The Modular number, the Congruence number, and Multiplicity One

Amod Agashe[*]and Kenneth Ribet

Abstract

Let N be a positive integer and let f be a newform of weight 2 on $\Gamma_0(N)$. In a joint paper with W. Stein, the authors introduced the notions of the modular number and the congruence number of the quotient abelian variety A_f of $J_0(N)$ associated to the newform f. These invariants are analogs of the notions of the modular degree and congruence primes respectively associated to optimal elliptic curves. In this article, we show that if p is a prime number such that every maximal ideal of the Hecke algebra of characteristic p that contains the annihilator ideal of f satisfies multiplicity one, then the modular number of A_f and the congruence number of A_f have the same p-adic valuation. We also discuss a more general setting that involves certain abelian subvarieties of $J_0(N)$ or $J_1(N)$ and state a result about the structure of the intersection of such abelian varieties as a module over the Hecke algebra, from which the statement in the previous sentence follows. We also give a numerical example where our result implies the failure of multiplicity one.

1 Introduction and some of the results

Let N be a positive integer and let $X_0(N)$ denote the modular curve over $\mathbf{Q}$ associated to the classification of 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 $\Gamma_0(N)$ and let I_f denote $\mathrm{Ann}_{\mathbf{T}}(f)$. Then the quotient abelian variety $A_f = J_0(N)/I_f J_0(N)$ is called the newform quotient associated to f. If f has integer Fourier coefficients, then A_f is an elliptic curve and in fact by [BCDT01] any elliptic curve over $\mathbf{Q}$ is isogenous to such an elliptic curve for some f. The dual abelian variety $A_f^\vee$ of A_f may be viewed as an abelian subvariety of $J_0(N)$. Recall that the *exponent* of a finite group G is the smallest positive integer n such that multiplication by n annihilates every element of G.

The exponent of the group $A_f^\vee \cap I_f J$ is called the *modular exponent* of A_f, denoted $\tilde{n}_{A_f}$, and its order is called the *modular number*, denoted n_{A_f} (see [ARS12, §3]). Suppose for the moment that f has integer Fourier coefficients, so that A_f is an elliptic curve, which we denote by E for emphasis. 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 $\phi_E : X_0(N) \to E$, whose degree is called the *modular degree* of E. The modular exponent $\tilde{n}_E$ of E is equal to the modular degree, and the modular number n_E is the square of the modular degree (see [ARS12, §3]). In general, for any newform f, the modular number n_{A_f} is a perfect square (e.g., see [AS05, Lemma 3.14]).

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

[*]The first author was partially supported by National Science Foundation Grant No. 0603668. Mathematics subject classification: 11G40.

cuspforms that are orthogonal to every g in G with respect to the Petersson inner product. The exponent of the quotient group

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

is called the *congruence exponent* of A_f (really, that of f), denoted $\tilde{r}_{A_f}$ and its order is called the *congruence number*, denoted r_{A_f} (see [ARS12, §3]). If f has integer Fourier coefficients, so that A_f is an elliptic curve, then the quotient group above is a quotient of $\mathbf{Z}$ (e.g., by (2) and (3) in Section 2), so that $r_{A_f} = \tilde{r}_{A_f}$, and either of them is the largest integer r such that there exists a cuspform $g \in S_2(\mathbf{Z})$ that is orthogonal to f under the Petersson inner product and whose n-th Fourier coefficient is congruent modulo r to the n-th Fourier coefficient of f for all positive integers n. We say that a prime is a *congruence prime for A_f* if it divides the congruence number r_{A_f}.

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 MaiMurty 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 congruence primes and the modular degree are quantities of significant interest. Theorem 3.6 of [ARS12] says that the modular exonent $\tilde{n}_{A_f}$ divides the congruence exponent $\tilde{r}_{A_f}$ and if p is a prime such that $p^2 \nmid N$, then $\mathrm{ord}_p(\tilde{n}_{A_f}) = \mathrm{ord}_p(\tilde{r}_{A_f})$.

