THE MODULAR DEGREE, CONGRUENCE PRIMES AND MULTIPLICITY ONE

AMOD AGASHÉ  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 $\mathbb{Q}$. By [BCDT01], we may view $E$ as an
abelian variety quotient over $\mathbb{Q}$ 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 $f_E = \sum a_n q^n \in \mathbb{Q}(\Gamma_0(N))$ be the newform attached to $E$. The
congruence number $r_E$ of $E$ is the largest integer such that there is an element
g = $\sum b_n q^n \in \mathbb{Q}(\Gamma_0(N))$ with integer Fourier coefficients $b_n$ that is orthogonal
to $f_E$ with respect to the Peterson inner product, and congruent to $f_E$ mod-
ulo $r_E$ (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, $m_E | r_E$. 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 $p$, $\text{ord}_p(r_E/m_E) \leq \frac{1}{2} \text{ord}_p(N)$. We prove this conjecture when $\text{ord}_p(N) \leq 1$.

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.

Acknowledgement. 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 $\mathbb{Q}$ 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 $J_0(N) = \text{Jac}(X_0(N))$ 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 $\mathbf{T} \to \mathbb{Z}[a_1, a_2, \ldots , a_n(f), \ldots]$ that sends $T_n$ to $a_n$. Then the quotient $E = J_0(N)/I_fJ_0(N)$ is an elliptic curve over $\mathbb{Q}$. We call $E$ the optimal quotient associated to $f$. Composing the embedding $X_0(N) \to J_0(N)$ that sends $\infty$ to 0 with the quotient map $J_0(N) \to E$, we obtain a surjective morphism of curves $\phi_E : X_0(N) \to E$.

Definition 2.1 (Modular Degree). The modular degree $m_E$ of $E$ is the degree of $\phi_E$.

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 Mazur 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 $\mathbb{Q}$ of conductor $N$, with modular degree $m_E$ and congruence number $r_E$. Then $m_E | r_E$ and if $\text{ord}_p(N) \leq 1$ then $\text{ord}_p(r_E) = \text{ord}_p(m_E)$.

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

The divisibility $m_E | r_E$ 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 $\text{ord}_p(N) = 1$ then $\text{ord}_p(r_E) = \text{ord}_p(m_E)$, follows from the more general Theorem 3.5 below. Note that [AU96, Prop. 3.3-3.4] implies the weaker statement that if $p \nmid N$ then $\text{ord}_p(r_E) = \text{ord}_p(m_E)$, since Prop. 3.3 implies

$$\text{ord}_p(r_E) - \text{ord}_p(m_E) = \text{ord}_p(#C) - \text{ord}_p(#E) - \text{ord}_p(#D),$$
Table 1: Differing Modular Degree and Congruence Number

<table>
<thead>
<tr>
<th>Curve</th>
<th>$m_E$</th>
<th>$r_E$</th>
<th>Curve</th>
<th>$m_E$</th>
<th>$r_E$</th>
<th>Curve</th>
<th>$m_E$</th>
<th>$r_E$</th>
</tr>
</thead>
<tbody>
<tr>
<td>54B1</td>
<td>2</td>
<td>6</td>
<td>99A1</td>
<td>4</td>
<td>12</td>
<td>128A1</td>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>64A1</td>
<td>2</td>
<td>4</td>
<td>108A1</td>
<td>6</td>
<td>18</td>
<td>128B1</td>
<td>8</td>
<td>32</td>
</tr>
<tr>
<td>72A1</td>
<td>4</td>
<td>8</td>
<td>112A1</td>
<td>8</td>
<td>16</td>
<td>128C1</td>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>80A1</td>
<td>4</td>
<td>8</td>
<td>112B1</td>
<td>4</td>
<td>8</td>
<td>128D1</td>
<td>8</td>
<td>32</td>
</tr>
<tr>
<td>88A1</td>
<td>8</td>
<td>16</td>
<td>112C1</td>
<td>8</td>
<td>16</td>
<td>135A1</td>
<td>12</td>
<td>36</td>
</tr>
<tr>
<td>92B1</td>
<td>6</td>
<td>12</td>
<td>120A1</td>
<td>8</td>
<td>16</td>
<td>144A1</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>96A1</td>
<td>4</td>
<td>8</td>
<td>124A1</td>
<td>6</td>
<td>12</td>
<td>144B1</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>96B1</td>
<td>4</td>
<td>8</td>
<td>126A1</td>
<td>8</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

and by Prop. 3.4 $\text{ord}_p(\#C) = 0$. (Here $c_E$ is the Manin constant of $E$.)

