The modular degree, congruence primes, and multiplicity one

Amod Agashe*, Kenneth A. Ribet, and William A. Stein

To Serge Lang,
our friend and teacher,
someone who always knew a fact from a hole in the ground

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. We find that the question has a negative answer, and show that in the counterexamples, multiplicity one (defined below) does not hold. At the same time, we prove a theorem about the relation between the two invariants: the modular degree divides the congruence number, 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.

*Agashe was partially supported by National Science Foundation Grant No. 0603668. Stein was partially supported by National Science Foundation Grant No. 0653968.

A. Agashe (✉)
Department of Mathematics, Florida State University, Tallahassee, Florida 32312, U.S.A.
e-mail: agashe@math.fsu.edu.

K.A. Ribet
Department of Mathematics, UC Berkeley Mail Code 3840, 970 Evans Hall Berkeley, CA 94720-3840
e-mail: ribet@math.berkeley.edu

W.A. Stein
University of Washington; Office: 423 Padelford Seattle, WA 98195-4350
e-mail: wstein@gmail.com

D. Goldfeld et al. (eds.), *Number Theory, Analysis and Geometry: In Memory of Serge Lang*, DOI 10.1007/978-1-4614-1260-1_2,

Key words elliptic curves • abelian varieties • modular degree • congruence primes • multiplicity one

Mathematics Subject Classification (2010): 11G05, 11610, 11G18, 11F33

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. We assume that the kernel of the map $J_0(N) \to E$ is connected, i.e., that E is an *optimal quotient* of $J_0(N)$ (this can always be done by replacing E by an isogenous curve if needed). 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 $[P] - [\infty] \in J_0(N)$.

Let $f_E = \sum a_n q^n \in S_2(\Gamma_0(N), \mathbf{C})$ 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 Petersson inner product, and congruent to f_E modulo r_E (i.e., $a_n \equiv b_n \pmod{r_E}$ for all 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 $r_E \neq m_E$, and show that in these examples, there is a maximal ideal $\mathfrak{m}$ of the Hecke algebra $\mathbf{T}$, such that $J_0(N)[\mathfrak{m}]$ has dimension more than two over $\mathbf{T}/\mathfrak{m}$ (this is the failure of multiplicity one alluded to above). We then conjecture that for any prime p, $\mathrm{ord}_p(r_E/m_E) \leq \frac{1}{2}\mathrm{ord}_p(N)$, and prove this conjecture when $\mathrm{ord}_p(N) \leq 1$.

In Section 3, we consider analogs of the modular degree and the congruence number for certain modular abelian varieties that are not necessarily elliptic curves; these include optimal quotients of $J_0(N)$ and $J_1(N)$ of any dimension associated to newforms. Section 3 may be read independently of Section 2. In Sections 4 and 5 we prove the main theorem of this paper (Theorem 3.6), and also give some examples of failure of what we call multiplicity one for differentials (see Definition 5.13).

Acknowledgments The authors are grateful to M. Baker, F. Calegari, B. Conrad, J. Cremona, G. Frey, H. W. Lenstra, Jr. and B. Noohi for discussions and advice regarding this paper. We would especially like to thank B. Conrad for the material in the appendix and for his suggestions concerning a number of technical facts that are inputs to our arguments. The first author is also grateful to the Max-Planck-Institut für Mathematik for its hospitality during a visit when he partly worked on this paper.

2 Elliptic curves

In Section 2.1, we discuss relationships between the modular degree and the congruence number of an elliptic curve. In Section 2.2 we recall the notion of multiplicity one and give new examples in which it fails.

2.1 Modular degree and congruence number

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 $\phi_E : X_0(N) \to E$. Recall that the *modular degree* m_E of E is the degree of ϕ_E.

Let $S_2(\mathbf{Z})$ denote the group of cuspforms of weight 2 on $\Gamma_0(N)$ with integral Fourier coefficients, and if G is a subgroup of $S_2(\mathbf{Z})$, let $G^\perp$ denote the subgroup of $S_2(\mathbf{Z})$ consisting of cuspforms that are orthogonal to f with respect to the Petersson inner product. The *congruence number* of E (really, that of f) is the positive integer r_E defined by either of the following equivalent conditions:

(i) r_E is the largest integer r such that there exists $g \in (\mathbf{Z}f)^\perp$ with $f \equiv g \bmod r$.
(ii) r_E is the order of the quotient group $\frac{S_2(\mathbf{Z})}{\mathbf{Z}f + (\mathbf{Z}f)^\perp}$.

We say that a prime is a *congruence prime for* E if it divides the congruence number r_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 may be of great interest.

Theorem 2.1. *Let E be an elliptic curve over $\mathbf{Q}$ of conductor N, with modular degree m_E and congruence number r_E. Then $m_E \mid r_E$ and if $\mathrm{ord}_p(N) \leq 1$, then $\mathrm{ord}_p(r_E) = \mathrm{ord}_p(m_E)$.*

Thus any prime that divides the modular degree of an elliptic curve E is a congruence prime for E, and if p is a congruence prime for E such that p^2 does not divide the conductor of E, then p divides the modular degree of E. The divisibility $m_E \mid r_E$ 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 that $m_E \mid r_E$, see [AU96, Lem 3.2] and [CK04]. We generalize this divisibility and prove it in Theorem 3.6(a). The second part of Theorem 2.1, i.e., that if $\mathrm{ord}_p(N) \leq 1$, then $\mathrm{ord}_p(r_E) = \mathrm{ord}_p(m_E)$, follows from the more general Theorem 3.6(b) below.

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			

Note that [AU96, Prop. 3.3–3.4] implies the weaker statement that if $p \nmid N$, then $\mathrm{ord}_p(r_E) = \mathrm{ord}_p(m_E)$, since [AU96, Prop. 3.3] implies

$$\mathrm{ord}_p(r_E) - \mathrm{ord}_p(m_E) = \mathrm{ord}_p(\#\mathcal{C}) - \mathrm{ord}_p(c_E) - \mathrm{ord}_p(\#\mathcal{D}),$$

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 (e.g., see [ARS06]), and $\mathcal{C}$ and $\mathcal{D}$ are certain groups.

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 $X_0(27)$ is $g = q - 2q^4 - q^7 + \cdots$, 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].

It is unclear whether there is a bound on the possible primes 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 2.2. *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 2.2 using Sage [S+09] for every optimal elliptic curve quotient of $J_0(N)$, with $N \leq 557$.

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

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

2.2 Multiplicity one and its failure

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 $\mathbf{T}/\mathfrak{m}$. The reason one calls this "multiplicitly one" is that if the canonical two-dimensional representation $\rho_{\mathfrak{m}}$ over $\mathbf{T}/\mathfrak{m}$ attached to $\mathfrak{m}$ (e.g., see [Rib90, Prop. 5.1]) is irreducible, then $J_0(N)[\mathfrak{m}]$ is a direct sum of copies of $\rho_{\mathfrak{m}}$ [Rib90, Thm. 5.2], and a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ satisfies *multiplicity one* precisely if the multiplicity of $\rho_{\mathfrak{m}}$ in this decomposition is one. Even if $\rho_{\mathfrak{m}}$ is reducible, the definition of multiplicity one given above is relevant (e.g., see [Maz77, Cor. 16.3]). The notion of multiplicity one, originally found in Mazur [Maz77], has played an important role in several places (e.g., in Wiles's proof of Fermat's last theorem: see Thm. 2.1 in [Wil95]).

In [MR91, §13], the authors find examples of failure of multiplicity one in which if p is the residue characteristic of $\mathfrak{m}$, then $p^3 \mid N$, and $\rho_{\mathfrak{m}}$ is modular of level N/p^2. Kilford [Kil02] found examples of failure of multiplicity one where N is prime and the residue characteristic of $\mathfrak{m}$ is 2. See also [Wie07] and [KW08] for examples of failure of multiplicity one in the $\Gamma_1(N)$ context. We now give examples of failure of multiplicity one where the square of the residue characteristic of $\mathfrak{m}$ divides the level (the residue characteristic is often odd).

Proposition 2.3. *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 $p \nmid m_E$. Then there is a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ with residue characteristic p such that $\dim_{\mathbf{T}/\mathfrak{m}} J_0(N)[\mathfrak{m}] > 2$, i.e., multiplicity one fails for $\mathfrak{m}$.*

The proposition follows from the more general Proposition 5.9 below. It follows from the proposition above that any example in Table 1 where simultaneously a prime divides r_E but does not divide m_E provides an example of failure of multiplicity one. In such examples, the associated representation $\rho_{\mathfrak{m}}$ may or may not be irreducible. For example, for the elliptic curve 54B1 and $p = 3$, we have $\mathrm{ord}_3(r_E) = 1$ but $\mathrm{ord}_3(m_E) = 0$, so there is a maximal ideal $\mathfrak{m}$ with residue characteristic 3 such that multiplicity one fails for $\mathfrak{m}$. The curve 54B1 has rational 3-torsion, so $\rho_{\mathfrak{m}}$ is reducible. On the other hand, for the elliptic curve 99A1, we have $\mathrm{ord}_3(r_E) = 1$ but $\mathrm{ord}_3(m_E) = 0$, so again there is a maximal ideal $\mathfrak{m}$ with residue characteristic 3 such that multiplicity one fails for $\mathfrak{m}$. Moreover, $J_0(99)$ is isogenous to a product of elliptic curves, none of which admit a rational 3-isogeny. Hence $\rho_{\mathfrak{m}}$ is irreducible.

The notion of multiplicity one at a maximal ideal $\mathfrak{m}$ is closely related to Gorensteinness of the completion of $\mathbf{T}$ at $\mathfrak{m}$ (e.g., see [Til97]). Kilford [Kil02] found examples of failure of Gorensteinness (and multiplicity one) at the prime 2 for certain prime levels. In the examples as above where multiplicity one fails for some maximal ideal, it would be interesting to do computations (e.g., as in [Kil02]) to see if the completion of the Hecke algebra at the maximal ideal is Gorenstein or not.

3 Modular abelian varieties of arbitrary dimension

For $N \geq 4$, let Γ be 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 A and B be abelian subvarieties of J such that $A + B = J$, $A \cap B$ is finite, and every endomorphism of J over $\mathbf{Q}$ preserves A and B. In this section, we generalize the notions of the congruence number and the modular degree to subvarieties A as above, and state a theorem relating the two numbers, which we prove in Sections 4 and 5.

We first give a general example of A and B as above. Up to isogeny, J is the product of factors $J_f^{e(f)}$ where f runs over the set of newforms of level dividing N, taken up to Galois conjugation, and $e(f)$ is the number of divisors of $N/N(f)$, where $N(f)$ is the level of f. Here J_f is the standard abelian subvariety of J attached to f by Shimura [Shi94, Thm. 7.14]. Let A' be the sum of $J_f^{e(f)}$ for some set of f's (taken up to Galois conjugation), and let B' be the sum of all the other $J_f^{e(f)}$'s. Clearly $A' + B' = J$. The J_f's are simple (over $\mathbf{Q}$), hence $A' \cap B'$ is finite. In view of the following lemma, A' and B' provide an example of A and B respectively as above. Note that by $\mathrm{End}(J)$ we mean the ring of endomorphisms of J defined over $\mathbf{Q}$.

Lemma 3.1. $\mathrm{End}(J)$ *preserves* A' *and* B'.

Proof. Suppose $\mathrm{End}(J)$ does not preserve A' (the case of B' is symmetric). Then since the J_f's are simple, that means that some abelian subvariety J_g of A' is isogenous to some abelian subvariety J_h of B', where $g \neq h$. Pick a prime ℓ. If f is a newform, then let ρ_f denote the canonical absolutely irreducible ℓ-adic representation attached to f. Now $\overline{\mathbf{Q}}_\ell \otimes V_\ell(J_f)^{\mathrm{ss}}$ is a direct sum of copies of $\rho_{\sigma(f)}$ as σ ranges over all embeddings into $\overline{\mathbf{Q}}$ of the field generated by the Fourier coefficients of f. Thus the above implies that there are distinct newforms g' and h' (of some level dividing N) such that $\rho_{g'} \cong \rho_{h'}$. Now each ρ_f satisfies $\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) = a_p(f)$ for all $p \nmid N\ell$. Thus for all $p \nmid N\ell$, we have $a_p(g') = a_p(h')$. By the multiplicity one theory (e.g., see [Li75, Cor. 3, pg. 300]), this means that $g' = h'$, a contradiction. □

We now give a more specific example, which will include the case of elliptic curves. Recall that $\mathbf{T}$ denotes the Hecke algebra. If $f = \sum a_n(f)q^n \in S_2(\Gamma)$ is a newform and $I_f = \ker(\mathbf{T} \to \mathbf{Z}[\ldots, a_n(f), \ldots])$, then $A_f = J/I_f J$ is the *newform quotient* associated to f. It is an abelian variety over $\mathbf{Q}$ of dimension equal to the degree of the field $\mathbf{Q}(\ldots, a_n(f), \ldots)$. Let ϕ_2 denote the quotient map $J \to A$. If C is an abelian variety, then we denote its dual abelian variety by $C^\vee$. There is a canonical principal polarization $\theta : J \cong J^\vee$. Dualizing ϕ_2, we obtain a closed immersion $\phi_2^\vee : A_f^\vee \to J^\vee$, which when composed with $\theta^{-1} : J^\vee \cong J$ gives us an injection $\phi_1 : A_f^\vee \hookrightarrow J$. One slight complication is that the isomorphism θ does not respect the action of $\mathbf{T}$, 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 the new quotient J^{new}, the action of the Hecke operators commutes with that of W_N, so since the quotient map $J \to A_f$ factors through J^{new}, the Hecke action on $A_f^\vee$ induced by the embedding $A_f^\vee \to J^\vee$ and the action on $A_f^\vee$ induced by the injection $\phi_1 : A_f^\vee \to J$ are the same. Hence $A_f^\vee$ is isomorphic to $\phi_1(A_f^\vee)$ as a $\mathbf{T}$-module, and $\phi_1(A_f^\vee) = J_f$ (this follows from the characterization of J_f in [Shi94, Thm. 7.14]). For simplicity, we will often denote $\phi_1(A_f^\vee) = J_f$ by just $A_f^\vee$. Let ϕ be the composite map $A_f^\vee \xrightarrow{\phi_1} J \xrightarrow{\phi_2} A_f$; then ϕ is a polarization (induced by dual of the polarization of J). Thus $A_f^\vee + I_f J = J$ and $A_f^\vee \cap I_f J$ is finite. Hence, in view of Lemma 3.1, $A_f^\vee$ and $I_f J$ provide an example of A and B as in the beginning of this section.

