A VISIBLE FACTOR OF THE HEEGNER INDEX

Amod Agashe

ABSTRACT. Let E be an optimal elliptic curve over $\mathbf{Q}$ of conductor N, such that the L-function of E vanishes to order one at $s = 1$. Let K be a quadratic imaginary field in which all the primes dividing N are split and such that the L-function of E over K also vanishes to order one at $s = 1$. In view of the Gross-Zagier theorem, the Birch and Swinnerton-Dyer conjecture says that the index in $E(K)$ of the subgroup generated by the Heegner point is equal to the product of the Manin constant of E, the Tamagawa numbers of E, and the square root of the order of the Shafarevich-Tate group of E (over K). We extract an integer factor from the index mentioned above and relate this factor to certain congruences of the newform associated to E with eigenforms of analytic rank bigger than one. We use the theory of visibility to show that, under certain hypotheses (which includes the first part of the Birch and Swinnerton-Dyer conjecture on rank), if an odd prime q divides this factor, then q divides the order of the Shafarevich-Tate group, as predicted by the Birch and Swinnerton-Dyer conjecture.

1. Introduction and results

Let N be a positive integer. Let $X = X_0(N)$ denote the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$, and let $J = J_0(N)$ denote the Jacobian of X, which is an abelian variety over $\mathbf{Q}$. Let $\mathbf{T}$ denote the Hecke algebra, which is the subring of endomorphisms of $J_0(N)$ generated by the Hecke operators (usually denoted T_ℓ for $\ell \nmid N$ and U_p for $p \mid N$). If g is an eigenform of weight 2 on $\Gamma_0(N)$, then let $I_g = \mathrm{Ann}_{\mathbf{T}} g$ and let A_g denote the quotient abelian variety $J/I_g J$, which is defined over $\mathbf{Q}$. Also, if g is an eigenform of weight 2 on $\Gamma_0(N)$, then the order of vanishing of the L-function $L(g, s)$ at $s = 1$ is called the *analytic rank of g*. Let f be a newform of weight 2 on $\Gamma_0(N)$ whose analytic rank is one and that has integer Fourier coefficients. Then $E = A_f$ is an elliptic curve whose L-function vanishes to order one at $s = 1$, i.e., E has analytic rank one (in general, the *analytic rank* of an elliptic curve is the order of vanishing of its L-function at $s = 1$). By [BCDT01], up to isogeny, all elliptic curves of analytic rank one arise this way. We denote the quotient map $J \to J/I_f = E$ by π.

Let K be a quadratic imaginary field of discriminant not equal to -3 or -4, such that all primes dividing N split in K and the L-function of E over K vanishes to order one at $s = 1$ (such a K exists by [Wal85]). Choose an ideal $\mathcal{N}$ of the ring of integers $\mathcal{O}_K$ of K such that $\mathcal{O}_K/\mathcal{N} \cong \mathbf{Z}/N\mathbf{Z}$. Then the complex tori $\mathbf{C}/\mathcal{O}_K$ and $\mathbf{C}/\mathcal{N}^{-1}$ define elliptic curves related by a cyclic N-isogeny, hence a complex valued point x of $X_0(N)$. This point, called a Heegner point (on $X_0(N)$), is defined over the Hilbert class field H of K. Let $P \in J(K)$ be the class of the divisor $\sum_{\sigma \in \mathrm{Gal}(H/K)} ((x) - (\infty))^\sigma$. We remark that sometimes P is called a Heegner point (on $J_0(N)$), and $\pi(P)$ is also called a

---

Heegner point (on E). We will use the term "Heegner point" rarely in this paper, and it should be clear from the context what point we mean.

Let $\text{III}(E/\mathbf{Q})$ and $\text{III}(E/K)$ denote the Shafarevich-Tate group of E over $\mathbf{Q}$ and K respectively. The inflation-restriction sequence shows that the natural map $\text{III}(E/\mathbf{Q}) \rightarrow \text{III}(E/K)$ has kernel a finite group of order a power of 2. By [GZ86, §V.2:(2.1)], since E/K has analytic rank one, $\pi(P)$ has infinite order, and by work of Kolyvagin (e.g., see [Kol90, Thm. A] or [Gro91, Thm. 1.3]), $E(K)$ has rank one and $\text{III}(E/K)$ is finite. In particular, $\text{III}(E/\mathbf{Q})$ is also finite, and the index in $E(K)$ of the subgroup generated by $\pi(P)$ is finite; note that this subgroup is just $\pi(\mathbf{T}P)$. By [GZ86, §V.2:(2.2)], the Birch and Swinnerton-Dyer conjecture says:

Conjecture 1.1 (Birch and Swinnerton-Dyer, Gross-Zagier).

$$(1) \qquad |E(K)/\pi(\mathbf{T}P)| \stackrel{?}{=} c_E \cdot \prod_{p|N} c_p(E) \cdot \sqrt{|\text{III}(E/K)|} \ ,$$

where c_E is the Manin constant of E (conjectured to be one), and $c_p(E)$ is the Tamagawa number of E at the prime p (i.e., the order of the arithmetic component group of E at the prime p – see Section 4 for details).