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 countexamples 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 precision 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

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

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

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

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 $\text{ord}_p(N) \leq 2$, so a special case of the conjecture is

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

**Remark 2.4.** It is often productive to parametrize elliptic curves by $X_1(N)$ instead of $X_0(N)$ (see, e.g., [Ste80] and [Vat05]). Suppose $E$ is an optimal
quotient of $X_1(N)$, let $m'$ 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 $m'=18$ 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 $m'=18$ 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 $\Gamma$ be a fixed choice of either $\Gamma_0(N)$ or $\Gamma_1(N)$, let $X$ be the modular curve over $\mathbb{Q}$ associated to $\Gamma$, and let $J$ be the Jacobian of $X$. Let $I$ be a saturated ideal of the corresponding Hecke algebra $T \subset \text{End}(J)$, so $T/I$ is torsion free. Then $A = A_I = J/IJ$ is an optimal quotient of $J$ since $IJ$ is an abelian subvariety.

**Definition 3.1 (Newform Quotient).** If $f = \sum a_n(f)q^n \in S_2(\Gamma)$ and $I_f = \ker(T \to \mathbb{Z}[a_1, a_2, a_3, \ldots])$, then $A = A_f = J/I_fJ$ is the newform quotient associated to $f$. It is an abelian variety over $\mathbb{Q}$ of dimension equal to the degree of the field $\mathbb{Q}(a_n(f), \ldots)$.

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

If $C$ is an abelian variety, let $C^\vee$ denote the dual of $C$. Let $\phi_2$ denote the quotient map $J \to A$. There is a canonical principal polarization $\theta : J \cong J^\vee$ arising from the theta divisor. Dualizing $\phi_2$, 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 $\phi_1 : A^\vee \to J$.

Since $\phi_2$ is a surjection, by [Lan83, §VI.3, Prop 3], $\ker(\phi_2^\vee)$ is finite. Since $\ker(\phi_2)$ is connected, $\ker(\phi_2^\vee)$ is trivial, so $\phi_2^\vee$ and $\phi_1$ are injections. Let $\phi$ be the composition

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

**Proposition 3.2.** The map $\phi$ is a polarization.

**Proof.** Let $i$ be the injection $\phi_2^\vee : A^\vee \to J^\vee$, and let $\Theta$ denote the theta divisor. From the definition of the polarization attached to an ample divisor, we see that the map $\phi$ is induced by the pullback $i^*(\Theta)$ of the theta divisor. The theta divisor is effective, and hence so is $i^*(\Theta)$. By [Mum70, §6, Application 1, p. 60], $\ker \phi$ is finite. Since the dimensions of $A$ and $A^\vee$ are the same, $\phi$ is an isogeny. Moreover, since $\Theta$ is ample, some power of it is very ample. Then the pullback of this very ample power by $i$ is again very ample, and hence a power of $i^*(\Theta)$ is very ample, so $i^*(\Theta)$ is ample (by [Har77, II.7.6]).

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 (Modular exponent and number). The modular exponent of \( A \) is the exponent of the kernel of the isogeny \( \phi \), and the modular number of \( A \) is the degree of \( \phi \).

We denote the modular exponent of \( A \) by \( n_A \) 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 \( \mathbb{C} \), 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 \( \infty \) have coefficients in \( R \). (Note that \( \Gamma \) is fixed for this whole section.) Let \( W(I) = S_2(\Gamma; \mathbb{Z})[I] \) denote the orthogonal complement of \( S_2(\Gamma; \mathbb{Z})[I] \) in \( S_2(\Gamma; \mathbb{Z}) \) with respect to the Petersson inner product.

Definition 3.4 (Congruence exponent and number). The exponent of the quotient group

\[
\frac{S_2(\Gamma; \mathbb{Z})}{S_2(\Gamma; \mathbb{Z})[I] + W(I)}
\]

is the congruence exponent \( r_A \) of \( A \) and its order is the congruence number \( r_A \).

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 3.5. If \( f \in S_2(\mathbb{C}) \) is a newform, then

(a) We have \( n_{A_f} \mid r_{A_f} \), and

(b) If \( p^2 \nmid N \), then \( \text{ord}_p(r_{A_f}) = \text{ord}_p(n_{A_f}) \).

Remark 3.6. When \( A_f \) is an elliptic curve, Theorem 3.5 implies that the modular degree divides the congruence number, 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

\[
n_{A_f} = (2^{11} \cdot 6947)^2 \mid r_{A_f} = (2^{10} \cdot 6947)^2.
\]

Note that 431 is prime and mod 2 multiplicity one fails for \( J_0(431) \) (see [Kj02]). (Contact the third author for compute code to verify the above assertions.)