The *exponent* of a finite group G is the smallest positive integer n such that every element of G has order dividing n (i.e., such that for all $x \in G, nx = 0$).

Definition 3.2. *The* modular exponent $\tilde{n}_A$ *of* A *is the exponent of* $A \cap B$ *and the* modular number n_A *of* A *is its order.*

Note that the definition is symmetric with respect to A and B. In fact, the definition depends on both A and B, unlike what the notation may suggest—we have suppressed the dependence on B for ease of notation, with the understanding that there is a natural choice of B (e.g., this is the case in the examples we gave above). If f is a newform, then by the modular exponent/number of A_f, we mean that of $A = A_f^\vee$, with $B = I_f J$. In this situation, since ϕ is a polarization, n_{A_f} is a perfect square (e.g., see [AS05, Lemma 3.14]). When A_f is an elliptic curve, ϕ is multiplication by the modular degree m_E. Hence $A \cap B = \ker(\phi)$ is $(\mathbf{Z}/m_E\mathbf{Z})^2$, and so for elliptic curves, the modular exponent is equal to the modular degree and the modular number is the square of the modular degree.

If R is a subring of $\mathbf{C}$, let $S_2(R) = S_2(\Gamma; R)$ denote the subgroup of $S_2(\Gamma; \mathbf{C})$ consisting of cups forms whose Fourier expansions at the cusp ∞ have coefficients in R. 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]). 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 $\mathbf{Z}$, and hence so is $S_2(\mathbf{Z})$. Let $\mathbf{T}_A$ be the image of $\mathbf{T}$ in $\mathrm{End}(A)$, and let $\mathbf{T}_B$ be the image of $\mathbf{T}$ in $\mathrm{End}(B)$ (since $\mathbf{T} \subset \mathrm{End}(J)$, $\mathbf{T}$ preserves A and B). Since $A + B = J$, the natural map $\mathbf{T} \to \mathbf{T}_A \oplus \mathbf{T}_B$ is injective, and moreover, its cokernel is finite (since $A \cap B$ is finite).

Let $S_A = \mathrm{Hom}(\mathbf{T}_A, \mathbf{Z})$ and $S_B = \mathrm{Hom}(\mathbf{T}_B, \mathbf{Z})$ be subgroups of $S_2(\mathbf{Z})$ obtained via the pairing above. Let $\mathrm{Ext}^1 = \mathrm{Ext}^1_{\mathbf{Z}}$ denote the first Ext functor in the category of $\mathbf{Z}$-modules.

Lemma 3.3. *There is a canonical isomorphism of* $\mathbf{T}$*-modules*

$$\mathrm{Ext}^1((\mathbf{T}_A \oplus \mathbf{T}_B)/\mathbf{T}, \mathbf{Z}) \cong S_2(\mathbf{Z})/(S_A + S_B).$$

The groups $S_2(\mathbf{Z})/(S_A + S_B)$ *and* $(\mathbf{T}_A \oplus \mathbf{T}_B)/\mathbf{T}$ *are isomorphic.*

Proof. Apply the $\mathrm{Hom}(-, \mathbf{Z})$ functor to the short exact sequence

$$0 \to \mathbf{T} \to \mathbf{T}_A \oplus \mathbf{T}_B \to (\mathbf{T}_A \oplus \mathbf{T}_B)/\mathbf{T} \to 0$$

to obtain a three-term exact sequence

$$0 \to \mathrm{Hom}(\mathbf{T}_A \oplus \mathbf{T}_B, \mathbf{Z}) \to \mathrm{Hom}(\mathbf{T}, \mathbf{Z}) \to \mathrm{Ext}^1((\mathbf{T}_A \oplus \mathbf{T}_B)/\mathbf{T}, \mathbf{Z}) \to 0. \quad (1)$$

The perfect $\mathbf{T}$-equivariant bilinear pairing $\mathbf{T} \times S_2(\mathbf{Z}) \to \mathbf{Z}$ given by $(t, g) \mapsto a_1(t(g))$ transforms (1) into an exact sequence

$$0 \to S_A \oplus S_B \to S_2(\mathbf{Z}) \to \mathrm{Ext}^1((\mathbf{T}_A \oplus \mathbf{T}_B)/\mathbf{T}, \mathbf{Z}) \to 0$$

of $\mathbf{T}$-modules, which proves the first claim in the lemma. Finally note that if G is any finite abelian group, then $\mathrm{Ext}^1(G, \mathbf{Z}) \approx G$ as groups, which gives the second result of the lemma. □

Definition 3.4. *The exponent of either of the isomorphic groups* $S_2(\mathbf{Z})/(S_A + S_B)$ *and* $(\mathbf{T}_A \oplus \mathbf{T}_B)/\mathbf{T}$ *is the* congruence exponent $\tilde{r}_A$ *of* A *and the order of the groups is the* congruence number r_A.

Note that this definition is also symmetric with respect to A and B, and again, the definition depends on both A and B, unlike what the notation may suggest — we have suppressed the dependence on B with the implicit understanding that B has been chosen (given A). If f is a newform, then by the congruence exponent/number of A_f, we mean that of $A = A_f^\vee$, with $B = I_f J$. In this situation, $\mathbf{T}_A = \mathbf{T}/I_f$ and $S_A = S_2(\mathbf{Z})[I_f]$. Recall that a subgroup H of an abelian group G is said to be *saturated* (in G) if G/H is torsion-free. Now $\mathrm{Hom}(\mathbf{T}_B, \mathbf{Z})$ is the unique saturated Hecke-stable complement of $S_2(\mathbf{Z})[I_f]$ in $S_2(\mathbf{Z})$, hence must equal $S_2(\mathbf{Z})[I_f]^\perp$, where we recall that $S_2(\mathbf{Z})[I_f]^\perp$ denotes the orthogonal complement of $S_2(\mathbf{Z})[I_f]$ in $S_2(\mathbf{Z})$ with respect to the Petersson inner product. Thus the congruence exponent $\tilde{r}_{A_f}$ is the exponent of the group

$$\frac{S_2(\mathbf{Z})}{S_2(\mathbf{Z})[I_f] + S_2(\mathbf{Z})[I_f]^\perp}, \quad (2)$$

and the congruence number r_{A_f} is its order. In particular, our definition of r_{A_f} generalizes the definition in Section 2.1 when A_f is an elliptic curve.

Remark 3.5. If R is a subring of $\mathbf{C}$, then $S_2(\mathbf{Z}) \otimes_{\mathbf{Z}} R = S_2(R)$ (see, e.g., the discussion in [DI95, §12]). Thus the analog of the group displayed in (2) 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.

The following generalizes Theorem 2.1:

Theorem 3.6. *Let A and B be as in the first paragraph of Section 3. Then:*

(a) $\tilde{n}_A \mid \tilde{r}_A$.

(b) Let $\Gamma = \Gamma_0(N)$. *If* $p \nmid N$, *then* $\mathrm{ord}_p(\tilde{r}_A) = \mathrm{ord}_p(\tilde{n}_A)$. *If* $f \in S_2(\Gamma_0(N), \mathbf{C})$ *is a newform, then* $\mathrm{ord}_p(\tilde{r}_{A_f}) = \mathrm{ord}_p(\tilde{n}_{A_f})$ *whenever* $p^2 \nmid N$.

We give the proof of part (a) of this theorem in Section 4 and of part (b) in Section 5. The two sections may be read independently of each other.

Remark 3.7. Let $f \in S_2(\Gamma, \mathbf{C})$ be a newform. When A_f is an elliptic curve, Theorem 3.6 implies that the modular degree divides the congruence number (since for an elliptic curve, the modular degree and modular exponent are the same), and that $n_{A_f} \mid r_{A_f}^2$ (since for an elliptic curve, the modular number is the square of the modular exponent). In general, for a higher dimensional newform quotient, 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 Theorem 3.6(a)

Since $\mathrm{End}(J)$ preserves A and B, we have a map $\mathrm{End}(J) \to \mathrm{End}(A) \oplus \mathrm{End}(B)$; moreover, since $A + B = J$, this map is injective. We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{T} & \longrightarrow & \mathbf{T}_A \oplus \mathbf{T}_B & \longrightarrow & \dfrac{\mathbf{T}_A \oplus \mathbf{T}_B}{\mathbf{T}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \vdots & & \\ 0 & \longrightarrow & \mathrm{End}(J) & \longrightarrow & \mathrm{End}(A) \oplus \mathrm{End}(B) & \longrightarrow & \dfrac{\mathrm{End}(A) \oplus \mathrm{End}(B)}{\mathrm{End}(J)} & \longrightarrow & 0. \end{array} \tag{3}$$

The first two vertical maps are clearly injections, and the rightmost vertical map is defined naturally so that the diagram is commutative. Let

$$e = (1, 0) \in \mathbf{T}_A \oplus \mathbf{T}_B,$$

and let e_1 and e_2 denote the images of e in the groups $(\mathbf{T}_A \oplus \mathbf{T}_B)/\mathbf{T}$ and $(\mathrm{End}(A) \oplus \mathrm{End}(B))/\mathrm{End}(J)$, respectively. Since $A \cap B$ is finite (in addition to the fact that $A + B = J$), the two quotient groups on the right side of (3) are finite, so e_1 and e_2 have finite order.

Lemma 4.1. *The element* $e_2 \in (\mathrm{End}(A) \oplus \mathrm{End}(B))/\mathrm{End}(J)$ *defined above has order* $\tilde{n}_A$.

Proof. By the *denominator* of any $\varphi \in \mathrm{End}(J) \otimes \mathbf{Q}$, we mean the smallest positive integer n such that $n\varphi \in \mathrm{End}(J)$. Let $\pi_A, \pi_B \in \mathrm{End}(J) \otimes \mathbf{Q}$ be projection onto A and B, respectively. Let n be the order of e_2, so n is the denominator of π_A, which equals the denominator of π_B (since $\pi_A + \pi_B = 1_J$, so that $\pi_B = 1_J - \pi_A$). We want to show that n is equal to $\tilde{n}_A$, the exponent of $A \cap B$.

Let i_A and i_B be the embeddings of A and B into J, respectively. We view $n\pi_A$ and $n\pi_B$ as morphisms $J \to A$ and $J \to B$, respectively. Let $\varphi = (n\pi_A, n\pi_B) \in \mathrm{Hom}(J, A \times B)$; then $\varphi \circ (i_A + i_B) = [n]_{A\times B}$. We have an exact sequence

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

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

$$[n]\Delta = (\varphi \circ (i_A + i_B))(\Delta) = \varphi \circ ((i_A + i_B)(\Delta)) = \varphi(\{0\}) = \{0\},$$

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

To show the opposite divisibility, consider the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A \cap B & \xrightarrow{x\mapsto(x,-x)} & A \times B & \longrightarrow & J & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle [\tilde{n}_A]} & & \downarrow{\scriptstyle ([\tilde{n}_A],0)} & & \vdots{\scriptstyle \psi} & & \\
0 & \longrightarrow & A \cap B & \xrightarrow{x\mapsto(x,-x)} & A \times B & \longrightarrow & J & \longrightarrow & 0,
\end{array}$$

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

Lemma 4.2. *The element* $e_1 \in (\mathbf{T}_A \oplus \mathbf{T}_B)/\mathbf{T}$ *has order* $\tilde{r}_A$.

