Reducibility and rational torsion in elliptic curves

Amod Agashe and Matthew Winters

Abstract

Let A be an optimal elliptic curve over $\mathbf{Q}$ and let N denote its conductor. Suppose N is square-free and r is a prime such that $r \nmid 6N$. We show that if $A[r]$ is reducible, then A has a rational r-torsion point. We mention some applications of this result, including an application to the second part of the Birch and Swinnerton-Dyer conjecture for A.

1 Introduction

Let A be an optimal elliptic curve over $\mathbf{Q}$, i.e., if N denotes the conductor of A, then A is the quotient of $J_0(N)$ associated to a newform f of weight 2 on $\Gamma_0(N)$ with integer Fourier coefficients. If A has a rational point of order a prime r, then clearly $A[r]$ is reducible as a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. The converse need not be true. For example, for $A = 99d1$ (the notation is as in [Cre97]), $A[5]$ is reducible, but A has no rational 5-torsion. However, the first author had conjectured:

Conjecture 1.1. *[Aga13, Conjecture 2.5] Suppose N is square-free, i.e., A is semistable, and r is an odd prime. If $A[r]$ is reducible, then A has a rational r-torsion point (recall that we are assuming that A is optimal).*

In this article, we prove

Theorem 1.2. *Suppose N is square-free and r a prime such that $r \nmid 6N$. If $A[r]$ is reducible, then A has a rational r-torsion point.*

Thus we prove the conjecture above, except for $r = 3$ and for $r \mid N$. The proof of the theorem is given in Section 3. The idea of the proof is very similar to that of the main theorem of [Aga18]: we use the hypotheses to show 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 the theorem (but

relaxing the hypothesis that $r \nmid N$), for at least one prime p that divides N, the sign of the Atkin-Lehner involution at p acting on f is -1, which is an interesting result on its own (see Proposition 2.6). Given the congruence between f and E, and the fact that f is ordinary at r (which we show), a result of Tang [Tan97, Thm 0.4] tells us that $A[r]$ has nontrivial intersection with a subgroup of the cuspidal group C, which is rational (since N is square-free), giving us the theorem.

In Section 2, we prove some results regarding the Fourier coefficients of f that are needed to show the congruence alluded to above, and in Section 3, we use these results to prove Theorem 1.2. In the rest of this section, we mention some applications of our theorem.

By a theorem of Mazur ([Maz77, Theorem III.5.1]), if r a prime bigger than 7, then r does not divide the order of the torsion subgroup of any elliptic curve over $\mathbf{Q}$. So we get:

Corollary 1.3. *Suppose N is square-free and r a prime such that $r > 7$ and $r \nmid N$. Then $A[r]$ is irreducible.*

This result is already known by [Maz78, Theorem 4]; however, the proof is different. In this context, we should also point out that if one drops the hypothesis that N is square-free, then there is a finite list of primes r such that an elliptic curve has a rational isogeny of degree r: see [Maz78, Theorem 1].

As mentioned in [Ser72, p. 307], if A is semistable (it need not be optimal) and r is a prime such that $A[r]$ is reducible as a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then this representation can be put in matrix form as

$$\begin{bmatrix} \chi' & * \\ 0 & \chi'' \end{bmatrix},$$

where χ' and χ'' are characters of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that one of them is the identity character and the other is the mod r cyclotomic character. If χ' is the identity character, then A has a rational point of order r; however, one does not know if χ' is the identity character (as per loc. cit.). Theorem 1.2 above implies that under the additional hypotheses that $r \nmid 6N$ and A is optimal, one may take χ' to be the identity character.

In the rest of this section, we discuss an application of our theorem to the second part of the Birch and Swinnerton-Dyer (BSD) conjecture for A. Let $L_A(s)$ denote the L-function of A. Let K_A denote the coefficient of the leading term of the Taylor series expansion of $L_A(s)$ at $s = 1$, and let R_A denote the regulator of A. Let Ω_A denote the volume of $A(\mathbf{R})$ calculated

using a generator of the group of invariant differentials on the Néron model of A. Let $Ш_A$ denote the Shafarevich-Tate group of A, which we assume is finite. If p is a prime that divides N, then let $c_p(A)$ denote the order of the arithmetic component group of A at p (also called the Tamagawa number of A at p). Then the *second part of the BSD conjecture* asserts the formula:

$$\frac{K_A}{\Omega_A \cdot R_A} \stackrel{?}{=} \frac{|Ш_A| \cdot \prod_p c_p(A)}{|A(\mathbf{Q})_{\mathrm{tor}}|^2} \ . \tag{1}$$