The theory of Euler systems, initiated by Kolyvagin [Kol90], can be used to show that under certain hypotheses and staying away from certain primes, the actual order of $\text{III}(E/K)$ divides the order predicted by the conjectural formula (1) (equivalently, that the right side of (1) divides the left side). For example, we have the following (see[Jet08, Cor. 1.5]):

Theorem 1.2 (Jetchev). *Suppose that ℓ is a prime such that $\ell \nmid 2N$, the image $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acting on $E[\ell]$ is isomorphic to $\text{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$, and ℓ divides at most one $c_p(E)$. Then*

$$\text{ord}_\ell(|\text{III}(E/K)|) \leq \text{ord}_\ell(|\text{III}(E/K)|_{\text{an}}),$$

where $|\text{III}(E/K)|_{\text{an}}$ denotes the value of $|\text{III}(E/K)|$ predicted by formula (1).

Our ultimate goal is to try to prove results in a direction opposite to those arising from the theory of Euler systems, i.e., that the left side of (1) divides the right side. Note that this often requires one to produce non-trivial elements of the Shafarevich-Tate group when the Birch and Swinnerton-Dyer conjecture predicts their existence, which is a difficult problem. When the elliptic curve has analytic rank zero, to our knowlegde, the only two general methods that give theoretical results in this direction are Ribet's method (more precisely, the adaptation of Ribet's proof of the converse to Herbrand's theorem, as in the work of Skinner-Urban, unpublished) and the theory of visibility (see [Aga10]). We remark that the theory of Euler systems can also be used to construct non-trivial elements of the Shafarevich-Tate group under certain hypotheses (e.g., see [McC91, p. 2]); however, to our knowledge, this construction has not been linked theoretically to predictions coming from the Birch and Swinnerton-Dyer conjecture. The theory of visibility can be applied to elliptic curves of any analytic rank, and in this article, we show that it gives fruitful results vis-a-vis the Birch and Swinnerton-Dyer conjectural formula for the order of the Shafarevich-Tate group in the analytic rank one case as well, in the direction we are interested in. In particular, we shall extract an integer factor of the left side of (1) which we will relate

to congruences of f with eigenforms of analytic rank bigger than one. Under certain hypotheses, these congruences will in turn be related to the right hand side of (1) using the theory of visibility. We now describe our results more precisely.

Let T be a non-empty set of Galois conjugacy classes of newforms of level dividing N and not containing f. Let S_T denote the subspace of $S_2(\Gamma_0(N), \mathbf{C})$ spanned by the forms $g(dz)$, where g runs over elements in the Galois conjugacy classes in T, and d ranges over the divisors of N/N_g, where N_g denote the level of g. Let I_T denote the annihilator of S_T under the action of $\mathbf{T}$. Recall that $J = J_0(N)$, and let J' denote the quotient abelian variety $J/(I_f \cap I_T)J$. For example, if T consists of the Galois conjugacy classes of all newforms of level dividing N except the conjugacy class of f, then $I_f \cap I_T = 0$, and so $J' = J$ in this case. The quotient map $\pi : J \to J/I_f J$ factors through $J' = J/(I_f \cap I_T)J$. Let π' denote the map $J' \to E$ and π'' the map $J \to J'$ in this factorization. Let B' denote the kernel of π'. Thus we have the following diagram:

$$
\begin{array}{ccccccccc}
 & & & & J & & & & \\
 & & & \pi'' \swarrow & \Big\downarrow & \searrow \pi & & & \\
0 & \longrightarrow & B' & \longrightarrow & J' & \xrightarrow{\ \pi'\ } & E & \longrightarrow & 0
\end{array}
$$

Note that J' and B' depend on the choice of the set T; we have suppressed the dependency in the notation for simplicity (for certain interesting choices of T, see Section 2). Let E' denote the image of $E^\vee \subseteq J$ in J' under the quotient map $\pi'' : J \to J'$ and let $\pi''(\mathbf{T}P)_f$ denote the free part of $\pi''(\mathbf{T}P)$. As we show in Lemma 3.1 below,

$$
\begin{aligned}
(2) \quad & |E(K)/\pi(\mathbf{T}P)| \\
& = \left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\!\left(H^1(K, B') \to H^1(K, J') \right) \right| \cdot \frac{\left| \frac{B'(K)+E'(K)}{B'(K)+\pi''(\mathbf{T}P)_f \cap E'(K)} \right|}{\left| \frac{B'(K)+\pi''(\mathbf{T}P)}{B'(K)+\pi''(\mathbf{T}P)_f \cap E'(K)} \right|} \ .
\end{aligned}
$$

Suppose in this paragraph that q is a prime that does not divide the order of the torsion subgroup of $\pi''(\mathbf{T}P)$ and that f is not congruent to a newform g in S_T of analytic rank one modulo a prime ideal over q in the ring of integers of the number field generated by the coefficients of f and g (for Fourier coefficients of index coprime to Nq). Then by Lemma 3.2 below, q does not divide the term $\left| \frac{B'(K)+\pi''(\mathbf{T}P)}{B'(K)+\pi''(\mathbf{T}P)_f \cap E'(K)} \right|$ in the denominator on the right side of equation (2). If x is a positive integer and r is a prime, then let x_r denote the highest power of r that divides x. Then in view of equation (2), the Birch and Swinnerton-Dyer conjectural formula (1) says:

$$
\begin{aligned}
(3) \quad & \left(c_{A_f} \cdot \prod_{p | N} c_p(E) \right)_q \cdot \sqrt{|\Sha(E/K)|_q} \\
& \overset{?}{=} \left| \frac{J'(K)}{B'(K) + E'(K)} \right|_q \cdot \left| \ker\!\left(H^1(K, B') \to H^1(K, J') \right) \right|_q \cdot \\
& \quad \left| \frac{B'(K) + E'(K)}{B'(K) + \pi''(\mathbf{T}P)_f \cap E'(K)} \right|_q .
\end{aligned}
$$

In particular, the conjecture predicts that the product

$$
\left| \frac{J'(K)}{B'(K) + E'(K)} \right|_q \cdot \left| \ker\!\left(H^1(K, B') \to H^1(K, J') \right) \right|_q
$$

divides $c_E \cdot \prod_{p|N} c_p(E) \cdot \sqrt{|\text{III}(E/K)|}$.