Proof. We want to show that the order r of e_1 equals the exponent of $M = (\mathbf{T}_A \oplus \mathbf{T}_B)/\mathbf{T}$. 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 $(a, b) \in \mathbf{T}_A \oplus \mathbf{T}_B$ 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., are in the image of $\mathbf{T}$ under the map $\mathbf{T} \to \mathbf{T}_A \oplus \mathbf{T}_B$), 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. □

Proof of Theorem 3.6(a). Since e_2 is the image of e_1 under the rightmost vertical homomorphism in (3), the order of e_2 divides that of e_1. Now apply Lemmas 4.1 and 4.2. □

5 Proof of Theorem 3.6(b)

Let $\mathbf{T}'$ be the saturation of $\mathbf{T} = \mathbf{Z}[\ldots, T_n, \ldots]$ in $\mathrm{End}(J)$, i.e.,

$$\mathbf{T}' = \mathrm{End}(J) \cap (\mathbf{T} \otimes \mathbf{Q}).$$

The quotient $\mathbf{T}'/\mathbf{T}$ is a finitely generated abelian group because both $\mathbf{T}$ and $\mathrm{End}(J)$ are finitely generated over $\mathbf{Z}$. Since $\mathbf{T}'/\mathbf{T}$ is also a torsion group, it is finite.

In Section 5.1, we introduce two ideals R and S of the Hecke algebra that are generalizations of the notions of the congruence exponent and the modular exponent respectively. We will see that $R \subset S$ and show that there is a natural injection $S/R \hookrightarrow \mathbf{T}'/\mathbf{T}$. In Section 5.2, we will prove that $\mathbf{T}$ and $\mathbf{T}'$ agree locally at a maximal ideal of $\mathbf{T}$ under the condition that we call "multiplicity one for differentials"; we also give examples where this condition does not hold. Theorem 3.6(b) itself is proved at the end of Section 5.1, by applying the results of Section 5.1 and a proposition that is proved in Section 5.2 to show that $R = S$ locally at a prime p such that $p \nmid N$ (when A is the dual of newform quotient, the condition that $p \nmid N$ can be replaced by $p^2 \nmid N$).

5.1 The congruence and intersection ideals

In this section, we work in slightly more generality, and take A and B to be as in the first paragraph of Section 3 (so Γ can be $\Gamma_1(N)$, and A need not be the dual of a newform quotient). Let $\pi_A : \mathbf{T} \to \mathbf{T}_A$ and $\pi_B : \mathbf{T} \to \mathbf{T}_B$ be the natural projection maps.

Definition 5.1. *With the setup as above, we define the* congruence ideal *as* $R = \pi_A(\ker(\pi_B)) \subset \mathbf{T}_A$, *and the* intersection ideal *as* $S = \mathrm{Ann}_{\mathbf{T}_A}(A \cap B)$.

Lemma 5.2. *We have* $R \subset S$.

Proof. By definition, R consists of restrictions to A of Hecke operators that vanish on B, while S consists of restrictions to A of Hecke operators that vanish on $A \cap B$. The lemma follows since the image in $\mathbf{T}_A$ of an operator that vanishes on B also vanishes on $A \cap B$. □

Remark 5.3. By Lemma 5.2, we have a surjection $\mathbf{T}_A/R \to \mathbf{T}_A/S$. Note that π_A induces an isomorphism

$$\frac{\mathbf{T}}{\ker(\pi_A) + \ker(\pi_B)} \xrightarrow{\simeq} \frac{\mathbf{T}_A}{R},$$

and we have an isomorphism

$$\frac{\mathbf{T}}{\ker(\pi_A) + \ker(\pi_B)} \xrightarrow{\simeq} \frac{\mathbf{T}_A \oplus \mathbf{T}_B}{\mathbf{T}}$$

obtained by sending $t \in \mathbf{T}$ to $(\pi_A(t), 0) \in \mathbf{T}_A \oplus \mathbf{T}_B$. Hence by Definition 3.4, the exponent of $\mathbf{T}_A/R$ is $\tilde{r}_A$ and its order is r_A. Also, $\tilde{n}_A$ is the exponent of $A \cap B$, and one expects that it is also the exponent of $\mathbf{T}_A/S$ (certainly multiplication by $\tilde{n}_A$ annihilates $\mathbf{T}_A/S$), which would give another proof that $\tilde{n}_A \mid \tilde{r}_A$. Instead of pursuing this question, we record the following result, which will be needed later.

Proposition 5.4. *If p is a prime such that the localizations of R and S at p coincide, then* $\mathrm{ord}_p(\tilde{r}_A) \leq \mathrm{ord}_p(\tilde{n}_A)$.

Proof. Under the hypothesis, the surjection $\mathbf{T}_A/R \to \mathbf{T}_A/S$ is an isomorphism locally at p. The lemma follows from the observations above that $\tilde{r}_A$ is the exponent of $\mathbf{T}_A/R$ and that $\tilde{n}_A$ annihilates $\mathbf{T}_A/S$. □

Lemma 5.5. *There is a natural inclusion $S/R \hookrightarrow \mathbf{T}'/\mathbf{T}$ of $\mathbf{T}$-modules.*

Proof. We have

$$\mathbf{T} \otimes \mathbf{Q} \cong (\mathbf{T}_A \otimes \mathbf{Q}) \oplus (\mathbf{T}_B \otimes \mathbf{Q}) \subset (\mathrm{End}(A) \otimes \mathbf{Q}) \oplus (\mathrm{End}(B) \otimes \mathbf{Q}) \cong \mathrm{End}(J) \otimes \mathbf{Q},$$

which we use to view $\mathbf{T}$ and $\mathbf{T}_A$ as sitting inside $\mathrm{End}(J) \otimes \mathbf{Q}$. Also, the groups $\mathrm{End}(J)$ and $\mathbf{T}'$ sit naturally in $\mathrm{End}(J) \otimes \mathbf{Q}$. By definition, $R = \mathbf{T}_A \cap \mathbf{T}$. Since an endomorphism of $A \times B$ factors through $A \times B \to J$ if and only if it kills $A \cap B$ embedded in $A \times B$ via $x \mapsto (x, -x)$, we have that $S = \mathbf{T}_A \cap \mathrm{End}(J)$ and this equals $\mathbf{T}_A \cap \mathbf{T}'$ (since a suitable multiple of any element of $\mathbf{T}_A$ lands in $\mathbf{T}$, when both are viewed as subgroups of $\mathbf{T} \otimes \mathbf{Q} \subset \mathrm{End}(J) \otimes \mathbf{Q}$). Hence we have $R = S \cap \mathbf{T}$ with intersection taken inside $\mathbf{T}' \subset \mathrm{End}(J) \otimes \mathbf{Q}$. Thus

$$S/R = S/(S \cap \mathbf{T}) \cong (S + \mathbf{T})/\mathbf{T} \hookrightarrow \mathbf{T}'/\mathbf{T}.$$ □

If $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$, then we say that two Hecke modules, with one contained in the other, *agree locally at* $\mathfrak{m}$ if their localizations at $\mathfrak{m}$ are the same. Let I_A denote the kernel of the map $\mathbf{T} \to \mathbf{T}_A$. As an immediate consequence of Lemma 5.5, we have:

Proposition 5.6. *If $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ containing I_A that is not in* $\mathrm{Supp}_{\mathbf{T}}(\mathbf{T}'/\mathbf{T})$*, then the corresponding maximal ideal $\mathfrak{m}/I_A$ of $\mathbf{T}_A$ is not in the support of S/R, i.e.: if $\mathbf{T}$ and $\mathbf{T}'$ agree locally at $\mathfrak{m}$, then R and S also agree locally at $\mathfrak{m}/I_A$.*

Remark 5.7. The ring

$$\mathbf{T}'' = \mathrm{End}(J) \cap (\mathbf{T}_A \times \mathbf{T}_B) = \mathbf{T}' \cap (\mathbf{T}_A \times \mathbf{T}_B)$$

is often of interest, where the intersection is taken in $\mathrm{End}(J) \otimes \mathbf{Q}$. We proved above that there is a natural inclusion $S/R \hookrightarrow \mathbf{T}'/\mathbf{T}$. This inclusion yields an isomorphism $S/R \xrightarrow{\sim} \mathbf{T}''/\mathbf{T}$, as is clear from the "if and only if" statement in the proof of Lemma 5.5. The ideals R and S are equal if the rings $\mathbf{T}$ and $\mathbf{T}''$ coincide. Even when $\mathbf{T}'$ is bigger than $\mathbf{T}$, its subring $\mathbf{T}''$ may be not far from $\mathbf{T}$.

The following lemma and proposition will not be used in the proof of Theorem 3.6(b), but they are of interest from the point of view of multiplicity one.

Lemma 5.8. *Let p be a prime and let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ with residue characteristic p. Suppose $\mathfrak{m}$ satisfies the multiplicity one condition (i.e., $J[\mathfrak{m}]$ is of dimension two over $\mathbf{T}/\mathfrak{m}$). Then the completions of $\mathbf{T}$ and $\mathbf{T}'$ at $\mathfrak{m}$ are isomorphic.*

Proof. As in [Maz77, p.92], consider the Tate module $\mathrm{Ta}_{\mathfrak{m}}(J)$, which is the Pontryagin dual of the $\mathfrak{m}$-divisible group associated to $J(\overline{\mathbf{Q}})$. Since $J[\mathfrak{m}]$ is of dimension two over $\mathbf{T}/\mathfrak{m}$, it follows that $\mathrm{Ta}_{\mathfrak{m}}(J)$ is free of rank 2 over $\mathbf{T}_{\mathfrak{m}}$, where the subscript denotes completion (see, e.g., [Til97, p. 332-333]). If r is an element of $\mathbf{T}'_{\mathfrak{m}}$, then r operates $\mathbf{T}_{\mathfrak{m}}$-linearly on $\mathrm{Ta}_{\mathfrak{m}}(J)$, and thus may be viewed as a 2×2 matrix with entries in $\mathbf{T}_{\mathfrak{m}}$. Further, some non-zero integer multiple of r operates on $\mathrm{Ta}_{\mathfrak{m}}(J)$ as an element of $\mathbf{T}_{\mathfrak{m}}$, i.e., as a scalar. Thus r must be a scalar to start with, i.e., actually lies in $\mathbf{T}_{\mathfrak{m}}$. Hence $\mathbf{T}'_{\mathfrak{m}} = \mathbf{T}_{\mathfrak{m}}$ as claimed. □

Proposition 5.9. *Let p be a prime such that all maximal ideals $\mathfrak{m}$ of $\mathbf{T}$ with residue characteristic p that contain I_A satisfy multiplicity one. Then $\mathrm{ord}_p(\tilde{r}_A) = \mathrm{ord}_p(\tilde{n}_A)$.*

Proof. This follows from Lemma 5.8, Lemma 5.5, Proposition 5.4, and Theorem 3.6(a). □

Proposition 5.10. *Let $\Gamma = \Gamma_0(N)$. Let p be a prime such that $p^2 \nmid N$, and let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ with residue characteristic p. If $p|N$, then assume that $I_f \subseteq \mathfrak{m}$ for some newform f. Then $\mathbf{T}$ and $\mathbf{T}'$ agree locally at $\mathfrak{m}$.*

Since the proof of this proposition is rather technical, we have postponed it to Section 5.2. Admitting this proposition, we may now finish the proof of Theorem 3.6(b).

Proof of Theorem 3.6(b). Recall that A and B are abelian subvarieties of $J = J_0(N)$ such that $A + B = J$, $A \cap B$ is finite, and every endomorphism of J over $\mathbf{Q}$ preserves A and B.

We first want to show that if a prime p does not divide N, then $\mathrm{ord}_p(\tilde{r}_A) = \mathrm{ord}_p(\tilde{n}_A)$. In view of Theorem 3.6(a) and Proposition 5.4, it suffices to check that R and S coincide locally at p. By Proposition 5.6, it suffices to check that $\mathbf{T}$ and $\mathbf{T}'$ are locally equal at all maximal ideals that divide p. If $p \nmid N$, then this follows from Proposition 5.10, which proves part of Theorem 3.6(b).

It remains to show that if $f \in S_2(\Gamma_0(N), \mathbf{C})$ is a newform and $p \parallel N$, then $\mathrm{ord}_p(\tilde{r}_{A_f}) = \mathrm{ord}_p(\tilde{n}_{A_f})$. Note that the Hecke algebra $\mathbf{T}$ acts on S/R through its quotient $\mathbf{T}_{A_f^\vee} = \mathbf{T}/\mathrm{Ann}_{\mathbf{T}} A_f^\vee$ since the action of $\mathbf{T}$ on R and on S factors through this quotient. Thus, in view of Theorem 3.6(a) and Proposition 5.4, it suffices to

check that R and S coincide locally at maximal ideals of $\mathbf{T}$ that divide p and contain $\mathrm{Ann}_{\mathbf{T}} A_f^\vee = I_f$ (the equality follows since I_f is saturated). But this follows from Proposition 5.6 and Proposition 5.10. □

5.2 *Multiplicity one for differentials*

This section is devoted to the proof of Proposition 5.10 as well as a discussion of the notion of multiplicity one for differentials (Definition 5.13). In this section, we take $\Gamma = \Gamma_0(N)$.