One might wonder if similar relations hold between the modular number r_{A_f} and congruence number n_{A_f} (as opposed to modular/congruence *exponents*). As mentioned earlier, if A_f is an elliptic curve, then $n_{A_f} = \tilde{n}^2_{A_f}$ and $r_{A_f} = \tilde{r}_{A_f}$, and so one sees that $n_{A_f} \mid r^2_{A_f}$. So to start with, one might wonder whether n_{A_f} divides $r^2_{A_f}$ even if A_f is not an elliptic curve (i.e., has dimension more than one); this question makes sense also because n_{A_f} is a perfect square, while r_{A_f} need not be a perfect square. It turns out that the answer to the question is no: as mentioned in [ARS12, Remark 3.7] we have

Example 1.1. There is a newform of degree 24 in $S_2(\Gamma_0(431))$ such that

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

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 $\rho_\mathfrak{m}$ (e.g., see [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]). It was remarked in [ARS12] that concerning Example 1.1 above where $n_{A_f} \nmid r^2_{A_f}$, the level 431 is prime and by [Kil02], mod 2 multiplicity one fails for $J_0(431)$. In this article, we show that multiplicity one is the only obstruction for the divisibility $n_{A_f} \mid r^2_{A_f}$ to fail. In fact, we show something stronger:

Theorem 1.2. *Let p be a prime such that every maximal ideal $\mathfrak{m}$ with residue characteristic p that contains I_f satisfies multiplicity one. Then* $\mathrm{ord}_p(n_{A_f}) = \mathrm{ord}_p(r^2_{A_f})$.

The theorem above follows from the more general Theorem 2.1 below. Example 1.1 above shows that the multiplicity one hypothesis cannot be completely removed from the theorem.

The theorem above is the analog of Proposition 5.9 of [ARS12], which says that under the hypotheses of the theorem above, we have $\mathrm{ord}_p(\tilde{n}_{A_f}) = \mathrm{ord}_p(\tilde{r}_{A_f})$. If A_f is an elliptic curve, then as remarked earlier, $n_{A_f} = \tilde{n}^2_{A_f}$ and $r_{A_f} = \tilde{r}_{A_f}$, so our theorem adds nothing new.

In the context of Example 1.1, our theorem gives a new proof that mod 2 multiplicity fails for $J_0(431)$ (the original proof being the one in [Kil02]). Note that in [ARS12], the authors found examples of failure of multiplicity one using Propostion 5.9 of loc. cit., which implies that if the modular exponent does not equal the congruence exponent for some newform f, then there is a maximal ideal of $\mathbf{T}$ that not satisfy multiplicity one. However, we could not have detected the failure of multiplicity one in Example 1.1 by checking if the modular *exponent* equals the congruence *exponent*, since the equality holds in the example for any newform f by [ARS12, Thm. 3.6(b)], considering that the level is prime in the example. At the same time, consideration of the modular *number* and the congruence *number* did dectect the failure of multiplicity one. It would be interesting to do more calculations to see when $n_{A_f} \not| \, r_{A_f}^2$, as this may give new instances of failure of multiplicity one.

We remark that our theorem gives information about the *order* of a certain intersection of abelian subvarieties of $J_0(N)$ in terms of congruences between modular forms (in fact, we give information in a more general setting in Section 2). We expect that the relation between a particular such intersection and certain congruences will be useful in understanding the "visible factor" in [Aga10], and hope that such relations will be useful in other contexts as well.

It is known that multiplicity one holds in several situations. We content ourselves by pointing out that by the main theorem in Section 1.2 of [MR91], a maximal ideal $\mathfrak{m}$ with residue characteristic p satisfies multiplicity one if either $p \not| \, N$ or $p || N$ and $\rho_{\mathfrak{m}}$ is not modular of level N/p. We also have:

Proposition 1.3. *Let p be an odd prime and $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ with residue characteristic p such that $\rho_{\mathfrak{m}}$ is irreducible. Assume that either*
(i) $p \not| \, N$ or
(ii) $p || N$ and $I_f \subseteq \mathfrak{m}$ for some newform f.
Then $\mathfrak{m}$ satisfies multiplicity one.