We have the following result towards this predicted divisibility:

Theorem 1.3. *Let q be a prime that divides the product*

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\left(H^1(K, B') \rightarrow H^1(K, J')\right) \right|.$$

1) Then q divides the order of $B' \cap E'$, and there is an eigenform g in S_T such that f is congruent to g modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the Fourier coefficients of f and g.

2) Suppose that $q \nmid 2N$ and that $E[q]$ is an irreducible representation of the absolute Galois group of $\mathbf{Q}$. Assume that the first part of the Birch and Swinnerton-Dyer conjecture holds for all quotients of $J_0(N)$ associated to eigenforms of analytic rank greater than one. Suppose that for all primes $p \mid N$, $p \not\equiv -w_p \pmod{q}$, where w_p is the sign of the Atkin-Lehner involution W_p acting on f and that for all primes p such that $p^2 \mid N$, we have $p \not\equiv -1 \pmod{q}$. Assume that f is not congruent to a newform g in T of level N and analytic rank one modulo a prime ideal over q in the ring of integers of the number field generated by the coefficients of f and g. Suppose, moreover, that for all primes $p \mid N$, f is not congruent to a newform g of level dividing N/p (for Fourier coefficients of index coprime to Nq) modulo a prime ideal over q in the ring of integers of the number field generated by the coefficients of f and g. Then q divides $|\text{III}(E/\mathbf{Q})|$ and $|\text{III}(E/K)|$.

We will give the proof of the theorem above in Section 3. For now, we just remark that the proof of the first part relies on some Galois cohomology arguments, and that the second part follows from the first using the theory of visibility.

Remark 1.4. If for some prime p dividing N, f is congruent to a newform g of level dividing N/p (for Fourier coefficients of index coprime to Nq) modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the coefficients of f and g, then under certain conditions it follows that q divides the orders of the arithmetic and geometric component groups of E at p – see Section 4 for details. In particular, by Corollary 4.2 in Section 4, if in addition to the congruence hypothesis above, $p^2 \nmid N$, $w_p = -1$, and $E[q]$ and $A_g[\mathfrak{q}]$ are irreducible as $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules, then q divides $c_p(E)$, which is a factor on the left side of (3). This is in conformity with the Birch and Swinnerton-Dyer conjectural formula.

The proof of the following corollary is given in Section 3.

Corollary 1.5. *Let q be a prime that divides the product*

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\left(H^1(K, B') \rightarrow H^1(K, J')\right) \right|.$$

Suppose that N is prime, $q \nmid N(N+1)$, $E[q]$ is an irreducible representation of the absolute Galois group of $\mathbf{Q}$, and f is not congruent to a newform g in T of level N and analytic rank one modulo a prime ideal over q in the ring of integers of the number field generated by the coefficients of f and g. Assume that the first part of the Birch and Swinnerton-Dyer conjecture holds for all quotients of $J_0(N)$ associated to eigenforms of analytic rank greater than one. Then q divides $|\text{III}(E/\mathbf{Q})|$ and $|\text{III}(E/K)|$.

Remark 1.6. N. Dummigan has informed us that the hypothesis that for all primes p dividing N, $p \not\equiv -w_p \bmod q$ can be eliminated from [DSW03, Thm. 6.1], and hence from Theorem 1.3; if this is the case, then the hypothesis that $q \nmid (N+1)$ can be eliminated from the corollary above.

In view of our discussion just preceding Theorem 1.3, the theorem and corollary above are partial results towards the Birch and Swinnerton-Dyer conjecture in the analytic rank one case, and provide theoretical evidence supporting the conjecture. Also, under certain hypotheses (the most serious of which is the first part of the Birch and Swinnerton-Dyer conjecture), we have shown that if a prime q divides a certain factor of the left side of the Birch and Swinnerton-Dyer conjectural formula (1), then q divides the right side the formula (which includes $\sqrt{|\text{III}(E/K)|}$ as a factor). Thus our result is a first step in trying to prove that the left side of the Birch and Swinnerton-Dyer conjectural formula (1) divides the right side. The next step would be to try to show that the other factor $\left|\frac{B'(K)+E'(K)}{B'(K)+\pi''(\mathbf{T}P)\cap E'(K)}\right|_q$ on the right side of equation (3) divides the left side of (3) under certain hypotheses on q. Unfortunately, we have nothing much to say about this factor, except that in analogy with the analytic rank zero situation [Aga10], we do not expect that one can use visibility with eigenforms at level N to explain all of the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group (as we do for the factor $\left|\frac{J'(K)}{B'(K)+E'(K)}\right| \cdot \left|\ker\big(H^1(K,B')\to H^1(K,J')\big)\right|$ in the proof of Theorem 1.3), and so we suspect that in order to explain the factor $\left|\frac{B'(K)+E'(K)}{B'(K)+\pi''(\mathbf{T}P)\cap E'(K)}\right|_q$, one may have to use the theory of visibility involving eigenforms at level a multiple of N (cf. [AS02b, §4.2]).