4 Proof of the Main Theorem

In this section we prove Theorem 3.5. We continue using the notation introduced so far.
4.1 Proof of Theorem 3.5 (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 \( J^v \) it acts as \( W_NTW_N \), 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 \( A^v \) induced by the embedding \( A^v \to J^v \) and the action on \( A^v \) induced by \( \phi_1 : A^v \to J \) are the same. Hence \( A^v \) is isomorphic to \( \phi_1(A^v) \) as a \( T \)-module.

Recall that \( f \) is a newform, \( I_f = \text{Ann}_T(f) \), and \( J = J_0(N) \). Let \( B = I_fJ \), so that \( A^v + B = J \), 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.** \( \text{Hom}(A^v, B) = 0 \).

**Proof.** If there were a nonzero element of \( \text{Hom}(A^v, B) \), then for all \( \ell \), the Tate module \( \text{Tate}_\ell(A^v) = \mathbb{Q} \otimes \lim_{\to \ell} A^v[\ell^n] \) would be a factor of \( \text{Tate}_\ell(B) \). One could then extract almost all prime-indexed coefficients of the corresponding eigenforms from the Tate modules, which would violate multiplicity one for systems of Hecke eigenvalues (see [Li75, Cor. 3, pg. 300]). \( \square \)

Let \( T_1 \) be the image of \( T \) in \( \text{End}(A^v) \), and let \( T_2 \) be the image of \( T \) in \( \text{End}(B) \). We have the following commutative diagram with exact rows:

\[
\begin{array}{cccccccccc}
0 & \rightarrow & T & \rightarrow & T_1 \oplus T_2 & \rightarrow & T_1 \oplus T_2 & \rightarrow & 0 \\
| & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \rightarrow & \text{End}(J) & \rightarrow & \text{End}(A^v) \oplus \text{End}(B) & \rightarrow & \frac{\text{End}(A^v) \oplus \text{End}(B)}{\text{End}(J)} & \rightarrow & 0. \\
\end{array}
\]

(2)

Let

\[ e = (1, 0) \in T_1 \oplus T_2, \]

and let \( e_1 \) and \( e_2 \) denote the images of \( e \) in the groups \( (T_1 \oplus T_2)/T \) and \( (\text{End}(A^v) \oplus \text{End}(B))/\text{End}(J) \), 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 \( e_1 \); this will be used in the proof of Proposition 4.5 below.

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

Let \( \pi_{A^v}, \pi_B \in \text{End}(J) \otimes \mathbb{Q} \) be projection onto \( A^v \) and \( B \), respectively. Note that the denominator of \( \pi_{A^v} \) equals the denominator of \( \pi_B \), since \( \pi_{A^v} + \pi_B = 1_J \), so that \( \pi_B = 1_J - \pi_{A^v} \).
Lemma 4.2. The element $e_2 \in \text{End}(A^\vee) \oplus \text{End}(B))/\text{End}(J)$ 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 $\pi_B$. 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

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

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

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

Let $\Delta$ 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

$$
\begin{array}{ccccccccc}
0 & \rightarrow & A^\vee \cap B & \xrightarrow{x \mapsto (x, -x)} & A^\vee \times B & \xrightarrow{i_{A^\vee} + i_B} & J & \rightarrow & 0 \\
\downarrow{[n_A]} & & \downarrow{[\{n_A\}, 0]} & & \downarrow{\psi} & & \downarrow{\psi} & & \\
0 & \rightarrow & A^\vee \cap B & \xrightarrow{x \mapsto (x, -x)} & A^\vee \times B & \xrightarrow{i_{A^\vee} + i_B} & J & \rightarrow & 0,
\end{array}
$$

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

\[\square\]

Lemma 4.3. The group $(T_1 \oplus T_2)/T$ is isomorphic to the quotient (1) in Definition 3.4, so $r_i = \#((T_1 \oplus T_2)/T)$ and $\hat{r}_A$ is the exponent of $(T_1 \oplus T_2)/T$. More precisely, $\text{Ext}^1((T_1 \oplus T_2)/T, \mathbb{Z})$ is isomorphic as a $T$-module to the quotient (1).