Proof. If $p \nmid N$, then the claim follows from Theorem 5.2(b) of [Rib90], so let us assume that $p || N$. Let $X_0(N)_{\mathbf{Z}_p}$ denote the minimal regular resolution of the compactified coarse moduli scheme over $\mathbf{Z}_p$ associated to $\Gamma_0(N)$ as in [DR73, § IV.3] and let $\Omega_{X_0(N)_{\mathbf{Z}_p}/\mathbf{Z}_p}$ 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 $\mathbf{F}_p$. It is shown in [ARS12, §5.2.2] that under the hypotheses above, $\dim_{\mathbf{T}/\mathfrak{m}} H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)_{\mathbf{F}_p}/\mathbf{F}_p})[\mathfrak{m}] \leq 1$. Let $J_{\mathbf{Z}_p}$ denote the Néron model of $J_0(N)$ over $\mathbf{Z}_p$ and let $J^0_{\mathbf{Z}_p}$ denote its identity component. Then 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 $J^0_{\mathbf{Z}_p}$ (see, e.g., [BLR90, §9.4–9.5]). Passing to tangent spaces along the identity section over $\mathbf{Z}_p$, we obtain an isomorphism $H^1(X_0(N)_{\mathbf{Z}_p}, \mathcal{O}_{X_0(N)_{\mathbf{Z}_p}}) \cong \mathrm{Tan}(J_{\mathbf{Z}_p})$. Reducing both sides modulo p and applying Grothendieck duality, we get $\mathrm{Tan}(J_{\mathbf{F}_p}) \cong \mathrm{Hom}(H^0(X_0(N)_{\mathbf{F}_p}, \Omega_{X_0(N)/\mathbf{F}_p}), \mathbf{F}_p)$. Thus from the above discussion, we see that $\mathrm{Tan}(J_{\mathbf{F}_p})/\mathfrak{m}\mathrm{Tan}(J_{\mathbf{F}_p})$ has dimension at most one over $\mathbf{T}/\mathfrak{m}$. Since $\mathrm{Tan}(J_{\mathbf{Z}_p})$ is a faithful $\mathbf{T} \otimes \mathbf{Z}_p$-module, we see that $\mathrm{Tan}(J_{\mathbf{F}_p})/\mathfrak{m}\mathrm{Tan}(J_{\mathbf{F}_p})$ is nontrivial, hence it is one dimensional over $\mathbf{T}/\mathfrak{m}$. With this input, the proof of multiplicity one in Theorem 2.1 of [Wil95], which is in the $\Gamma_1(N)$ context, but is a formal argument involving abelian varieties (apart from the input above), carries over in the $\Gamma_0(N)$ context with the obvious modifications (in particular, replacing $X_1(N/p, p)_{\mathbf{Z}_p}$ in loc. cit. by $X_0(N)_{\mathbf{Z}_p}$) to prove our claim (see p. 487-488 of loc. cit., as well as [Til97], where the input above is the equation (**) on p. 339). □

We remark that the condition that $p^2 \not| \, N$ in condition (ii) of the proposition above cannot be removed, as follows from the counterexamples in [ARS12, §2.2]. From Theorem 1.2 and Proposition 1.3, we obtain:

Corollary 1.4. *Let p be an odd prime. Suppose that either*
(i) $p \not| N$ or
(ii) $p || N$ and $A_f^\vee[\mathfrak{m}]$ is irrreducible for every maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ with residue characteristic p.
Then $\mathrm{ord}_p(n_{A_f}) = \mathrm{ord}_p(r_{A_f}^2)$.

Proof. The corollary is clear from Theorem 1.2 and Proposition 1.3 in the case where $p \not| N$, so let us assume that $p||N$. By Theorem 1.2 and Proposition 1.3, it suffices to show that $\rho_\mathfrak{m}$ is irreducible for every maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ with residue characteristic p such that $I_f \subseteq \mathfrak{m}$.

Let $\mathfrak{m}$ be such a maximal ideal. Then note that $A_f^\vee[\mathfrak{m}]$ is non-trivial since $\mathbf{T}/I_f$ acts faithfully on $A_f^\vee$. Let D denote the direct sum of $A_f^\vee[\mathfrak{m}]$ and its Cartier dual. Let ℓ be a prime that does not divide Np and let Frob_ℓ denote the Frobenius element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ at ℓ. As discussed in [Maz77, p. 115], by the Eichler-Shimura relation, the characteristic polynomial of Frob_ℓ acting on D is $(X^2 - a_\ell X + \ell)^d = 0$, where a_ℓ is the image of T_ℓ in $\mathbf{T}/\mathfrak{m}$ and d is the $\mathbf{T}/\mathfrak{m}$-dimension of $A_f^\vee[\mathfrak{m}]$. But this is also the characteristic polynomial of Frob_ℓ acting on the direct sum of d copies of $\rho_\mathfrak{m}$. By the Chebotarev density theorem and the Brauer-Nesbitt theorem, the semisimplification of D is $\rho_\mathfrak{m}^d$. Thus the semisimplification of $A_f^\vee[\mathfrak{m}]$ is a direct sum of certain number of copies of $\rho_\mathfrak{m}$. But $A_f^\vee[\mathfrak{m}]$ is irreducible by hypothesis, so $\rho_\mathfrak{m} = A_f^\vee[\mathfrak{m}]$. Thus $\rho_\mathfrak{m}$ is also irreducible, as was to be shown. □

