The Birch and Swinnerton-Dyer conjectural formula and visibility

Project description

Amod Agashe

This proposal falls broadly in the area of number theory and more specifically in arithmetic geometry. It is concerned with a part of the Birch and Swinnerton-Dyer (BSD) conjecture on elliptic curves and abelian varieties.

1 Introduction

A fundamental problem of number theory is: given a set of polynomial equations with rational coefficients, find all of its rational solutions and investigate their structure. In many cases, the Birch and Swinnerton-Dyer conjecture (henceforth abbreviated BSD conjecture) predicts the existence of such solutions and describes some of their structure without actually finding the solutions. The importance and centrality of this conjecture in mathematics is underscored by the fact that a part of the conjecture was selected as one of the seven millennium prize problems by the Clay Mathematical Institute.

While much work has been done on the BSD conjecture for elliptic curves (for a summary, see [Sil92, §16] and [IR90, §20.5]), the principal investigator (PI) of this project was one of the first [Aga00] to do calculations regarding this conjecture for abelian varieties of arbitrary dimension. Working with L. Merel and W. Stein, the PI obtained partial results and computational evidence towards this conjecture for certain quotients of Jacobians of modular curves. These quotients form a large class of abelian varieties (which includes elliptic curves) that are of great importance in arithmetic geometry. For example, the proof of the celebrated Fermat's Last Theorem relies on properties of such quotients. For these abelian varieties, we study the second part of the BSD conjecture, which is a conjectural formula that relates several fundamental invariants of the abelian variety. In particular, the conjecture gives a computable formula for the order of the Shafarevich-Tate group of the abelian variety, a mysterious invariant that arises in the calculation of the rational points on the abelian variety (e.g., see [Sil92, Chapter X]), and elsewhere.

The theory of visibility has recently been used to give new evidence for this conjectural formula. As a concrete example, consider the elliptic curve $y^2+xy = x^3+x^2-1154x-15345$ (denoted $681B1$ in [Cre97]). The BSD conjectural formula predicts that the order of the Shafarevich-Tate group of this elliptic curve is 9. Using the idea of visibility, Cremona and Mazur gave an explicit construction of a subgroup of the Shafarevich-Tate group of order 9 (see [CM00, p. 22], and [AS05, Appendix]). The PI proposes to generalize the techniques used in this example (and several others) with the goal of showing that for certain quotients of Jacobians of modular curves, the order of the Shafarevich-Tate group predicted by the BSD conjecture divides the actual order, assuming the first part of the BSD conjecture on rank. In fact our methods do more: they give explicit constructions of the conjectured elements of the Shafarevich-Tate group.

The PI will also investigate certain other arithmetic invariants appearing in the BSD formula, viz., the orders of the torsion group and the component groups of an abelian variety. These groups are of interest independent of the BSD formula – the torsion group addresses part of the problem of finding rational solutions to equations, and component groups play an important role in the study of abelian varieties (e.g., in Ribet's proof that the Shimura-Taniyama-Weil conjecture implies Fermat's last theorem). Thanks to work of Mazur and Emerton, when the level of the modular curve is prime, the torsion and component groups are well understood. The PI proposes

to extend their techniques to square-free level in order to characterize the primes that can divide the orders of the torsion and component groups in this more general situation.

In the next section (Section 2), we give the precise definitions of the objects we are interested in and give a more technical overview of the proposal. The research part of the proposal consists of two parts: Section 3 concerns the orders of the torsion group and the component groups and Sections 4, 5, and 6 involve the application of the theory of visibility to study the Shafarevich-Tate group. The two parts can be read more or less independently of each other (after reading Section 2), although there is some cross-referencing. In any case, the two parts fit together nicely to provide a bigger picture for the BSD formula. In Section 7, we discuss the broader impacts of our proposal.

2 The Birch and Swinnerton-Dyer conjectural formula for modular abelian varieties

In this section, we state the BSD conjectural formula and introduce the abelian varieties for which we would like to study this formula. We mention what is known regarding the formula and summarize more precisely what we wish to accomplish in this proposal.

2.1 The Birch and Swinnerton-Dyer conjectural formula

We recall briefly the BSD conjecture as generalized by Tate to abelian varieties (e.g., see [Lan91, III.5]). Throughout, if G is a finite group, then we use the symbol $|G|$ to denote the order of G.

Let A be an abelian variety defined over $\mathbf{Q}$ (in particular, A could be an elliptic curve and not much would be lost by restricting to that case for the moment). Attached to A is a complex-valued function $L_A(s)$ (sometimes denoted $L(A,s)$) defined on the part of the complex plane where $\mathrm{Re}(s)$ is sufficiently large. It is called the *L-function* of A and is obtained by packaging information about the number of points of A over finite fields. Suppose that the function $L_A(s)$ extends to an analytic function on the entire complex plane (as is conjectured). Then the order of vanishing of $L_A(s)$ at $s=1$ is called the *analytic rank* of A. The *first part of the BSD conjecture* says that the rank of the Mordell-Weil group $A(\mathbf{Q})$ is equal to the analytic rank of A.

Suppose that $L_A(1) \neq 0$. The Shafarevich-Tate group of A, denoted $Ш_A$, consists of equivalence classes of principal homogeneous spaces of A that are locally trivial everywhere; assume $Ш_A$ is finite, as conjectured. If B is an abelian variety over $\mathbf{Q}$, then we denote by $B(\mathbf{Q})_{\mathrm{tor}}$ the torsion subgroup of the finitely generated abelian group $B(\mathbf{Q})$, and by $B^\vee$ the dual abelian variety of B (if B is an elliptic curve, then $B^\vee = B$). Throughout this article, we shall use the symbol $\stackrel{?}{=}$ to denote an equality which is conjectural. The *second part of the BSD conjecture* asserts the formula:

$$\frac{L_A(1)}{\Omega_A} \stackrel{?}{=} \frac{|Ш_A| \cdot \prod_p c_p(A)}{|A(\mathbf{Q})_{\mathrm{tor}}| \cdot |A^\vee(\mathbf{Q})_{\mathrm{tor}}|}\ , \tag{1}$$

where $c_p(A)$ is the order of the arithmetic component group of the special fiber at the prime p of the Néron model of A, and the symbol Ω_A denotes the volume of $A(\mathbf{R})$ calculated using a set of generators of the group of invariant differentials on the Néron model of A (for details, see [AS05]). There is a similar formula even when $L_A(1) = 0$, but we will not be considering that case in this proposal. We will refer to the formula above as the *BSD (conjectural) formula*. The significance of this formula is that it can often be used to compute the order of the Shafarevich-Tate group of A.

2.2 Modular abelian varieties

Let N be a positive integer and let $X_0(N)$ be the modular curve over $\mathbf{Q}$ associated with the problem of parametrizing elliptic curves with a cyclic subgroup of order N. We will often refer to N as the *level*. Let $J_0(N)$ denote the Jacobian of $X_0(N)$; it is an abelian variety defined over $\mathbf{Q}$ whose points correspond to degree-zero divisor classes on $X_0(N)$. The *Hecke algebra*, denoted $\mathbf{T}$, is the subring of endomorphisms of $J_0(N)$ generated by the Hecke operators. Fix a newform f of weight 2 on $\Gamma_0(N)$. Let I_f be the ideal of all the elements of $\mathbf{T}$ that annihilate f and let $A = A_f$ denote the quotient abelian variety $J_0(N)/I_f J_0(N)$. We call A the newform quotient or the modular abelian variety associated to f. If the newform f has rational Fourier coefficients, then the quotient A is an elliptic curve over $\mathbf{Q}$, and the Shimura-Taniyama-Weil conjecture, which is now a theorem, asserts that any elliptic curve over $\mathbf{Q}$ is isogenous to some such quotient. In fact, in what follows, the dimension of A does not play a significant role, so **the reader may assume for simplicity that A is just an elliptic curve** (more or less throughout the proposal).

It is known that $L_A(s)$ extends to an analytic function on the complex plane. Most of this proposal is concerned with the case when $L_A(1) \neq 0$, so let us assume that $L_A(1) \neq 0$ for the rest of this section. In that case, it follows by results of [KL89] that $A(\mathbf{Q})$ and $Ш_A$ are both finite. The results of [Shi77] imply that $L_A(1)/\Omega_A$ is a rational number. When A is an elliptic curve, there are formulas to calculate this rational number as well as all other invariants in (1) except $|Ш_A|$; this allows one to compute the conjectural order of $Ш_A$ and obtain numerical evidence towards the BSD conjectural formula (e.g., see [Cre97]). Also, one can use the theory of Euler systems to bound $|Ш_A|$ from above in terms of the order conjectured by the BSD formula (staying away from certain primes), as in the work of Kolyvagin and of Kato (e.g., see [Rub98, Thm 8.6]). Moreover, the Eisenstein series method, which is a generalization of Ribet's converse to Herbrand's theorem, is being used (for example by Skinner-Urban) to show that the BSD conjectured order of $Ш_A$ divides the actual order (again staying away from certain primes). Finally, the theory of visibility has been used to construct non-trivial elements of $Ш_A$ computationally and thus to give evidence for the BSD formula in particular examples (e.g., see [CM00] and [AS05]).