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

$$0 \rightarrow \text{Hom}(T_1 \oplus T_2, \mathbb{Z}) \rightarrow \text{Hom}(T, \mathbb{Z}) \rightarrow \text{Ext}^1((T_1 \oplus T_2)/T, \mathbb{Z}) \rightarrow 0. \quad (3)$$

The term $\text{Ext}^1((T_1 \oplus T_2, \mathbb{Z})$ is 0 is because $\text{Ext}^1(M, \mathbb{Z}) = 0$ for any finitely generated free abelian group. Also, $\text{Hom}((T_1 \oplus T_2)/T, \mathbb{Z}) = 0$ since $(T_1 \oplus T_2)/T$ is torsion. There is a $T$-equivariant bilinear pairing $T \times S_2(\mathbb{Z}) \rightarrow \mathbb{Z}$ 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

\[0 \to S_2(\mathbb{Z})[I_f] \oplus W(I_f) \to S_2(\mathbb{Z}) \to \text{Ext}^1((T_1 \oplus T_2)/T, \mathbb{Z}) \to 0\]

of \(T\) modules. Here we use that \(\text{Hom}(T_2, \mathbb{Z})\) is the unique saturated Hecke-stable complement of \(S_2(\mathbb{Z})[I_f]\) in \(S_2(\mathbb{Z})\), hence must equal \(S_2(\mathbb{Z})[I_f]^+ = W(I_f)\). Finally note that if \(G\) is any finite abelian group, then \(\text{Ext}^1(G, \mathbb{Z}) \approx G\) as groups, which gives the desired result.

**Lemma 4.4.** The element \(e_1 \in (T_1 \oplus T_2)/T\) has order \(\tilde{\tau}_A\).

**Proof.** By Lemma 4.3, the lemma is equivalent to the assertion that the order \(r\) of \(e_1\) equals the exponent of \(M = (T_1 \oplus T_2)/T\). 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 \((a, b) \in T_1 \oplus T_2\) be such that its image in \(M\) is \(x\). By definition of \(e_1\) and \(r\), we have \((r, 0) \in T\), and since \(1 = (1, 1) \in T\), we also have \((0, r) \in T\). Thus \((Tr, 0)\) and \((0, Tr)\) are both subsets of \(T\) (i.e., in the image of \(T\) under the map \(T \to T_1 \oplus T_2\)), so \(r(a, b) = (ra, rb) = (ra, 0) + (0, rb) \in T\). 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 \(f \in S_2(\mathbb{C})\) is a newform, then \(\tilde{n}_A | \tilde{\tau}_A\).

**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 3.5.

### 4.2 Proof of Theorem 3.5 (b)

Recall that \(T = \mathbb{Z}[J_0, J_0, \ldots]\) is the subring of \(\text{End}(J_0(\mathbb{N}))\) generated by the Hecke operators \(T_n\) for all \(n \geq 1\). Let \(T'\) be the saturation of \(T\) in \(\text{End}(J_0(\mathbb{N}))\), i.e., the set of elements of \(\text{End}(J_0(\mathbb{N})) \otimes \mathbb{Q}\) some positive multiple of which lie in \(T\). The quotient \(T'/T\) is a finitely generated abelian group because both \(T\) and \(\text{End}(J_0(\mathbb{N}))\) are finitely generated over \(\mathbb{Z}\). Since \(T'/T\) is also a torsion group, it is finite.

In Section 4.2.1, we will give some conditions under which \(T\) and \(T'\) agree locally at maximal ideal of \(T\). 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 \(T'/T\), and finally deduce that this ratio is one (for quotients associated to newforms) locally at a prime \(p\) such that \(p^2 \nmid N\).
4.2.1 Multiplicity One

In [Maz77], Mazur proves that if $N$ is prime, then $T = T'$; he combines this result with the equality

$$T \otimes \mathbb{Q} = \text{End}(J_0(p)) \otimes \mathbb{Q}$$

of [Rib75] or [Rib81], to deduce that $T = \text{End}(J_0(p))$ (when $N$ is prime). His method shows in the general case (when the level is not necessarily prime) that $T$ and $T'$ agree locally at a maximal ideal for which a certain space of differentials has dimension at most one. 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 $R = \mathbb{Z}[\frac{1}{m}]$. Let $X_0(N)_R$ denote the minimal regular model of $X_0(N)$ over $R$. Let $\Omega$ denote the sheaf of regular differentials on $X_0(N)_R$, as in [Maz78, §2(e)]. If $\ell$ is a prime such that $\ell^2 \nmid N$, then $X_0(N)_{F_\ell}$ denotes the special fiber of $X_0(N)_R$ at the prime $\ell$.

Lemma 4.6 (Mazur). Let $m$ be a maximal ideal of $T$ of residue characteristic $\ell$ such that $\ell^2 \nmid N$. Suppose that

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

Then $T$ and $T'$ agree locally at $m$.

**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 $\text{End}_{\mathbb{Q}} J_0(N)$ on $M$, and the action of $T$ on $M$ via the inclusion $T \subseteq \text{End}_{\mathbb{Q}} J_0(N)$ is faithful. Hence we have an injection $\phi: T \hookrightarrow \text{End}_T M$. Suppose $m$ is a maximal ideal of $T$ that satisfies the hypotheses of the lemma.