As mentioned earlier, the theory of Euler systems gives results in the direction opposite to our results, viz., that the right side of the Birch and Swinnerton-Dyer conjectural formula (1) divides the left side (under certain hypotheses). Thus our result fits well in the ultimate goal of trying to prove the Birch and Swinnerton-Dyer conjectural formula in the analytic rank one case. As remarked earlier, the theory of Euler systems can also be used to construct non-trivial elements of the Shafarevich-Tate group under certain hypotheses (e.g., see [McC91, p. 2]); however, to our knowledge, this construction has not been linked to any predictions coming from the Birch and Swinnerton-Dyer conjecture.

In Section 2, we make some further remarks about our main result. In Section 3, we prove some lemmas that were referred to in this section, and give the proof of Theorem 1.3. In Section 4, we discuss the relationship between congruences with forms of lower level and the component group, which was alluded to in Remark 1.4.

2. Some further remarks

In this section we discuss some interesting choices for the set T, on which several of the quantities in our main results depend, and also discuss a potential example where the product

$$(4) \qquad \left|\frac{J'(K)}{B'(K)+E'(K)}\right| \cdot \left|\ker\big(H^1(K,B')\to H^1(K,J')\big)\right|$$

is nontrivial (recall that our main results concern this product).

As mentioned in Section 1, if T consists of the Galois conjugacy classes of all newforms of level dividing N except the conjugacy class of f, then $J' = J$. If instead, we choose a T with the restriction that it does not contain any newform of analytic rank one, then the hypothesis in Theorem 1.3 and Corollary 1.5 that f is not congruent to a newform g in T of level N and analytic rank one modulo a prime ideal over q in the ring of integers of the number field generated by the coefficients of f and g is automatic, and hence can be dropped. Under this restriction, there are two interesting choices of T, which are the two extreme cases. The first is where T consists of conjugacy classes of *all* newforms of level dividing N that have analytic rank not equal to one; this is the biggest choice of T for which the hypothesis mentioned two sentences above can be dropped. The other extreme choice of T is where T consists of the conjugacy class of a *single* newform g on $\Gamma_0(N)$ having analytic rank not equal to one. By the first part of Theorem 1.3, in order that an odd prime q divides the product in (4) above, g has to have odd analytic rank (otherwise the N-th Fourier coefficients of f and g will not be congruent modulo a prime ideal over q). Also, in order for the strategy of the proof of Theorem 1.3 to show that this prime q divides the order of the Shafarevich-Tate group of E, g must have analytic rank bigger than one. Thus among the sets T consisting of the conjugacy class of a single newform g on $\Gamma_0(N)$, the only ones for which our results are non-trivial are the ones where the newform g has odd analytic rank bigger than one. One advantage of such a choice of T is that we are able to prove a sort of converse to the first part of Theorem 1.3.

Recall that f is a newform with integer Fourier coefficients that has analytic rank one.

Proposition 2.1. *Suppose there is a newform g with integral Fourier coefficients that has analytic rank greater than one such that f and g are congruent modulo an odd prime q (as mentioned earlier, the analytic rank of g will necessarily be odd). Take T to be the singleton set $\{g\}$ in the definition of J' and B' in Section 1. Suppose that either $q \nmid N$ or that $q || N$ and $A_f[q]$ and $A_g[q]$ are irreducible representations of the absolute Galois group of $\mathbf{Q}$. Then q divides the product*

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\left(H^1(K, B') \to H^1(K, J') \right) \right|.$$

Proof. The proposition follows from [Aga09], as we now indicate. Take $p = q$ in loc. cit. Since B' is isogenous to $A_g^\vee$, we see that $F' = B'$ in the notation of loc. cit. Our result now follows from Lemma 2.1, Lemma 2.2, and Theorem 4.4 of loc. cit. $\square$

As mentioned before, the proposition above is a result that is in a direction opposite to that of the first part of Theorem 1.3, and is a partial result in trying to characterize the primes that divide the factor $\left| \frac{J'(K)}{B'(K)+E'(K)} \right| \cdot \left| \ker\left(H^1(K, B') \to H^1(K, J') \right) \right|$ of the "analytic" left side of the Birch and Swinnerton-Dyer conjectural formula (1), which we related to the "arithmetic" right side of this formula. Notice the similarity with the rank zero case in [Aga10], where we isolated a factor of the "analytic" left side of the Birch and Swinnerton-Dyer formula that could be characterized in terms of congruences analogous to the ones above and related these congruences to the "arithmetic" right side (the results for the analytic rank zero case are more precise).

While we showed in Proposition 2.1 that the product

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\big(H^1(K,B') \to H^1(K,J')\big) \right|$$

is non-trivial for a particular choice of T under certain hypotheses, one may wonder how often the hypotheses are satisfied. It would be nice to have some numerical data where these hypotheses are satisfied, so that the product above is non-trivial. If this happens, then in view of Theorem 1.3, we expect that either $\Sha(E/\mathbf{Q})$ is non-trivial or an arithmetic component group of E is non-trivial, of which the former seems more likely. Since it is difficult to compute the actual order of the Shafarevich-Tate group, we looked at the Birch and Swinnerton-Dyer conjectural orders in Cremona's online "Elliptic curve data" [Cre]. Unfortunately the conjectural orders of the Shafarevich-Tate groups of elliptic curves of analytic rank one at low levels are usually one or powers of 2, which makes it difficult to find examples where the hypotheses of Proposition 2.1 can be verified easily. For levels up to 30000, we found only one optimal elliptic curve of Mordell-Weil rank one for which the conjectural order of the Shafarevich-Tate group was divisible by an *odd* prime: the curve E with label 28042A, for which the conjectural order of the Shafarevich-Tate group is 9. At the same level, the curve $F = 28042B$ has Mordell-Weil rank 3 and the newforms f and g corresponding to 28042A and 28042B respectively have Fourier coefficients that are congruent modulo 3 for every prime index up to 100 (although this is not enough to conclude that the newforms are congruent modulo 3 for all Fourier coefficients, cf. [AS02a]). We do not know how to verify the hypotheses in Proposition 2.1 that 3 does not divide the order of the torsion subgroup of the projection of $\mathbf{T}P$ in J' and that $E[3]$ and $F[3]$ are irreducible representations of the Galois group of K (we remark though that by [Cre], E and F have no 3-torsion over $\mathbf{Q}$). So while we cannot be sure that Proposition 2.1 applies to show that 3 divides the product