2.3 Past work and a summary of the proposal

In his thesis [Aga00], the PI proved a formula (conjectured by W. Stein) that expresses $L_A(1)/\Omega_A$ as a computable rational number when $L_A(1) \neq 0$. This formula was used in [AS05] to obtain some of the first nontrivial numerical evidence for the BSD formula for abelian varieties of arbitrary dimension. By comparing the formula for $L_A(1)/\Omega_A$ to the right hand side of the BSD formula, the PI and W. Stein proved [AS05, §4.3] that if N is square-free, then multiplication by $|A(\mathbf{Q})_{\mathrm{tor}}|$ annihilates the odd part of the denominator of $L_A(1)/\Omega_A$, which is consistent with formula (1). In recent work [AM04], the PI and L. Merel used visibility to show that the primes dividing a certain explicit factor of L_A/Ω_A divide $|Ш_A|$ (assuming the first part of the BSD conjecture).

While the most interesting term on the right hand side of the BSD formula (1) is the order of the Shafarevich-Tate group, the other terms, viz., the orders of the torsion and component groups are also of independent interest; in any case, they need to be understood from the point of view of the BSD formula. When the level N is prime, it follows from [Eme03] (which builds on [Maz77]) that $c_N(A) = |A(\mathbf{Q})_{\mathrm{tor}}| = |A^\vee(\mathbf{Q})_{\mathrm{tor}}| = |C_A|$, where C_A is the subgroup of $A(\mathbf{Q})_{\mathrm{tor}}$ generated by the image of the divisor $(0) - (\infty)$. In Section 3 of this proposal, the PI plans to extend the techniques of Mazur and Emerton to non-prime level, and in particular, prove that if the level N is square-free, then if an odd prime $\ell > 3$ divides either $c_p(A)$ (for some prime $p \,|\, N$) or $|A(\mathbf{Q})_{\mathrm{tor}}|$ or $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$, then ℓ divides $|C_A|$ or f is congruent modulo ℓ to a newform of lower level.

The rest of the proposal is devoted to using the theory of visibility to show that the BSD conjectural order of the Shafarevich-Tate group divides the actual order for modular abelian varieties of analytic rank zero. All of the *theoretical* results that we get using visibility arguments are contingent on the first part of the BSD conjecture for *all* modular abelian varieties, so for ease of exposition, let us assume this for the rest of this section.

In [AM04] the PI and L. Merel extract an explicit factor of $L_A(1)/\Omega_A$ that measures congruences between f and eigenforms g of the same level such that $L_{A_g}(1) = 0$, and then use the theory of visibility to show that the odd primes that divide this factor divide $|Ш_A|$ (under certain mild hypotheses). The PI proposes to extend this work (Section 5) to show that the *entire* factor divides $|Ш_A|$ (staying away from certain primes).

However, one cannot extend this method to the remaining factors of $L_A(1)/\Omega_A$, since one cannot always use congruences with forms of the *same* level to explain all of the Shafarevich-Tate group (this is borne out by examples). At the same time, W. Stein has conjectured that every element of $Ш_A$ is visible in $J_0(NM)$ for some M. In Section 6, we sketch a novel plan to use a formula of Gross for the special L-value over a quadratic imaginary extension of $\mathbf{Q}$ and visibility via congruences with forms of possibly *higher* level to show that the *full* order of $Ш_A$ predicted by the second part of the BSD conjecture can be accounted for (under an auxiliary hypothesis).

The currently available visibility theorems are more suited for computations, and are not sufficient for some of the projects in this proposal. In Section 4, we will indicate a plan to prove a more general visibility theorem that is suitable for *theoretical* applications.

We would like to emphasize that unlike some other methods that give lower bounds for $|Ш_A|$ (e.g., the Eisenstein series method of Skinner-Urban), the theory of visibility gives an explicit construction of elements of the Shafarevich-Tate group using the generators of the Mordell-Weil group of another abelian variety. This explicit construction could be much more valuable for computation than just having a theoretical lower bound.

Finally, while our projects on the torsion and component groups on the one hand and visibility and the Shafarevich-Tate group on the other hand are largely independent of each other, they fit together nicely in conformity with the BSD formula – one can specify which set of primes divide which quantity and what cancellations one can expect. Thus in the course of this proposal, we will study the fine structure of how all the quantities in the BSD formula interact, which would substantially improve our understanding of the formula even if the conjectural formula were proved by some other method.

3 The torsion and component groups

As before, let f be a newform of weight 2 on $\Gamma_0(N)$, and let $A = A_f$ be the quotient of $J_0(N)$ associated to f. Note that unlike the other sections, in this section, we do *not* assume that $L_A(1) \neq 0$. The divisor $(0) - (\infty)$ generates a finite subgroup of $J_0(N)$, which we denote C. The image of C under the quotient map $J_0(N) \to A$ is a cyclic subgroup of $A(\mathbf{Q})_{\text{tor}}$; we denote this subgroup by C_A and call it the *cuspidal subgroup of* A (note that this is *not* the subgroup generated by the images of all the cuspidal divisors, but by the image of just $(0) - (\infty)$). If p is a prime that divides N, then let $\mathcal{A}_p$ denote the special fiber at p of the Néron model of A and let $\mathcal{A}_p^0$ denote the identity component of $\mathcal{A}_p$. The *(geometric) component group* of A at p, denoted $\Phi_p(A)$ is the quotient group $\mathcal{A}_p/\mathcal{A}_p^0$; by abuse of notation, we often write $\Phi_p(A)$ also for $\Phi_p(A)(\overline{\mathbf{F}}_p)$. The *arithmetic component group* of A is just $\Phi_p(A)(\mathbf{F}_p)$, whose order is $c_p(A)$ (as defined earlier).

In the landmark paper [Maz77], Mazur proved that if the level N is prime, then $C = J_0(N)(\mathbf{Q})_{\text{tor}}$ and that the specialization map induces an isomorphism $C \cong \Phi_N(J_0(N))$. Build-

ing on Mazur's results, Emerton [Eme03] proved that when N is prime, $C_A = A(\mathbf{Q})_{\mathrm{tor}}$ and the specialization map induces an isomorphism $C_A \cong \Phi_N(A)$; moreover, he showed that $\Phi_N(A)$ has trivial Galois action, so $c_N(A) = |C_A|$. Thus the picture for prime level is very satisfactory, especially from the point of view of the BSD conjecture, since this shows that there is siginificant cancellation on the right hand side of the BSD formula (1). We will now investigate what happens when the level N is not necessarily prime.

3.1 The order of the torsion subgroup

The cuspidal subgroup C_A does not always account for the entire torsion subgroup $A(\mathbf{Q})_{\mathrm{tor}}$ when the level is not prime. At the request of the PI, W. Stein computed a table [Ste] of optimal elliptic curves whose torsion subgroup is strictly bigger than the image of the cuspidal group. As an example, for the elliptic curve 66C1 of [Cre97], the cuspidal subgroup is trivial, while the torsion subgroup has order 10. However, in all of the several examples that the PI checked in Stein's table, he found that for an optimal elliptic curve A:

Observation 3.1. If an odd prime ℓ divides the order of the torsion subgroup $A(\mathbf{Q})_{\mathrm{tor}}$ but does not divide the order of the cuspidal subgroup C_A, then there is a prime $p \,|\, N$ such that $w_p = -1$ and f is congruent modulo ℓ to a newform of level dividing N/p.

Here (and henceforth), w_p denotes the eigenvalue of the Atkin-Lehner involution W_p acting on f. The product of the W_p's for $p \mid N$ is the Fricke involution W_N, whose eigenvalue is denoted w_N. The significance of the operator W_N is that it acts by multiplication by -1 on $(0) - (\infty)$.

As an example of Observation 3.1, for the newform f corresponding to 66C1, $w_2 = w_3 = -1$, and 66C1 is congruent to 11A1 modulo 5. Note that when we talk about a congruence between newforms of different levels, we mean a congruence for all coefficients of index coprime to the two levels (which is a congruence for almost every prime index).

Project 3.2. Prove Observation 3.1 for any newform quotient, perhaps under some restrictive hypotheses (e.g., that the level is square-free).

