JOURNAL
de Théorie des Nombres
de BORDEAUX
*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Amod AGASHE

**Rational torsion in elliptic curves and the cuspidal subgroup**

Tome 30, n° 1 (2018), p. 81-91.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_1_81_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **30** (2018), 81–91

# Rational torsion in elliptic curves and the cuspidal subgroup

par Amod AGASHE

Résumé. Soit $A$ une courbe elliptique sur $\mathbf{Q}$ de conducteur $N$ sans facteurs carré, ayant un point rationnel d'ordre un nombre premier $r$ ne divisant pas $6N$. On montre alors que $r$ divise l'ordre du sous-groupe cuspidal $C$ de $J_0(N)$. Si $A$ est une courbe de Weil, on peut la considérer comme une sous-variéte abélienne de $J_0(N)$. Notre preuve montre plus precisément que $r$ divise l'ordre de $A \cap C$. De plus, sous les hypothèses plus haut, mais sans supposer que $r$ ne divise pas $N$, on montre qu'il existe un facteur premier $p$ de $N$ tel que la valeur propre de l'involution d'Atkin–Lehner $W_p$ agissant sur la forme modulaire associée à $A$ est égale à $-1$.

Abstract. Let $A$ be an elliptic curve over $\mathbf{Q}$ of square free conductor $N$ that has a rational torsion point of prime order $r$ such that $r$ does not divide $6N$. We show that then $r$ divides the order of the cuspidal subgroup $C$ of $J_0(N)$. If $A$ is optimal, then viewing $A$ as an abelian subvariety of $J_0(N)$, our proof shows more precisely that $r$ divides the order of $A \cap C$. Also, under the hypotheses above minus the hypothesis that $r$ does not divide $N$, we show that for some prime $p$ that divides $N$, the eigenvalue of the Atkin–Lehner involution $W_p$ acting on the newform associated to $A$ is $-1$.

## 1. Introduction

Let $A'$ be an elliptic curve over $\mathbf{Q}$ of square free conductor $N$ and let $A$ be the optimal curve in the isogeny class (over $\mathbf{Q}$) of $A'$. Let $X_0(N)$ denote the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$, and let $J_0(N)$ be its Jacobian. By [4], we may view $A$ as an abelian variety quotient over $\mathbf{Q}$ of $J_0(N)$. By dualizing, $A$ can also be viewed as an abelian subvariety of $J_0(N)$, as we shall do in the rest of this article. The *cuspidal subgroup* $C$ of $J_0(N)(\mathbf{C})$ is the group of degree zero divisors on $X_0(N)(\mathbf{C})$ that are

Manuscrit reçu le 21 février 2016, révisé le 30 janvier 2017, accepté le 12 septembre 2016.
2010 *Mathematics Subject Classification.* 11G05, 14H52.
*Mots-clefs.* Elliptic curves, torsion subgroup, cuspidal subgroup.
This material is based upon work supported by the National Science Foundation under Grant No. 0603668.

supported on the cusps. It is known that $C$ is finite. Since $N$ is square free, the cusps of $X_0(N)$ are defined over $\mathbf{Q}$, so $C \subseteq J_0(N)(\mathbf{Q})_{\text{tor}}$.

When $N$ is prime, Mazur [12] showed that $C = J_0(N)(\mathbf{Q})_{\text{tor}}$; so in particular, $A(\mathbf{Q})_{\text{tor}} \subseteq C$. The torsion and cuspidal groups are of independent interest and importance, and relations between them are of great significance. For example, using such a relation, Emerton [10] showed that when $N$ is prime, the orders of $A(\mathbf{Q})_{\text{tor}}$ and the arithmetic component group of $A$ are the same, which implies a significant cancellation in the formula given by the second part of the Birch and Swinnerton-Dyer conjecture for $A$ (when $N$ is prime), which is in accord with the conjecture (see, e.g. [2, §4.3]).

Based on some numerical data of Cremona [6] and Stein [14], we suspect that $A(\mathbf{Q})_{\text{tor}} \subseteq C$ more generally when $N$ is square free, i.e., that again the cuspidal divisors "explain" the existence of all the rational torsion points in $A$. In this paper, we prove the following result in this direction:

**Theorem 1.1.** *Recall that $A'$ is an elliptic curve over $\mathbf{Q}$ of square free conductor $N$ and $A$ is the optimal curve in the isogeny class of $A'$. Suppose $r$ is a prime that does not divide $6N$.*

(1) *If $r$ divides the order of $A(\mathbf{Q})_{\text{tor}}$, then $r$ divides the order of $A \cap C$ (in particular, $r$ divides the order of the cuspidal subgroup $C$).*
(2) *If $r$ divides the order of $A'(\mathbf{Q})_{\text{tor}}$, then $r$ divides the order of the cuspidal subgroup $C$.*