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\big(H^1(K,B') \to H^1(K,J')\big) \right|$$

for $T = g$, it is quite encouraging that for the first example where the conjectural order of the Shafarevich-Tate group of an elliptic curve is divisible by an odd prime, there is a congruence modulo the same prime that might show that the product above is divisible by the prime in question, and hence explain why the prime divides the conjectural and actual order of the Shafarevich-Tate group.

In view of the remarks above, we hope that our article motivates more detailed computations similar to those in [AS05] for the analytic rank one case, especially since all this pertains to the Birch and Swinnerton-Dyer conjecture.

3. Proofs

In this section, we first prove two lemmas referred to in Section 1. After that, we give the proof of Theorem 1.3 and Corollary 1.5. We continue to use the notation introduced in Section 1.

Lemma 3.1. *We have*

$$|E(K)/\pi(\mathbf{T}P)|$$

$$= \left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\big(H^1(K,B') \to H^1(K,J')\big) \right| \cdot \frac{\left| \frac{B'(K)+E'(K)}{B'(K)+\pi''(\mathbf{T}P)_f \cap E'(K)} \right|}{\left| \frac{B'(K)+\pi''(\mathbf{T}P)}{B'(K)+\pi''(\mathbf{T}P)_f \cap E'(K)} \right|} \ .$$

Proof. By [Aga09, Prop. 4.2], we have

$$(5) \quad |E(K)/\pi(\mathbf{T}P)| = \left| \frac{J'(K)}{B'(K) + \pi''(\mathbf{T}P)} \right| \cdot \left| \ker\big(H^1(K,B') \to H^1(K,J')\big) \right|.$$

Also note that $\mathbf{T}P \cap E^\vee(K)$ is infinite since f has analytic rank one (as follows by [GZ86, Thm 6.3]). It follows that $\pi''(\mathbf{T}P)_f \cap E'(K)$ is of finite index in $E'(K)$. This shows that the group $\frac{B'(K)+E'(K)}{B'(K)+\pi''(\mathbf{T}P)_f \cap E'(K)}$ is finite. Also, the group

$$\frac{B'(K) + \pi''(\mathbf{T}P)}{B'(K) + \pi''(\mathbf{T}P)_f \cap E'(K)}$$

is finite since J' is isogenous to the direct sum of E' and B'. In view of this, the lemma follows from equation (5). □

Lemma 3.2. *Suppose q is a prime that does not divide the order of the torsion subgroup of $\pi''(\mathbf{T}P)$. Assume that f is not congruent to a newform g in S_T of analytic rank one modulo a prime ideal over q in the ring of integers of the number field generated by the coefficients of f and g (for Fourier coefficients of index coprime to Nq). Then q does not divide $\left| \frac{B'(K)+\pi''(\mathbf{T}P)}{B'(K)+\pi''(\mathbf{T}P)_f \cap E'(K)} \right|$.*

Proof. If h is a newform of level N_h dividing N, then let B_h denote the abelian subvariety of $J_0(N_h)$ associated to h by Shimura [Shi94, Thm. 7.14], and let J_h denote the sum of the images of B_h in $J = J_0(N)$ under the usual degeneracy maps; note that J_h depends only on the Galois conjugacy class of h. Then J' is isogenous to the direct sum of E' and the J_h's as h ranges over representatives of Galois conjugacy classes in T. If h is such a newform, then $\mathbf{T}P \cap J_h(K)$ is infinite if and only if h has analytic rank one (this follows by [GZ86, Thm 6.3] if h has analytic rank bigger than one, and the fact that $J_h(K)$ is finite if h has analytic rank zero, by [KL89]). Also, if g is a newform in T of analytic rank one, then q does not divide the order of $E^\vee \cap J_g$, considering that by hypothesis, f is not congruent to g modulo any prime ideal over q in the ring of integers of the number field generated by the coefficients of f and g for Fourier coefficients of index coprime to Nq (this follows by a generalization of the result that the modular degree of an elliptic curve divides its congruence number – cf. the proof of Theorem 1.3 in Section 3. From the discussion above, we see that q does not divide the order of the torsion part of the group $\pi''(\mathbf{T}P)_f/(\pi''(\mathbf{T}P)_f \cap E'(K))$. The lemma now follows from the hypothesis that q does not divide the order of the torsion subgroup of $\pi''(\mathbf{T}P)$. □

The rest of this section is devoted to giving the proof of Theorem 1.3. Following a similar situation in [CM00], consider the short exact sequence

$$(6) \qquad\qquad 0 \to B' \cap E' \to B' \oplus E' \to J' \to 0,$$

where the map $B' \cap E' \to B' \oplus E'$ is the anti-diagonal embedding $x \mapsto (-x, x)$ and the map $B' \oplus E' \to J'$ is given by $(b', e') \mapsto b' + e'$.