Based on numerical evidence, the first author has conjectured:

Conjecture 1.4. *[Aga13, Conjecture 2.4] If an odd prime ℓ divides $c_p(A)$ for some prime p that divides N, then either ℓ divides $|A(\mathbf{Q})_{\mathrm{tor}}|$ or the newform f is congruent to a newform of level dividing N/p (for all Fourier coefficients whose indices are coprime to $N\ell$) modulo a prime ideal over ℓ in a number field containing the Fourier coefficients of both newforms.*

This indicates some conjectural cancellation between the numerator and denomintor of the right side of the BSD formula (1) above (for more on such cancellations, see [Aga13]). Towards the conjecture above, the first author proved:

Proposition 1.5. *[Aga13, Proposition 2.3] Let ℓ be an odd prime such that either $\ell \nmid N$ or for all primes r that divide N, $\ell \nmid (r-1)$. If ℓ divides the order of the geometric component group of A at p for some prime $p||N$, then either $A[\ell]$ is reducible or the newform f is congruent to a newform of level dividing N/p (for all Fourier coefficients whose indices are coprime to $N\ell$) modulo a prime ideal over ℓ in a number field containing the Fourier coefficients of both newforms.*

Note that if p is a prime that divides N, and if a prime ℓ divides $c_p(A)$, then ℓ also divides the order of the geometric component group of A at p.

In view of Theorem 1.2, from the proposition above, we get:

Corollary 1.6. *Suppose N is squarefree and let ℓ be a prime such that $\ell \nmid 6N$. If ℓ divides the order of the geometric component group of A at p for some prime $p \mid N$, then either ℓ divides $|A(\mathbf{Q})_{\mathrm{tor}}|$ or the newform f is congruent to a newform of level dividing N/p (for all Fourier coefficients whose indices are coprime to $N\ell$) modulo a prime ideal over ℓ in a number field containing the Fourier coefficients of both newforms.*

The corollary above is a better result towards Conjecture 1.4 than the proposition above, when the hypothesis in the first line of the corollary hold.

Since, as mentioned earlier, if r a prime bigger than 7, then r cannot not divide $|A(\mathbf{Q})_{\mathrm{tor}}|$, we also have:

Corollary 1.7. *Suppose N is squarefree and let ℓ be a prime such that $\ell > 7$ and $\ell \nmid N$. If ℓ divides the order of the geometric component group of A at p for some prime $p \mid N$, then the newform f is congruent to a newform of level dividing N/p (for all Fourier coefficients whose indices are coprime to $N\ell$) modulo a prime ideal over ℓ in a number field containing the Fourier coefficients of both newforms.*

Acknowledgement: We are grateful to E. Ghate for some comments regarding our main result.

2 Some results on Fourier coefficients

Let $a_n = a_n(f)$ denote the n-th Fourier coefficient of f. If p is a prime that divides N, then let w_p denote the sign of the Atkin-Lehner involution W_p acting on f. Let $\mathbf{T}$ denote the Hecke algebra, and let $I_f = \mathrm{Ann}_{\mathbf{T}} f$. Consider the quotient map $\mathbf{T} \to \mathbf{T}/I_f \cong \mathbf{Z}$, where in the last map, T_n maps to a_n for all integers $n \geq 1$. Let $\mathfrak{m}$ denote the inverse image of $(r) \subseteq \mathbf{Z}$. Then $\mathfrak{m}$ is a maximal ideal. Let $\rho_{\mathfrak{m}}$ denote the canonical representation associated to $\mathfrak{m}$ (see [Rib90, Prop. 5.1]). Then $\rho_{\mathfrak{m}}$ is the semisimplification of $A[r]$, and hence is reducible. Let r be a prime such that $A[r]$ is reducible. We do not assume the hypothesis in the main theorem that $r \nmid 6N$ yet.

The following lemma is perhaps well known.