The proof of the theorem is given in Section 4. The main ingredient in the proof of part (1) is to show that the hypotheses imply that the newform $f$ associated to $A$ is congruent to an Eisenstein series $E$ modulo $r$ (the tricky part is to get the congruence for Fourier coefficients of indices that are not coprime to $N$). As part of the proof of this congruence, we show that under the hypotheses of part (1) of the theorem (but relaxing the hypothesis that $r \nmid N$), for at least one prime $p$ that divides $N$, the sign of the Atkin-Lenher involution at $p$ acting on $f$ is $-1$, which is an interesting result on its own (see Proposition 3.6). Given the congruence between $f$ and $E$, and the fact that $f$ is ordinary at $r$ (which we show), a result of Tang [17, Thm. 0.4] tells us that $A[r]$ has nontrivial intersection with a subgroup of the cuspidal group $C$, thus giving us part (1) of the theorem above. Part (2) follows from part (1) by [9, Thm. 1.2] which says that if $\ell$ is a prime such that $\ell^2 \nmid N$ (which holds for $\ell = r$, given our hypothesis), then if $A'$ has a rational torsion point of order $\ell$, then so does $A$ (see also Remark 4.1).

By[12, III.5.1], the only primes that can divide the order of $A'(\mathbf{Q})_{\text{tor}}$ are 2, 3, 5 and 7, and moreover there is a finite list of possibilities for $A'(\mathbf{Q})_{\text{tor}}$. In particular, our theorem gives new information only when $r$ is 5 or 7 (and $r \nmid N$). We expect that by doing more work (using ideas from [12]), one should be able to prove that for every prime $r \nmid 6N$, the $r$-primary part of $A(\mathbf{Q})_{\text{tor}}$ is contained in $C$; again, by Mazur's result mentioned above, this

gives no new information (since we are assuming that $r \neq 2, 3$). However, the hope is that such a result may hold (and the proof may generalize) for higher-dimensional abelian subvarieties $A$ of $J_0(N)$ associated to newforms. Finally, it would also be desirable to see if the hypothesis that $r \nmid 6N$ can be removed. The present article may be viewed as our first step in relating rational torsion of modular abelian varieties to the cuspidal subgroup when $N$ is square free, as well as generalizing some of the techniques of Mazur [12] for prime $N$ to square free $N$.

In any case, the theorem above puts restrictions on when 5 and 7 can divide the order of $A'(\mathbf{Q})_{\mathrm{tor}}$, and may be useful in its computations, since the order of the cuspidal subgroup $C$ can be computed (see, e.g., [14]). It may also be useful theoretically in certain situations where there is an explicit formula for the order of $C$. For example, if $N$ is a product of two primes $p$ and $q$, then by [5, §3.4], the only odd primes that divide the order of $C$ are the ones that divide $(p^2 - 1)(q^2 - 1)$. As a computational application, taking $p = 1013$ and $q = 10007$, we see that 5 and 7 cannot divide the order of the rational torsion subgroup of any elliptic curve over $\mathbf{Q}$ of conductor $N = 1013 \cdot 10007$.

We remark that there is significant overlap between the results and techniques of this article, and those of [13], [19], and [20] (which were pointed out to us by the anonymous referee) and some of the results of this article follow from the discussions in the latter articles. However, these latter articles appeared much after this present article was first written.

The organization of this article is as follows. In Section 2, we show how to construct certain desirable Eisenstein series. In Section 3, we state some other preliminary results needed for the proof of Theorem 1.1. These results concern certain constraints on the Fourier coefficients of $f$ arising out of the existence of rational $r$-torsion, and could be of independent interest. Finally, we give the proof of Theorem 1.1 in Section 4. Note that in any given section, we continue to use the notation introduced in earlier sections.

**Acknowledgement.** We are grateful to Barry Mazur for pointing out a construction that we used in the proof of Proposition 2.1, and to Neil Dummigan for conveying the proof of Lemma 3.2, as well as for some very useful comments on an earlier draft.

## 2. Certain Eisenstein series

If $g = g(z)$ is a modular form, then we will denote its Fourier expansion $\sum_{n \geq 0} a_n(g) q^n$ at the cusp $\infty$ (where $q = e^{2\pi i z}$ as usual) by $g(q)$. If $n$ is a positive integer, then $\sigma(n)$ denotes the sum of all the positive divisors of $n$.

**Proposition 2.1.** *Recall that $N$ is square free. For every prime $p$ that divides $N$, suppose we are given an integer $\delta_p \in \{1, p\}$ such that $\delta_p = 1$ for at least one $p$. Then there is an Eisenstein series $E$ of weight 2 on $\Gamma_0(N)$*

*which is an eigenfunction for all the Hecke operators such that for all primes $\ell \nmid N$, we have $a_\ell(E) = \ell + 1$, and for all primes $p \mid N$, we have $a_p(E) = \delta_p$.*

*Proof.* The normalized Eisenstein series $e$ of weight 2 and level 1 has $q$-expansion $e(q) = 1/24 - \sum_{n\geq 1} \sigma(n)q^n$. It is not a modular form of level 1, but it is an eigenfunction for all the Hecke operators. We shall construct the desired Eisenstein series by starting with $e$ and "raising the level".