Lemma 3.3. *Suppose q is a prime that divides $\left| \frac{J'(K)}{B'(K)+E'(K)} \right|$. Then q divides the order of $B' \cap E'$.*

Proof. The long exact sequence associated to (6) gives us

$$\cdots \to B'(K) \oplus E'(K) \to J'(K) \to H^1(K, B' \cap E') \to H^1(K, B' \oplus E') \to \cdots ,$$

from which we get

(7) $$\frac{J'(K)}{B'(K) + E'(K)} = \ker\left(H^1(K, B' \cap E') \to H^1(K, B' \oplus E')\right).$$

Since q divides $\left| \frac{J'(K)}{B'(K)+E'(K)} \right|$, there is an element σ of the right hand side of (7) of order q. Now $B' \cap E'$ is finite, and so $\sigma \in H^1(K, B' \cap E')$ has order dividing $|B' \cap E'|$. Hence q divides $|B' \cap E'|$. $\qquad\square$

Lemma 3.4. *Suppose q is a prime that divides $\left|\ker\left(H^1(K, B') \to H^1(K, J')\right)\right|$. Then q divides the order of $B' \cap E'$.*

Proof. By hypothesis, there is an element σ of $\ker\left(H^1(K, B') \to H^1(K, J')\right)$ of order q. The long exact sequence associated to (6) gives us

(8) $$\cdots \to H^1(K, B' \cap E') \to H^1(K, B') \oplus H^1(K, E') \to H^1(K, J') \to \cdots .$$

The element $(\sigma, 0) \in H^1(K, B') \oplus H^1(K, E')$ of order q in the middle group in (8) maps to zero in the rightmost group $H^1(K, J')$ in (8), and thus by the exactness of (8), there is a non-trivial element $\sigma' \in H^1(K, B' \cap E')$ of order divisible by q that maps to $(0, \sigma) \in H^1(K, B') \oplus H^1(K, E')$. Again, since $B' \cap E'$ is finite and so is $\sigma' \in H^1(K, B' \cap E')$ has order dividing $|B' \cap E'|$, we see that q divides $|B' \cap E'|$. $\quad\square$

Proof of Theorem 1.3. We start by proving the first part of the theorem. By Lemmas 3.3 and 3.4, we see that q divides the order of $B' \cap E'$, which was the first claim in the first part of Theorem 1.3. The other claim in the first part of the theorem is that there is an eigenform g in S_T such that f is congruent to g modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the Fourier coefficients of f and g. This second claim follows from the first claim, using an argument similar to the one in [Aga10, §5], which in turn mimics the proof that the modular degree divides the congruence number [ARS], as we now explain.

If h is a newform of level N_h dividing N, then let B_h denote the abelian subvariety of $J_0(N_h)$ associated to h by Shimura [Shi94, Thm. 7.14], and let J_h denote the sum of the images of B_h in $J = J_0(N)$ under the usual degeneracy maps; note that J_h depends only on the Galois conjugacy class of h. Let C denote $(I_f \cap I_T)J$. Then C is the abelian subvariety of J generated by J_g where g ranges over Galois conjugacy classes of newforms of level dividing N other than orbit of f and other than the classes in T. Let B denote the abelian subvariety of J generated by J_g where g ranges over Galois conjugacy classes of newforms of level dividing N other than the orbit of f and let A denote the abelian subvariety of J generated by J_g where g ranges over Galois conjugacy classes of newforms of level dividing N other than the classes in T. Then $E' = A/C$ and $B' = B/C$. Now applying the arguments of [Aga10, §5] but

with A, B, and C as above, the fact that q divides the order of $E' \cap B' = A/C \cap B/C$ implies that there is an eigenform g in the subspace of $S_2(\Gamma_0(N), \mathbf{C})$ generated by the newforms in T such that f is congruent to g modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the Fourier coefficients of f and g. This finishes the proof of the first part of Theorem 1.3.

We now turn to proving the second part of Theorem 1.3. By the first part, there is an eigenform g in S_T such that f is congruent to g modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers $\mathcal{O}$ of the number field generated by the Fourier coefficients of f and g. By the definition of S_T and the hypotheses of the theorem, it follows that g has analytic rank greater than one (note that g has to be new, and cannot be of analytic rank zero, since the eigenvalues of the Atkin-Lehner involution would have different signs and q is odd).