The corollary above is the analog of Theorem 3.6(b) of [ARS12], which says that $\mathrm{ord}_p(\tilde{n}_{A_f}) = \mathrm{ord}_p(\tilde{r}_{A_f})$ provided $p^2 \not| N$, in the setting of modular/congruence *numbers* as opposed to modular/congruence *exponents* (although, note that we have an extra irreducibility hypothesis in our corollary). We remark that the proofs of both results rely ultimately on "multiplicity one for differentials" (as defined in [ARS12, §5.2]).

If the level N is prime, then more can be said. By Prop. II.14.2 and Corollary II.16.3 of [Maz77], every maximal ideal $\mathfrak{m}$ such that $\rho_\mathfrak{m}$ is reducible also satisfies multiplicity one. Thus in view of Theorem 1.2 and Proposition 1.3, we obtain the following:

Corollary 1.5. *Suppose the level N is prime and let p be an odd prime. Then $\mathrm{ord}_p(n_{A_f}) = \mathrm{ord}_p(r_{A_f}^2)$.*

Also, much is known in this situation if $\rho_\mathfrak{m}$ is irreducible and $\mathfrak{m}$ has residue characteristic is 2 – we refer to [Kil02] and the references therein for details. But note that by the examples in [Kil02] or by Example 1.1 and Theorem 1.2, multiplicity one need not hold for a maximal ideal $\mathfrak{m}$ of residue characteristic 2 with $\rho_\mathfrak{m}$ irreducible even if the level N is prime.

The organization of the rest of this article is as follows. In Section 2, we describe a more general setup, which includes abelian subvarieties of $J_1(N)$, and state a more general version of Theorem 1.2 (Theorem 2.1 below). Section 3 is devoted to the proof of the main result in Section 2.

Acknowldegements: The first author would like to thank J. Tilouine for some discussion regarding the proof of Proposition 1.3 above.

2 A more general setup and some more results

For the benefit of the reader, we repeat below some of the discussion in [ARS12, Section 3]. For $N \geq 4$, let Γ be either $\Gamma_0(N)$ or $\Gamma_1(N)$. Let X denote the modular curve over $\mathbf{Q}$ associated to Γ, and let J be the Jacobian of X. Let J_f denote the standard abelian subvariety of J attached to f by Shimura [Shi94, Thm. 7.14]. 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 action, and $e(f)$ is the number of divisors of $N/N(f)$, where $N(f)$ is the level of f. Let A be the sum of $J_f^{e(f)}$ for some set of f's (taken up to Galois action), 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. By [ARS12, Lemma 3.1], $\mathrm{End}(J)$ preserves A and B, where if C is an abelian variety over $\mathbf{Q}$, by $\mathrm{End}(C)$ we mean the ring of endomorphisms of C defined over $\mathbf{Q}$. If f is a newform of weight 2 on Γ and A_f is its associated newform quotient, then $A_f^\vee$ and $I_f J$ provide an example of A and B respectively as above, as shown in the discussion following Lemma 3.1 in [ARS12].

There is an alternate way to describe the A and B in the previous paragraph. Since $\mathbf{T} \otimes \mathbf{Q}$ breaks up as a direct sum of algebras corresponding to Galois orbits of newforms of level dividing N, the abelian subvariety A corresponds to an idempotent $e \in \mathbf{T} \otimes \mathbf{Q}$, and conversely, given an idempotent $e \in \mathbf{T} \otimes \mathbf{Q}$, the image of J under e (viewed as an element of $\mathrm{End}(J) \otimes \mathbf{Q}$, which is to be multiplied by a large enough integer to make the product an element of $\mathrm{End}(J)$), is the corresponding A (and then B is the image of $(1 - e)$).