The PI proposes to do this by checking what are the obstructions to the methods of Mazur (in [Maz77]) when the level is not assumed to be prime. Mazur considers separately the cases where W_N acts as -1 and 1 (on a certain finite group scheme).

Consider the case where $w_p = -1$. If the level is prime, then Mazur shows that the torsion subgroup is cuspidal based on the fact that $W_p = W_N$ acts as -1 on $(0) - (\infty)$ as well. In the general case where N is not prime, we need to consider the operators U_p for $p \mid N$. Suppose $w_p = -1$. Then U_p acts as $-w_p = 1$ on the piece corresponding to f, and U_p acts as multiplication by p on $(0) - (\infty)$. Thus if $p \equiv 1 \bmod \ell$ then this does not obstruct the torsion group from being fully cuspidal. If $p \not\equiv 1 \bmod \ell$, then Mazur's level lowering result (see [Rib90, Thm. 6.1]) applied to an irreducible part of the torsion subgroup should show that f is congruent modulo ℓ to a newform of level dividing N/p (for this we may have to assume that N is square-free). Thus congruences with newforms of lower level can cause an obstruction to the torsion group from being fully cuspidal.

Now consider the case where $w_p = 1$. When the level is prime, Mazur shows that this cannot happen by using a technical argument involving moduli stacks and the fact that there are no (nontrivial) cuspforms on $\Gamma_0(1)$. The PI will look more closely at this argument to see what can be salvaged when the level is not prime. However, one cannot rule out the case $w_p = 1$, since this does happen in tables of Stein.

3.2 The orders of the component groups

Recall that for prime level, the cuspidal subgroup explains the full component group (arithmetic or geometric). However, this is not the case for non-prime level. For example, for the elliptic curve $E = 66C1$, as mentioned above, the cuspidal subgroup is trivial, but from [Cre97], one finds that $c_2(E) = 10$ and $c_3(E) = 5$. Moreover, even the full torsion subgroup does not always explain the arithmetic component group. At the same time, in all the examples that the PI checked in [Cre97], he found that for an optimal elliptic curve A:

Observation 3.3. If an odd prime ℓ divides $c_p(A)$ for some $p|N$ but ℓ does not divide the order of the torsion group $A(\mathbf{Q})_{\mathrm{tor}}$, then $w_p = -1$ and f is congruent modulo ℓ to a newform of level dividing N/p.

For example, for the elliptic curve $E = 114\mathrm{C}1$, we find that $5|c_2(E) = 20$, but $5\nmid|E(\mathbf{Q})_{\mathrm{tor}}| = 4$. One finds that $w_2(E) = -1$ and the newform 114C1 is congruent modulo 5 the newform 57A1. More generally, one may ask when an odd prime p can divide the order of an arithmetic component group but not divide the order of the cuspidal subgroup, which is potentially smaller than the torsion group. In view of Observation 3.1, the answer seems to be the same: $w_p = -1$ and f is congruent modulo ℓ to a newform of level dividing N/p. For example, this happens for the previously discussed newform 66C1: one finds that 66C1 is congruent to 11A1 modulo 5.

Project 3.4. Explain Observation 3.3. More precisely, show that if an odd prime ℓ divides $c_p(A)$, then ℓ divides the order of C_A or for some prime p that divides the level N, f is congruent modulo ℓ to a newform of level dividing N/p (perhaps under the hypotheses that $\ell \neq 3$ and that the level is square-free).

The PI proposes to do this by generalizing methods of [Eme03], where Emerton shows that when N is prime, the specialization map induces an isomorphism $C_A \cong \Phi_N(A)$. One of the key facts behind Emerton's proof is his result that for any level (not necessarily prime), a prime in the support of the component group is either Eisenstein or finite.

By Ribet's lower lowering argument, finiteness implies congruences with newforms of lower level, which is not possible if N is prime: this is one of the key facts used by Emerton. When the level is not prime, congruences with newforms of lower level can cause an obstruction to the argument, and hence it is not surprising that they appear in Observation 3.3. Moreover these congruences contribute to the *arithmetic* component group only if $w_p = -1$ (cf. [Dum04, §7] and [Maz77, Appendix, §3]); this explains why one needs $w_p = -1$ in Observation 3.3.

Finally, we have to show that apart from the primes of congruence with lower level, the only other primes that can divide the order of the component group are those that divide the order of the torsion group (or the cuspidal group). For prime level, Emerton uses Mazur's result [Maz77, p. 99] that for $J_0(N)$, the specialization map from the cuspidal group to the component group is an isomorphism, in order to deduce the corresponding isomorphism for the quotient A. Now when the level N is not prime, but square-free, the component group has been studied in [Maz77, Appendix] where it is shown that for $J_0(N)$, the order of the quotient of the component group by the image of the cuspidal group is divisible only by the primes 2 and 3. Using this result, the PI expects that a generalization of the techniques of Emerton would show that apart from 2, 3, and the primes of congruence with lower level, the only other primes that can divide the order of the component group of A are those that divide the order of the cuspidal group of A.

3.3 Relevance for the Birch and Swinnerton-Dyer formula

The PI and W. Stein [AS05, Prop. 4.6] showed that when $L_A(1) \neq 0$, the odd part of the denominator of $\frac{L_A(1)}{\Omega_A}$ divides $|C_A|$ (this is also discussed towards the end of Section 5.1). Thus in the BSD conjectural formula

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

one expects significant cancellation on the right side. By [Eme03], when the level N is prime, $c_N(A) = |A(\mathbf{Q})_{\mathrm{tor}}| = |A^\vee(\mathbf{Q})_{\mathrm{tor}}| = |C_A|$, and hence the denominator on the right side is just $|C_A|$.

When the level is not prime, if the BSD conjectural formula is true, then there should again be enough cancellation so that the denominator divides $|C_A|$. Thus the contributions to the torsion and arithmetic component group that are *not* explained by the cuspidal group should cancel (when the analytic rank is zero). To this end, our Projects 3.2 and 3.4 on the torsion and component groups would show that the extra contributions to torsion and arithmetic component groups come at the same set of odd primes: those ℓ such that for some $p \,|\, N$, $w_p = -1$ and f is congruence modulo ℓ to a newform of level dividing N/p. But as discussed above, much more should be true: the exponents of these primes in $\prod_p c_p(A)$ and $|A(\mathbf{Q})_{\mathrm{tor}}| \cdot |A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ should be the same when A has analytic rank zero. In fact, in addition to Observations 3.1 and 3.3, the PI found the following in all examples he checked in Stein's table:

Observation 3.5. Suppose a prime ℓ divides the order of the torsion group, but not the order of the cuspidal group. If $w_N = -1$, then there exist distinct primes p and q dividing N such that $w_p = w_q = -1$ and f is congruent modulo ℓ to a form of level dividing N/pq. If $w_N = 1$, then there usually exists only one prime p dividing N such that $w_p = -1$ and f is congruent modulo ℓ to a newform of level dividing N/p.

For example, in the case of the elliptic curve $E = 66C1$ which has trivial cuspidal group and $w_N = -1$, one finds that $c_2(E) = 10$, $c_3(E) = 5$, $c_{11}(E) = 1$ and $|E(\mathbf{Q})_{\mathrm{tor}}| = 10$. Thus the odd parts of $c_2(E) \cdot c_3(E) \cdot c_{11}(E)$ and $|E(\mathbf{Q})_{\mathrm{tor}}|^2$ are the same, i.e., the contributions from congruences with lower level cancel on the right hand side of (2). This is consistent with the BSD formula by the discussion above. For the elliptic curve $E = 123A1$, which has trivial cuspidal subgroup, but $w_N = 1$, one finds that $c_3(E) = 5$, $c_{41}(E) = 1$, and $|E(\mathbf{Q})_{\mathrm{tor}}| = 5$; so $\frac{c_3(E) \cdot c_{41}(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2} = \frac{1}{5}$. Thus the contributions from congruences with lower level on the right hand side of the BSD formula (2) need *not* cancel when $w_N = 1$.

While the different behavior of the torsion group in the two cases $w_N = -1$ and $w_N = 1$ may seem strange, what is true in both cases is that if f is congruent to an eigenform g whose true level is M (where $M \,|\, N$), then W_M acts as -1 on g. Thus for example if W_N acts as -1 on f, then the level has to drop twice so that W_M acts again as -1 on g (considering that if the level drops by a prime p, then $w_p = -1$). We expect that our investigations in Projects 3.2 and 3.4 will throw some light on this matter.

As regards the component group, if part of it is due to congruences with lower level, the level need *not* drop by two primes even if the analytic rank is zero (e.g., it doesn't in the case the example 114C1 we gave before, for which $w_N = -1$). Thus there seems to be no distinction between the cases $w_N = -1$ and $w_N = 1$ as far as the arithmetic component group is concerned.