Let $g = \sum_{n\geq 0} a_n(g)q^n$ be a normalized eigenfunction of some level $M$ and let $r$ be a prime that does not divide $M$. Let $(B_r g)(z) = g(rz)$. Then we have (see, e.g., [3, p. 141])

$$\begin{aligned} B_r\Big(\sum_{n\geq 0} a_n q^n\Big) &= \sum_{n\geq 0} a_n q^{nr}, \\ U_r\Big(\sum_{n\geq 0} a_n q^n\Big) &= \sum_{n\geq 0} a_{nr} q^n, \\ \text{and} \quad T_\ell\Big(\sum_{n\geq 0} a_n q^n\Big) &= \sum_{n\geq 0} a_{n\ell} q^n + \sum_{n\geq 0} \ell a_n q^{n\ell}, \qquad \forall\ \ell \nmid Mr, \end{aligned} \tag{2.1}$$

where $T_\ell$ and $U_r$ are the usual Hecke operators at level $Mr$. For the moment, let $T_r$ denote the $r$-th Hecke operator of level $M$; then equation (2.1) holds for $T_r$ as well. Thus from the formulas above, we see that $T_r = U_r + rB_r$. Since $g$ is an eigenfunction for $T_r$ with eigenvalue $a_r(g)$, we deduce that $U_r(g) = a_r(g) \cdot g - r \cdot B_r(g)$ and $U_r(B_r(g)) = g$. Thus $U_r$ preserves the complex vector space $V$ generated by $g$ and $B_r(g)$, and the characteristic polynomial of $U_r$ on this subspace is $U_r^2 - a_r(g)U_r + r$. The elements of $V$ are eigenvectors for all the other Hecke operators. Now suppose $a_r(g) = 1 + r$, as will be the case in our application. Then the characteristic polynomial becomes $U_r^2 - (1+r)U_r + r$, whose roots are 1 and $r$. Thus the action of $U_r$ is diagonalizable on $V$. Moreover, one checks that a basis of normalized eigenvectors (for all the Hecke operators) is $g_r = g - r \cdot B_r(g) = g(q) - r \cdot g(q^r)$ and $\tilde{g}_r = g - B_r(g) = g(q) - g(q^r)$, with eigenvalues 1 and $r$ respectively for $U_r$. If $g$ is actually a modular form, then so are $g_r$ and $\tilde{g}_r$. Since $g$ is normalized, $a_r(g_r) = 1$ and $a_r(\tilde{g}_r) = r$. Moreover, since raising levels by $r$ does not disturb the Fourier coefficients at other primes, for all primes $\ell \neq r$, we have $a_\ell(g_r) = a_\ell(\tilde{g}_r) = a_\ell(g)$.

Now pick a prime $p$ that divides $N$ such that $\delta_p = 1$. Taking $M = 1$, $r = p$, and $g = e$ in the discussion above, and considering that $a_p(e) = \sigma(p) = 1 + p$, we get an Eisenstein series $e_p$ that is an eigenvector for all the Hecke operators such that for all primes $\ell \neq p$, we have $a_\ell(e_p) = a_\ell(e) = \sigma(\ell) = \ell + 1$, and $a_p(e_p) = 1$. Moreover, $e_p$ is a modular form of level $p$ (see, e.g., [8, p. 47]). This proves the desired result if $N = p$.

If another prime $s$ divides $N$, then we apply the procedure two paragraphs above, taking $M = p$, $r = s$, and $g = e_p$. Since $a_s(e_p) = a_s(e) = 1 + s$,

we get an eigenform for all Hecke operators such that for all primes $\ell \nmid N$, the $\ell$-th Fourier coefficient is $\ell + 1$, the $p$-th Fourier coefficient is 1, and the $s$-th Fourier coefficient may be chosen to be 1 or $s$. This proves the desired result if $N = ps$.

Since $N$ is square free, and raising levels by a prime that divides $N$ does not disturb the Fourier coefficients at other primes, we see that repeating the procedure in the previous paragraph we get an eigenform $E$ with $a_\ell(E) = \ell + 1$ for all primes $\ell \nmid N$, $a_p(E) = 1$, and for all primes $s \mid N$ with $s \neq p$, $a_s(E)$ can be chosen to be 1 or $s$. □

The fact that one can construct interesting Eisenstein series by raising levels as in the proof above was pointed out to us by B. Mazur. In fact, a series as in the proposition above was used for the special case when $N$ is prime in [12] (the series $e'$ in §II.5 on p. 78 in loc. cit.).

## 3. Some results on Fourier coefficients

As before, $f$ denotes the newform of weight 2 on $\Gamma_0(N)$ associated to $A$. Then $f$ has integer Fourier coefficients. Let $w_p$ denote the sign of the Atkin–Lehner involution $W_p$ acting on $f$. In this section, we discuss how the existence of rational $r$-torsion in $A$ puts some restrictions on the Fourier coefficients of $f$.

The following lemma is perhaps well known.