The second part of Theorem 1.3 now follows from Theorem 6.1 of [DSW03], as we now indicate (for details of some of the definitions below, see [DSW03]). Let $T_{\mathfrak{q}}$ denote the $\mathfrak{q}$-adic Tate module of $E^{\vee} = E$. Let $L_{\mathfrak{q}}$ denote the quotient field of $\mathcal{O}_{\mathfrak{q}}$, let $V_{\mathfrak{q}} = T_{\mathfrak{q}} \otimes_{\mathcal{O}_{\mathfrak{q}}} L_{\mathfrak{q}}$, and let $A_{\mathfrak{q}}$ denote $V_{\mathfrak{q}}/T_{\mathfrak{q}}$. We denote the corresponding objects for $A_g^{\vee}$ by $T'_{\mathfrak{q}}$, $V'_{\mathfrak{q}}$, and $A'_{\mathfrak{q}}$. Let r denote the dimension of $H^1_f(\mathbf{Q}, V'_{\mathfrak{q}})$ over $L_{\mathfrak{q}}$. Then r is at least the analytic rank of g (since we are assuming the first part of the Birch and Swinnerton-Dyer conjecture for $A_g^{\vee}$), i.e., at least 2. Theorem 6.1 of loc. cit. tells us that the $\mathfrak{q}$-torsion subgroup of the Selmer group $H^1_f(\mathbf{Q}, A_{\mathfrak{q}})$ of E has $\mathcal{O}_{\mathfrak{q}}/\mathfrak{q}$-rank at least r. Since the abelian group $E(K)$ has rank one, the abelian subgroup $E(\mathbf{Q})$ has rank at most one, and so the image of $H^1_f(\mathbf{Q}, V_{\mathfrak{q}})$ in the $\mathfrak{q}$-torsion subgroup of $H^1_f(\mathbf{Q}, A_{\mathfrak{q}})$ has $\mathcal{O}_{\mathfrak{q}}/\mathfrak{q}$-rank at most one. This shows that $|\text{Ш}(E/\mathbf{Q})|$ is divisible by q^{r-1}, in particular by $q^{2-1} = q$ (since $r \geq 2$). Since the natural map $\text{Ш}(E/\mathbf{Q}) \to \text{Ш}(E/K)$ has kernel a finite group of order a power of 2 and q is odd, we see that q divides the order of $\text{Ш}(E/K)$ as well. This finishes the proof of Theorem 1.3.   □

Proof of Corollary 1.5. Since $w_N = 1$, we have $N \not\equiv -1 \pmod{q}$ by hypothesis. Also, since the level is prime, there are no newforms of lower level. The corollary now follows from Theorem 1.3.   □

4. Appendix: Congruences with forms of lower level and the component group

Let N be a positive integer, and let f be a newform of weight 2 on $\Gamma_0(N)$ having integer Fourier coefficients. Denote by E the optimal elliptic curve over $\mathbf{Q}$ associated to f. Let p be a prime that divides N. Let $\mathcal{E}$ denote the Néron model of E over $\mathbf{Z}$, and let $\mathcal{E}_{\mathbf{F}_p}$ denote the special fiber of $\mathcal{E}$ at p. Denote by $\mathcal{E}^0_{\mathbf{F}_p}$ the connected component of $\mathcal{E}_{\mathbf{F}_p}$ containing the identity. The component group $\Phi_{E,p}$ is defined by the exact sequence

$$(9) \qquad\qquad 0 \to \mathcal{E}^0_{\mathbf{F}_p} \to \mathcal{E}_{\mathbf{F}_p} \to \Phi_{E,p} \to 0 \ .$$

Then the *geometric component group* of E at p is $\Phi_{E,p}(\overline{\mathbf{F}}_p)$ and the arithmetic *arithmetic component group* of E at p is $\Phi_{E,p}(\mathbf{F}_p)$, whose order is called the *Tamagawa number* of E at p.

In this section, we prove the following three results relating congruences with forms of lower level and the geometric and arithmetic component groups. These results are perhaps well known, but we could not find a suitable reference. We are grateful to the anonymous referee for outlining the proofs of Propositions 4.1 and 4.3 below.

Proposition 4.1. *Let q be a prime such that $q \neq p$. Suppose f is congruent to a newform g of level dividing N/p (for Fourier coefficients of index coprime to Nq) modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the coefficients of f and g. Assume that $E[q]$ and $A_g[\mathfrak{q}]$ are irreducible as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. Then q divides the order of the geometric component group of E at p.*

Corollary 4.2. *Let q be a prime such that $q \neq p$. Assume that $p||N$ and $w_p = -1$, where recall that w_p is the sign of the Atkin-Lehner involution W_p acting on the newform associated to E. Suppose f is congruent to a newform g of level dividing N/p (for Fourier coefficients of index coprime to Nq) modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the coefficients of f and g. Assume that $E[q]$ and $A_g[\mathfrak{q}]$ are irreducible as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. Then q divides the order of the arithmetic component group of E at p.*

Proof. By Proposition 4.1, q divides the order of $\Phi_{E,p}(\overline{\mathbf{F}}_p)$. Considering that $p||N$, the Frobenius endomorphism acts as $-w_p$ on $\Phi_{E,p}(\overline{\mathbf{F}}_p)$. Since $w_p = -1$, this action is trivial and thus $\Phi_{E,p}(\mathbf{F}_p) = \Phi_{E,p}(\overline{\mathbf{F}}_p)$. The corollary follows. $\square$

Proposition 4.3. *Suppose $p||N$. Let q be an odd prime not equal to p such that either $q^2 \nmid N$ or $p \not\equiv 1 \bmod q$. Assume that $E[q]$ is irreducible as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module. If q divides the order of the geometric component group at p, then f is congruent to a newform g of level dividing N/p (for Fourier coefficients of index coprime to Nq) modulo a prime ideal over q in the ring of integers of the number field generated by the coefficients of f and g.*

Remark 4.4. One of the two hypotheses that $p \not\equiv 1 \bmod q$ and that $E[q]$ is irreducible as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module made in Proposition 4.3 above is essential. For example, the unique optimal elliptic curve of conductor 11 has Tamagawa number 5 (at 11), but since the level 11 is prime, there can be no congruences with lower level (for this example, with $p = 11$ and $q = 5$, $p \equiv 1 \bmod q$ and q divides $|E(\mathbf{Q})_{\mathrm{tor}}| = 5$, so that $E[q]$ is reducible as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module; at the same time, all other hypotheses of Proposition 4.3 are satisfied).