**Claim:** The map $\phi$ is surjective locally at $m$.

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

We shall use the subscript $(m)$ to denote localization at $m$. Thus $M_{(m)}$ is free of rank one over $T_{(m)}$. The composite $\psi: T'_{(m)} \rightarrow \text{End}_{T_{(m)}} (M_{(m)}) \phi^{-1} T_{(m)}$ gives a section of the inclusion $T_{(m)} \hookrightarrow T'_{(m)}$. Let $x \in T'_{(m)}$, and let $n$ be an integer such that $nx \in T_{(m)}$. Let $y = \psi(x) \in T_{(m)}$. Then $nx = \psi(\phi(nx)) = \psi(y) = n\psi(x) = ny$. Since $T_{(m)}$ is torsion-free, this means that $x = y \in T_{(m)}$. Thus $T_{(m)} = T'_{(m)}$, as was to be shown.

$\square$
If $m$ is a maximal ideal of the Hecke algebra $T$ of residue characteristic $\ell$, we say that $m$ satisfies *multiplicity one for differentials* if $\dim(H^0(X_0(N)_{\mathbb{F}_\ell}, \Omega)[m]) = 1$. Thus multiplicity one for $H^0(X_0(N)_{\mathbb{F}_\ell}, \Omega)[m]$ implies that $T$ and $T'$ agree at $m$.

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

**Lemma 4.7 (Mazur).** Let $m$ be a maximal ideal of $T$ of residue characteristic $\ell$ such that $\ell \nmid N$, then

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

*Proof.* This result is stated at the end of the proof of Prop. 9.4 on p. 95 of [Maz77]. The argument works even if $N$ is not prime (provided $\ell \nmid N$): the key point is to construct a $q$-expansion map on $H^0(X_0(N)_{\mathbb{F}_\ell}, \Omega)$ that is injective (see p. 71 of [Maz77]). Using this, the result above follows formally, e.g., as in the proof of Prop. 9.3 on p. 94-95 of [Maz77]. In the proof of Prop. 9.3, Mazur invokes tensor products and eigenvectors; the reader may find the following alternative approach easier to follow.

We have an $\mathbb{F}_\ell$-vector space that embeds in $\mathbb{F}_\ell[[q]]$, for example the space $V = H^0(X_0(N)_{\mathbb{F}_\ell}, \Omega)[m]$ of differentials that are killed by a maximal ideal $m$. This space is a $T/m$-vector space, and we want to see that its dimension over $T/m$ is at most 1. Note that $V$ embeds in $\text{Hom}_{\mathbb{F}_\ell}(T/m, \mathbb{F}_\ell)$ via the standard duality that sends $v \in V$ to the linear form whose value on a Hecke operator $T$ is the coefficient of $q$ in $v[T]$. The group $\text{Hom}_{\mathbb{F}_\ell}(T/m, \mathbb{F}_\ell)$ has the same size as $T/m$, which completes the argument because $\text{Hom}_{\mathbb{F}_\ell}(T/m, \mathbb{F}_\ell)$ has dimension 1 as a $T/m$-vector space. 

In the context of Mazur's paper, where the level $N$ is prime, we see from Lemma 4.7 that $T$ and $T'$ agree away from $N$. At $N$, we can still use the $q$-expansion principle because of the arguments in [Maz77, Ch.II §4]. Thus in the prime level case, $T = T'$, as we asserted above.

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

If $m$ is a maximal ideal of $T$ of residue characteristic $\ell$, then we say that $m$ is ordinary if $T_\ell \nsubseteq m$ (note that $T_\ell$ is often denoted $U_\ell$ if $\ell \nmid N$). For our purposes, the following lemma is convenient:

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

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

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 $X_0(M)$, 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 $m$ 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 $m$ 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 $m$ 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 $T = \mathbb{Z}[T_2] \subset \text{End}(J_0(22))$, where $T_2^2 - a_2 T_2 + 2 = 0$. Since $a_2 = -2$, we have $T \cong \mathbb{Z}[\sqrt{-1}]$. We can choose the square root of $-1$ to be $T_2 + 1$. Then $T_2$ is a generator of the unique maximal ideal $m$ of $T$ 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 $T$ and $T'$ agree locally at each maximal ideal $m$ that is either prime to $N$ or that satisfies the following supplemental hypothesis: the residue characteristic of $m$ divides $N$ only to the first power and $m$ is ordinary.