**Lemma 3.1.** *Suppose a prime $r$ divides the order of $A(\mathbf{Q})_{\mathrm{tor}}$. Then for all primes $\ell \nmid N$, we have $a_\ell(f) \equiv 1 + \ell \bmod r$ and if $p \mid N$, then $a_p(f) = -w_p$.*

*Proof.* The proof of the first claim follows from the discussion in [12, p. 112–113]; we repeat some of the arguments in loc. cit. for the convenience of the reader. Let $P$ be a point of order $r$ in $A(\mathbf{Q})_{\mathrm{tor}}$ and let $G$ be a finite quotient of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ through which the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $J_0(N)[r]$ factors. Denote by $V$ the $(\mathbf{T}/r\mathbf{T})[G]$-submodule of $J_0(N)[r]$ generated by $P$ and by $\mathfrak{m}$ the annihilator in $\mathbf{T}$ of $V$. Let $S = \operatorname{Spec} \mathbf{Z}$, and let $J$ denote the Néron model of $J_0(N)$ over $S$. Let $V_{/S}$ denote the quasi-finite subgroup scheme of $J[r]$ whose associated Galois module is $V$. Since $N$ is square free, $J_0(N)$ has semi-stable reduction, and the argument at the bottom of p. 113 in [12] shows that $V_{/S}$ is either $\mu_r \otimes_{\mathbf{F}_r} \mathbf{T}/\mathfrak{m}$ or $\mathbf{Z}/r\mathbf{Z} \otimes_{\mathbf{F}_r} \mathbf{T}/\mathfrak{m}$ (in our case, since the eigenvalues of $f$ are integers, $\mathbf{T}/\mathfrak{m} \cong \mathbf{F}_r$, and since $P$ is defined over $\mathbf{Q}$, $V_{/S}$ is $\mathbf{Z}/r\mathbf{Z}$). In any case, if $\ell$ is a prime that does not divide $N$, then the Eichler–Shimura relation $T_\ell = \mathrm{Frob}_\ell + \ell/\mathrm{Frob}_\ell$ on $J_{/\mathbf{F}_\ell}$ (where $\ell/\mathrm{Frob}_\ell$ is the Verschiebung of $J_{/\mathbf{F}_\ell}$) tells us that $T_\ell \equiv (1 + \ell) \bmod \mathfrak{m}$. In particular, $T_\ell - (1 + \ell)$ annihilates $P$. Since $T_\ell P = a_\ell(f)P$, we see that $T_\ell - a_\ell(f)$ annihilates $P$, and hence so does $a_\ell(f) - (1 + \ell)$. But $P$ has order $r$, so $r$ divides $a_\ell(f) - (1 + \ell)$, and hence $a_\ell(f) \equiv 1 + \ell \bmod r$.

If $p \mid N$, then $a_p(f) = -w_p$ because $U_p = -W_p$ on the new subspace of $S_2(\Gamma_0(N), \mathbf{C})$. This finishes the proof of the lemma. $\square$

Keeping in mind the strategy of the proof of our main theorem (Theorem 1.1) mentioned in the introduction, we see from the lemma above and Proposition 2.1 that coming up with an Eisenstein series $E$ such that $a_\ell(f) \equiv a_\ell(E) \bmod r$ for all primes $\ell \nmid N$ is rather easy. Proving the congruence for all $\ell \mid N$ for a suitable Eisenstein series is the tricky part, for which we need the results below.

The following lemma is stated as a fact without a detailed proof in [9, §4]; the ingredients of the proof were communicated to us by N. Dummigan. The referee of this article has also pointed out that a generalization of the lemma below can be seen in the proof of [20, Lemma 2.1].

**Lemma 3.2** (Dummigan)**.** *Let $r$ be an odd prime that divides the order of $A(\mathbf{Q})_{\text{tor}}$. If $p$ is a prime that divides $N$ such that $w_p = 1$, then $r \mid (p+1)$.*

*Proof.* By the hypothesis, there is a nontrivial point $P$ in $A(\mathbf{Q})[r]$. Then $P \in A(\mathbf{Q}_p)[r]$. Since $p^2 \nmid N$ (as $N$ is square free) and $w_p = 1$, the elliptic curve $A$ has non-split multiplicative reduction at $p$. Thus there is a $q \in \mathbf{Q}_p^*$ and a Tate curve $E_q$ over $\mathbf{Q}_p$, such that $A$ is isomorphic to $E_q$ over an unramified quadratic extension $K$ of $\mathbf{Q}_p$. Now $E_q(\overline{\mathbf{Q}}_p) \cong \overline{\mathbf{Q}}_p/q^{\mathbf{Z}}$ over $\mathbf{Q}_p$; let $x \in \overline{\mathbf{Q}}_p$ be such that its image is in $E_q(\overline{\mathbf{Q}}_p)[r]$ corresponds to $P$. Since $rP = 0$, we have $x^r \in q^{\mathbf{Z}}$, i.e., $x^r = q^n$ for some $n \in \mathbf{Z}$. Let $\zeta_r$ be a primitive root of unity in $\overline{\mathbf{Q}}_p$, and let $q^{1/r}$ denote a choice of a root of $X^r = q$ in $\overline{\mathbf{Q}}_p$. Then $x = \zeta_r^a q^{b/r}$, for some $a, b \in \{0, \ldots, r-1\}$.