Finally, one would also like to know how the contributions from the cuspidal group distribute among $\prod_p c_p(A)$ and $|A(\mathbf{Q})_{\mathrm{tor}}| \cdot |A^\vee(\mathbf{Q})_{\mathrm{tor}}|$. When the analytic rank is zero, considering that the denominator of $L_A(1)/\Omega_A$ divides $|C_A|$ and in view of the BSD formula, one expects that $|C_A|$

divides each of $\prod_p c_p(A)$, $|A(\mathbf{Q})_{\mathrm{tor}}|$, and $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ only once ("generically" speaking). This seems provable (more generally when $w_N = -1$) in view of the description of the order of the component group of $J_0(N)$ in [Maz77, Appendix] and the order of the cuspidal group of $J_0(N)$ in [Lig75] – for example, the factors appearing in the expressions for the orders of the two groups are similar. When $w_N = 1$, the cuspidal group of A is trivial (since W_N acts as -1 on $(0) - (\infty)$).

While we have been talking about the torsion group of A, we have not yet addressed the torsion group of its dual. In [Eme03], Emerton treats both torsion groups simultaneously (for prime level) by looking more generally at torsion groups of subquotients (which includes both A and its dual); we plan to follow the same strategy and expect that it will work for arbitrary level as well.

Finally, while we have been talking about characterizing the primes that can divide the torsion and component groups, one would like to also show when they actually *do* divide the torsion and component groups, and say something about the exact order of these groups (as opposed to just describing the primes in their support). The PI will investigate this issue also in the projects mentioned above. We can summarize our discussion above as:

Project 3.6. Investigate the exact cancellations happening on the right hand side of the BSD formula, i.e., in the ratio of $\prod_p c_p(A)$ to $|A(\mathbf{Q})_{\mathrm{tor}}| \cdot |A^\vee(\mathbf{Q})_{\mathrm{tor}}|$, at least when the level is square-free and staying away from the prime 2 (and perhaps 3 as well).

To the knowledge of the PI, for non-prime level, the torsion and component groups have not been studied well, especially with regard to the BSD formula. In view of the patterns mentioned above and the ensuing discussions, the PI feels that the projects above are important problems that can be resolved and deserve immediate investigation.

4 Visibility theory

Mazur [CM00] introduced the notion of visibility in order "visualize" elements of Shafarevich-Tate groups as subvarieties of some ambient abelian variety. Let J be an abelian variety and let C be an abelian subvariety of J, both defined over $\mathbf{Q}$. Then the subgroup of $Ш_C$ visible in J is defined as $\mathrm{Vis}_J(Ш_C) = \ker(Ш_C \to Ш_J)$. An element of $Ш_C$ is said to be *visible* in J if it is in $\mathrm{Vis}_J(Ш_C)$. We have the following result [AS02, Thm. 3.1]:

Theorem 4.1. *Let N' be a positive integer, and let C and B be abelian subvarieties of $J_0(N')$ such that $C(\mathbf{Q})$ is finite. Let m be an odd integer coprime to*

$$N' \cdot \#\Big(\Big(\frac{C+B}{B}\Big)(\mathbf{Q})_{\mathrm{tor}}\Big) \cdot \#B(\mathbf{Q})_{\mathrm{tor}} \cdot \prod_{\ell | N'} \Big(c_\ell(C) \cdot c_\ell(B)\Big). \tag{3}$$

Suppose $B[m] \subseteq C$. Then there is an injection $B(\mathbf{Q})/mB(\mathbf{Q}) \hookrightarrow \mathrm{Vis}_{J_0(N')}(Ш_C)$. In particular, if B has positive Mordell-Weil rank, then m divides $|Ш_C|$.

Simply put, this theorem says that for an abelian variety, nontrivial intersections with abelian varieties of higher Mordell-Weil rank often imply the existence of nontrivial elements of the Shafarevich-Tate group. One usually uses Theorem 4.1 as follows: as before, let f be a newform of weight 2 on $\Gamma_0(N)$, and let $A = A_f$ be the quotient of $J_0(N)$ associated to f. Suppose for this section that $L_{A_f}(1) \neq 0$; then $A_f^\vee(\mathbf{Q})$ is finite. In the theorem, we take $N' = N$, $J = J_0(N)$, and $C = A_f^\vee$. If f is congruent to another eigenform g on $\Gamma_0(N)$ such that $L(g,1) = 0$, then we take $B = A_g^\vee$ and m to be a divisor of the order of the intersection of $A_f^\vee$ and $A_g^\vee$. Then either by assuming the first part of the BSD conjecture or by an explicit calculation, B has positive Mordell-Weil rank, and usually m is coprime to the product in (3) above. The hypothesis $B[m] \subseteq C$ is

difficult to check in general, but if B is an elliptic curve, it can be checked computationally. Then the theorem implies that m divides $|Ш_{A_f^\vee}| = |Ш_{A_f}|$ (the equality comes from the Cassels-Tate pairing).

For example [AS02, §4.1] there is a newform f of level 389 such that A_f has finite Mordell-Weil group, and f is congruent modulo 5 to another newform g of level 389 such that A_g is an elliptic curve with Mordell-Weil rank 2. Moreover, the hypotheses of the visibility theorem are satisfied for $C = A_f^\vee$, $B = A_g^\vee$, $N' = 389$, and $m = 5$, so we get an injection $(\mathbf{Z}/5\mathbf{Z})^2 \hookrightarrow Ш_{A_f^\vee}$, which shows that $|Ш_{A_f^\vee}| \geq 5^2$. The BSD conjecture predicts that $|Ш_{A_f^\vee}| = 5^2$, and thus visibility explains the BSD conjectural order of $Ш_{A_f^\vee}$.

However, one cannot always explain the Shafarevich-Tate group using congruences with eigenforms of the *same* level. For example [CM00, p. 25], there is a newform f of level 5389 such that the BSD formula predicts that $|Ш_{A_f^\vee}| = 3^2$, but 3 does not divide the order of $\mathrm{Vis}_{J_0(5389)}(Ш_{A_f^\vee})$. However, for any M, one can consider the image A' of $A_f^\vee$ in $J_0(NM)$ using a certain standard map $J_0(N) \to J_0(NM)$. W. Stein found that f is congruent modulo 3 to a newform g' of level $7 \cdot 5389$ such that $A_{g'}$ has positive Mordell-Weil rank. He then used Theorem 4.1 above to conclude that there is an injection $(\mathbf{Z}/3\mathbf{Z})^2 \hookrightarrow \mathrm{Vis}_{J_0(7\cdot 5389)} Ш_{A'}$, from which he deduced that $|Ш_{A_f^\vee}| = 3^2$. Thus in this case, visibility explains all of the conjectured $Ш_{A_f^\vee}$, using congruences at a *higher* level MN. We shall loosely call this phenomenon *visibility at higher level*. In fact, Stein conjectures that this happens more generally:

Conjecture 4.2 (Stein). *If $L_{A_f}(1) \neq 0$, then all of $Ш_{A_f^\vee}$ can be explained by using an appropriate generalization of Theorem 4.1, by taking $N' = NM$ for various positive integers M and using appropriate abelian subvarieties B of $J_0(NM)$.*

Note that one is not claiming that there is a *single* $J_0(NM)$ which explains all of $Ш_{A_f^\vee}$, but that for various M's there exist abelian varieties B as in Theorem 4.1 such that the images of the injections as in the second-last sentence in Theorem 4.1 explain all of $Ш_{A_f^\vee}$. Apart from computational evidence, the reason behind making the conjecture above is that one knows [AS02, Prop 1.3] that given $x \in Ш_A$, there exists *some* abelian variety J and an injection $\phi : A^\vee \to J$ such that x is visible in J, moreover J is a quotient of $J_1(NM)$ for some M.