Lemma 2.1. *For all primes $\ell \nmid N$, we have $a_\ell(f) \equiv 1 + \ell \bmod r$ and for all primes $p \mid N$, we have $a_p(f) = -w_p$.*

Proof. Suppose $\ell \nmid N$. Since $\rho_{\mathfrak{m}}$ is reducible, it follows from [Yoo16, p. 362] that $T_\ell - \ell - 1 \in \mathfrak{m}$. Thus the image of T_ℓ in $\mathbf{T}/\mathfrak{m}$ is $\ell + 1$, but $\mathbf{T}/\mathfrak{m} \cong \mathbf{Z}/(r)$, and this image is a_ℓ. 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. □

Next, we have:

Proposition 2.2. *[Aga18, 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 $a_p(E) = \delta_p$.*

Keeping in mind the strategy of the proof of our main theorem (Theorem 1.2) mentioned in the introduction, we see from the lemma and proposition above that coming up with an Eisenstein series E such that $a_p(f) \equiv a_p(E) \bmod r$ for all primes $p \nmid N$ is rather easy. Proving the congruence for all $p \mid N$ for a suitable Eisenstein series is the tricky part, for which we need the results below.

Lemma 2.3 (Yoo)**.** *Suppose $r \geq 3$. If p is a prime such that $p \mid N$, $p \neq r$, and $w_p = 1$, then $p \equiv -1 \mod r$.*

Proof. The argument is essentially given in the proof of [Yoo16, Lemma 2.1]; we repeat it here for the convenience of the reader. Since $\rho_{\mathfrak{m}}$ is reducible, $\rho_{\mathfrak{m}} \cong \mathbf{1} \oplus \chi_r$, where $\mathbf{1}$ is the trivial character and χ_r is the mod r cyclotomic character (in [Yoo19, Prop 2.1], this result is attributed to work of Ribet, but it also follows from the discussion in Section 1 taken from [Ser72]). On the other hand, the semisimplification of the restriction of $\rho_{\mathfrak{m}}$ to $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ is isomorphic to $\epsilon \oplus \epsilon\chi_r$, where ϵ is the unramified quadratic character with $\epsilon(\mathrm{Frob})_p = a_p = -1$ because $\mathfrak{m}$ is p-new (cf. [DDT94, Theorem 3.1(e)]). From this, we get $p \equiv -1 \mod r$. □

Lemma 2.4. *Suppose $r \mid N$. Then $w_r = -1$.*

Proof. As mentioned on p. 363 in [Yoo16], we have $U_r \equiv 1 \mod \mathfrak{m}$ by [Rib, Lemma 1.1]; it is mentioned on p. 362 in [Yoo16] that the quoted lemma also follows from the result by Deligne given in [Edi92, Theorem 2.5]. So if $w_r = 1$, then $a_r = -1$, and so $-1 \equiv 1 \mod \mathfrak{m}$, i.e. $2 \in \mathfrak{m}$, which is not possible since r is odd; thus $w_r = -1$. □

As mentioned in the introduction, the proof of the main theorem of this article is similar to that of the main theorem of [Aga18], and the rest of this paper is nearly identical to the part of [Aga18] that comes after the proof of Corollary 3.4 in loc. cit., with a small number of necessary changes. However, we have repeated the discussion (with the necessary changes) in order to be clear and complete.

Following [Maz77, 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 [Kat73, §1.3] (see also [DR73, § 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 [Maz77, 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 2.5 (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 [Maz77] 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 [Maz77] by $\phi(N)$, where ϕ is the Euler ϕ-function. □

Proposition 2.6. *Suppose $r > 3$. Then there is a prime p that divides N such that $w_p = -1$.*

Proof. By Lemma 2.4, if $r \mid N$, then $w_r = -1$, and we are done. Thus we may assume henceforth that $r \nmid N$. Suppose, contrary to the conclusion of the Proposition, that for every prime p that divides N, we have $w_p = 1$. Then by Lemma 2.3, for every prime p that divides N, we have $p \equiv -1 \bmod r$ (note that $p \neq r$ since $r \nmid N$).