Since $K$ is unramified over $\mathbf{Q}_p$, its Galois group is generated by the Frobenius endomorphism, which we will denote by $\sigma$. Now $A(\overline{\mathbf{Q}}_p)[r]$ is the same as $E_q(\overline{\mathbf{Q}}_p)[r]$, except that the Galois action on $A(\overline{\mathbf{Q}}_p)[r]$ is twisted by a nontrivial unramified quadratic character. Thus since $P \in A(\mathbf{Q}_p)$, we have $\sigma(x) = 1/x$ modulo $q^{\mathbf{Z}}$. So the valuation of $\sigma(x)x$ is an integer multiple of that of $q$, and since $\sigma$ preserves valuations, we have $2b/r \in \mathbf{Z}$. If $b \neq 0$, then this is possible only if $r = 2$.

Now consider the case where $b = 0$. Then $a \neq 0$, and $x = \zeta_r^a$. If $\zeta_r \notin \mathbf{Q}_p$, then $\sigma(\zeta_r^a) = \zeta_r^{ap}$ and so $\zeta_r^{ap} = 1/\zeta_r^a$. Since $\zeta_r^a$ is also a primitive $r$-th root of unity, we have $r \mid (p+1)$. If $\zeta_r \in \mathbf{Q}_p$, then since $\sigma$ fixes $\zeta_r$, we have $\zeta_r = 1/\zeta_r$, i.e., $r = 2$. This proves the lemma. $\square$

**Remark 3.3.** In the lemma above, the hypothesis that $r$ is odd is necessary. For example, the elliptic curve $14A1$ has rational 2-torsion and $w_2 = 1$ (taking $r = p = 2$, we do not have $r \mid (p+1)$).

**Corollary 3.4.** *Let $r$ be an odd prime that divides the order of $A(\mathbf{Q})_{\text{tor}}$. If $r \mid N$, then $w_r = -1$.*

*Proof.* If $w_r = 1$, then by Lemma 3.2 (taking $p = r$), $r \mid (r+1)$, i.e., $r \mid 1$, which is impossible. So $w_r = -1$. □

Following [12, p. 77 and p. 70], by a holomorphic modular form in $\omega^{\otimes k}$ on $\Gamma_0(N)$ defined over a ring $R$, we mean a modular form in the sense of [11, §1.3] (see also [7, §VII.3]). Thus such an object is a rule which assigns to each pair $(E_{/T}, H)$, where $E$ is an elliptic curve over an $R$-scheme $T$ and $H$ is a finite flat subgroup scheme of $E_{/T}$ of order $N$, a section of $\omega_{E_{/T}}^{\otimes 2}$, where $\omega_{E_{/T}}$ is the sheaf of invariant differentials. If $r$ is a prime such that $r \nmid 6N$ and $f$ is a modular form of weight 2 on $\Gamma_0(N)$ with coefficients in $\mathbf{Z}[\frac{1}{6N}]$, then by [12, Lemma II.4.8], there is a holomorphic modular form in $\omega^{\otimes 2}$ on $\Gamma_0(N)$ defined over $\mathbf{Z}/r\mathbf{Z}$, which we will denote $f \bmod r$, such that the $q$-expansion of $f \bmod r$ agrees with the $q$-expansion of $f$ modulo $r$.

**Lemma 3.5** (Mazur)**.** *Let $R$ be a ring such that $1/N \in R$. Let $g$ be a holomorphic modular form in $\omega^{\otimes k}$ on $\Gamma_0(N)$ defined over $R$. Suppose that for some prime $p$ that divides $N$, the $q$-expansion of $g$ is a power series in $q^p$, i.e., there is $h(q) \in R[[q]]$ such that $g(q) = h(q^p)$. Then $h(q)$ is the $q$-expansion of a holomorphic modular form in $\omega^{\otimes k}$ on $\Gamma_0(N/p)$ defined over $R$.*

*Proof.* The lemma is proved in [12] under the condition that $N$ is prime, and $p = N$ (Lemma II.5.9 in loc. cit.). The same proof works mutatis mutandis to give the lemma above, with the only change to be made being to replace certain occurrences of $N$ by $p$ (e.g., $q^N$ becomes $q^p$ everywhere) and the occurrences of $N-1$ at the bottom of p. 84 in [12] by $\phi(N)$, where $\phi$ is the Euler $\phi$-function. □

**Proposition 3.6.** *Suppose there is a prime $r$ bigger than 3 such that $r$ divides the order of $A(\mathbf{Q})_{\mathrm{tor}}$. Then there is a prime $p$ that divides $N$ such that $w_p = -1$.*

*Proof.* Suppose, contrary to the conclusion of the lemma, that for every prime $p$ that divides $N$, we have $w_p = 1$. By Corollary 3.4, $r \nmid N$.

If $M$ is a postive integer, then let us say that a holomorphic modular form $g$ in $\omega^{\otimes 2}$ on $\Gamma_0(M)$ defined over $\mathbf{Z}/r\mathbf{Z}$ is *special at level $M$* if $a_n(g) \equiv \sigma(\frac{n}{(n,M)}) \prod_{p|M} (-1)^{\mathrm{ord}_p(n)} \bmod r$ for all positive integers $n$. Using Lemma 3.1 and the fact that $f$ is an eigenvector for all the Hecke operators, we see that $f \bmod r$ is special at level $N$.