Let p be a prime such that $p^2 \nmid N$. Let $M_0(N)$ denote the compactified coarse moduli scheme associated to $\Gamma_0(N)$ (as in [DR73, § IV.3]) over $\mathbf{Z}_p$, and let $X_0(N)_{\mathbf{Z}_p}$ denote its minimal regular resolution obtained by suitable blow-up of the points $j = 0, 1728$ in characteristic dividing N, when they are supersingular (cf. [Maz77, p.63]). Let $\Omega_{X_0(N)/\mathbf{Z}_p}$ denote the relative dualizing sheaf of $X_0(N)_{\mathbf{Z}_p}$ over $\mathbf{Z}_p$ (it is the sheaf of regular differentials as in [MR91, §7]). We denote by $X_0(N)_{\mathbf{F}_p}$ the special fiber of $X_0(N)_{\mathbf{Z}_p}$ at the prime p and by $\Omega_{X_0(N)/\mathbf{F}_p}$ the relative dualizing sheaf of $X_0(N)_{\mathbf{F}_p}$ over $\mathbf{F}_p$.

The usual Hecke operators and the Atkin–Lehner involutions (corresponding to primes dividing N) of $J_0(N)$ over $\mathbf{Q}$ extend uniquely to act on the base change to $\mathbf{Z}_p$ of the Néron model of $J_0(N)$, which we denote by $J_{\mathbf{Z}_p}$. The natural morphism $\mathrm{Pic}^0_{X_0(N)/\mathbf{Z}_p} \to J_{\mathbf{Z}_p}$ identifies $\mathrm{Pic}^0_{X_0(N)/\mathbf{Z}_p}$ with the identity component of $J_{\mathbf{Z}_p}$ (see, e.g., [BLR90, §9.4–9.5]). Passing to tangent spaces along the identity section over $\mathbf{Z}_p$, we obtain an isomorphism $H^1(X_0(N)_{\mathbf{Z}_p}, \mathcal{O}_{X_0(N)_{\mathbf{Z}_p}}) \cong \mathrm{Tan}(J_{\mathbf{Z}_p})$. Using Grothendieck duality, one gets an isomorphism $\mathrm{Cot}(J_{\mathbf{Z}_p}) \cong H^0(X_0(N)_{\mathbf{Z}_p}, \Omega_{X_0(N)/\mathbf{Z}_p})$, where $\mathrm{Cot}(J_{\mathbf{Z}_p})$ is the cotangent space at the identity section (cf. [Maz78, p. 140]). Now the Hecke operators and the Atkin–Lehner involutions act on $\mathrm{Cot}(J_{\mathbf{Z}_p})$, and hence via the last isomorphism above, we get an action of the Hecke operators and the Atkin–Lehner involutions on $H^0(X_0(N)_{\mathbf{Z}_p}, \Omega_{X_0(N)/\mathbf{Z}_p})$. Following the proof of Prop. 3.3 on p. 68 of [Maz77], specialization induces an isomorphism

$$\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p}) \cong \mathrm{H}^0(X_0(N)_{\mathbf{Z}_p}, \Omega_{X_0(N)/\mathbf{Z}_p}) \otimes_{\mathbf{Z}_p} \mathbf{F}_p.$$

In this way, we get an action of the Hecke operators and the Atkin–Lehner involutions on $H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$ as well.

The following lemma is implicit in [Maz77, p. 95].

Lemma 5.11 (Mazur). *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ of residue characteristic p (recall that $p^2 \nmid N$). Suppose*

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

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

Proof. Let M denote the group $H^1(X_0(N)_{\mathbf{Z}_p}, \mathcal{O}_{X_0(N)})$, 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 $\mathbf{T} \subset \mathrm{End}_{\mathbf{Q}} J_0(N)$ 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. It suffices to show that M is generated by a single element over $\mathbf{T}$ locally at $\mathfrak{m}$, and in turn, by Nakayama's lemma, it suffices to check that the dimension of the $\mathbf{T}/\mathfrak{m}$-vector space $M/\mathfrak{m}M$ is at most one. Now $M/\mathfrak{m}M$ is dual to $H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$. Since we are assuming that $\dim_{\mathbf{T}/\mathfrak{m}} H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}] \leq 1$, we have $\dim_{\mathbf{T}/\mathfrak{m}}(M/\mathfrak{m}M) \leq 1$, which proves the claim.

Remark 5.12. Note that Lemma 5.8 may provide an alternate route to the conclusion of the previous lemma (sometimes one can prove multiplicity one for a maximal ideal without relying on multiplicity one for differentials, e.g., see [Dia97]). Observe that in the proofs of Lemmas 5.11 and 5.8, all we needed was (locally) a non-zero free $\mathbf{T}$-module (of finite rank, say) that is attached functorially to J. In Lemma 5.11, the module we used was $H^1(X_0(N)_{\mathbf{Z}_p}, \mathcal{O}_{X_0(N)})$; locally, it is free because its reduction modulo $\mathfrak{m}$ is of the same dimension as its generic rank (namely 1). In Lemma 5.8, we used the $\mathfrak{m}$-adic Tate module, whose reduction mod $\mathfrak{m}$ is of the same dimension as its generic rank (namely 2).

Definition 5.13. *If $\mathfrak{m}$ is a maximal ideal of the Hecke algebra $\mathbf{T}$ of residue characteristic p, we say that $\mathfrak{m}$ satisfies* multiplicity one for differentials *if*

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

The above condition, which first appeared in [Maz77], plays an important role in several places, including Wiles's proof of Fermat's last theorem (see [Wil95, Lemma 2.2]). It has been used to prove multiplicity one for $\mathfrak{m}$ (as in Section 2.2) and Gorensteinness of the completion of $\mathbf{T}$ at $\mathfrak{m}$ (under certain hypotheses; see, e.g., [Til97]).

5.2.1 Failure of multiplicity one for differentials

In this section, we digress to discuss examples of failure of multiplicity one for differentials. The reader interested in the proof of Proposition 5.10 may jump to Section 5.2.2 below.

By Lemma 5.11, if $p^2 \nmid N$ and if the multiplicity one condition for differentials holds at $\mathfrak{m}$, then $\mathbf{T}$ and $\mathbf{T}'$ agree locally at $\mathfrak{m}$. It is thus of interest to compute the quotient group $\mathbf{T}'/\mathbf{T}$ for various N. We compute this index in Sage [S+09]. and

Table 2 Nonzero Quotients $\mathbf{T}'/\mathbf{T}$ for $N \leq 325$

44	C_2	160	$C_2^3 \oplus C_4 \oplus C_8$	245	C_7^2
46	C_2	162	C_3^4	248	$C_2^7 \oplus C_4 \oplus C_8$
54	C_3	164	C_2^3	250	C_5^8
56	C_2	166	C_2	252	$C_2^2 \oplus C_6^3 \oplus C_{12}$
60	C_2	168	$C_2^5 \oplus C_4$	254	C_2^2
62	C_2	169	C_{13}	256	$C_2^3 \oplus C_4^2 \oplus C_8^2 \oplus C_{16}$
64	C_2	171	C_3^2	260	C_2^6
68	C_2	172	C_2^3	261	C_3^4
72	C_2	174	C_2	262	C_2^2
76	C_2	175	C_5	264	$C_2^7 \oplus C_4^3$
78	C_2	176	$C_2^2 \oplus C_4^2 \oplus C_8$	268	C_2^5
80	C_4	180	$C_2 \oplus C_6^2$	270	$C_3^9 \oplus C_6^2$
84	C_2	184	$C_2^5 \oplus C_4 \oplus C_8$	272	$C_2^3 \oplus C_4^4 \oplus C_8$
88	$C_2 \oplus C_4$	186	C_2^2	275	C_5^4
92	$C_2^2 \oplus C_4$	188	$C_2^4 \oplus C_4^2$	276	$C_2^7 \oplus C_4^2$
94	C_2^2	189	C_3^5	278	C_2
96	C_2^3	190	C_2^3	279	C_3^4
99	C_3^2	192	$C_2^3 \oplus C_4^3 \oplus C_8$	280	$C_2^7 \oplus C_4^3$
104	C_2^2	196	C_{14}	282	C_2^2
108	$C_3^2 \oplus C_6$	198	C_3^4	284	$C_2^6 \oplus C_4^3$
110	C_2	200	$C_2^3 \oplus C_{10}$	286	C_2^4
112	$C_2 \oplus C_4$	204	C_2^5	288	$C_2^7 \oplus C_4^3 \oplus C_{12} \oplus C_{24}$
116	C_2^2	206	C_2^2	289	C_{17}^2
118	C_2	207	C_3^4	290	C_2
120	$C_2^3 \oplus C_4$	208	$C_2^2 \oplus C_4^3$	292	C_2^5
124	$C_2^2 \oplus C_4$	210	C_2	294	C_7^4
125	C_5^2	212	C_2^4	296	$C_2^6 \oplus C_4^2$
126	$C_3 \oplus C_6$	214	C_2	297	$C_3^8 \oplus C_9$
128	$C_2 \oplus C_4 \oplus C_8$	216	$C_3 \oplus C_6^5 \oplus C_{12}$	300	$C_2^2 \oplus C_{10}^3$
132	C_2^3	220	$C_2^5 \oplus C_4$	302	C_2^3
135	C_3^3	224	$C_2^5 \oplus C_4^2 \oplus C_8$	304	$C_2^4 \oplus C_4^4 \oplus C_8$
136	$C_2^2 \oplus C_4$	225	C_5	306	C_3^6
140	C_2^3	228	C_2^5	308	C_2^7
142	C_2^3	230	C_2^2	310	C_2^3
144	$C_2^3 \oplus C_4$	232	$C_2^4 \oplus C_4^2$	312	$C_2^{11} \oplus C_4^2 \oplus C_8$
147	C_7	234	$C_3^2 \oplus C_6^2$	315	C_3^6
148	C_2^2	236	$C_2^5 \oplus C_4$	316	$C_2^6 \oplus C_4^2$
150	C_5	238	C_2^4	318	C_2^4
152	$C_2^3 \oplus C_4$	240	$C_2^7 \oplus C_4^3 \oplus C_8$	320	$C_2^6 \oplus C_4^3 \oplus C_8^3 \oplus C_{16}$
153	C_3	242	C_{11}^2	322	C_2^2
156	$C_2^3 \oplus C_4$	243	$C_3^4 \oplus C_9^2$	324	$C_3^7 \oplus C_6^3 \oplus C_{18}$
158	C_2^2	244	C_2^4	325	C_5^3

obtain Table 2, where the first column contains N for $N \leq 325$ and the second column contains the quotient group $\mathbf{T}'/\mathbf{T}$, where C_n denotes a cyclic group of order n.

In each case in which a prime p divides $[\mathbf{T}' : \mathbf{T}]$ but $p^2 \nmid N$, Lemma 5.11 implies that there is some maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ of residue characteristic p for which multiplicity one for differentials does not hold. For example, when $N = 46$, we find that $[\mathbf{T}' : \mathbf{T}] = 2$, and $2^2 \nmid N$; thus there is a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ of residue characteristic 2 for which multiplicity one for differentials does not hold.

In Table 2, we observe that whenever p divides $[\mathbf{T}' : \mathbf{T}]$, then $p = 2$ or $p^2 \mid N$. This raises the question: is it true that if p is odd and $p^2 \nmid N$, then multiplicity one for differentials holds for maximal ideals $\mathfrak{m}$ of $\mathbf{T}$ of residue characteristic p? Lemma 5.20 below gives an affirmative answer in one direction (the other direction is usually easy), but under the hypothesis that if $p \mid N$ then U_p acts as a non-zero scalar on $H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$.

5.2.2 Proof of Proposition 5.10

The main point is to prove that the hypothesis

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

of Lemma 5.11 holds for suitable maximal ideals $\mathfrak{m}$. This is achieved in Lemma 5.20 below, whose proof requires an Eichler–Shimura type relation for U_p (Lemma 5.15 below). We obtain this relation by modifying the argument in [Wil80, §5], which is in the $\Gamma_1(N)$ context, to the $\Gamma_0(N)$ situation. Let L denote the maximal unramified extension of $\mathbf{Q}_p$ and let $\mathcal{O}_L$ denote the ring of integers of L. For the sake of completeness, we state below a lemma that is well known (e.g., it is used implicitly in [Wil80, p. 18]); the proof was indicated to us by F. Calegari.