**Proof.** This follows easily from Lemmas 4.6, 4.7, and 4.8. \qed

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 $m$ dividing $N$ is ordinary, and we recover Mazur’s equality $T = T'$ in this special case.

### 4.2.2 Degrees and Congruences

Let $e \in T \otimes \mathbb{Q}$ be as in Section 4.1, and let $p, N, M$ be as on page 10 before the statement of Lemma 4.8. Let $A \subset J_0(pM)$ be the image of $e$ (note that we denoted this image by $A'$ in Section 4.1). For $t \in T$, let $t_A$ be the restriction of $t$ to $A$, and let $t_B$ be the image of $t$ in $\text{End}(B)$. Let $T_A$ be the subgroup of $\text{End}(A)$ consisting of the various $t_A$, and define $T_B$ similarly. As before, we obtain an injection $j : T \hookrightarrow T_A \times T_B$ with finite cokernel. Because $j$ is an injection, we refer to the maps $\pi_A : T \to T_A$ and $\pi_B : T \to T_B$, given by $t \mapsto t_A$ and $t \mapsto t_B$, respectively, as “projections”.

**Definition 4.10 (Congruence ideal).** The congruence ideal associated with the projector $e$ is $I = \pi_A(\text{ker}(\pi_B)) \subset T_A$. 
Viewing $T_A$ as $T_A \times \{0\}$, we may view $T_A$ as a subgroup of $T \otimes Q \cong (T_A \times T_B) \otimes Q$. Also, we may view $T$ as embedded in $T_A \times T_B$, via the map $j$.

**Lemma 4.11.** We have $I = T_A \cap T$.

A larger ideal of $T_A$ is $J = \text{Ann}_{T_A}(A \cap B)$; 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 $T_A$ of an operator that vanishes on $B$ also vanishes on $A \cap B$. \qed

**Lemma 4.13.** We have $J = T_A \cap \text{End}(J_0(pM)) = T_A \cap T'$.

**Proof.** This is elementary; it is an analogue of Lemma 4.11. \qed

**Proposition 4.14.** There is a natural inclusion $J/I \hookrightarrow T'/T$ of $T$-modules.

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

$$T \to T_A \times T_B \to T \otimes Q \subset \text{End}(J_0(pM)) \otimes Q.$$

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

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

\qed

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

Note that the Hecke algebra $T$ acts on $J/I$ through its quotient $T_A$, since the action of $T$ 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 $T_A$, which we denote $T_{p,A}$, is invertible modulo every maximal ideal of $T_A$ 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 $m \mid p$ is a maximal ideal of $T$ that arises by pullback from a maximal ideal of $T_A$, then $m$ 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
The Modular Degree and Congruences

is simple: regarding $I$ and $J$ as $T_A$-modules, we realize that we need to test that $I = J$ at maximal ideals of $T_A$ that divide $p$. These ideals correspond to maximal ideals $m \mid p$ of $T$ that are automatically ordinary, so we have $I = J$ locally at $m$ because of Proposition 4.9. By Proposition 4.9, we have $T = T'$ 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 $I \subset T_A$ 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 degree”. In this case, the inclusion $I \subset J$ corresponds to the divisibility $\tilde{n}_{A,\ell} \mid \tilde{r}_{A,\ell}$, 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 3.5.

Remark 4.16. The ring

$$R = \text{End}(J_0(pM)) \cap (T_A \times T_B)$$

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

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 [Wit95]). 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 $[T' : T]$ for various $N$. We can compute this index in Magma, e.g., the following commands compute the index for $N = 54$: $J := JZero(54)$; $T := HeckeAlgebra(J)$;
Table 2: The Index \([T': T]\)