In this proposal, we describe a plan that uses visibility at higher level to show that the BSD conjectured value of $Ш_{A_f}$ divides the actual value (assuming the first part of the BSD conjecture). Before doing that, we need to overcome a slight drawback with Theorem 4.1: it is difficult to verify the hypothesis that $B[m] \subseteq C$. In fact if the dimension of B is significantly bigger than that of C, then this condition may not be satisfied. As an alternative to Theorem 4.1, one has the following theorem (see [AM04, Prop. 5.5]), which is easily extracted from [DSW03]:

Theorem 4.3. *Suppose N is square-free and f is a newform on $\Gamma_0(N)$ with $L_{A_f}(1) \neq 0$. Let q be an odd prime such that $q \nmid N$. Suppose $g \in S_2(\Gamma_0(N), \mathbf{C})$ is an eigenform such that A_g has positive Mordell-Weil rank, and $f \equiv g$ modulo a maximal ideal $\mathfrak{q}$ of $\mathbf{T}$ lying over q. Assume the following:*
1) $A_f[\mathfrak{q}]$ is an irreducible representation of the absolute Galois group of $\mathbf{Q}$.
2) For all primes $p|N$, $p \not\equiv -w_p \pmod{q}$.
3) The following does **not** *happen: for all primes $p|N$, if f is congruent* mod $\mathfrak{q}$ *to a newform of level dividing N/p (for Fourier coefficients of index coprime to Nq), then $w_p = 1$.*
Then if for some prime $p \mid N$, f is congruent mod $\mathfrak{q}$ *to a newform of level dividing N/p (for Fourier coefficients of index coprime to Nq), then $\mathfrak{q}$ divides $c_p(A_f)$; otherwise, $\mathfrak{q}$ divides $|Ш(A_f)|$. In any case, $\mathfrak{q}$ divides $|Ш(A_f)| \cdot \prod_{p|N} c_p(A_f)$.*

Recall that w_p denotes the eigenvalue of f under the Atkin-Lehner involution W_p. The appearance of the component groups is not surprising and in fact makes sense from the viewpoint of the BSD conjectural formula (see Section 3.2). We remark that the hypotheses 1) and 2) can probably be replaced by the simpler hypothesis that q does not divide $|A(\mathbf{Q})_{\mathrm{tor}}|$; firstly, under the latter condition, hypothesis 1) is already proved by Mazur [Maz77] when the level is prime, and the PI will try to generalize his arguments. Secondly, hypothesis 2) is related to the requirement that q does not divide the order of the cuspidal group (see Section 3.1), and will follow if $q \nmid |A(\mathbf{Q})_{\mathrm{tor}}|$. Hypothesis 3) is a bit more mysterious: the PI will investigate examples where this happens (e.g., see [AM04, Eg. 5.6(1)]), to get a better idea of what to expect.

Theorem 4.3 has the advantage that there is no hypothesis that $A_g^\vee[q] \subseteq A_f^\vee$, and so it lends itself well for theoretical applications. But it has the disadvantage that a priori it does not extend to congruences modulo powers of q (which is needed in Project 5.2) or to the case where f is not new at level N (which is needed for visibility at higher level in Section 6.2). Theorem 4.1 did not have these restrictions, but it had the annoying hypothesis that $B[m] \subseteq C$.

The PI proposes to "amalgamate" the two theorems above, with an eye towards the BSD conjectural formula (see Project 5.2):

Project 4.4. Prove a theorem of following form:
Suppose N is square-free. Let f and g be eigenforms of level dividing N such that A_f has Mordell-Weil rank zero and A_g has positive Mordell-Weil rank. Let A'_f and A'_g be the images of $A_f^\vee$ and $A_g^\vee$ under suitable degeneracy maps in $J_0(N)$. Let m denote the largest divisor of $|A'_f \cap A'_g|$ that is coprime to $2N \cdot |A_f(\mathbf{Q})_{\mathrm{tor}}|$ and to the degrees of the degeneracy maps. Then m divides $|Ш(A_f)| \cdot \prod_{p|N} c_p(A_f)$.

The key idea behind the proofs of Theorems 4.1 and 4.3 is the same: to transfer the Mordell-Weil part of one motive to the Shafarevich-Tate group of the other using intersections (or congruences). However the techniques used in the proof are different: the first one uses the language of abelian varieties, whereas the second one uses the language of representations (as in the Bloch-Kato conjecture [BK90]). The PI will look more closely at the proofs to see if the techniques can be applied in parallel for Project 4.4. Another approach is to consider the terms in Theorem 4.1 as modules over the Hecke algebra $\mathbf{T}$, and prove a formula involving order ideals (instead of integers). Thus m will get replaced by an ideal $\mathfrak{m}$ of $\mathbf{T}$ over m, and the hypothesis $B[m] \subseteq C$ would get replaced by $B[\mathfrak{m}] \subseteq C$, which is more likely to hold since $B[\mathfrak{m}]$ is considerably smaller than $B[m]$; in fact, the proof of Theorem 4.1 in [AS02] already works if $\mathfrak{m}$ is principal. This generalized version of Theorem 4.1 may resolve Project 4.4. Also, there is a third version of the visibility theorem, due to Cremona and Mazur [AS05, Appendix], where the hypothesis is of the form $B[m] = C[m]$, and can probably be replaced by the hypothesis $B[\mathfrak{m}] = C[\mathfrak{m}]$ to yield the desired theorem in Project 4.4.

5 A formula for the special L-value and visibility at the same level

Before discussing our plan that uses visibility at a higher level to show that the BSD conjectured value of $Ш_A$ divides the actual value (Section 6), we first discuss how a part of $Ш_A$ can be explained by visibility at the *same* level. As before, f is a newform on $\Gamma_0(N)$ such that $L_A(1) \neq 0$, where A is the modular abelian variety associated to f. In Section 5.1, we extract an explicit factor of $L_A(1)/\Omega_A$ which measures certain congruences, and in Section 5.2 we relate this factor to $Ш_A$.

5.1 A formula for $L_A(1)/\Omega_A$

We start with the definitions of some terms that will be needed to describe our formula. We have an isomorphism of real vector spaces $H_1(X_0(N), \mathbf{Z}) \otimes \mathbf{R} \xrightarrow{\simeq} \mathrm{Hom}_{\mathbf{C}}(H^0(X_0(N), \Omega^1), \mathbf{C})$, given by integrating differentials along cycles. The *winding element*, denoted e, is the element of $H_1(X_0(N), \mathbf{Z}) \otimes \mathbf{R}$ that corresponds under the isomorphism above to the map which takes a differential ω to $-\int_0^{i\infty} \omega$. Let π denote the quotient map $J_0(N) \to A$, and let π_* denote the induced map $H_1(J_0(N), \mathbf{Z}) \to H_1(A, \mathbf{Z})$. We have the complex conjugation involution on $X_0(N)$ given by $\tau \mapsto -\overline{\tau}$, which induces an action on several groups below; if G is such a group, then we denote by G^+ the subgroup of elements of G that are invariant under this induced action. Let H be short for $H_1(J_0(N), \mathbf{Z})$ and let $\Im$ denote the annihilator of the divisor $(0) - (\infty)$ in $J_0(N)(\mathbf{C})$ under the action of the Hecke algebra; then $\Im e \subseteq H^+$.

For simplicity, let us assume that N is square-free. In [Aga00, Prop. 4.1.6] (see also [AS05]), the PI proved that up to powers of 2,

$$\frac{L_A(1)}{\Omega_A} = \frac{\left|\pi_*\left(\frac{H^+}{\Im e}\right)\right|}{|\pi_*(\mathbf{T}e/\Im e)|}\ , \tag{4}$$

The Hecke algebra $\mathbf{T}$ acts on the group $H_1(X_0(p), \mathbf{Z}) \otimes \mathbf{R}$; let I_e be the annihilator ideal of the winding element e with respect to this action. If G is a group on which $\mathbf{T}$ acts and I is an ideal of $\mathbf{T}$, then we denote by $G[I]$ the subgroup of elements that are annihilated by I.

Following an idea of Merel, we rewrite formula (4) as (again up to powers of 2)

$$\frac{L_A(1)}{\Omega_A} = \frac{\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right| \cdot \left|\pi_*\left(\frac{H^+[I_e]}{\Im e}\right)\right|}{|\pi_*(\mathbf{T}e/\Im e)|}\ . \tag{5}$$

The factor $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ measures a certain intersection, using which one can show [AM04, Prop 4.5] that if an odd prime q divides the factor $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$, then f is congruent mod q to an eigenform g such that $L(g, 1) = 0$. Assuming the first part of the BSD conjecture, A_g has positive Mordell-Weil rank and one can use visibility (e.g., Theorem 4.3) to relate this congruence to $Ш_A$, as we do presently in Section 5.2. Note that this is in conformity with the BSD formula, which, in view of formula (5), becomes (up to powers of 2):

$$\frac{\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right| \cdot \left|\pi_*\left(\frac{H^+[I_e]}{\Im e}\right)\right|}{|\pi_*(\mathbf{T}e/\Im e)|} \stackrel{?}{=} \frac{|Ш_A| \cdot \prod_{p|N} c_p(A)}{|A(\mathbf{Q})_{\mathrm{tor}}| \cdot |A^\vee(\mathbf{Q})_{\mathrm{tor}}|}\ . \tag{6}$$

Also, note that the group $\pi_*(\mathbf{T}e/\Im e)$ is the subgroup of $A_f(\mathbf{Q})_{\mathrm{tor}}$ generated by $\pi((0) - (\infty))$, and hence $|\pi_*(\mathbf{T}e/\Im e)|$ divides $|A_f(\mathbf{Q})_{\mathrm{tor}}|$ (see the proof of Prop. 4.6 of [AS05]).