The *modular exponent* $\tilde{n}_A$ of A is defined as the exponent of $A \cap B$ and the *modular number* n_A of A is its order (see [ARS12, §3]). Note that the definition is symmetric with respect to A and B. If f is a newform, then by the modular exponent/number of A_f, we mean that of $A = A_f^\vee$, with $B = I_f J$, which agrees with our earlier definition.

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. Let $\mathbf{T}$ denote the Hecke algebra corresponding to the group Γ. There is a $\mathbf{T}$-equivariant bilinear pairing

$$\mathbf{T} \times S_2(\mathbf{Z}) \to \mathbf{Z} \tag{1}$$

given by $(t, g) \mapsto a_1(t(g))$, which is perfect (e.g., see [AU96, Lemma 2.1] or [Rib83, Theorem 2.2]). Let $\mathbf{T}_A$ denote 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 $\mathbf{T} \subseteq \mathrm{End}(J)$, $\mathbf{T}$ 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 the subgroups of $S_2(\mathbf{Z})$ obtained via the pairing in (1). By [ARS12, Lemma 3.3], we have an isomorphism

$$\frac{S_2(\mathbf{Z})}{S_A + S_B} \cong \frac{\mathbf{T}_A \oplus \mathbf{T}_B}{\mathbf{T}} \; . \tag{2}$$

Also, we have an isomorphism

$$\frac{\mathbf{T}}{I_A + I_B} \xrightarrow{\simeq} \frac{\mathbf{T}_A \oplus \mathbf{T}_B}{\mathbf{T}} \tag{3}$$

obtained by sending $t \in \mathbf{T}$ to $(\pi_A(t), 0) \in \mathbf{T}_A \oplus \mathbf{T}_B$, where π_A is the projection map $\mathbf{T} \to \mathbf{T}_A$. By definition [ARS12], the exponent of either of the isomorphic groups in (2) or (3) is the *congruence exponent* $\tilde{r}_A$ of A and the order of either group 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 $S_A = S_2(\mathbf{Z})[I_f]$. Also, $\mathrm{Hom}(\mathbf{T}_B, \mathbf{Z})$ is the unique saturated Hecke-stable complement of $S_2(\mathbf{Z})[I_f]$ in $S_2(\mathbf{Z})$, hence must equal $S_2(\mathbf{Z})[I_f]^\perp$. This shows that the new definition of the congruence number/exponent generalizes our earlier definition for A_f.

Let $I_A = \mathrm{Ann}_{\mathbf{T}}(A)$ and $I_B = \mathrm{Ann}_{\mathbf{T}}(B)$. Theorem 3.6(a) of [ARS12] says that the modular exponent $\tilde{n}_A$ divides the congruence exponent $\tilde{r}_A$, and Propostion 5.9 of loc. cit. says that if p is a prime such that all maximal ideals $\mathfrak{m}$ of $\mathbf{T}$ containing $I_A + I_B$ satisfy multiplicity one, then $\mathrm{ord}_p(\tilde{r}_A) = \mathrm{ord}_p(\tilde{n}_A)$. Our main theorem deals with the case of modular/congruence numbers as opposed to modular/congruence exponents. In view of the case of newform quotients discussed in Section 1, one would like to understand the relation between the modular number n_A and the *square* of the congruence number r_A. As mentioned earlier, it is not true that n_A divides r_A^2 in general. At the same time, we have:

Theorem 2.1. *Let p be a prime such that every maximal ideal $\mathfrak{m}$ with residue characteristic p that contains $I_A + I_B$ satisfies multiplicity one. Then $\mathrm{ord}_p(n_A) = \mathrm{ord}_p(r_A^2)$.*

The theorem above follows immediately from:

Theorem 2.2. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ that satisfies multiplicity one. Then on tensoring with $\mathbf{T}_{\mathfrak{m}}$, $A \cap B$ is free of rank two over $\frac{\mathbf{T}}{I_A + I_B}$.*

We will prove this theorem in Section 3. Note that Theorem 2.1 is an analog of Propostion 5.9 of [ARS12] in the context of modular/congruence numbers as opposed to modular/congruence exponents. For results on multiplicity one in the $\Gamma = \Gamma_1(N)$ context, see, e.g., [Til97] and the references therein.