Lemma 5.14. *Let E be an elliptic curve over $\mathcal{O}_L$ with good ordinary reduction. Then the subgroup schemes of E of order p are p copies of $\mathbf{Z}/p\mathbf{Z}$ and one copy of $\boldsymbol{\mu}_p$.*

Proof. Let $G = E[p]$, and consider its connected-étale sequence

$$0 \to G^0 \to G \to G^{\mathrm{et}} \to 0.$$

Now G^0 is in the kernel of the reduction map, and we know that the reduction of $E[p]$ has non-trivial order. Hence G^{et} is non-trivial. By Cartier duality, G^0 is also non-trivial. Hence G^{et} is a $\mathbf{Z}/p\mathbf{Z}$ and by duality, G^0 is a $\boldsymbol{\mu}_p$. Thus one of the subgroup schemes of E of order p is a copy of $\boldsymbol{\mu}_p$. Let H be any other subgroup scheme of E of order p. Then H^0 has to be trivial, since otherwise $H = H^0$ is a non-trivial subgroup scheme of $G^0 = \boldsymbol{\mu}_p$, hence is equal to $G^0 = \boldsymbol{\mu}_p$, which has already been accounted for. Thus H is étale, and hence is a copy of $\mathbf{Z}/p\mathbf{Z}$. The lemma follows, since there are $p + 1$ subgroup schemes of order p in $E[p]$, hence in E. □

We assume that $p||N$ until just after the proof of Lemma 5.18. Let $M = N/p$. We will use the superscript h to denote the subscheme of $M_0(N)$ obtained by

removing the supersingular points in characteristic p. Following [DR73, VI.6.9] and [DR73, § V.2], the $\overline{\mathbf{F}}_p$-valued points of $M_0(N)^h$ are in one-to-one correspondence with isomorphism classes of triples consisting of

(a) a generalized elliptic curve E over $\overline{\mathbf{F}}_p$, whose smooth locus we denote E^{sm},
(b) a subgroup of $E^{\mathrm{sm}}[p]$ isomorphic to $\boldsymbol{\mu}_p$ or to $\mathbf{Z}/p\mathbf{Z}$, and
(c) a subgroup $\mathbf{Z}/M\mathbf{Z}$ of $E^{\mathrm{sm}}[M]$,

such that the subgroup generated by the subgroups in (b) and (c) above meets every irreducible component of every geometric fiber of E over $\overline{\mathbf{F}}_p$. Also, $M_0(N)_{\overline{\mathbf{F}}_p}$ has two irreducible components, which may be described according as whether the subgroup in (b) is isomorphic to $\boldsymbol{\mu}_p$ or to $\mathbf{Z}/p\mathbf{Z}$. As mentioned earlier, $X_0(N)_{\overline{\mathbf{F}}_p}$ is obtained from $M_0(N)_{\overline{\mathbf{F}}_p}$ by suitable blowups and consists of two copies of $X_0(M)_{\overline{\mathbf{F}}_p}$ identified at supersingular points, along with some copies of $\mathbf{P}^1$ (see the description of $X_0(N)_{\overline{\mathbf{F}}_p}$ on p. 175–177 of [Maz77] for details). One of the copies of $X_0(M)_{\overline{\mathbf{F}}_p}$ corresponds to the irreducible component of $M_0(N)_{\overline{\mathbf{F}}_p}$ where the subgroup in (b) is isomorphic to $\mathbf{Z}/p\mathbf{Z}$; we denote this copy by C_0. The other copy of $X_0(M)_{\overline{\mathbf{F}}_p}$ corresponds to the irreducible component of $M_0(N)_{\overline{\mathbf{F}}_p}$ where the subgroup in (b) is isomorphic to $\boldsymbol{\mu}_p$, and contains the cusp ∞; we denote this copy by C_1. We denote the copies (if any) of $\mathbf{P}^1$ by $C_2, \ldots, C_r$, where r is one less than the total number of irreducible components of $X_0(N)_{\overline{\mathbf{F}}_p}$.

The usual endomorphisms U_p and W_p of $J_0(N)$ over $\mathbf{Q}$ can be extended by base change to L, and extend uniquely to act on the Néron model of $J_0(N)$ over $\mathcal{O}_L$. Since the formation of Néron models is compatible with completions and unramified base change, this action is compatible with the already-defined action on the Néron model of $J_0(N)$ over $\mathbf{Z}_p$. The identity component of the special fiber of the Néron model of $J_0(N)$ over $\mathcal{O}_L$ is $\mathrm{Pic}^0_{X_0(N)/\overline{\mathbf{F}}_p}$, whose maximal abelian variety quotient is $\prod_{i=0}^r \mathrm{Pic}^0_{C_i/\overline{\mathbf{F}}_p}$ (cf. [DR73, I.3.7] and [BLR90, §9.2, Example 8]). Thus we get an action of U_p and W_p on $\mathrm{Pic}^0_{X_0(N)/\overline{\mathbf{F}}_p}$ and on $\prod_{i=0}^r \mathrm{Pic}^0_{C_i/\overline{\mathbf{F}}_p}$. Let Frob_p denote the Frobenius morphism on $C_{0/\overline{\mathbf{F}}_p}$.

Lemma 5.15. *The endomorphisms U_p and W_p of $\prod_{i=0}^r \mathrm{Pic}^0_{C_i/\overline{\mathbf{F}}_p}$ satisfy $U_p = \mathrm{Frob}_p + (p-1)W_p$ on $\mathrm{Pic}^0_{C_0/\overline{\mathbf{F}}_p}$.*

Proof. The proof is a modification of the proof of Theorem 5.3 in [Wil80], along with some details borrowed from the proof of Theorem 5.16 in B. Conrad's appendix to [RS01].

It suffices to check the desired identity on a Zariski dense subset of $\mathrm{Pic}^0_{C_0/\overline{\mathbf{F}}_p}(\overline{\mathbf{F}}_p) = J(C_0)(\overline{\mathbf{F}}_p)$, where $J(C_0)$ is the Jacobian of C_0. If g is the genus of C_0, then fixing a base point, we get a surjection $C_0^g \to J(C_0)$. Hence if U is any dense open subset of $C_0(\overline{\mathbf{F}}_p)$, then U^g hits a Zariski dense subset of $J(C_0)(\overline{\mathbf{F}}_p)$. Taking U to be the ordinary locus of $C_0(\overline{\mathbf{F}}_p)$, it thus suffices to prove the desired identity on divisors of the form $(Q)-(Q')$, where the elliptic curves corresponding to $Q, Q' \in C_0(\overline{\mathbf{F}}_p)$ are ordinary.

Let $\mathcal{M}_0(N)$ denote the algebraic stack over $\mathcal{O}_L$ associated to $\Gamma_0(N)$ by [DR73, IV.3.3, IV.4.2], whose associated coarse moduli scheme is $M_0(N)$ (over $\mathcal{O}_L$). Let $\pi : \mathcal{M}_0(N) \to M_0(N)$ denote the associated natural map. If $k = \overline{\mathbf{F}}_p$ or an algebraic closure of L, then π is an isomorphism on k-valued points, and so we will often identify points on $M_0(N)(k)$ with points on $\mathcal{M}_0(N)(k)$. Let Q be an ordinary point on $C_0(\overline{\mathbf{F}}_p)$. Then Q is given by a triple $(\overline{E}, \overline{C}, \overline{D})$, where $\overline{E}$ is an ordinary elliptic curve over $\overline{\mathbf{F}}_p$, $\overline{C}$ is a subgroup isomorphic to $\mathbf{Z}/p\mathbf{Z}$, and $\overline{D}$ is a subgroup isomorphic to $\mathbf{Z}/M\mathbf{Z}$. We can choose a Weierstrass model $E \hookrightarrow \mathbf{P}^2_{\mathcal{O}_L}$ lifting $\overline{E}$; then E is canonically an elliptic curve by [KM85, Chap. 2]. By Lemma 5.14 and its proof, there is a subgroup C of E isomorphic to $\mathbf{Z}/p\mathbf{Z}$ that lifts $\overline{C}$. Also, as argued in [RS01, p. 219], there is a subgroup D of E isomorphic to $\mathbf{Z}/M\mathbf{Z}$ that lifts $\overline{D}$. Then (E, C, D) gives a point on $\mathcal{M}_0(N)(\mathcal{O}_L)$ (cf. [DR73, V.1.6]), whose image in $M_0(N)(\mathcal{O}_L)$ corresponds to a point P in $X_0(N)(\mathcal{O}_L)$ (since E has ordinary reduction). We will use a bar to denote specialization. Thus we have $Q = \overline{P}$. Similarly, given another point $Q' \in C_0(\overline{\mathbf{F}}_p)$, we will denote the corresponding associated quantities by a prime superscript (thus P' in $X_0(N)(\mathcal{O}_L)$ denotes a lift of Q', etc.). As mentioned in the previous paragraph, it suffices to prove the relation claimed in the lemma for elements of the form $(Q) - (Q')$ in $\mathrm{Pic}^0_{C_0/\overline{\mathbf{F}}_p}(\overline{\mathbf{F}}_p)$. Viewing P and P' as relative effective Cartier divisors of degree one, we see that $U_p((Q) - (Q'))$ is the image of $U_p((P) - (P'))$ under specialization, i.e., $U_p((Q) - (Q')) = \overline{U_p((P) - (P'))}$.

We next compute $U_p((P) - (P'))$. Now $\mathrm{Pic}^0{}_{X_0(N)/\mathcal{O}_L}$ is the identity component of $J_0(N)_{\mathcal{O}_L}$, and we have $J_0(N)_{\mathcal{O}_L}(\mathcal{O}_L) = J_0(N)(L) \subseteq J_0(N)(\overline{L})$, where $\overline{L}$ is an algebraic closure of L. Denoting base change to $\overline{L}$ by a subscript $\overline{L}$, we have

$$\begin{aligned} U_p((E_{\overline{L}}, C_{\overline{L}}, D_{\overline{L}}) &- (E'_{\overline{L}}, C'_{\overline{L}}, D'_{\overline{L}})) \\ &= \sum_{A_{\overline{L}}} (E_{\overline{L}}/A_{\overline{L}}, (C_{\overline{L}} + A_{\overline{L}})/A_{\overline{L}}, (D_{\overline{L}} + A_{\overline{L}})/A_{\overline{L}}) \\ &- \sum_{A'_{\overline{L}}} (E'_{\overline{L}}/A'_{\overline{L}}, (C'_{\overline{L}} + A'_{\overline{L}})/A'_{\overline{L}}, (D'_{\overline{L}} + A'_{\overline{L}})/A'_{\overline{L}}), \end{aligned} \tag{4}$$

where $A_{\overline{L}}$ runs through the subgroups of $E_{\overline{L}}$ of order p except $C_{\overline{L}}$ (and similarly for $A'_{\overline{L}}$). Enlarging L by a finite extension if needed (which does not change the residue field $\overline{\mathbf{F}}_p$) we may assume that there are $p + 1$ subgroups of order p in E_L. Their scheme-theoretic closures in E over $\mathcal{O}_L$ are the subgroups schemes mentioned in Lemma 5.14. If A is a subgroup scheme of E of order p, then we denote the quotient map $E \to E/A$ by α_A. Consider the Cartier divisors corresponding to $U_p((P) - (P'))$ and to

$$\Big(\pi(E/\boldsymbol{\mu}_p, \alpha_{\boldsymbol{\mu}_p}(C), \alpha_{\boldsymbol{\mu}_p}(D)) + \sum_B \pi(E/B, \mathrm{cl}(\alpha_B(C)), \alpha_B(D))\Big)$$

$$-\Big(\pi(E'/\boldsymbol{\mu}'_p, \alpha_{\boldsymbol{\mu}'_p}(C'), \alpha_{\boldsymbol{\mu}'_p}(D')) + \sum_{B'} \pi(E'/B', \mathrm{cl}(\alpha_{B'}(C')), \alpha_{B'}(D'))\Big),$$

where B runs through the subgroups of E isomorphic to $\mathbf{Z}/p\mathbf{Z}$ except for C, and $\mathrm{cl}(\alpha_B(C))$ denotes the Zariski closure of $\alpha_B(C)$ in E/B (and similarly with prime superscripts). These two divisors coincide since they induce the same $\overline{L}$-point by (4).

Passing to special fibers, and noting that the special fiber of the Néron model of E/A is given by $\overline{E}/\overline{A}$, we find that

$$U_p((Q)-(Q')) = \overline{U_p((P)-(P'))}$$
$$= \left((\overline{E}/\overline{\boldsymbol{\mu}}_p, \overline{\alpha}_{\boldsymbol{\mu}_p}(\overline{C}), \overline{\alpha}_{\boldsymbol{\mu}_p}(\overline{D})) + \sum_B (\overline{E}/\overline{B}, \overline{\mathrm{cl}(\alpha_B(C))}, \overline{\alpha}_B(\overline{D}))\right) \quad (5)$$
$$-\left((\overline{E'}/\overline{\boldsymbol{\mu}'}_p, \overline{\alpha}_{\boldsymbol{\mu}'_p}(\overline{C'}), \overline{\alpha}_{\boldsymbol{\mu}'_p}(\overline{D'})) + \sum_{B'} (\overline{E'}/\overline{B'}, \overline{\mathrm{cl}(\alpha_{B'}(C'))}, \overline{\alpha}_{B'}(\overline{D'}))\right), \quad (6)$$

where B again runs through the subgroups of E isomorphic to $\mathbf{Z}/p\mathbf{Z}$ except for C (and a similar statment holds with prime superscripts).

