maximal ideal of the Hecke algebra $\mathbf{T}$ of residue characteristic ℓ, we say that $\mathfrak{m}$ satisfies *multiplicity one for differentials* if

$$\dim(\mathrm{H}^0(X_0(N)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]) \leq 1.$$

By Lemma 4.6, multiplicity one for $\mathrm{H}^0(X_0(N)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$ implies that $\mathbf{T}$ and $\mathbf{T}'$ agree at $\mathfrak{m}$.

There is quite a bit of literature on the question of multiplicity 1 for $\mathrm{H}^0(X_0(N)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$. The easiest case is that ℓ is prime to the level N:

Lemma 4.7 (Mazur). *If $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ of residue characteristic ℓ such that $\ell \nmid N$, then*

$$\dim_{\mathbf{T}/\mathfrak{m}} \mathrm{H}^0(X_0(N)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}] \leq 1.$$

Proof. Mazur deduces this lemma from injectivity of the q-expansion map. The reader may find the following alternative approach to part of the argument easier to follow than the one on p. 95 of [Maz77]. We have an $\mathbf{F}_\ell$-vector space that embeds in $\mathbf{F}_\ell[[q]]$, for example a space V of differentials that is killed by a maximal ideal $\mathfrak{m}$. This space is a $\mathbf{T}/\mathfrak{m}$-vector space, and we want to see that its dimension over $\mathbf{T}/\mathfrak{m}$ is at most 1. Mazur invokes tensor products and eigenvectors; alternatively, we note that V embeds in $\mathrm{Hom}_{\mathbf{F}_\ell}(\mathbf{T}/\mathfrak{m}, \mathbf{F}_\ell)$ via the standard duality that sends $v \in V$ to the linear form whose value on a Hecke operator T is the qth coefficient of $v|T$. The group $\mathrm{Hom}_{\mathbf{F}_\ell}(\mathbf{T}/\mathfrak{m}, \mathbf{F}_\ell)$ has the same size as $\mathbf{T}/\mathfrak{m}$, which completes the argument because $\mathrm{Hom}_{\mathbf{F}_\ell}(\mathbf{T}/\mathfrak{m}, \mathbf{F}_\ell)$ has dimension 1 as a $\mathbf{T}/\mathfrak{m}$-vector space. □

In the context of Mazur's paper, where the level N is prime, we see from Lemma 4.7 that $\mathbf{T}$ and $\mathbf{T}'$ agree away from N. Locally at N, Mazur proved that $\mathbf{T} = \mathbf{T}'$ by an analogue of the arguments that he used away from N; see Chapter II of [Maz77] (and especially Prop. 9.4 and 9.5 of that chapter) as well as [MR91], where these arguments are taken up in a context where the level is no longer necessarily prime (and where one works locally at a prime whose square does not divide the level). Thus in the prime level case, $\mathbf{T} = \mathbf{T}'$, as we asserted above.

Now let p be a prime such that $p \parallel N$, and let $M = N/p$. The question of multiplicity 1 at p for $\mathrm{H}^0(X_0(pM)_{\mathbf{F}_p}, \Omega)[\mathfrak{m}]$ is discussed in [MR91], where the authors establish multiplicity 1 for maximal ideals $\mathfrak{m} \mid p$ for which the associated mod p Galois representation is irreducible and *not* p-old. (A representation of level pM is p-old if it arises from $S_2(\Gamma_0(M))$.)

If $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ of residue characteristic ℓ, then we say that $\mathfrak{m}$ is ordinary if $T_\ell \notin \mathfrak{m}$ (note that T_ℓ is often denoted U_ℓ if $\ell \mid N$). For our purposes, the following lemma is convenient:

Lemma 4.8 (Wiles). *If $\mathfrak{m}$ is an ordinary maximal ideal of $\mathbf{T}$ of characteristic p, then*

$$\dim_{\mathbf{T}/\mathfrak{m}} \mathrm{H}^0(X_0(pM)_{\mathbf{F}_p}, \Omega)[\mathfrak{m}] \leq 1.$$

This is essentially Lemma 2.2 in [Wil95, pg. 485]; we make a few comments about how it applies on our situation:

1. Wiles considers $X_1(M,p)$ instead of $X_0(pM)$, which means that he is using $\Gamma_1(M)$-structure instead of $\Gamma_0(M)$-structure. This surely has no relevance to the issue at hand.