**Claim.** *If $M$ is a square free integer and $g$ is a holomorphic modular form in $\omega^{\otimes 2}$ on $\Gamma_0(M)$ defined over $\mathbf{Z}/r\mathbf{Z}$ that is special at level $M$ and $s$ is a prime that divides $M$, then there exists a holomorphic modular form in $\omega^{\otimes 2}$ on $\Gamma_0(M/s)$ defined over $\mathbf{Z}/r\mathbf{Z}$ that is special at level $M/s$ (which is also square free).*

*Proof of the claim.* By Proposition 2.1, there is an Eisenstein series $E$ which is an eigenvector for all the Hecke operators, with $a_\ell(E) = \ell + 1$ for all primes $\ell \nmid M$, $a_p(E) = p$ for all primes $p$ that divide $M$ except $p = s$, and $a_s(E) = 1$. Let $p_1, \ldots, p_t$ be the distinct primes that divide $M/s$. Then for any positive integer $n$,

$$a_n(E) \equiv \sigma\left(\frac{n}{(n, M)}\right) \prod_{i=1}^{t} {p_i}^{\mathrm{ord}_{p_i}(n)} \bmod r.$$

Since by Lemma 3.2, $p_i \equiv -1 \bmod r$ for $i = 1, \ldots, t$, we see that $a_n(E) \equiv a_n(g) \bmod r$ if $n$ is coprime to $s$, and thus $(E(q) - g(q)) \bmod r$ is a power series in $q^s$, i.e., there is an $h(q) \in (\mathbf{Z}/r\mathbf{Z})[[q]]$ with $h(q^s) \equiv (E(q) - g(q)) \bmod r$. By Lemma 3.5, $h(q)$ is the $q$-expansion of a holomorphic modular form, which we again denote $h$, in $\omega^{\otimes 2}$ on $\Gamma_0(M/s)$ defined over $\mathbf{Z}/r\mathbf{Z}$.

Let $g' = h/2$. We shall now show that $g'$ is special of level $M/s$. Let $n$ be a positive integer, $m' = \frac{n}{(n,s)}$, and $e = \mathrm{ord}_s(n)$ (so $n = m's^e$). Then

$$a_n(h) = a_{m's^e}(h) \equiv a_{m's^{e+1}}(E - g) = a_{m's^{e+1}}(E) - a_{m's^{e+1}}(g) \bmod r. \tag{3.1}$$

Now $a_n(E) = a_{m'}(E)a_{s^{e+1}}(E)$ since $E$ is an eigenfunction and $a_n(g) \equiv a_{m'}(g)a_{s^{e+1}}(g) \bmod r$ since $g$ is special. Putting this in (3.1), we get

$$\begin{aligned} a_n(h) &\equiv a_{m'}(E)a_{s^{e+1}}(E) - a_{m'}(g)a_{s^{e+1}}(g) \\ &\equiv a_{m'}(g)(a_s(E)^{e+1} - a_s(g)^{e+1}) \bmod r, \end{aligned} \tag{3.2}$$

where the last congruence follows since $a_{m'}(g) \equiv a_{m'}(E) \bmod r$, considering that $m'$ is coprime to $s$. Now

$$a_s(E)^{e+1} - a_s(g)^{e+1} = 1 - (-1)^{e+1} \equiv 1 - s^{e+1} \bmod r, \tag{3.3}$$

since by Lemma 3.2, $s \equiv -1 \bmod r$. Also,

$$1 - s^{e+1} = (1 - s)(1 + s + \cdots + s^e) \equiv 2\sigma(s^e) \bmod r, \tag{3.4}$$

again considering that by Lemma 3.2, $s \equiv -1 \bmod r$. Thus putting (3.4) in (3.3), and the result in (3.2), we get

$$\begin{aligned} a_n(h) &\equiv a_{m'}(g) \cdot 2\sigma(s^e) \\ &\equiv 2\sigma\left(\frac{m'}{(m', M)}\right) \prod_{p \mid M} (-1)^{\mathrm{ord}_p(m')} \cdot \sigma(s^e) \bmod r, \end{aligned} \tag{3.5}$$

where the last congruence follows since $g$ is special at level $M$. Now since $n = m's^e$, with $m'$ coprime to $s$ and $s \nmid (M/s)$, we have

$$\begin{aligned} \sigma\left(\frac{m'}{(m', M)}\right)\sigma(s^e) = \sigma\left(\frac{m's^e}{(m', M)}\right) &= \sigma\left(\frac{m's^e}{(m's^e, M/s)}\right) \\ &= \sigma\left(\frac{n}{(n, M/s)}\right) \end{aligned} \tag{3.6}$$

and

$$\prod_{p|M}(-1)^{\mathrm{ord}_p(m')} = \prod_{p|M,\ p\neq s}(-1)^{\mathrm{ord}_p(m's^e)} = \prod_{p|(M/s)}(-1)^{\mathrm{ord}_p(n)}. \tag{3.7}$$