Let F_p denote the relative Frobenius map $\overline{E} \to \overline{E}^{(p)}$ over $\overline{\mathbf{F}}_p$. Now $\boldsymbol{\mu}_p$ is in the kernel of F_p, and since the quotient map $\overline{\alpha}_{\boldsymbol{\mu}_p}$ has the same degree as F_p, there is an isomorphism $\phi : \overline{E}/\overline{\boldsymbol{\mu}}_p \xrightarrow{\cong} \overline{E}^{(p)}$ such that $F_p = \phi \circ \overline{\alpha}_{\boldsymbol{\mu}_p}$. Also ϕ induces an isomorphism $\overline{\alpha}_{\boldsymbol{\mu}_p}(\overline{C}) \xrightarrow{\cong} \overline{C}^{(p)}$ and $\overline{\alpha}_{\boldsymbol{\mu}_p}(\overline{D}) \xrightarrow{\cong} \overline{D}^{(p)}$. Thus the first term in (5) is identified with $(\overline{E}^{(p)}, \overline{C}^{(p)}, \overline{D}^{(p)})$, which is the image under Frob_p of $\overline{P} = (\overline{E}, \overline{C}, \overline{D})$. Similarly, the first term in (6) is $\mathrm{Frob}_p(\overline{P'})$.

As for the sum over B in (5), note that in each term, we are quotienting by a group B which is isomorphic to $\mathbf{Z}/p\mathbf{Z}$, and hence $\mathrm{cl}(\alpha_B(C))$ is of $\boldsymbol{\mu}_p$-type. In a manner similar to the computation of the action of U_p, we find that

$$W_p((\overline{E}, \overline{C}, \overline{D}) - (\overline{E'}, \overline{C'}, \overline{D'}))$$
$$= (\overline{E}/\overline{C}, \overline{E}[p]/\overline{C}, (\overline{D}+\overline{C})/\overline{C}) \quad (7)$$
$$- (\overline{E'}/\overline{C'}, \overline{E'}[p]/\overline{C'}, (\overline{D'}+\overline{C'})/\overline{C'}). \quad (8)$$

Considering that $\overline{P} = (\overline{E}, \overline{C}, \overline{D})$, with $\overline{C}$ isomorphic to $\mathbf{Z}/p\mathbf{Z}$, we see that $\overline{E}[p]/\overline{C}$ is isomorphic to $\boldsymbol{\mu}_p$. Also, if B is as in the sum in (5), then $\overline{B}$ is a $\mathbf{Z}/p\mathbf{Z}$, but there is only one copy of $\mathbf{Z}/p\mathbf{Z}$ in $\overline{E}$, since E has good ordinary reduction; hence $\overline{B} = \overline{C}$. Thus each of the terms in the sum over B in (5) is the term in (7). A similar statment holds with prime superscripts (viz., each of the terms in the sum over B' in (6) is the term in (8)).

The lemma now follows from the previous two paragraphs. □

Since we are assuming that $p||N$, the curve $X_0(N)_{\overline{\mathbf{F}}_p}$ has ordinary double point singularities, and so the differentials in $H^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$ may be identified with meromorphic differentials $(\omega_i)_{i=0,\ldots,r}$ on $\coprod_{i=0}^r C_i$ whose only possible poles are at points on $\coprod_{i=0}^r C_i$ lying over an intersection point of two components in $X_0(N)_{\overline{\mathbf{F}}_p}$ and where the sum of the residues at the points lying

over an intersection point is zero; such differentials are called *regular differentials* (see [Con00, §5.2] for the justification that the relative dualizing sheaf under Grothendieck duality is indeed the sheaf of regular differentials). By a *holomorphic differential* in $H^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$, we mean a regular differential all of whose corresponding ω_i have no poles at all (i.e., for all i, $\omega_i \in H^0(C_i, \Omega_{C_i/\overline{\mathbf{F}}_p})$). The subspace of holomorphic differentials may be identified with $\prod_{i=0}^r H^0(C_i, \Omega_{C_i/\overline{\mathbf{F}}_p})$ (which we will often do implicitly), and we let i_1 denote the corresponding injection $\prod_{i=0}^r H^0(C_i, \Omega_{C_i/\overline{\mathbf{F}}_p}) \hookrightarrow H^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$.

In a manner similar to the description in the third paragraph of Section 5.2, Grothendieck duality gives an isomorphism

$$\Theta : H^0(X_0(N)_{\mathcal{O}_L}, \Omega_{X_0(N)/\mathcal{O}_L}) \xrightarrow{\cong} \mathrm{Cot}(\mathrm{Pic}^0_{X_0(N)/\mathcal{O}_L}), \tag{9}$$

where Cot denotes the cotangent space at the identity section. Since we have an action of U_p and W_p on $\mathrm{Pic}^0_{X_0(N)/\mathcal{O}_L}$ (by viewing it as the identity component of the Néron model of $J_0(N)$ over $\mathcal{O}_L$), we may use Θ to get an action of these operators on $H^0(X_0(N)_{\mathcal{O}_L}, \Omega_{X_0(N)/\mathcal{O}_L})$. As before, Prop. 3.3 on p. 68 of [Maz77] implies that base change to $\overline{\mathbf{F}}_p$ gives an isomorphism

$$\mathrm{H}^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p}) \cong \mathrm{H}^0(X_0(N)_{\mathcal{O}_L}, \Omega_{X_0(N)/\mathcal{O}_L}) \otimes_{\mathcal{O}_L} \overline{\mathbf{F}}_p. \tag{10}$$

From this, we get an action of U_p and W_p on $H^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$.

Corollary 5.16. *The endomorphisms U_p and W_p of $\mathrm{H}^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$ preserve the subspace $\prod_{i=0}^r H^0(C_i, \Omega_{C_i/\overline{\mathbf{F}}_p})$, and satisfy $U_p = \pm \mathrm{Frob}_p^* + (p-1)W_p$ on $H^0(C_0, \Omega_{C_0/\overline{\mathbf{F}}_p})$, where Frob_p^* denotes pullback by Frob_p and where we have a possible sign ambiguity $\pm$ (which will not affect us later).*

Proof. The proof is based on the following diagram; we describe below some of the maps in it that have not been defined yet.

$$\begin{array}{ccc}
H^0(X_0(N)_{\mathcal{O}_L}, \Omega_{X_0(N)/\mathcal{O}_L}) & \xrightarrow{\Theta} & \mathrm{Cot}(\mathrm{Pic}^0_{X_0(N)/\mathcal{O}_L}) \\
\downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\
H^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p}) & \xrightarrow{\theta} & \mathrm{Cot}(\mathrm{Pic}^0_{X_0(N)/\overline{\mathbf{F}}_p}) \\
\uparrow{\scriptstyle i_1} & & \uparrow{\scriptstyle i_2} \\
\prod_{i=0}^r H^0(C_i, \Omega_{C_i/\overline{\mathbf{F}}_p}) & \xrightarrow{\theta'} & \prod_{i=0}^r \mathrm{Cot}(\mathrm{Pic}^0_{C_i/\overline{\mathbf{F}}_p}).
\end{array}$$

Firstly, Cot always denotes the cotangent space at the identity section. The map π_1 is obtained by base change to $\overline{\mathbf{F}}_p$. By (10), π_1 is surjective. The map π_2 is obtained by observing that $\mathrm{Pic}^0_{X_0(N)/\overline{\mathbf{F}}_p}$ is the identity component of the special fiber of the Néron model of $J_0(N)$ over $\mathcal{O}_L$, and hence maps to the identity component of the Néron model of $J_0(N)$ over $\mathcal{O}_L$, which is $\mathrm{Pic}^0{}_{X_0(N)/\mathcal{O}_L}$. The map θ is obtained using Grothendieck duality. The compatibility of Grothendieck duality under base change (see [Con00]) implies that the top square in the diagram above commutes.

Now we have already defined actions of U_p and W_p on $\mathrm{Pic}^0_{X_0(N)/\mathcal{O}_L}$ and on $\mathrm{Pic}^0_{X_0(N)/\overline{\mathbf{F}}_p}$ (just before Lemma 5.15). Thus we get actions of U_p and W_p on $\mathrm{Cot}(\mathrm{Pic}^0_{X_0(N)/\mathcal{O}_L})$ and on $\mathrm{Cot}(\mathrm{Pic}^0_{X_0(N)/\overline{\mathbf{F}}_p})$. From the definitions of these actions we see that π_2 is compatible with the actions on its domain and codomain. Recall that we used the isomorphism Θ to induce actions of U_p and W_p on $H^0(X_0(N)_{\mathcal{O}_L}, \Omega_{X_0(N)/\mathcal{O}_L})$ and then used formula (10) to get actions on $H^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$. Thus Θ and π_1 are also compatible with the actions of U_p and W_p on their domain and codomain. Let $\omega \in H^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$, and let $\Omega \in H^0(X_0(N)_{\mathcal{O}_L}, \Omega_{X_0(N)/\mathcal{O}_L})$ be such that $\pi_1(\Omega) = \omega$. Then $\theta(U_p(\omega)) = \theta(\pi_1(U_p(\Omega))) = \pi_2(\Theta(U_p(\Omega))) = \pi_2(U_p(\Theta(\Omega))) = U_p(\pi_2(\Theta(\Omega))) = U_p(\theta(\pi_2(\Omega))) = U_p(\theta(\omega))$. Thus we see that the isomorphism θ is compatible with the action of U_p (and similarly for W_p) on its domain and codomain.

Now we turn to the bottom square in the diagram above. As mentioned earlier, the injection i_2 arises because $\prod_{i=0}^r \mathrm{Pic}^0_{C_i/\overline{\mathbf{F}}_p}$ is the maximal abelian variety quotient of the identity component $\mathrm{Pic}^0_{X_0(N)/\overline{\mathbf{F}}_p}$ of the special fiber of the Néron model of $J_0(N)$ over $\mathcal{O}_L$. The map θ' is the isomorphism coming from Serre duality.

Next, by [Con00, §5.2], the Grothendieck duality isomorphism θ is the same as the isomorphism coming from the duality theory of Rosenlicht (as in [Ser88, Chap. IV]), perhaps up to multiplication by -1. Assume for the moment that there is no sign ambiguity, so that θ is indeed the isomorphism coming from the duality theory of Rosenlicht. One can check that the Serre duality isomorphism θ' is induced by the Rosenlicht duality isomorphism θ via the inclusions i_1 and i_2 by looking at the proof of the two dualities in [Ser88, Chaps. II and IV]. Note that in [Ser88], the curve X over the field k (notation as in loc. cit.) is assumed to be irreducible. This hypothesis is needed in loc. cit. (for our purposes) only to show that $H^1(X, k(X)) = 0$ (p. 12, loc. cit.); the latter condition holds so long as X is reduced (see top of p. 165 in [AK70], as well as the bottom of p. 138 and top of p. 132 therein), which is true in our case (taking $X = X_0(N)_{\overline{\mathbf{F}}_p}$ and $k = \overline{\mathbf{F}}_p$) . We remark that our contention that the Serre duality isomorphism θ' is induced by the Rosenlicht duality isomorphism θ via the inclusions i_1 and i_2 also follows from Section 6 (an appendix provided to us by Brian Conrad), by taking $C = X_0(N)_{\overline{\mathbf{F}}_p}$ and C' to be any of the C_i in Section 6. In any case, we conclude that the bottom square in the diagram above commutes as well, perhaps up to multiplication by -1.

Now the action of U_p and W_p on $\prod_{i=0}^r \mathrm{Pic}^0_{C_i/\overline{\mathbf{F}}_p}$ was defined by identifying it as the maximal abelian variety quotient of $\mathrm{Pic}^0_{X_0(N)/\overline{\mathbf{F}}_p}$. Thus we see that i_2 is

compatible with the action of U_p and W_p on its domain and codomain. Considering that moreover the isomorphism θ is compatible with the action of U_p (and W_p) and the bottom square in the diagram above commutes, perhaps up to multiplication by -1, we see that U_p and W_p preserve $\prod_{i=0}^{r} H^0(C_i, \Omega_{C_i/\overline{\mathbf{F}}_p})$. Now since θ is compatible with the action of U_p and W_p on its domain and codomain, so is θ'. Thus we may use the isomorphism θ' to translate the identity in Lemma 5.15 from the right to the left of θ' to get the desired identity in the corollary, where the $\pm$ ambiguity in front of $\mathrm{Frob}_p{}^*$ is really due to the sign ambiguity about the compatibility of the action of U_p and W_p on the two sides of the isomorphism θ'. □

Remark 5.17. We defined the action of the Hecke operators and the Atkin–Lehner involution in characteristic p from their definition in characteristic 0 in a somewhat indirect manner via the Néron mapping property, Grothendieck duality, etc (cf. beginning of Section 5.2). This has made our proofs rather complicated, since we have to show several compatibilities (as in the previous Corollary 5.16 and the upcoming Lemma 5.18). After this article was written, B. Conrad pointed out to us that one can define the action of the Hecke operators on suitable Artin stacks over $\mathbf{Z}$ for $\Gamma_0(N)$-structures (see [Con07]) in such a way that the definition agrees with the usual definition of the Hecke operators over $\mathbf{Q}$. This naturallly defines the action of the Hecke operators on objects related to $X_0(N)$ such as differentials, Picard groups, etc., in characteristic p and these definitions are automatically "compatible" with the corresponding definitions in characteristic zero. This alternative method would have been a less complicated way to proceed.