2. Wiles assumes (on page 480) that p is an odd prime, but again this assumption is not relevant to our question.

3. The condition that $\mathfrak{m}$ is ordinary does not appear explicitly in the statement of Lemma 2.2 in [Wil95]; instead it is a reigning assumption in the context of his discussion.

4. We see by example that Wiles's "ordinary" assumption is less stringent than the assumption in [MR91]; note that [MR91] rule out cases where $\mathfrak{m}$ is both old and new at p, whereas Wiles is happy to include such cases. (On the other hand, Wiles's assumption is certainly nonempty, since it rules out maximal ideals $\mathfrak{m}$ that arise from non-ordinary (old) forms of level M. Here is an example with $p = 2$ and $M = 11$, so $N = 22$: There is a unique newform $f = \sum a_n q^n$ of level 11, and $\mathbf{T} = \mathbf{Z}[T_2] \subset \mathrm{End}(J_0(22))$, where $T_2^2 - a_2 T_2 + 2 = 0$. Since $a_2 = -2$, we have $\mathbf{T} \cong \mathbf{Z}[\sqrt{-1}]$. We can choose the square root of -1 to be $T_2 + 1$. Then T_2 is a generator of the unique maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ with residue characteristic 2, and this maximal ideal is not ordinary.)

We now summarize the conclusions we can make from the lemmas so far:

Proposition 4.9. *The modules $\mathbf{T}$ and $\mathbf{T}'$ agree locally at each maximal ideal $\mathfrak{m}$ that is either prime to N or that satisfies the following supplemental hypothesis: the residue characteristic of $\mathfrak{m}$ divides N only to the first power and $\mathfrak{m}$ is ordinary.*

Proof. This follows easily from Lemmas 4.6, 4.7, and 4.8. □

In Mazur's original context, where the level N is prime, we have $T_N^2 = 1$ because there are no forms of level 1. Accordingly, each $\mathfrak{m}$ dividing N is ordinary, and we recover Mazur's equality $\mathbf{T} = \mathbf{T}'$ in this special case.

4.2.2 Degrees and Congruences

Let $e \in \mathbf{T} \otimes \mathbf{Q}$ be as in Section 4.1, and let p, N, M be as before Lemma 4.8. The image of e in $J_0(pM)$ is the $\mathbf{T}$-stable abelian subvariety denoted $A^\vee$ in Section 4.1, but since we shall now exclusively work with this subvariety rather than the corresponding optimal quotient of $J_0(pM)$ (which was denoted A earlier), we will now write A to denote the image of e (without risk of confusion). We also write B to denote the unique $\mathbf{T}$-stable abelian subvariety of $J_0(pM)$ complementary to A.

For $t \in \mathbf{T}$, let t_A be the restriction of t to A, and let t_B be the image of t in $\mathrm{End}(B)$. Let $\mathbf{T}_A$ be the subgroup of $\mathrm{End}(A)$ consisting of the various t_A, and define $\mathbf{T}_B$ similarly. As before, we obtain an injection $j : \mathbf{T} \hookrightarrow \mathbf{T}_A \times \mathbf{T}_B$ with finite cokernel. Because j is an injection, we refer to the maps $\pi_A : \mathbf{T} \to \mathbf{T}_A$ and $\pi_B : \mathbf{T} \to \mathbf{T}_B$, given by $t \mapsto t_A$ and $t \mapsto t_B$, respectively, as "projections".

DEFINITION 4.10. The *congruence ideal* associated with the projector e is $I = \pi_A(\ker(\pi_B)) \subset \mathbf{T}_A$.

Viewing $\mathbf{T}_A$ as $\mathbf{T}_A \times \{0\}$, we may view $\mathbf{T}_A$ as a subgroup of $\mathbf{T} \otimes \mathbf{Q} \cong (\mathbf{T}_A \times \mathbf{T}_B) \otimes \mathbf{Q}$. Also, we may view $\mathbf{T}$ as embedded in $\mathbf{T}_A \times \mathbf{T}_B$, via the map j.