5.2 The visible factor

Using the observation just above formula (6), the PI and L. Merel showed [AM04, Thm. 5.7]:

Theorem 5.1. *Suppose N is square-free, and q is a prime such that q divides $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$, but $q \nmid 2N$, and q satisfies hypotheses 1), 2), and 3) of Theorem 4.3. Assume the first part of the Birch and Swinnerton-Dyer conjecture on rank for all newforms g of level dividing N. Then if for some primes $p|N$, f is congruent* mod $\mathfrak{q}$ *to a newform of level dividing N/p (for Fourier coefficients of index coprime to Nq), then $\mathfrak{q}$ divides $c_p(A_f)$; otherwise, $\mathfrak{q}$ divides $|Ш(A_f)|$. In any case, $\mathfrak{q}$ divides $|Ш(A_f)| \cdot \prod_{p|N} c_p(A_f)$.*

The statement becomes much simpler if the level N is prime; in that case it just says that if q is a prime that divides $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$, and $q \nmid 2N(N-1)$, then q divides $|Ш(A_f)|$, assuming the first part of the BSD conjecture. The interesting thing that happens at non-prime level is that a prime dividing $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ may not divide $|Ш(A_f)|$, but divide some $c_p(A_f)$ instead (for an example, see [AM04, Eg. 5.8]). This is still in agreement with the conjectural formula (6).

The PI proposes to improve Theorem 5.1 as follows:

Project 5.2. Show that the part of the factor $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ that is coprime to $2N|A(\mathbf{Q})_{\mathrm{tor}}|$ divides $|Ш(A_f)| \cdot \prod_{p|N} c_p(A_f)$ (assuming the first part of the BSD conjecture on rank).

This would follow if our earlier Project 4.4 is successful. If not, there is another approach: in the proof of Theorem 5.1 in [AM04, §4], the group $\pi_*\left(\frac{H^+}{H^+[I_e]}\right)$ is shown to be the intersection of certain subquotients of $J_0(N)$, which in turn is related to congruences, and then to $|Ш_A|$. However, if the hypothesis $B[m] \subseteq C$ in Theorem 4.1 is improved as discussed towards the end of Section 4, then one can show *directly* that $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ divides $|Ш_A|$ (provided there are no congruences with lower level, and again assuming the first part of the BSD conjecture).

6 A formula of Gross and visibility at a higher level

In this section we sketch a novel plan (Section 6.2) to exploit a generalized version of a formula of Gross on the special L-value to show that the BSD conjectured value of the Shafarevich-Tate group of modular abelian varieties of analytic rank zero can be explained by visibility at *higher* level (assuming the first part of the BSD conjecture on rank and an auxiliary hypothesis). Gross' formula has already seen many important applications (e.g., [BD97] and the sequels, and [Vat02]), and in Section 6.1, we give another application to show a squareness in the special L-value.

We caution the reader that in our effort to avoid technicalities for the sake of simplicity, we may have missed some details in some of the definitions and formulas below, but this should not affect our overall argument. The PI will put more details and updates on this part of the proposal at `http://www.math.missouri.edu/~agashe/nsf.html`.

6.1 Squareness of the special L-value

In this subsection we assume that the level N is prime, but we state some of the definitions in more generality, as they will be needed in the next subsection. For details, the reader may see [BD96, §1-2] and [Vat02, §2]. Let K be a quadratic imaginary field whose discriminant $-D$ is coprime to N. Write $N = N^+N^-$, where N^+ is divisible only by those primes which split in K, and N^- is divisible only by primes that are inert in K. In this subsection, we will assume that $N^- = N$ (and so $N^+ = 1$).

Let B be the definite quaternion algebra of discriminant N^-. Let R be the Eichler order of level N^+ of B that is denoted R_{N^+,N^-} in [BD96, §1.1]. Let $\hat{\mathbf{Z}}$ denote the profinite completion of $\mathbf{Z}$ and let $\hat{\mathbf{Q}} = \mathbf{Q} \otimes \hat{\mathbf{Z}}$. Let $\hat{R} = R \otimes \hat{\mathbf{Z}}$ and $\hat{B} = B \otimes \hat{\mathbf{Q}}$. Let m be the number of double cosets $\hat{R}^* \backslash \hat{B}^* / B^*$ and let $g_1, \ldots, g_m$ be representatives for the double cosets. For $i = 0, \ldots, m$, let $R_i = g_i^{-1} \hat{R} g_i \cap B$; these are again Eichler orders of B. For example, when $N^+ = 1$, the R_i's may be taken to be the right (maximal) orders of representatives of left ideal classes of any fixed maximal order, as in [Gro87, §3].

Let $\mathcal{O}$ denote the ring of integers of K. If $\sigma : K \to B$ is a morphism of algebras and R' is an order of B, then we say that the pair (σ, R') is an optimal embedding if $\sigma(K) \cap R' = \sigma(\mathcal{O})$.

An oriented optimal embedding (σ, R') where R' is an Eichler order of level N^+ in B is called a Heegner point (sometimes called Gross point). Assume that $D > 4$, and for each $i = 1, \ldots, m$, let h_i denote the number of oriented optimal embeddings of $\mathcal{O}$ in R_i modulo conjugation by R_i^*. Let $\mathcal{P}$ denote divisor group supported on the R_i's (i.e., consisting of formal $\mathbf{Z}$-linear combinations of R_i's). Following Gross [Gro87], we define $e_D = \sum_{i=1}^m h_i[R_i] \in \mathcal{P} \otimes \mathbf{Q}$. Thus e_D is the formal sum of all Heegner points obtained from $\mathcal{O}$ and the R_i's (up to conjugation).

Let $\varepsilon_D = (\frac{-D}{\cdot})$ denote the non-trivial quadratic character associated to $K = \mathbf{Q}(\sqrt{-D})$. As before, let f be a newform on $\Gamma_0(N)$ such that $L_{A_f}(1) \neq 0$ and let $f \otimes \varepsilon_D$ denote the twist of f by ε_D. We have an action of the Hecke algebra $\mathbf{T}$ on $\mathcal{P}$. If M is a $\mathbf{T}$-module, then let π_f denote the operator on M corresponding to the projection to the f-isotypical component of M (i.e., where $\mathbf{T}$ acts via the eigenvalues of f). Let $w_i = |R_i^*/\langle \pm 1 \rangle|$. We define a pairing $\langle\ ,\ \rangle : \mathcal{P} \times \mathcal{P} \to \mathbf{Z}$ by requiring that $\langle R_i, R_j \rangle = \delta_{ij} w_i$. Then Gross' formula [Gro87, Cor. 11.6] reads:

$$L(f,1)\ L(f \otimes \varepsilon_D, 1) = \frac{(f,f)}{\sqrt{D}}\ \langle \pi_f(e_D), \pi_f(e_D) \rangle, \tag{7}$$

where (f,f) denotes the Petersson inner product.

Let $\mathcal{P}^0$ denote the subgroup of $\mathcal{P}$ of divisors of degree zero (i.e., whose coefficients add to zero). Let $a_E = \sum_{i=0}^g \frac{[R_i]}{w_i}$ denote the Eisenstein element and let $e_D^0 = e_D - \frac{\deg(e_D)}{\deg(a_E)} \cdot a_E$. Let $\Im$ be the ideal generated by $T_\ell - (1+\ell)$ for primes $\ell \nmid N$ and $U_p - 1$ for primes $p \mid N$. Then $\Im a_E = 0$, and so $\Im e_D^0 = \Im e_D$. Since $e_D^0 \in \mathcal{P}^0$, we have $\Im e_D = \Im e_D^0 \in \mathcal{P}^0$. Using some results from [RDH04], which rely on [Eme02], the PI and L. Merel [AM04, §6] show that Gross' formula implies that up to powers of 2,

$$\frac{L_{A_f}(1)}{\Omega_{A_f}} \cdot \frac{L(A_{f \otimes \varepsilon_D}, 1)}{(i\sqrt{D})^d \Omega_{A_f}^-} = \frac{\left| \pi_f\left(\frac{\mathcal{P}^0}{\Im e_D^0} \right) \right|^2}{|\pi_f(\mathbf{T}/\Im)|^2}\ , \tag{8}$$

where $d = \dim A$, $A_{f \otimes \varepsilon_D}$ is the modular abelian variety associated to $f \otimes \varepsilon_D$, and $\Omega_{A_f}^- = \mathrm{disc}(H_1(A_f, \mathbf{Z})^- \times S_2(\Gamma_0(N), \mathbf{Z})[I_f] \to \mathbf{C})$ is the "minus" period. Note that $\frac{L(A_{f \otimes \varepsilon_D}, 1)}{(i\sqrt{D})^d \Omega_{A_f}^-}$ is in fact an integer, and that the left hand side of (8) is just the rational part of the special L-value of A_f considered over $\mathbf{Q}(\sqrt{-D})$. Compare this formula to our formula (4) for $L_A(1)/\Omega_A$; by extending our base field to $\mathbf{Q}(\sqrt{-D})$, we have obtained a square for the special L-value (up to a power of 2).