By [Maz77, Prop. II.3.3] we have an isomorphism

$$\mathrm{H}^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p}) \cong \mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p}) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p,$$

using which we may identify $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$ as a subspace of $\mathrm{H}^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$. Just before Corollary 5.16, we defined an action of U_p (and W_p) on $\mathrm{H}^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$.

Lemma 5.18. *The action of U_p (respectively W_p) on $\mathrm{H}^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$ preserves the subspace $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$, and agrees with the action of U_p (respectively W_p) on this subspace that we defined earlier in the third paragraph of Section 5.2.*

Proof. We have the following diagram, obtained by the obvious base changes:

$$\begin{array}{ccccc}
H^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p}) & \leftarrow & H^0(X_0(N)_{\mathcal{O}_L}, \Omega_{X_0(N)/\mathcal{O}_L}) & \xrightarrow{\Theta} & \mathrm{Cot}(\mathrm{Pic}^0_{X_0(N)/\mathcal{O}_L}), \\
\uparrow & & \uparrow & & \uparrow \\
H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p}) & \leftarrow & H^0(X_0(N)_{\mathbf{Z}_p}, \Omega_{X_0(N)/\mathbf{Z}_p}) & \xrightarrow{\Theta'} & \mathrm{Cot}(\mathrm{Pic}^0_{X_0(N)/\mathbf{Z}_p}),
\end{array}$$

where the map Θ' is the isomorphism coming from Grothendieck duality as discussed in the third paragraph of Section 5.2. Now the action of U_p and W_p on $\mathrm{Cot}(\mathrm{Pic}^0_{X_0(N)/\mathcal{O}_L}) = \mathrm{Cot}(J_0(N)_{\mathcal{O}_L})$ (where $J_0(N)_{\mathcal{O}_L}$ is the Néron model of $J_0(N)$ over $\mathcal{O}_L$) was obtained by base changing from $\mathbf{Z}_p$. Considering that the formation of Néron models is compatible with completions and unramified base change, we see that the rightmost vertical map above is compatible under the action of U_p and W_p. Also, the action of U_p and W_p on $H^0(X_0(N)_{\mathcal{O}_L}, \Omega_{X_0(N)/\mathcal{O}_L})$ (respectively on $H^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$) was obtained via the isomorphism Θ (respectively Θ'). Thus the rightmost two horizonal maps above are also compatible under the action of U_p and W_p on their domain and codomain. Finally, the compatibility of Grothendieck duality under base change (see [Con00]) implies that the right square in the diagram above commutes. Arguing as in the third paragraph of the proof of Corollary 5.16, one sees then that the middle vertical map above is compatible under the action of U_p and W_p.

Now the already-defined action of U_p and W_p on $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$ in the third paragraph of Section 5.2 is obtained via the lower leftward pointing arrow in the diagram above, and the action of U_p and W_p on $\mathrm{H}^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$ is obtained via the upper leftward pointing arrow in the diagram above. Thus the leftmost two horizontal arrows are compatible under the action of U_p and W_p on their domain and codomain. Repeated applications of [Maz77, Prop. II.3.3] show that the left square also commutes. Using all this, we see that the action of U_p (respectively W_p) on $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$ viewed as a subspace of $\mathrm{H}^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$ agrees with the action of U_p (respectively W_p) on $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$ defined in the third paragraph of Section 5.2, and in particular that U_p and W_p preserve this subspace. □

We now revert to the assumption that p is a prime such that $p^2 \nmid N$ (in particular p may not necessarily divide N). The Tate curve over $\mathbf{F}_p[[q]]$ gives rise to a morphism from $\mathrm{Spec}\ \mathbf{F}_p[[q]]$ to the smooth locus of $X_0(N)_{\mathbf{F}_p} \to \mathrm{Spec}\ \mathbf{F}_p$. Since the module of completed Kähler differentials for $\mathbf{F}_p[[q]]$ over $\mathbf{F}_p$ is free of rank 1 on the basis dq, we obtain a map

$$q\text{-exp} : H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p}) \to \mathbf{F}_p[[q]].$$

If $p \nmid N$, then by a *holomorphic differential* in $H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$, we mean any differential in $H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$.

Lemma 5.19. *Recall that p is a prime such that $p^2 \nmid N$, and $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ with residue characteristic p. If $p|N$, then assume that U_p acts as a non-zero scalar on $H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$. Then the map q-exp restricted to homomorphic differentials in $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$ is injective.*

Proof. The essential argument is quite standard, going back to Mazur, so we only sketch the ideas. For some of the details, we refer the reader to the proof

of Lemma 4.2 in [ARS06]. If $p \nmid N$, the injectivity follows from the q-expansion principle. So suppose that $p \parallel N$, and let $M = N/p$. Recall that $X_0(N)_{\overline{\mathbf{F}}_p}$ is obtained from $M_0(N)_{\overline{\mathbf{F}}_p}$ by suitable blowups at supersingular points and consists of two copies of $X_0(M)_{\overline{\mathbf{F}}_p}$ identified at supersingular points, along with some copies of $\mathbf{P}^1$. Suppose $\omega \in H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$ is a holomorphic differential that is in the kernel of q-exp. Then the q-expansion principle implies that ω vanishes on the copy of $X_0(M)_{\overline{\mathbf{F}}_p}$ containing the cusp ∞, i.e., on C_1. By Corollary 5.16 and Lemma 5.18, we have $U_p(\omega|_{C_0}) = \pm \mathrm{Frob}_p{}^*(\omega|_{C_0}) + (p-1)W_p(\omega|_{C_0})$. But pullback by Frob_p is the trivial map and W_p swaps C_0 and C_1, so $U_p(\omega|_{C_0}) = (p-1)(\omega|_{C_1}) = 0$. Now by hypothesis, U_p acts as multiplication by a non-zero scalar, hence ω is trivial on C_0. Thus ω is trivial on both copies of $X_0(M)_{\overline{\mathbf{F}}_p}$. One can show that then ω is trivial on the copies of $\mathbf{P}^1$ as well (see the proof of Lemma 4.2 in [ARS06]). Thus ω is trivial on $X_0(N)_{\overline{\mathbf{F}}_p}$, hence on $X_0(N)_{\mathbf{F}_p}$. □

Lemma 5.20. *We continue our hypotheses that p is a prime such that $p^2 \nmid N$, $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ with residue characteristic p, and if $p|N$, then U_p acts as a non-zero scalar on $H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$. Then*

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

Proof. The idea behind the proof is the same as in the proof of Lemma 2.2 in [Wil80, p. 485-487], which in turn builds on ideas from p. 94–95 of [Maz77]. However, parts of our arguments are somewhat different, and may be considered alternatives to some of the methods in the works cited in the previous sentence.

If $\omega \in \mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$ and $n \geq 1$, then let $a_n(\omega)$ denote the coefficient of q^n in q-exp(ω). We have a pairing $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p}) \times \mathbf{T} \to \mathbf{F}_p$ that takes (ω, T) to $a_1(T\omega)$. This induces a map

$$\psi : \mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}] \to \mathrm{Hom}_{\mathbf{F}_p}(\mathbf{T}/\mathfrak{m}, \mathbf{F}_p),$$

which is a homomorphism of $\mathbf{T}/\mathfrak{m}$-vector spaces.

Claim 1: If $\omega \in \ker(\psi)$, then q-exp(ω) is trivial.

Proof. Following the proof of Prop. 3.3 on p. 68 of [Maz77], we have

$$\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p}) \cong \mathrm{H}^0(X_0(N)_{\mathbf{Z}_p}, \Omega_{X_0(N)/\mathbf{Z}_p}) \otimes_{\mathbf{Z}_p} \mathbf{F}_p, \tag{11}$$

and

$$\mathrm{H}^0(X_0(N)(\mathbf{C}), \Omega_{X_0(N)(\mathbf{C})/\mathbf{C}}) \cong \mathrm{H}^0(X_0(N)_{\mathbf{Z}_p}, \Omega_{X_0(N)/\mathbf{Z}_p}) \otimes_{\mathbf{Z}_p} \mathbf{C}. \tag{12}$$

The definition of the action of the Hecke operators on $\mathrm{H}^0(X_0(N)_{\mathbf{Z}_p}, \Omega_{X_0(N)/\mathbf{Z}_p})$ defined in the third paragraph of Section 5.2 shows that this action is compatible

with the action of the Hecke operators on $\mathrm{H}^0(X_0(N)(\mathbf{C}), \Omega_{X_0(N)(\mathbf{C})/\mathbf{C}})$ under (12). Also, the action of the Hecke operators on $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$ was defined in the third paragraph of Section 5.2 via their action on $\mathrm{H}^0(X_0(N)_{\mathbf{Z}_p}, \Omega_{X_0(N)/\mathbf{Z}_p})$ using (11), so these actions are clearly compatible under (11). Now

$$\mathrm{H}^0(X_0(N)(\mathbf{C}), \Omega_{X_0(N)(\mathbf{C})/\mathbf{C}}) \cong \mathrm{H}^0(J_0(N)(\mathbf{C}), \Omega_{J_0(N)(\mathbf{C})/\mathbf{C}}) \cong S_2(\Gamma_0(N), \mathbf{C}),$$

and thus $a_1(T_n\omega) = a_n(\omega)$ for $\omega \in \mathrm{H}^0(X_0(N)(\mathbf{C}), \Omega_{X_0(N)(\mathbf{C})/\mathbf{C}})$. Hence, by (11), (12), and the discussion above, we also have the formula $a_1(T_n\omega) = a_n(\omega)$ for $\omega \in \mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})$.

Thus if $\omega \in \ker(\psi)$, then $a_n(\omega) = a_1(T_n\omega) = 0$ for all $n \geq 1$, i.e., q-exp(ω) is trivial, as was to be shown. □

Claim 2: The $\mathbf{T}/\mathfrak{m}$-dimension of the subspace of holomorphic differentials in $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$ is at most 1.

Proof. If ω is a holomorphic differential in $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$ and $\psi(\omega) = 0$, then by Claim 1, q-exp(ω) is trivial, and hence by Lemma 5.19, ω is trivial. This proves that ψ is injective when restricted to the subspace of holomorphic differentials. Now the group $\mathrm{Hom}_{\mathbf{F}_p}(\mathbf{T}/\mathfrak{m}, \mathbf{F}_p)$ has the same size as $\mathbf{T}/\mathfrak{m}$, which completes the argument because ψ embeds the subspace of holomorphic differentials in $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$ into $\mathrm{Hom}_{\mathbf{F}_p}(\mathbf{T}/\mathfrak{m}, \mathbf{F}_p)$, which has dimension 1 as a $\mathbf{T}/\mathfrak{m}$-vector space. □

Claim 2 proves the lemma in the case when $p \nmid N$. We now prove that $\dim_{\mathbf{T}/\mathfrak{m}} \mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}] \leq 1$ when $p||N$, which will finish the proof of the lemma. Following the proof of Lemma 2.2 in [Wil95], we break the argument into two cases:

Case I: There is no non-zero holomorphic differential in

$$\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}].$$

Suppose ω_1 and ω_2 are two differentials in $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$. Then we can find a pair $(\mu, \lambda) \in (\mathbf{T}/\mathfrak{m})^2$ with $(\mu, \lambda) \neq (0, 0)$ such that $\mu\psi(\omega_1) - \lambda\psi(\omega_2) = 0$, i.e., $\psi(\mu\omega_1 - \lambda\omega_2) = 0$. Hence by Claim 1, q-exp$(\mu\omega_1 - \lambda\omega_2) = 0$. Viewing $\mu\omega_1 - \lambda\omega_2$ as an element of $\mathrm{H}^0(X_0(N)_{\overline{\mathbf{F}}_p}, \Omega_{X_0(N)/\overline{\mathbf{F}}_p})$, we see that $\mu\omega_1 - \lambda\omega_2$ vanishes on C_1 (recall that C_1 is the copy of $X_0(N/p)_{\overline{\mathbf{F}}_p}$ that contains the cusp ∞) by the "q-expansion principle" (see the proof of Lemma 4.2 in [ARS06] for details). Now $C_2, \ldots, C_r$ (the copies of $\mathbf{P}^1$) arise as chains that link C_1 and C_0 (recall that C_0 is the copy of $X_0(N/p)_{\overline{\mathbf{F}}_p}$ that does not contain the cusp ∞) and each of $C_2, \ldots, C_r$ has at most two points of intersection, with all intersection points being ordinary double points (see the description of $X_0(N)_{\overline{\mathbf{F}}_p}$ on p. 175–177 of [Maz77] for details). Taking into consideration the definition of regular differentials and the residue theorem we see that $\mu\omega_1 - \lambda\omega_2$ is holomorphic

on the curves among $C_2, \ldots, C_r$ that intersect C_1 (for details, see the proof of Lemma 4.2 in [ARS06] in a similar situation). Now a curve among $C_2, \ldots, C_r$ that does *not* intersect C_1 intersects exactly one curve among $C_2, \ldots, C_r$ that *does* intersect C_1. Hence by repeating the argument above, $\mu\omega_1 - \lambda\omega_2$ is holomorphic on each curve in $C_2, \ldots, C_r$ that does *not* intersect C_1 as well. Thus $\mu\omega_1 - \lambda\omega_2$ is holomorphic on all of $X_0(N)_{\overline{\mathbf{F}}_p}$ except perhaps on C_0. But the only possible poles of $\mu\omega_1 - \lambda\omega_2$ on C_0 are over points of intersection with other components, and again, considering the definition of regular differentials, we see that there are no such poles, i.e., $\mu\omega_1 - \lambda\omega_2$ is holomorphic on C_0 as well. Thus $\mu\omega_1 - \lambda\omega_2$ is holomorphic everywhere and is an element of $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$. Hence it is trivial by the hypothesis of this case. Thus ω_1 and ω_2 are linearly dependent. Since ω_1 and ω_2 were arbitrary, this shows that $\dim_{\mathbf{T}/\mathfrak{m}} \mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}] \leq 1$ in this case.