LEMMA 4.11. *We have* $I = \mathbf{T}_A \cap \mathbf{T}$.

A larger ideal of $\mathbf{T}_A$ is $J = \mathrm{Ann}_{\mathbf{T}_A}(A \cap B)$; it consists of restrictions to A of Hecke operators that vanish on $A \cap B$.

LEMMA 4.12. *We have* $I \subset J$.

Proof. The image in $\mathbf{T}_A$ of an operator that vanishes on B also vanishes on $A \cap B$. □

LEMMA 4.13. *We have* $J = \mathbf{T}_A \cap \mathrm{End}(J_0(pM)) = \mathbf{T}_A \cap \mathbf{T}'$.

Proof. This is elementary; it is an analogue of Lemma 4.11. □

PROPOSITION 4.14. *There is a natural inclusion* $J/I \hookrightarrow \mathbf{T}'/\mathbf{T}$ *of* $\mathbf{T}$*-modules.*

Proof. Consider the map $\mathbf{T} \to \mathbf{T} \otimes \mathbf{Q}$ given by $t \mapsto te$. This homomorphism factors through $\mathbf{T}_A$ and yields an injection $\iota_A : \mathbf{T}_A \hookrightarrow \mathbf{T} \otimes \mathbf{Q}$. Symmetrically, we also obtain $\iota_B : \mathbf{T}_B \hookrightarrow \mathbf{T} \otimes \mathbf{Q}$. The map $(t_A, t_B) \mapsto \iota_A(t_A) + \iota_B(t_B)$ is an injection $\mathbf{T}_A \times \mathbf{T}_B \hookrightarrow \mathbf{T} \otimes \mathbf{Q}$. The composite of this map with the inclusion $j : \mathbf{T} \hookrightarrow \mathbf{T}_A \times \mathbf{T}_B$ defined above is the natural map $\mathbf{T} \hookrightarrow \mathbf{T} \otimes \mathbf{Q}$. We thus have a sequence of inclusions

$$\mathbf{T} \hookrightarrow \mathbf{T}_A \times \mathbf{T}_B \hookrightarrow \mathbf{T} \otimes \mathbf{Q} \subset \mathrm{End}(J_0(pM)) \otimes \mathbf{Q}.$$

By Lemma 4.11 and Lemma 4.13, we have $I = \mathbf{T}_A \cap \mathbf{T}$ and $J = \mathbf{T}_A \cap \mathbf{T}'$. Thus $I = J \cap \mathbf{T}$, where the intersection is taken inside $\mathbf{T}'$. Thus

$$J/I = J/(J \cap \mathbf{T}) \cong (J + \mathbf{T})/\mathbf{T} \hookrightarrow \mathbf{T}'/\mathbf{T}.$$

□

COROLLARY 4.15. *If* $\mathfrak{m}$ *is a maximal ideal not in* $\mathrm{Supp}_{\mathbf{T}}(\mathbf{T}'/\mathbf{T})$*, then* $\mathfrak{m}$ *is not in the support of* J/I*, i.e., if* $\mathbf{T}$ *and* $\mathbf{T}'$ *agree locally at* $\mathfrak{m}$*, then* I *and* J *also agree locally at* $\mathfrak{m}$.

Note that the Hecke algebra $\mathbf{T}$ acts on J/I through its quotient $\mathbf{T}_A$, since the action of $\mathbf{T}$ on I and on J factors through this quotient.

Now we specialize to the case where A is ordinary at p, in the sense that the image of T_p in $\mathbf{T}_A$, which we denote $T_{p,A}$, is invertible modulo every maximal ideal of $\mathbf{T}_A$ that divides p. (This case occurs when A is a subvariety of the p-new subvariety of $J_0(pM)$, since the square of $T_{p,A}$ is the identity.)