Let $n = \mathrm{numr}(\frac{N-1}{12})$. Using the above formula and the theory visibility (as in Theorem 4.3 for prime level), the PI and L. Merel obtained the following result [AM04, Thm. 6.1]:

Theorem 6.1. *Let q be an odd prime such that q divides $\frac{L_{A_f}(1)}{\Omega_{A_f}}$, but $q \nmid n$. Suppose the following: (*) there exists a fundamental discriminant $-D$ that is coprime to N such that $L(A_{f \otimes \varepsilon_D}, 1) \neq 0$ and q does not divide $\frac{L(A_{f \otimes \varepsilon_D}, 1)}{(i\sqrt{D})^d \Omega_{A_f}^-}$.*

Then q^2 divides $\frac{L_{A_f}(1)}{\Omega_{A_f}}$ and the Birch and Swinnerton-Dyer conjectural value of $|Ш(A_f)|$.

Note that the denominator of $L_{A_f}(1)/\Omega_{A_f}$ divides n, and since we are assuming that $q \nmid n$, it makes sense to talk about q dividing $L_{A_f}(1)/\Omega_{A_f}$. Under just the first statement in Theorem 6.1, it follows that q^2 divides the actual order of $Ш(A_f)$ (see [AM04, Rmk. 6.3(2)]), so Theorem 6.1 provides evidence towards the BSD formula (1). Regarding the hypothesis (*) above, it is known

that there exist infinitely many D such that $L(A_{f\otimes\varepsilon_D},1)\neq 0$ (by results of Waldspurger), but the existence of D such that q does not divide $\frac{L(A_{f\otimes\varepsilon_D},1)}{(i\sqrt{D})^d\Omega^-_{A_f}}$ is not known; however one expects the latter to hold heuristically speaking: because assuming the BSD conjecture for the twisted L-value, the Shafarevich-Tate group of the twist of A_f should change with D (and hence be not divisible by q often), and since $q\nmid n$, q is not expected to divide the orders of the component groups and the torsion subgroups of the twists, generically speaking.

Project 6.2. Generalize Theorem 6.1 and formula (8) to the case where the level N is square-free.

The PI plans to do this by considering the generalization to arbitrary level of Gross' formula, which is proved in [Gro87] for prime level. Such a generalization holds by work of Zhang [Zha04], and has already been quoted (see, e.g., [BD97, Thm. 1.1] and [Vat02, p. 16]). It should be very similar to formula (7). In order to put the generalized Gross formula in a form similar to formula (8), we have to generalize to arbitrary level some of the results of [Eme02] for prime level. Emerton already indicates in Section 7 of [Eme02] to what extent his results extend to non-prime level; also Hida [Hid04] has recently shown different (and more generalizable) proofs of some of the results in [Eme02]. Finally, in the generalized version of Theorem 6.1, we may have to assume that q does not divide the orders of certain component groups and torsion groups.

6.2 Visibility at higher level

The goal of this section is to describe our plan for the following:

Project 6.3. For square-free N, show that the odd part of the BSD conjectured value of $|Ш_{A_f}|$ can be accounted for by visibility at the same and higher level, assuming the first part of the BSD conjecture and an auxiliary hypothesis similar to (*) in Theorem 6.1.

The PI proposes to do this by exploiting a generalized version of Gross' formula. We continue using the notation of the previous section, but drop the assumption that N is prime.

For simplicity, we will assume that formula (8) holds for square-free level away from the prime 2 (it most likely does, as indicated above). Let $I_{e_D^0}$ denote the annihilator of e_D^0 under the action of $\mathbf{T}$. Then in a manner similar to the derivation of formula (5) in Section 5.1, we can rewrite equation (8), up to powers of 2, as:

$$\frac{L_{A_f}}{\Omega_{A_f}}\cdot\frac{L(A_{f\otimes\varepsilon_D},1)}{(i\sqrt{D})^d\Omega^-_{A_f}}=\frac{\left|\pi\left(\frac{\mathcal{P}^0}{\mathcal{P}^0[I_{e_D^0}]}\right)\right|^2\cdot\left|\pi\left(\frac{\mathcal{P}^0[I_{e_D^0}]}{\Im e_D^0}\right)\right|^2}{|\pi_f(\mathbf{T}/\Im)|^2}\ . \tag{9}$$

Compare this to formula (5) for $L_{A_f}(1)/\Omega_{A_f}$, which we reproduce below, up to powers of 2 (assuming N is square-free, so that we can ignore the Manin constant c_A):

$$\frac{L_A(1)}{\Omega_A}=\frac{\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|\cdot\left|\pi_*\left(\frac{H^+[I_e]}{\Im e}\right)\right|}{|\pi_*(\mathbf{T}e/\Im e)|}\ . \tag{10}$$

As discussed in Section 5.2, the factor $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ in the formula above measures certain congruences (at the same level) that can be related to $Ш_A$ using visibility. However, usually such a congruence prime q divides the factor $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ only once, whereas by Theorem 6.1, q^2

divides $\frac{L_A(1)}{\Omega_A}$. Thus the factor $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ does not capture *all* of the part of $Ш_A$ that can be explained by visibility at the *same* level N.

Now if an odd prime q divides the factor $\left|\pi\left(\frac{\mathcal{P}^0}{\mathcal{P}^0[I_{e_D^0}]}\right)\right|$ in formula (9) above, then f is congruent modulo q to an eigenform g of level N such that $L(g,1)=0$ or $L(g\otimes\varepsilon_D,1)=0$ (this is similar to the observation made after formula (5)). Thus if q is a congruence prime as above, then q^2 divides the first factor $\left|\pi\left(\frac{\mathcal{P}^0}{\mathcal{P}^0[I_{e_D^0}]}\right)\right|^2$ in formula (9) above. Generally speaking, if we a choose D satisfying (*), then we expect that q^2 is the highest power of q that divides the numerator in the right hand side of formula (9), and hence that the factor $\left|\pi\left(\frac{\mathcal{P}^0}{\mathcal{P}^0[I_{e_D^0}]}\right)\right|^2$ captures *all* of the part of $Ш_A$ visible at the *same* level N. Thus we expect that the other factor $\left|\pi\left(\frac{\mathcal{P}^0[I_{e_D^0}]}{\Im e_D^0}\right)\right|^2$ is *not* divisible by congruence primes that explain visibility at the same level.

Now can think of formula (8) as obtained by a "parametrization at level N", and instead one can consider a formula obtained by a "parametrization at level NM" by either adding extra ramification corresponding to M to the quaternion algebra B or by multiplying the level N^+ of the Eichler orders by M (there will be some restrictions on how many primes can divide M). One expects that a formula similar to (8) should hold even after adding ramification to B, considering that Zhang [Zha04] works at a higher level ND to deduce a formula at level N. Thus we expect the following formula for "level NM" up to powers of 2:

$$\frac{L_{A_f}(1)}{\Omega_{A_f}}\cdot\frac{L(A_{f\otimes\varepsilon_D},1)}{(i\sqrt{D})^d\Omega^-_{A_f}}=\left|\pi_f\left(\frac{\mathcal{P}^0_{NM}}{\mathcal{P}^0_{NM}[I_{e^0_{D,NM}}]}\right)\right|^2\cdot\left|\pi_f\left(\frac{\mathcal{P}^0_{NM}[I_{e^0_{D,NM}}]}{\Im_{NM}e^0_{D,NM}}\right)\right|^2, \tag{11}$$

where we have put subscripts NM to emphasize that the objects are at "level NM".

As before If Conjecture 4.2 on visibility at higher level is true, then for some M, q mus the remaining factor $\left|\pi\left(\frac{\mathcal{P}^0_{NM}[I_{e^0_{D,NM}}]}{\Im_{NM}e^0_{D,NM}}\right)\right|$ should not be divisible by q.