<table>
<thead>
<tr>
<th>11</th>
<th>1</th>
<th>51</th>
<th>1</th>
<th>91</th>
<th>1</th>
<th>131</th>
<th>1</th>
<th>171</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>1</td>
<td>52</td>
<td>1</td>
<td>92</td>
<td>16</td>
<td>132</td>
<td>8</td>
<td>172</td>
<td>8</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>53</td>
<td>1</td>
<td>93</td>
<td>1</td>
<td>133</td>
<td>1</td>
<td>173</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>54</td>
<td>3</td>
<td>94</td>
<td>4</td>
<td>134</td>
<td>1</td>
<td>174</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>55</td>
<td>1</td>
<td>95</td>
<td>1</td>
<td>135</td>
<td>27</td>
<td>175</td>
<td>5</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>56</td>
<td>2</td>
<td>96</td>
<td>8</td>
<td>136</td>
<td>16</td>
<td>176</td>
<td>512</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>57</td>
<td>1</td>
<td>97</td>
<td>1</td>
<td>137</td>
<td>1</td>
<td>177</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>58</td>
<td>1</td>
<td>98</td>
<td>1</td>
<td>138</td>
<td>4</td>
<td>178</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>59</td>
<td>1</td>
<td>99</td>
<td>9</td>
<td>139</td>
<td>1</td>
<td>179</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>60</td>
<td>2</td>
<td>100</td>
<td>1</td>
<td>140</td>
<td>8</td>
<td>180</td>
<td>72</td>
</tr>
<tr>
<td>21</td>
<td>1</td>
<td>61</td>
<td>1</td>
<td>101</td>
<td>1</td>
<td>141</td>
<td>1</td>
<td>181</td>
<td>1</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
<td>62</td>
<td>2</td>
<td>102</td>
<td>1</td>
<td>142</td>
<td>8</td>
<td>182</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
<td>63</td>
<td>1</td>
<td>103</td>
<td>1</td>
<td>143</td>
<td>1</td>
<td>183</td>
<td>1</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
<td>64</td>
<td>2</td>
<td>104</td>
<td>4</td>
<td>144</td>
<td>32</td>
<td>184</td>
<td>1024</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>65</td>
<td>1</td>
<td>105</td>
<td>1</td>
<td>145</td>
<td>1</td>
<td>185</td>
<td>1</td>
</tr>
<tr>
<td>26</td>
<td>1</td>
<td>66</td>
<td>1</td>
<td>106</td>
<td>1</td>
<td>146</td>
<td>1</td>
<td>186</td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td>1</td>
<td>67</td>
<td>1</td>
<td>107</td>
<td>1</td>
<td>147</td>
<td>7</td>
<td>187</td>
<td>1</td>
</tr>
<tr>
<td>28</td>
<td>1</td>
<td>68</td>
<td>2</td>
<td>108</td>
<td>54</td>
<td>148</td>
<td>4</td>
<td>188</td>
<td>256</td>
</tr>
<tr>
<td>29</td>
<td>1</td>
<td>69</td>
<td>1</td>
<td>109</td>
<td>1</td>
<td>149</td>
<td>1</td>
<td>189</td>
<td>243</td>
</tr>
<tr>
<td>30</td>
<td>1</td>
<td>70</td>
<td>1</td>
<td>110</td>
<td>2</td>
<td>150</td>
<td>5</td>
<td>190</td>
<td>8</td>
</tr>
<tr>
<td>31</td>
<td>1</td>
<td>71</td>
<td>1</td>
<td>111</td>
<td>1</td>
<td>151</td>
<td>1</td>
<td>191</td>
<td>1</td>
</tr>
<tr>
<td>32</td>
<td>1</td>
<td>72</td>
<td>2</td>
<td>112</td>
<td>8</td>
<td>152</td>
<td>32</td>
<td>192</td>
<td>4096</td>
</tr>
<tr>
<td>33</td>
<td>1</td>
<td>73</td>
<td>1</td>
<td>113</td>
<td>1</td>
<td>153</td>
<td>9</td>
<td>193</td>
<td>1</td>
</tr>
<tr>
<td>34</td>
<td>1</td>
<td>74</td>
<td>1</td>
<td>114</td>
<td>1</td>
<td>154</td>
<td>1</td>
<td>194</td>
<td>1</td>
</tr>
<tr>
<td>35</td>
<td>1</td>
<td>75</td>
<td>1</td>
<td>115</td>
<td>1</td>
<td>155</td>
<td>1</td>
<td>195</td>
<td>1</td>
</tr>
<tr>
<td>36</td>
<td>1</td>
<td>76</td>
<td>2</td>
<td>116</td>
<td>4</td>
<td>156</td>
<td>32</td>
<td>196</td>
<td>14</td>
</tr>
<tr>
<td>37</td>
<td>1</td>
<td>77</td>
<td>1</td>
<td>117</td>
<td>1</td>
<td>157</td>
<td>1</td>
<td>197</td>
<td>1</td>
</tr>
<tr>
<td>38</td>
<td>1</td>
<td>78</td>
<td>2</td>
<td>118</td>
<td>2</td>
<td>158</td>
<td>4</td>
<td>198</td>
<td>81</td>
</tr>
<tr>
<td>39</td>
<td>1</td>
<td>79</td>
<td>1</td>
<td>119</td>
<td>1</td>
<td>159</td>
<td>1</td>
<td>199</td>
<td>1</td>
</tr>
<tr>
<td>40</td>
<td>1</td>
<td>80</td>
<td>4</td>
<td>120</td>
<td>32</td>
<td>160</td>
<td>256</td>
<td>200</td>
<td>80</td>
</tr>
<tr>
<td>41</td>
<td>1</td>
<td>81</td>
<td>1</td>
<td>121</td>
<td>1</td>
<td>161</td>
<td>1</td>
<td>201</td>
<td>1</td>
</tr>
<tr>
<td>42</td>
<td>1</td>
<td>82</td>
<td>1</td>
<td>122</td>
<td>1</td>
<td>162</td>
<td>81</td>
<td>202</td>
<td>1</td>
</tr>
<tr>
<td>43</td>
<td>1</td>
<td>83</td>
<td>1</td>
<td>123</td>
<td>1</td>
<td>163</td>
<td>1</td>
<td>203</td>
<td>1</td>
</tr>
<tr>
<td>44</td>
<td>2</td>
<td>84</td>
<td>2</td>
<td>124</td>
<td>16</td>
<td>164</td>
<td>8</td>
<td>204</td>
<td>32</td>
</tr>
<tr>
<td>45</td>
<td>1</td>
<td>85</td>
<td>1</td>
<td>125</td>
<td>25</td>
<td>165</td>
<td>1</td>
<td>205</td>
<td>1</td>
</tr>
<tr>
<td>46</td>
<td>2</td>
<td>86</td>
<td>1</td>
<td>126</td>
<td>18</td>
<td>166</td>
<td>2</td>
<td>206</td>
<td>4</td>
</tr>
<tr>
<td>47</td>
<td>1</td>
<td>87</td>
<td>1</td>
<td>127</td>
<td>1</td>
<td>167</td>
<td>1</td>
<td>207</td>
<td>81</td>
</tr>
<tr>
<td>48</td>
<td>1</td>
<td>88</td>
<td>8</td>
<td>128</td>
<td>64</td>
<td>168</td>
<td>128</td>
<td>208</td>
<td>256</td>
</tr>
<tr>
<td>49</td>
<td>1</td>
<td>89</td>
<td>1</td>
<td>129</td>
<td>1</td>
<td>169</td>
<td>13</td>
<td>209</td>
<td>1</td>
</tr>
<tr>
<td>50</td>
<td>1</td>
<td>90</td>
<td>1</td>
<td>130</td>
<td>1</td>
<td>170</td>
<td>1</td>
<td>210</td>
<td>2</td>
</tr>
</tbody>
</table>
Index (Saturation(T), T);” We obtain Table 2, where the first column contains N and the second column contains [T' : T]:

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

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

In Table 2, whenever $p \nmid [T' : T]$, then $p^2 \mid 2N$. This is consistent with Proposition 4.9, which moreover asserts that when $2^2 \nmid N$ and $2 \mid [T' : T]$ there is no non-ordinary (old) maximal ideal of characteristic 2 in the support of $T'/T$. The first case when $2 \mid |N$ and $2 \mid [T' : T]$ is $N = 46$, where we find (via a Magma calculation) that $G = T'/T \cong \mathbb{Z}/2\mathbb{Z}$, and the Hecke operator $T_2$ acts as 0 on $G$, so the annihilator of $G$ in $T$ is not ordinary, which does not contradict Proposition 4.9.

Moreover, notice that Theorem 3.5(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 if $p^2 \nmid N$. The conclusion of Theorem 3.5(b) does not hold for the counterexamples in Section 2 (e.g., for 54B1), which are all new elliptic curves, which shows that multiplicity one for differentials does not hold for certain maximal ideals that arise from the new quotient of the Hecke algebra.

5.2 Multiplicity One for Jacobians

We say that a maximal ideal $m$ of $T$ satisfies multiplicity one if $J_0(N)[m]$ is of dimension two over $T/m$. 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 $\mathbb{Q}$ of conductor $N$ and $p$ is a prime such that $p \mid r_E$ but $p \nmid m_E$. Let $m$ be the annihilator in $T$ of $E[p]$. Then multiplicity one fails for $m$, i.e., $\dim_{T/m} J_0(N)[m] > 2$.

Proof. View $E$ as an abelian subvariety of $J = J_0(N)$ and consider the complementary $T$-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 $E[m_E]$. Because $p \nmid m_E$, we have $E[p] \cap A = 0$. On the other hand, let $m$ be the annihilator of $E[p]$ inside $T$. Then $J[m]$ contains $E[p]$ and also $A[m]$, and because $p$ is a congruence prime, the submodule $A[m] \subset J[m]$ is nonzero. Thus the sum $E[p] + A[m]$ is a direct sum and is larger than $E[p]$, which is of dimension two over $T/m = \mathbb{Z}/p\mathbb{Z}$. Hence the dimension of $J[m]$ over $T/m$ is bigger than two, as claimed.

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

References