If $\mathfrak{m} \mid p$ is a maximal ideal of $\mathbf{T}$ that arises by pullback from a maximal ideal of $\mathbf{T}_A$, then $\mathfrak{m}$ is ordinary in the sense used above. When A is ordinary at p, it follows from Proposition 4.9 and Corollary 4.15 that $I = J$ locally at p. The reason is simple: regarding I and J as $\mathbf{T}_A$-modules, we realize that we need to test that $I = J$ at maximal ideals of $\mathbf{T}_A$ that divide p. These ideals correspond to maximal ideals $\mathfrak{m} \mid p$ of $\mathbf{T}$ that are automatically ordinary, so we have $I = J$ locally at $\mathfrak{m}$ because of Proposition 4.9. By Proposition 4.9, we have $\mathbf{T} = \mathbf{T}'$ locally at primes away from the level pM. Thus we conclude that $I = J$ locally at all primes $\ell \nmid pM$ and also at p, a prime that divides the level pM exactly once.

Suppose, finally, that A is the abelian variety associated to a newform f of level pM. The ideal $I \subset \mathbf{T}_A$ measures congruences between f and the space of forms in $S_2(\Gamma_0(pM))$ that are orthogonal to the space generated by f. Also, $A \cap B$ is the kernel in A of the map "multiplication by the modular element e". In this case, the inclusion $I \subset J$ corresponds to the divisibility $\tilde{n}_A \mid \tilde{r}_A$, and we have equality at primes at which $I = J$ locally. We conclude that the congruence exponent and the modular exponent agree both at p and at primes not dividing pM, which completes our proof of Theorem 3.7(b).

Remark 4.16. The ring

$$R = \mathrm{End}(J_0(pM)) \cap (\mathbf{T}_A \times \mathbf{T}_B)$$

is often of interest, where the intersection is taken in $\mathrm{End}(J_0(pM)) \otimes \mathbf{Q}$. We proved above that there is a natural inclusion $J/I \hookrightarrow \mathbf{T}'/\mathbf{T}$. This inclusion yields an isomorphism $J/I \xrightarrow{\sim} R/\mathbf{T}$. Indeed, if (t_A, u_B) is an endomorphism of $J_0(pM)$, where $t, u \in \mathbf{T}$, then $(t_A, u_B) - u = (t_A, 0)$ is an element of J. The ideals I and J are equal to the extent that the rings $\mathbf{T}$ and R coincide. Even when $\mathbf{T}'$ is bigger than $\mathbf{T}$, its subring R may be not far from $\mathbf{T}$.

5 Failure of Multiplicity One

In this section, we discuss examples of failure of multiplicity one (in two different but related senses). The notion of multiplicity one, originally due to Mazur [Maz77], has played an important role in several places (e.g., in Wiles's proof of Fermat's last theorem [Wil95]). This notion is closely related to Gorensteinness of certain Hecke algebras (e.g., see [Til97]). Kilford [Kil02] found examples of failure of Gorensteinness (and multiplicity one) at the prime 2 for certain prime levels. Motivated by the arguments in Section 4, in this section we give examples of failure of multiplicity one for primes (including odd primes) whose square divides the level.

5.1 Multiplicity One for Differentials

In connection with the arguments in Section 4, especially Lemmas 4.6 and 4.8, it is of interest to compute the index $[\mathbf{T}' : \mathbf{T}]$ for various N. We can compute this index in Magma, e.g., the following commands compute the index for $N = 54$: "`J := JZero(54); T := HeckeAlgebra(J); Index(Saturation(T), T);`" We obtain Table 2, where the first column contains N and the second column contains $[\mathbf{T}' : \mathbf{T}]$:

Let $\mathfrak{m}$ be a maximal ideal of the Hecke algebra $\mathbf{T} \subset \mathrm{End}(J_0(N))$ of residue characteristic p. Recall that we say that $\mathfrak{m}$ satisfies *multiplicity one for differentials* if $\dim(\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega)[\mathfrak{m}]) \leq 1$.

In each case in which $[\mathbf{T}' : \mathbf{T}] \neq 1$, Lemma 4.6 implies that there is some maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ such that $\dim(\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega)[\mathfrak{m}]) > 1$, which is an example of failure of multiplicity one for differentials.