Using (3.6) and (3.7) in (3.5), and recalling that $g' = h/2$, we see that

$$a_n(g') \equiv \sigma\left(\frac{n}{(n, M/s)}\right) \prod_{p|(M/s)}(-1)^{\mathrm{ord}_p(n)} \bmod r,$$

i.e., $g'$ is special of level $M/s$. □

Starting with $f \bmod r$ (note that $r \nmid 6N$), and repeatedly using the claim, we see that there is a holomorphic modular form that is special of level 1, which is nontrivial since the coefficient of $q$ is 1 mod $r$ for a special form (of any level). But by [12, Lemma II.5.6(a)], there are no nontrivial holomorphic modular forms of level 1 in $\omega^{\otimes 2}$ defined over a field of characteristic other than 2 and 3. This contradiction proves the lemma. □

In the proof above, the idea of "lowering levels" and getting a contradiction is taken from an observation in [12], where $N$ is prime and the level is "lowered" only once (see the proof of Prop. II.14.1 on p. 114 of loc. cit.). We noticed that the Fourier coefficients work out so nicely (in view of Lemma 3.2) that the "level lowering" process can be repeated (when $N$ is not necessarily prime), giving the proof above.

**Remark 3.7.** After a first draft of this paper was written, based on numerical evidence, the author had conjectured in [1] that if $N$ is squarefree and the odd part of $E(\mathbf{Q})_{\mathrm{tor}}$ is non-trivial, then $w_p = -1$ for at least one prime $p$ that divides $N$. This was proved recently by D. Lorenzini (preprint). His techniques use explicit Weierstrass equations, and we hope that our proof of Proposition 3.6 may still be useful if the main result of this article were to be generalized to higher-dimensional abelian subvarieties $A$ of $J_0(N)$ associated to newforms.

## 4. Proof of Theorem 1.1

Recall that the hypotheses are that $N$ is a square free integer and $r$ is a prime such that $r \nmid 6N$ and $r$ divides the order of $A(\mathbf{Q})_{\mathrm{tor}}$. We have to show that $r$ divides the order of the cuspidal subgroup $C$.

If $p$ is a prime that divides $N$, then let $\delta_p = -w_p$ if $w_p = -1$ and $\delta_p = p$ if $w_p = 1$. By Proposition 3.6, for at least one $p$, we have $w_p = -1$, i.e., $\delta_p = 1$. Hence by Proposition 2.1, there is an Eisenstein series $E$ such that for all primes $\ell \nmid N$, we have $a_\ell(E) = \ell + 1$, and for all primes $p \,|\, N$, $a_p(E) = 1 = -w_p$ if $w_p = -1$ and $a_p(E) = p$ if $w_p = 1$. In view of Lemma 3.2, if $p \mid N$ and $w_p = 1$, we have $a_p(E) = p \equiv -1 = -w_p \bmod r$.

Considering that $f$ and $E$ are eigenfunctions for all the Hecke operators, we see from the paragraph above and by Lemma 3.1 that $a_n(f) \equiv a_n(E) \bmod r$ for all $n \geq 1$. Hence $(f(q) - E(q)) \bmod r$ is a constant; call this constant $c$. Since $r \nmid 6N$, we may consider the holomorphic modular form $(f - E) \bmod r$ in $\omega^{\otimes 2}$ on $\Gamma_0(N)$ defined over $\mathbf{Z}/r\mathbf{Z}$. Using Lemma 3.5, for any prime $p$ dividing $N$ we get a holomorphic modular form in $\omega^{\otimes 2}$ on $\Gamma_0(N/p)$ defined over $\mathbf{Z}/r\mathbf{Z}$, whose $q$-expansion is the same constant $c$. By repeating this process (which we can do since at each stage we have a $q$-expansion that is constant – in fact, the same constant $c$), we get a holomorphic modular form in $\omega^{\otimes 2}$ on $\Gamma_0(1)$ defined over $\mathbf{Z}/r\mathbf{Z}$, whose $q$-expansion is $c$. By [12, Lemma II.5.6(a)], there are no nontrivial holomorphic modular forms of level 1 in $\omega^{\otimes 2}$ defined over a field of characteristic other than 2 and 3. Thus $c \equiv 0 \bmod r$, and so $a_n(f) \equiv a_n(E) \bmod r$ for $n = 0$ as well. Hence $f \equiv E \bmod r$.

To $E$ is associated a subgroup $C_E$ of $C$ by Stevens (see [15, Def. 1.8.5] and [16, Def. 4.1]). Since $r \nmid N$, by Lemma 3.1, $a_r \equiv (1 + r) \equiv 1 \bmod r$; in particular, $f$ is ordinary at $r$. By [17, Thm. 0.4], $A[r] \cap C_E \neq 0$, and thus $r$ divides the order of $A \cap C$. The fact that $r$ divides the order of $C_E$ follows from the intermediate result Prop. 1.9 of [17] as well. This proves part (1) of Theorem 1.1. As mentioned in the introduction, part (2) follows from part (1) by taking $\ell = r$ in [9, Thm. 1.2] (Dummigan's theorem in turn follows from the proof of Prop. 5.3 in [18]).