In formula (11), if an odd prime q divides the factor $\left|\pi_f\left(\frac{\mathcal{P}^0_{NM}}{\mathcal{P}^0_{NM}[I_{e^0_{D,NM}}]}\right)\right|$, then f is congruent modulo q to an eigenform g of level NM such that $L(g,1)=0$ or $L(g\otimes\varepsilon_D,1)=0$ (this is similar to the observation after formula (5)). If we a choose D satisfying (*), then $L(g\otimes\varepsilon_D,1)=0$ is not possible, since then q would divide $\frac{L(A_{f\otimes\varepsilon_D},1)}{(i\sqrt{D})^d\Omega^-_{A_f}}$ (by a congruence argument). Thus $L(g,1)=0$, and one can use visibility to show that q divides $|Ш_{A_f}|$. The term $\left|\pi_f\left(\frac{\mathcal{P}^0_{NM}}{\mathcal{P}^0_{NM}[I_{e^0_{D,NM}}]}\right)\right|^2$, being a square, usually captures *all* of the part of $Ш_{A_f}$ that is visible at level NM (in view of Theorem 6.1) – this was not the case in formula (5), where the factor $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ does not capture *all* of the visible part of $Ш_{A_f}$, even at the same level.

Let q be a prime that divides $\frac{L_{A_f}(1)}{\Omega_{A_f}}$, but does not divide the orders of the component groups (and thus is expected to divide $|Ш_{A_f}|$). Suppose we can prove the following:

(**) there exists an M such that q does not divide the second factor $\left|\pi_f\left(\frac{\mathcal{P}^0_{NM}[I_{e^0_{D,NM}}]}{\Im_{NM}e^0_{D,NM}}\right)\right|$ above.

Then q would divide the first factor $\left|\pi_f\left(\frac{\mathcal{P}^0_{NM}}{\mathcal{P}^0_{NM}[I_{e^0_{D,NM}}]}\right)\right|$, which would imply by the argument just above that q divides $|Ш_{A_f}|$ (recall that we are assuming the first part of the BSD conjecture on

rank). Following Project 5.2, one should be able to extend this result to powers of q, and thus by taking different M's for different q's, account for the part of the BSD conjectured order of $Ш_{A_f}$ that is coprime to $2N \cdot |A(\mathbf{Q})| \cdot \prod_{p|N} c_p(A_f)$.

Note that $\left| \pi_f \left(\frac{\mathcal{P}^0_{NM}[I_{e^0_{D,NM}}]}{\Im_{NM} e^0_{D,NM}} \right) \right|$ divides the order of the torsion part of $\frac{\mathcal{P}^0_{NM}}{\Im_{NM} e^0_{D,NM}} = \frac{\mathcal{P}^0_{NM}}{\Im_{NM} e_{D,NM}}$. Thus to prove (**), it suffices to prove that

(***) for some M, q does not divide the torsion part of $\frac{\mathcal{P}^0_{NM}}{\Im_{NM} e^0_{D,NM}}$,

which is reasonable to expect, considering that we have a large choice of M's (and D's).

At the PI's request, D. Kohel did some computations that give some evidence towards (***). For example, there is a newform f of level $N = 1283$ for which the BSD conjecture predicts that $q = 5$ divides $|Ш_{A_f}|$. The 5-torsion part of $Ш_{A_f}$ is not visible at level 1283, but W. Stein made computations which suggest that it could be visible at level $3 \cdot 1283$. D. Kohel has checked that 5 divides the order of the torsion part of $\frac{\mathcal{P}^0_{NM}}{\Im_{NM} e_{D,NM}}$ for $M = 1$ for every D, but not for $M = 3$ for several D (he considered Eichler orders of level 1 and 3 respectively in the quaternion algebra ramified at 1283). This is as predicted by (***). The PI expects that this calculation can be used to show that the entire odd part of $|Ш_{A_f}|$ can be explained by visibility at the higher level $3 \cdot 1283$, but has not yet checked that (*) is satisfied.

There are two approaches that the PI plans to follow to prove (***). One approach is to write the group $\frac{\mathcal{P}^0_{NM}}{\Im_{NM} e^0_{D,NM}}$ in terms of generators and relations, and show that in some suitable limit $M \to \infty$, the group is torsion-free. For example, we can try to show some kind of linear independence of the $t_i e^0_{D,NM}$ for certain generators t_i of $\Im$ – a similar idea was used crucially in [Mer96, Prop. 3] and in a combinatorial lemma in [Par99, §5]. The other strategy is to use the explicit action of the Hecke operators (especially as the level N^+M of the Eichler orders changes when we vary M) in terms of certain Bruhat-Tits trees and prove the appropriate properties for these graphs – this brings to mind work of Vatsal [Vat02], which however is in a different direction (changing the conductor of the Hecke character). As mentioned earlier, D. Kohel is doing some computations of the groups involved above, and the PI will consider them at each stage of either strategy mentioned above.

The PI feels that there is enough flexibility and structure in the strategies above that if the conjectured part of the Shafarevich-Tate group can indeed be explained by visibility at higher level (and there is computational and theoretical evidence to believe this), then our plan should prove it (assuming the first part of the BSD conjecture on rank and the auxiliary hypothesis (*)).

7 Broader impact

The projects mentioned above emphasize the need for doing computations in number theory – several of them are based on patterns observed by the PI in [Ste] and [Cre97]. Also, some of the computational needs of our project that involves the use of Gross' formula may serve as a motivation for D. Kohel (personal communication) to develop a general package for computations involving the arithmetic of quaternion algebras – this should be helpful for many applications to number theory outside this proposal.

While working in arithmetic geometry, the PI is also involved in applications of elliptic curves to cryptography [ALV04], which has broader applications to society. He is also teaching a graduate course on the topic, and co-advised an undergraduate student (belonging to an underrepresented group) for a reading course on the applications of number theory to cryptography. The PI is cur-

rently advising one graduate student and co-advising another, and some of the funding will be used to support graduate student research and provide travel money for students to attend conferences elsewhere. We also plan to use the funds to invite outside speakers to the number theory seminar at the University of Missouri. Thus the funding of this project would help promote number theory activity beyond the already established number theory centers and build partnerships.

References

[Aga00] A. Agashe, *The Birch and Swinnerton-Dyer formula for modular abelian varieties of analytic rank zero*, Ph.D. thesis, University of California, Berkeley (2000), available at `http://www.math.missouri.edu/~agashe/math.html`.

[ALV04] A. Agashe, A. Lauter, and R. Venkatesan, *Constructing elliptic curves with known number of points over a prime field*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 1–17.

[AM04] A. Agashe and L. Merel, *A visible factor of the special L-value*, preprint (2004), available at `http://www.math.missouri.edu/~agashe/math.html`.

[AS02] A. Agashe and W. A. Stein, *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.

[BD96] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves*, Invent. Math. **126** (1996), no. 3, 413–456.

[BD97] ———, *A rigid analytic Gross-Zagier formula and arithmetic applications*, Ann. of Math. (2) **146** (1997), no. 1, 111–147.

[BK90] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

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

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

[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.

[Dum04] N. Dummigan, *Level-lowering for higher congruences of modular forms*, preprint (2004), available at `http://www.shef.ac.uk/personal/n/neildummiganshomepage/papers.html`.

[Eme02] Matthew Emerton, *Supersingular elliptic curves, theta series and weight two modular forms*, J. Amer. Math. Soc. **15** (2002), no. 3, 671–714 (electronic).

[Eme03] ———, *Optimal quotients of modular Jacobians*, Math. Ann. **327** (2003), no. 3, 429–458.

[Gro87] Benedict H. Gross, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115–187.

[Hid04] H. Hida, *The integral basis problem of Eichler*, preprint (2004), available at http://www.math.ucla.edu/~hida.

[IR90] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[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.

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry.

[Lig75] Gérard Ligozat, *Courbes modulaires de genre* 1, Société Mathématique de France, Paris, 1975, Bull. Soc. Math. France, Mém. 43, Supplément au Bull. Soc. Math. France Tome 103, no. 3. MR MR0417060 (54 #5121)

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

[Mer96] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449.

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

[RDH04] M. Rebolledo-Dhuin Hochart, *Module supersingulier et poinits rationnels des courbes modulaires*, Ph.D. thesis, Chevaleret (2004), available at `http://www.math.jussieu.edu/~maru`.

[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.

[Rub98] K. Rubin, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), Cambridge Univ. Press, Cambridge, 1998, pp. 351–367.

[Shi77] G. Shimura, *On the periods of modular forms*, Math. Ann. **229** (1977), 211–221.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992.

[Ste] W. A. Stein, `http://modular.fas.harvard.edu/Tables/non_zeroinf_tor.txt`.

[Vat02] V. Vatsal, *Uniform distribution of Heegner points*, Invent. Math. **148** (2002), no. 1, 1–46.

[Zha04] S.-W. Zhang, *Gross-Zagier formula for* GL(2) II, preprint (2004).