In Table 2, whenever $p \mid [\mathbf{T}' : \mathbf{T}]$, then $p^2 \mid 2N$. This is a consequence of Proposition 4.9, which moreover asserts that when 2 exactly divides N and $2 \mid [\mathbf{T}' : \mathbf{T}]$ then there is a non-ordinary (old) maximal ideal of characteristic 2 in the support of $\mathbf{T}'/\mathbf{T}$.

Moreover, notice that Theorem 3.7(b) (whose proof is in Section 4.2) follows formally from two key facts: that A_f is new and that multiplicity one for differentials holds for ordinary maximal ideals with residue characteristic $p \mid\mid N$ and for all maximal ideals with residue characteristic $p \nmid N$. The conclusion of Theorem 3.7(b) does not hold for the counterexamples in Section 2 (e.g., for 54B1), which are all new elliptic curves, so multiplicity one for differentials does not hold for certain maximal ideals that arise from the new quotient of the Hecke algebra. Note that in all examples we have $p \mid (r/m)$ with $p^2 \mid N$, which raises the question: are there non-ordinary counterexamples with $p \mid\mid N$?

5.2 Multiplicity One for Jacobians

We say that a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ satisfies *multiplicity one* if $J_0(N)[\mathfrak{m}]$ is of dimension two over $\mathbf{T}/\mathfrak{m}$. We sometimes use the phrase "multiplicity one for $J_0(N)$" in order to distinguish this notion from the notion of multiplicity one for differentials.

Proposition 5.1. *Suppose E is an optimal elliptic curve over $\mathbf{Q}$ of conductor N and p is a prime such that $p \mid r_E$ but $p \nmid m_E$. Let $\mathfrak{m}$ be the annihilator in $\mathbf{T}$ of $E[p]$. Then multiplicity one fails for $\mathfrak{m}$, i.e., $\dim_{\mathbf{T}/\mathfrak{m}} J_0(N)[\mathfrak{m}] > 2$.*

Proof. Using the principal polarization $E \cong E^\vee$ we view E as an abelian subvariety of $J = J_0(N)$ and consider the complementary $\mathbf{T}$-stable abelian subvariety A of E (thus A is the kernel of the modular parametrization map $J \to E$). In this setup, $J = E + A$, and the intersection of E and A is $E[m_E]$. Here we use that the composite map $E \simeq E^\vee \to J^\vee \to J \to E$ is a polarization, and hence is multiplication by a positive integer m_E. Because $p \nmid m_E$, we have $E[p] \cap A = 0$. On the other hand, let $\mathfrak{m}$ be the annihilator of $E[p]$ inside $\mathbf{T}$.

Table 2: The Index $[\mathbf{T}' : \mathbf{T}]$

11	1
12	1
13	1
14	1
15	1
16	1
17	1
18	1
19	1
20	1
21	1
22	1
23	1
24	1
25	1
26	1
27	1
28	1
29	1
30	1
31	1
32	1
33	1
34	1
35	1
36	1
37	1
38	1
39	1
40	1
41	1
42	1
43	1
44	2
45	1
46	2
47	1
48	1
49	1
50	1
51	1
52	1
53	1
54	3
55	1
56	2
57	1
58	1
59	1
60	2
61	1
62	2
63	1
64	2
65	1
66	1
67	1
68	2
69	1
70	1
71	1
72	2
73	1
74	1
75	1
76	2
77	1
78	2
79	1
80	4
81	1
82	1
83	1
84	2
85	1
86	1
87	1
88	8
89	1
90	1
91	1
92	16
93	1
94	4
95	1
96	8
97	1
98	1
99	9
100	1
101	1
102	1
103	1
104	4
105	1
106	1
107	1
108	54
109	1
110	2
111	1
112	8
113	1
114	1
115	1
116	4
117	1
118	2
119	1
120	32
121	1
122	1
123	1
124	16
125	25
126	18
127	1
128	64
129	1
130	1
131	1
132	8
133	1
134	1
135	27
136	16
137	1
138	4
139	1
140	8
141	1
142	8
143	1
144	32
145	1
146	1
147	7
148	4
149	1
150	5
151	1
152	32
153	9
154	1
155	1
156	32
157	1
158	4
159	1
160	256
161	1
162	81
163	1
164	8
165	1
166	2
167	1
168	128
169	13
170	1
171	9
172	8
173	1
174	4
175	5
176	512
177	1
178	1
179	1
180	72
181	1
182	1
183	1
184	1024
185	1
186	4
187	1
188	256
189	243
190	8
191	1
192	4096
193	1
194	1
195	1
196	14
197	1
198	81
199	1
200	80
201	1
202	1
203	1
204	32
205	1
206	4
207	81
208	256
209	1
210	2