**Remark 4.1.** Neil Dummigan remarked to us that one need not use [9, Thm. 1.2] to deduce part (2) of Theorem 1.1 from part (1) since our methods prove a special case of [9, Thm. 1.2] that if $A'$ is an elliptic curve of square free conductor $N$ having a rational point of order $r$ for a prime $r$ such that $r \nmid 6N$, then the optimal curve $A$ in the isogeny class of $A'$ also has a rational point of order $r$. Clearly, this shows that part (2) implies part (1). The proof of the claim above is as follows: Lemma 3.1 holds with $A$ replaced by $A'$ under the additional hypothesis that $r$ is odd (by considering reduction modulo $\ell$, we see that if $\ell$ is a prime such that $\ell \nmid N$, then $r$ divides $|A'(\mathbf{F}_\ell)| = |A(\mathbf{F}_\ell)| = a_\ell(f) - (1 + \ell)$) and Lemma 3.2 also holds with $A$ replaced by $A'$ (the fact that $w_p = 1$ implies that $A$ has non-split multiplicative reduction; hence so does $A'$ and the proof goes through with $A$ replaced by $A'$). In the proofs of Proposition 3.6 and Theorem 1.1, the only place where the hypothesis that $A$ has a rational point of order $r$ is used is in quoting Lemmas 3.1 and 3.2. Since the conclusions of these Lemmas hold under the hypothesis that $A'$ (instead of $A$) has a rational point of order $r$ (and the hypothesis that $r$ is odd, which is already assumed in Theorem 1.1), the proof of Theorem 1.1 goes through to prove that $A$ has a rational point of order $r$, as claimed.

## References


[1] A. Agashe, "Conjectures concerning the orders of the torsion subgroup, the arithmetic component groups, and the cuspidal subgroup", *Exp. Math.* **22** (2013), no. 4, p. 363-366.

[2] A. Agashe & W. A. Stein, "Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero", *Math. Comput.* **74** (2005), no. 249, p. 455-484.

[3] A. O. L. Atkin & J. Lehner, "Hecke operators on $\Gamma_0(m)$", *Math. Ann.* **185** (1970), p. 134-160.

[4] C. Breuil, B. Conrad, F. Diamond & R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises", *J. Am. Math. Soc.* **14** (2001), no. 4, p. 843-939.

[5] S.-K. Chua & S. Ling, "On the rational cuspidal subgroup and the rational torsion points of $J_0(pq)$", *Proc. Am. Math. Soc.* **125** (1997), no. 8, p. 2255-2263.

[6] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997, 376 pages.

[7] P. Deligne & M. Rapoport, "Les schémas de modules de courbes elliptiques", in *Modular Functions of one Variable II, Proc. internat. Summer School, Univ. Antwerp 1972*, Lect. Notes Math., vol. 349, Springer, 1973, p. 143-316.

[8] F. Diamond & J. Im, "Modular forms and modular curves", in *Seminar on Fermat's last theorem*, CMS Conf. Proc., vol. 17, American Mathematical Society (publ. for the Canadian Mathematical Society), 1995, p. 39-133.

[9] N. Dummigan, "Rational torsion on optimal curves", *Int. J. Number Theory* **1** (2005), no. 4, p. 513-531.

[10] M. Emerton, "Optimal quotients of modular Jacobians", *Math. Ann.* **327** (2003), no. 3, p. 429-458.

[11] N. M. Katz, "$p$-adic properties of modular schemes and modular forms", in *Modular Functions of one Variable III, Proc. internat. Summer School, Univ. Antwerp 1972*, Lect. Notes Math., vol. 350, Springer, 1973, p. 69-190.

[12] B. Mazur, "Modular curves and the Eisenstein ideal", *Publ. Math., Inst. Hautes Étud. Sci.* **47** (1977), p. 33-186.

[13] M. Ohta, "Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II", *Tokyo J. Math.* **37** (2014), no. 2, p. 273-318.

[14] W. A. Stein, "The Cuspidal Subgroup of $J_0(N)$", `http://wstein.org/Tables/cuspgroup/index.html`.

[15] G. Stevens, *Arithmetic on modular curves*, Progress in Mathematics, vol. 20, Birkhäuser, 1982, xvii+214 pages.

[16] ———, "The cuspidal group and special values of $L$-functions", *Trans. Am. Math. Soc.* **291** (1985), no. 2, p. 519-550.

[17] S.-L. Tang, "Congruences between modular forms, cyclic isogenies of modular elliptic curves and integrality of $p$-adic $L$-functions", *Trans. Am. Math. Soc.* **349** (1997), no. 2, p. 837-856.

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

[19] H. Yoo, "On Eisenstein ideals and the cuspidal group of $J_0(N)$", *Isr. J. Math.* **214** (2016), no. 1, p. 359-377.

[20] ———, "Rational torsion points on Jacobians of modular curves", *Acta Arith.* **172** (2016), no. 4, p. 299-304.



Amod Agashe
Department of Mathematics
Florida State University
1017 Academic Way
Tallahassee, FL 32306, USA
*E-mail*: `agashe@math.fsu.edu`
*URL*: `http://www.math.fsu.edu/~agashe/math.html`