Let $\pi_A : \mathbf{T} \to \mathbf{T}/I_A = \mathbf{T}_A$ and $\pi_B : \mathbf{T} \to \mathbf{T}/I_B = \mathbf{T}_B$ denote the natural projection maps. In this setup, in[ARS12], we defined the *congruence ideal* as $R = \pi_A(\ker(\pi_B)) \subset \mathbf{T}_A$, and the *intersection ideal* as $S = \mathrm{Ann}_{\mathbf{T}_A}(A \cap B)$. By [ARS12, Lem. 5.2], we have $R \subseteq S$. Moreover, π_A induces a natural isomorphism

$$\frac{\mathbf{T}}{I_A + I_B} \xrightarrow{\simeq} \frac{\mathbf{T}_A}{R}.$$

Thus from Thorem 2.2, we obtain

Proposition 2.3. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ that contains I_A and satisfies multiplicity one. Then on tensoring with the completion of $\mathfrak{m}/I_A$, $R = S$.*

The proposition above is not new: it follows from Proposition 5.6 and Lemma 5.8 of [ARS12]. Our proof above is analogous to the arguments in [ARS12] (in this article, we use homology groups in the proof of Thorem 2.2, while the proof of Lemma 5.8 of [ARS12] uses Tate modules).

3 Proof of Theorem 2.2

We have (e.g., by [AS05, Prop. 3.2]) the following natural isomorphism of $\mathbf{T}$-modules:

$$A \cap B \cong \frac{H_1(J, \mathbf{Z})}{H_1(A, \mathbf{Z}) + H_1(B, \mathbf{Z})}$$

Also, by [Aga10, Lem 4.3], we have $H_1(A, \mathbf{Z}) = H_1(J, \mathbf{Z})[I_A]$ and $H_1(B, \mathbf{Z}) = H_1(J, \mathbf{Z})[I_B]$. Thus

$$A \cap B \cong \frac{H_1(J, \mathbf{Z})}{H_1(J, \mathbf{Z})[I_A] + H_1(J, \mathbf{Z})[I_B]}. \tag{4}$$

Recall that $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ that satisfies multiplicity one. Then $H_1(J, \mathbf{Z}) \otimes_{\mathbf{T}} \mathbf{T}_{\mathfrak{m}}$ is free of rank two over $\mathbf{T}_{\mathfrak{m}}$, by a standard argument due to Mazur (see [Maz77, Lem. II.15.1] or Corollary (3) of Theorem 3.4 in [Til97]). Thus by (4), on tensoring with $\mathbf{T}_{\mathfrak{m}}$, $A \cap B$ is free of rank two over $\frac{\mathbf{T}}{\mathbf{T}[I_A] + \mathbf{T}[I_B]}$. The theorem now follows from the following lemma.

Lemma 3.1. $\mathbf{T}[I_A] = I_B$ *and* $\mathbf{T}[I_B] = I_A$.

Before giving the proof of this lemma, we need another lemma, which is in a slightly more general setup. In this paragraph, the symbol g stands for a newform of some level N_g dividing N. Let S'_g denote the subspace of $S_2(\Gamma_0(N), \mathbf{C})$ spanned by the forms $g(dz)$ where d ranges over the divisors of N/N_g. Let $[g]$ denote the Galois orbit of g, and let $S_{[g]}$ denote the $\mathbf{Q}$-subspace of forms in $\oplus_{h\in[g]} S'_h$ with rational Fourier coefficients. We have $S_2(\Gamma_0(N), \mathbf{Q}) = \oplus_{[g]} S_{[g]}$, where the sum is over Galois conjugacy classes of newforms of some level dividing N. Let X be a subset of the set of Galois conjugacy classes of newforms of some level dividing N, and let $I = \mathrm{Ann}_{\mathbf{T}}(\oplus_{[g]\in X} S_{[g]})$. If g is a newform of some level dividing N, then $S_{[g]}$ is preserved by $\mathbf{T}$; let $\mathbf{T}_{[g]}$ denote the image of $\mathbf{T}$ acting on $S_{[g]}$. Then the natural map

$$\phi : \mathbf{T} \otimes \mathbf{Q} \to \oplus_{[g]} \mathbf{T}_{[g]}$$

is an isomorphism of $\mathbf{T}\otimes\mathbf{Q}$ algebras, where $[g]$ ranges over all Galois conjugacy classes of newforms of level dividing N (see, e.g., [Par99, Thm. 3.5]). We have the decomposition

$$\oplus_{[g]} \mathbf{T}_{[g]} = \left(\oplus_{[g]\in X} \mathbf{T}_{[g]} \right) \oplus \left(\oplus_{[g]\notin X} \mathbf{T}_{[g]} \right) . \tag{5}$$