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 2.1 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. By Proposition 2.2, 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 $p_i \equiv -1 \bmod r$ 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 $h(q^s)$ equal to $(E(q) - g(q)) \bmod r$. By Lemma 2.5, $h(q)$ 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

$$a_n(h) = a_{m's^e}(h) \equiv a_{m's^{e+1}}(E - g) = a_{m's^{e+1}}(E) - a_{m's^{e+1}}(g) \bmod r. \quad (2)$$

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 (2), we get

$$\begin{aligned} a_n(h) &\equiv a_{m'}(E)a_{s^{e+1}}(E) - a_{m'}(g)a_{s^{e+1}}(g) \\ &\equiv a_{m'}(g)(a_s(E)^{e+1} - a_s(g)^{e+1}) \bmod r, \end{aligned} \quad (3)$$

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

$$a_s(E)^{e+1} - a_s(g)^{e+1} = 1 - (-1)^{e+1} \equiv 1 - s^{e+1} \bmod r, \quad (4)$$

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

$$1 - s^{e+1} = (1 - s)(1 + s + \cdots + s^e) \equiv 2\sigma(s^e) \bmod r, \quad (5)$$

again considering that $s \equiv -1 \bmod r$. Thus putting (5) in (4), and the result in (3), we get

$$a_n(h) \equiv a_{m'}(g) \cdot 2\sigma(s^e) \equiv 2\sigma\left(\frac{m'}{(m', M)}\right) \prod_{p|M} (-1)^{\mathrm{ord}_p(m')} \cdot \sigma(s^e) \bmod r, \quad (6)$$

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

$$\sigma\left(\frac{m'}{(m', M)}\right)\sigma(s^e) = \sigma\left(\frac{m's^e}{(m', M)}\right) = \sigma\left(\frac{m's^e}{(m's^e, M/s)}\right) = \sigma\left(\frac{n}{(n, M/s)}\right) \quad (7)$$

and

$$\prod_{p|M}(-1)^{\mathrm{ord}_p(m')} = \prod_{p|M,\ p\neq s}(-1)^{\mathrm{ord}_p(m's^e)} = \prod_{p|(M/s)}(-1)^{\mathrm{ord}_p(n)}. \tag{8}$$

Using (7) and (8) in (6), 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 [Maz77, 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. □

As mentioned in [Aga18], in the proof above, the idea of "lowering levels" and getting a contradiction is taken from an observation in [Maz77], 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 that the "level lowering" process can be repeated (when N is not necessarily prime), giving the proof above.

3 Proof of Theorem 1.2

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 2.6, for at least one p, we have $w_p = -1$, i.e., $\delta_p = 1$. Hence by Proposition 2.2, 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 2.3, if $p \mid N$ and $w_p = 1$ (note that $p \neq r$ since $r \nmid N$), 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 2.1 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 2.5, 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 [Maz77, 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 [Ste82, Def. 1.8.5] and [Ste85, Def. 4.1]). Since $r \nmid N$, by Lemma 2.1, $a_r \equiv (1 + r) \equiv 1 \bmod r$; in particular, f is ordinary at r. Then by [Tan97, Thm 0.4], $A[r] \cap C_E \neq 0$. Since C_E is rational (as N is square-free), we find that A has a rational r-torsion point.

References

[Aga13] Amod Agashe, *Conjectures concerning the orders of the torsion subgroup, the arithmetic component groups, and the cuspidal subgroup*, Exp. Math. **22** (2013), no. 4, 363–366. MR 3171097

[Aga18] ———, *Rational torsion in elliptic curves and the cuspidal subgroup*, J. Théor. Nombres Bordeaux **30** (2018), no. 1, 81–91. MR 3809710

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[DDT94] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Internat. Press, Cambridge, MA, 1994, pp. 1–154.

[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.

[Edi92] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594.

[Kat73] N. M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972) (Berlin), Springer, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350.

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

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

[Rib] K. A. Ribet.

[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.

[Ser72] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Ste82] G. Stevens, *Arithmetic on modular curves*, Birkhäuser Boston Inc., Boston, Mass., 1982. MR 87b:11050

[Ste85] Glenn Stevens, *The cuspidal group and special values of L-functions*, Trans. Amer. Math. Soc. **291** (1985), no. 2, 519–550.

[Tan97] Shu-Leung Tang, *Congruences between modular forms, cyclic isogenies of modular elliptic curves and integrality of p-adic L-functions*, Trans. Amer. Math. Soc. **349** (1997), no. 2, 837–856.

[Yoo16] Hwajong Yoo, *On Eisenstein ideals and the cuspidal group of* $J_0(N)$, Israel J. Math. **214** (2016), no. 1, 359–377. MR 3540618

[Yoo19] ———, *Non-optimal levels of a reducible* $\bmod \ell$ *modular representation*, Trans. Amer. Math. Soc. **371** (2019), no. 6, 3805–3830. MR 3917209