Case II: There is a non-zero holomorphic differential

$$\omega \in \mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}].$$

By Lemma 5.19, q-exp(ω) is non-trivial, and so by Claim 1, $\psi(\omega) \neq 0$. Let $\omega' \in \mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$. Then there is a $\lambda \in \mathbf{T}/\mathfrak{m}$ such that $\psi(\omega') - \lambda\psi(\omega) = 0$, i.e., $\psi(\omega' - \lambda\omega) = 0$. As in the proof of Case I, we conclude that $\omega' - \lambda\omega$ is holomorphic; in particular ω' is holomorphic. Thus every differential in $\mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$ is holomorphic. Then by Claim 2, $\dim_{\mathbf{T}/\mathfrak{m}} \mathrm{H}^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}] \leq 1$ in this case as well. □

(Proof of Proposition 5.10). Recall that the hypotheses of Proposition 5.10 are that p is a prime such that $p^2 \nmid N$, $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ with residue characteristic p such that if $p|N$, then $I_f \subseteq \mathfrak{m}$ for some newform f. We wish to show that then $\mathbf{T}$ and $\mathbf{T}'$ agree locally at $\mathfrak{m}$.

If $p \nmid N$, then the result follows from Lemmas 5.11 and 5.20. If f is a newform and $p|N$, then U_p acts as ± 1 on f, and hence $U_p \pm 1 \in I_f$. Thus if $p|N$ and $I_f \subseteq \mathfrak{m}$ for some newform f, then U_p acts as a non-zero scalar (± 1) on $H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p})[\mathfrak{m}]$ (note that the action of U_p on regular differentials was defined compatibly with the usual action of U_p on complex differentials, i.e., on cuspforms; cf. the proof of Claim 1 in the proof of Lemma 5.20). The proposition follows again from Lemmas 5.11 and 5.20. □

6 Duality theory: an appendix by Brian Conrad

Let k be a field and let C be a proper reduced k-scheme with pure dimension 1. Assume that C is generically smooth, and let $C' \subseteq C$ be a non-empty reduced closed subscheme with pure dimension 1 (so C' is also generically smooth). The case of most interest to us is when C is a geometrically connected and semistable

curve and C' is a smooth geometrically irreducible component. The inclusion $C' \to C$ induces a natural map of k-groups $\mathrm{Pic}_{C/k} \to \mathrm{Pic}_{C'/k}$, and on tangent spaces at the identity this is the canonical pullback map

$$\theta : \mathrm{H}^1(C, \mathcal{O}_C) \to \mathrm{H}^1(C', \mathcal{O}_{C'})$$

(as we see by computing with dual numbers over k). Each of C and C' satisfies Serre's condition (S_1) by reducedness, so each is Cohen–Macaulay. Thus, by Serre duality we can identify the map of cotangent spaces with the map $\mathrm{H}^0(C', \omega_{C'/k}) \to \mathrm{H}^0(C, \omega_{C/k})$ dual to θ. We wish to give a concrete description of this latter map. To do this, we first review some basic definitions and identifications in duality theory.

In what follows we use Grothendieck's approach to duality theory, which has the merit of permitting more localization operations than in Serre's approach. Since C and C' are Cohen–Macaulay with pure dimension 1, their relative dualizing complexes over k are naturally identified with $\omega_{C/k}[1]$ and $\omega_{C'/k}[1]$ respectively [Con00, 3.5.1]. Since (by construction) the formation of the relative dualizing complex is compatible with Zariski-localization on the source, we have canonical isomorphisms $\omega_{C'/k}|_{C'^{\mathrm{sm}}} \simeq \Omega^1_{C'^{\mathrm{sm}}/k}$ and $\omega_{C/k}|_{C^{\mathrm{sm}}} \simeq \Omega^1_{C^{\mathrm{sm}}/k}$ that coincide on the open locus $U = C^{\mathrm{sm}} \cap C'$ that is dense in C' (and supported in C'^{sm}). If we let $j : C^{\mathrm{sm}} \to C$ and $j' : C'^{\mathrm{sm}} \to C'$ denote the canonical dense open immersions then, by [Con00, 5.2.1] the natural maps

$$\omega_{C'/k} \to j'_*(\Omega^1_{C'^{\mathrm{sm}}/k}), \quad \omega_{C/k} \to j_*(\Omega^1_{C^{\mathrm{sm}}/k})$$

are injective. By construction this is compatible with the natural isomorphism $\omega_{C/k}|_U \simeq \omega_{C'/k}|_U$. Letting $\eta : \mathrm{Spec}(K) \to C$ and $\eta' : \mathrm{Spec}(K') \to C'$ denote the canonical maps from the schemes of generic points, $\omega_{C'/k}$ maps isomorphically onto a coherent subsheaf of $\eta'_*(\Omega^1_{K'/k})$ and likewise for $\omega_{C/k}$ in $\eta_*(\Omega^1_{K/k})$; these image subsheaves are the so-called sheaves of *regular differentials*, and a classical result of Rosenlicht describes these images explicitly using residues when k is algebraically closed [Con00, 5.2.3]. We will not require Rosenlicht's result for the statement or proof of the theorem below.

Using Grothendieck's theory of relative trace maps, the canonical closed immersion $\iota : C' \to C$ over k induces a trace morphism $\mathrm{Tr}_\iota : \iota_*(\omega_{C'/k}) \to \omega_{C/k}$ whose formation commutes with Zariski-localization on C, so over the dense open $U = \iota^{-1}(C^{\mathrm{sm}}) \subseteq C'$ it induces the natural isomorphism $\omega_{C'/k}|_U \simeq \omega_{C/k}|_U$, or equivalently it is the identity map on $\Omega^1_{U/k}$. Hence, Tr_ι is compatible with the canonical inclusions $\omega_{C'/k} \hookrightarrow \eta'_*(\Omega^1_{K'/k})$ and $\omega_{C/k} \hookrightarrow \eta_*(\Omega^1_{K/k})$. In particular, the map Tr_ι is compatible with the natural identification of meromorphic 1-forms on C' with meromorphic 1-forms on C (i.e., compatible with the injection $\Omega^1_{K'/k} \hookrightarrow \Omega^1_{K/k}$).

Having summarized some inputs from duality theory, we can now state the result we want to prove.

Theorem 6.1. *The pullback* $\mathrm{H}^1(C, \mathcal{O}_C) \to \mathrm{H}^1(C', \mathcal{O}_{C'})$ *is dual to the natural map*

$$\mathrm{H}^0(C', \omega_{C'/k}) = \mathrm{H}^0(C, \iota_*(\omega_{C'/k})) \to \mathrm{H}^0(C, \omega_{C/k}).$$

Proof. Let $\mathrm{Tr}_C : \mathrm{H}^1(C, \omega_{C/k}) \to k$ and $\mathrm{Tr}_{C'} : \mathrm{H}^1(C', \omega_{C'/k}) \to k$ be the canonical trace maps, so our problem is to prove that for $s \in \mathrm{H}^1(C, \mathcal{O}_C)$ and $\xi' \in \mathrm{H}^0(C', \omega_{C'/k}) \subseteq \Omega^1_{K'/k}$,

$$\mathrm{Tr}_{C'}(\xi' \cup s|_{C'}) = \mathrm{Tr}_C(\mathrm{Tr}_\iota(\xi') \cup s)$$

in k. By the functoriality of Grothendieck's trace map, $\mathrm{Tr}_{C'} = \mathrm{Tr}_C \circ \mathrm{H}^1(\mathrm{Tr}_\iota)$ as maps $\mathrm{H}^1(C', \omega_{C'/k}) \to k$. Thus, it suffices to show that the map $\mathrm{H}^1(C', \omega_{C'/k}) \to \mathrm{H}^1(C, \omega_{C/k})$ induced by Tr_ι carries $\xi' \cup s|_{C'}$ to $\mathrm{Tr}_\iota(\xi') \cup s$. We may view dualizing sheaves as subsheaves $\omega_{C/k} \subseteq \eta_*(\Omega^1_{K/k})$ and $\omega_{C'/k} \subseteq \eta'_*(\Omega^1_{K'/k})$ in terms of which we have seen that the abstract trace map Tr_ι is induced by the natural inclusion $\Omega^1_{K'/k} \subseteq \Omega^1_{K/k}$.

To do the computation we work with Čech theory. Let $\{U_n\}$ be an ordered finite open affine cover of C and let $U'_n = U_n \cap C'$, so $\{U'_n\}$ is an open affine cover of C'. The cohomology class s corresponds to a Čech 1-cocycle $\{s_{n,m}\}_{n<m}$ with $s_{n,m} \in \mathcal{O}_C(U_n \cap U_m)$, so s' corresponds to $\{s'_{n,m}\}$ with $s'_{n,m} = s_{n,m}|_{U'_n \cap U'_m}$. Identifying ξ' with an element of $\Omega^1_{K'/k}$, $\xi' \cup s|_{C'} \in \mathrm{H}^1(C', \omega_{C'/k})$ corresponds to $\{s'_{n,m}\xi'\}_{n<m}$ and $\mathrm{Tr}_\iota(\xi') \cup s \in \mathrm{H}^1(C, \omega_{C/k})$ corresponds to $\{s_{n,m}\xi'\}_{n<m}$, where ξ' is viewed in $\Omega^1_{K/k}$ in the natural way. The product $s_{n,m}\xi'$ at the generic points of $U_n \cap U_m$ vanishes at generic points not in C', so the required equality is clear even at the level of Čech 1-cocycles. □

References

[AK70] A. Altman and Steven Kleiman, *Introduction to Grothendieck duality theory*, Lecture Notes in Mathematics, Vol. 146, Springer-Verlag, Berlin, 1970.

[ARS06] A. Agashe, K. Ribet and W. Stein, *The Manin Constant*, Pure and Applied Mathematics Quarterly, Special issue: In honor of John H. Coates (2006), to appear.

[AS05] A. Agashe and W. A. Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484, with an appendix by J. Cremona and B. Mazur.

[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* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[Con00] B. Conrad, *Grothendieck duality and base change*, Lecture Notes in Mathematics, Vol. 1750, Springer-Verlag, Berlin, 2000.

[Con07] B. Conrad, *Arithmetic moduli of generalized elliptic curves*, J. Inst. Math. Jussieu **6** (2007), no. 2, 209–278.

[CK04] A. C. Cojocaru and E. 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, available at `http://www.maths.nott.ac.uk/personal/jec/book/`.

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

[Dia97] F. Diamond, *The Taylor-Wiles construction and multiplicity one*, Invent. Math. **128** (1997), no. 2, 379–391.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972) (Berlin), Springer, 1973, Lecture Notes in Math., Vol. 349 pp. 143–316.

[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.

[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.

[KM85] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Princeton University Press, Princeton, N.J., 1985.

[KW08] L. J. P. Kilford and Gabor Wiese, *On the failure of the Gorenstein property for Hecke algebras of prime weight*, Experiment. Math. **17** (2008), no. 1, 37–52. MR MR2410114 (2009c:11075).

[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).

[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.

[Rib90] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[RS01] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., Vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 143–232.

[Ser88] J-P. Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, Vol. 117, Springer-Verlag, New York, 1988, Translated from the French.

[Shi94] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

[S+09] W. A. Stein et al., *Sage Mathematics Software (Version 4.2)*, The Sage Development Team, 2009, `http://www.sagemath.org`.

[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.

[Wie07] G. Wiese, *Multiplicities of Galois representations of weight one*, Algebra Number Theory **1** (2007), no. 1, 67–85, With an appendix by Niko Naumann.

[Wil80] A. Wiles, *Modular curves and the class group of* $\mathbf{Q}(\zeta_p)$, Invent. Math. **58** (1980), no. 1, 1–35.

[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.

http://www.springer.com/978-1-4614-1259-5

Number Theory, Analysis and Geometry
In Memory of Serge Lang
Goldfeld, D.; Jorgenson, J.; Jones, P.; Ramakrishnan, D.;
Ribet, K.; Tate, J.T. (Eds.)
2012, XX, 704 p., Hardcover
ISBN: 978-1-4614-1259-5