Then $J[\mathfrak{m}]$ contains $E[p]$ and also $A[\mathfrak{m}]$, and because p is a congruence prime, the submodule $A[\mathfrak{m}] \subset J[\mathfrak{m}]$ is nonzero. Thus the sum $E[p] + A[\mathfrak{m}]$ is a direct sum and is larger than $E[p]$, which is of dimension 2 over $\mathbf{T}/\mathfrak{m} = \mathbf{Z}/p\mathbf{Z}$. Hence the dimension of $J[\mathfrak{m}]$ over $\mathbf{T}/\mathfrak{m}$ is bigger than 2, as claimed. □

Proposition 5.1 implies that any example in which simultaneously $p \nmid m_E$ and $\mathrm{ord}_p(r_E) \neq \mathrm{ord}_p(m_E)$ produces an example in which multiplicity one for $J_0(N)$ fails. For example, for the curve 54B1 and $p = 3$, we have $\mathrm{ord}_3(r_E) = 1$ but $\mathrm{ord}_3(m_E) = 0$, so multiplicity one at 3 fails for $J_0(54)$.

REFERENCES

[ARS06] A. Agashe, K. Ribet and W. Stein, *The Manin Constant*, QJPAM, Coates Volume (2006), to appear.

[AU96] A. Abbes and E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. 103 (1996), no. 3, 269–286.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993).

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), no. 4, 843–939 (electronic).

[CK04] Alina Carmen Cojocaru and Ernst Kani, *The modular degree and the congruence number of a weight 2 cusp form*, Acta Arith. 114 (2004), no. 2, 159–167.

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, `http://www.maths.nott.ac.uk/personal/jec/book/`.

[CSS97] G. Cornell, J. H. Silverman, and G. Stevens (eds.), *Modular forms and Fermat's last theorem (boston,ma, 1995)*, New York, Springer-Verlag, 1997, Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.

[DI95] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133.

[Fre97] G. Frey, *On ternary equations of Fermat type and relations with elliptic curves*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 527–548.

[FM99] G. Frey and M. Müller, *Arithmetic of modular curves and applications*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 11–48.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Kil02] L. J. P. Kilford, *Some non-Gorenstein Hecke algebras attached to spaces of modular forms*, J. Number Theory 97 (2002), no. 1, 157–164.

[Lan83] S. Lang, *Abelian varieties*, Springer-Verlag, New York, 1983, Reprint of the 1959 original.

[Li75] W-C. Li, *Newforms and functional equations*, Math. Ann. 212 (1975), 285–315.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), no. 2, 129–162.

[MR91] B. Mazur and K. A. Ribet, *Two-dimensional representations in the arithmetic of modular curves*, Astérisque (1991), no. 196–197, 6, 215–255 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[Mum70] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Mur99] M. R. Murty, *Bounds for congruence primes*, Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), Amer. Math. Soc., Providence, RI, 1999, pp. 177–192.

[Rib75] K. A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. Math. (2) 101 (1975), 555–562.

[Rib81] K. A. Ribet, *Endomorphism algebras of abelian varieties attached to newforms of weight* 2, Seminar on Number Theory, Paris 1979–80, Progr. Math., vol. 12, Birkhäuser Boston, Mass., 1981, pp. 263–276.

[Rib83] K. A. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. 71 (1983), no. 1, 193–205.

[Ste89] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. 98 (1989), no. 1, 75–106.

[Stu87] J. Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Springer, Berlin, 1987, pp. 275–280.

[Til97] J. Tilouine, *Hecke algebras and the Gorenstein property*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 327–342.

[Vat05] V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves*, J. Inst. Math. Jussieu 4 (2005), no. 2, 281–316.

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 (1995), no. 3, 443–551.

[Zag85] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. 28 (1985), no. 3, 372–384.