We now prove Propositions 4.1 and 4.3. From the exact sequence (9), we deduce the exact sequence:

$$(10) \qquad\qquad 0 \to \mathcal{E}^0_{\mathbf{F}_p}(\overline{\mathbf{F}}_p) \to \mathcal{E}_{\mathbf{F}_p}(\overline{\mathbf{F}}_p) \to \Phi_{E,p}(\overline{\mathbf{F}}_p) \to 0 \ .$$

Suppose that $q \neq p$. If $p||N$, then $\mathcal{E}^0_{\mathbf{F}_p}$ is a multiplicative group, and the multiplication by q map on $\mathcal{E}^0_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)$ is surjective. If $p^2 | N$, then $\mathcal{E}^0_{\mathbf{F}_p}$ is an additive group, but since $q \neq p$, the multiplication by q map on $\mathcal{E}^0_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)$ is still surjective. Considering the snake lemma applied to the multiplication by q map on the exact sequence (10)

above, and using the fact that the multiplication by q map on $\mathcal{E}^0_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)$ is surjective, we get the exact sequence:

$$(11) \qquad 0 \to \mathcal{E}^0_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)[q] \to \mathcal{E}_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)[q] \to \Phi_{E,p}(\overline{\mathbf{F}}_p)[q] \to 0 \ .$$

Let I_p denote the inertia subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. Then the reduction map induces an isomorphism of Galois modules $E[q]^{I_p} \cong \mathcal{E}_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)[q]$ (e.g., see [ST68, p. 495]).

Proof of Proposition 4.1. Recall that in addition to the hypotheses made above on q, we are assuming that f is congruent to a newform g of level dividing N/p (for Fourier coefficients of index coprime to Nq) modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the coefficients of f and g and that $E[q] = E[\mathfrak{q}]$ and $A_g[\mathfrak{q}]$ are irreducible as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. Then by the Chebotarev and Brauer-Nesbitt theorems, $E[q] \cong A_g[\mathfrak{q}]$ as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. Hence $E[q]$ is unramified at p, and so $E[q]^{I_p} = E[q]$. Thus $\mathcal{E}_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)[q] \cong E[q]^{I_p}$ has dimension 2 over $\mathbf{F}_q$. Now $\mathcal{E}^0_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)[q]$ has dimension at most one over $\mathbf{F}_q$. Hence the exact sequence (11) shows that $\Phi_{E,p}(\overline{\mathbf{F}}_p)[q]$ is non-trivial, i.e., q divides the order of the geometric component group at p. $\qquad\square$

Proof of Proposition 4.3. Recall that in addition to the hypotheses made above on q, we are assuming that $\Phi_{E,p}(\overline{\mathbf{F}}_p)[q]$ is non-trivial. Suppose $p^2 \nmid N$. Then $\mathcal{E}^0_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)[q]$ has dimension one over $\mathbf{F}_q$, and hence by the exact sequence (11), we see that $E[q]^{I_p} \cong \mathcal{E}_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)[q]$ is two dimensional over $\mathbf{F}_q$. Thus $E[q]^{I_p} = E[q]$, i.e., $E[q]$ is unramified at p. Our result now follows from [Rib90, p. 1-2]. $\qquad\square$

Acknowledgements

We are grateful to Neil Dummigan for answering some questions regarding [DSW03]. We would also like to thank John Cremona and Mark Watkins for some numerical data that encouraged the author to pursue the investigations in this article. We are also grateful to the anonymous referee for pointing out the connection between congruences with forms of lower level and the component group, as discussed in Section 4.

References

[Aga09]   Amod Agashe, *Visibility and the Birch and Swinnerton-Dyer conjecture for analytic rank one*, Int. Math. Res. Not. IMRN (2009), no. 15, 2899–2913.
[Aga10]   A. Agashe, *A visible factor of the special L-value*, J. Reine Angew. Math. **644** (2010), 159–187.
[ARS]   A. Agashe, K. Ribet, and W. A. Stein, *The modular degree, congruence primes, and multiplicity one*, to appear in a special Springer volume in honor of Serge Lang, available at
            http://www.math.fsu.edu/~agashe/math.html.
[AS02a]   A. Agashe and W. A. Stein, Appendix to Joan-C. Lario and René Schoof: *Some computations with Hecke rings and deformation rings*, Experiment. Math. **11** (2002), no. 2, 303–311.
[AS02b]   ———, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185.
[AS05]   ———, *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.
[BCDT01]   C. Breuil, B. Conrad, F. Diamond, and R. 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).

[CM00]   J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28.

[Cre]   J. E. Cremona, *Elliptic curve data*,
         `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`.

[DSW03] N. Dummigan, W. A. Stein, and M. Watkins, *Constructing elements in Shafarevich-Tate groups of modular motives*, Number theory and algebraic geometry, London Math. Soc. Lecture Note Ser., vol. 303, Cambridge Univ. Press, Cambridge, 2003, pp. 91–118.

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[GZ86]   B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 87j:11057

[Jet08] D. Jetchev, *Global divisibility of Heegner points and Tamagawa numbers*, Compos. Math. **144** (2008), no. 4, 811–826.

[KL89]   V. A. Kolyvagin and D. Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196.

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[McC91] W. G. McCallum, *Kolyvagin's work on Shafarevich-Tate groups*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 295–316.

[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.

[ST68]   J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[Wal85] J.-L. Waldspurger, *Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie*, Compositio Math. **54** (1985), no. 2, 173–242.

Department of Mathematics, Florida State University, Tallahassee, FL 32312, U.S.A

E-mail address: `agashe@math.fsu.edu`