Let $\widehat{I}$ denote $\mathrm{Ann}_{\mathbf{T}}(I)$.

Lemma 3.2. *The image of $I \otimes \mathbf{Q}$ under ϕ is $\oplus_{[g]\notin X} \mathbf{T}_{[g]}$, and the image of $\widehat{I} \otimes \mathbf{Q}$ is $\oplus_{[g]\in X} \mathbf{T}_{[g]}$. Thus $\mathbf{T} \otimes \mathbf{Q} \cong I \otimes \mathbf{Q} \oplus \widehat{I} \otimes \mathbf{Q}$ as $\mathbf{T} \otimes \mathbf{Q}$-modules.*

Proof. It is clear that the image of $I \otimes \mathbf{Q}$ in (5) under ϕ is $\oplus_{[g]\notin X} \mathbf{T}_{[g]}$. As for the image of $\widehat{I} \otimes \mathbf{Q}$, it clearly contains $\oplus_{[g]\in X} \mathbf{T}_{[g]}$. Conversely, if $x \in \widehat{I} \otimes \mathbf{Q}$, then it annihilates the element $(0, 1)$ in the decomposition of (5) (since $(0, 1)$ is in the image of $I \otimes \mathbf{Q}$ under ϕ), so the image of $x \cdot (0, 1)$ in $\oplus_{[g]} \mathbf{T}_{[g]}$ must be zero. Thus $x \in \oplus_{[g]\in X} \mathbf{T}_{[g]}$, which finishes the proof the lemma. □

Proof of Lemma 3.1. First, note that $\mathbf{T}[I_A] = \widehat{I_A}$. By Lemma 3.2, taking X to be the set of newforms corresponding to A, we see that the image of $I_A \otimes \mathbf{Q}$ under ϕ in the decomposition (5) is $\oplus_{[g]\notin X} \mathbf{T}_{[g]}$, and by a similar argument, the image of $I_B \otimes \mathbf{Q}$ is $\oplus_{[g]\in X} \mathbf{T}_{[g]}$. Thus $I_B \subseteq \widehat{I_A}$ and also, by Lemma 3.2, we see that $I_B \otimes \mathbf{Q} = \widehat{I_A} \otimes \mathbf{Q}$. But I_B and $\widehat{I_A}$ are both saturated in $\mathbf{T}$, and so it follows that $I_B = \widehat{I_A}$. This shows that $I_B = \mathbf{T}[I_A]$. Swapping the roles of A and B, we see that $I_A = \mathbf{T}[I_B]$, which finishes the proof of the lemma. □

References

[Aga10] A. Agashe, *A visible factor of the special L-value*, J. Reine Angew. Math. (Crelle's journal) **644** (2010), 159–187.

[ARS12] Amod Agashe, Kenneth A. Ribet, and William A. Stein, *The modular degree, congruence primes, and multiplicity one*, Number theory, analysis and geometry, Springer, New York, 2012, pp. 19–49. MR 2867910

[AS05] Amod Agashe and William 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 (electronic), With an appendix by J. Cremona and B. Mazur.

[AU96] Ahmed Abbes and Emmanuel Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. **103** (1996), no. 3, 269–286. MR 97f:11038

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

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR 91i:14034

[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, pp. 143–316. Lecture Notes in Math., Vol. 349.

[Fre97] G. Frey, *On ternary equations of Fermat type and relations with elliptic curves*, Modular forms and Fermat's last theorem (Boston, MA, 1995) (New York) (G. Cornell, J. H. Silverman, and G. Stevens, eds.), Springer, 1997, Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995, pp. 527–548.

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

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

[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. MR 2000g:11038

[Par99] Pierre Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116.

[Rib83] Kenneth 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.

[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.

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

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