The Birch and Swinnerton-Dyer conjectural formula

Project description

Amod Agashe

1 Introduction

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. 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 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.

We study the second part of the BSD conjecture, which is a formula that relates several fundamental invariants of the elliptic curve or 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, and is an analog of the ideal class group. The theory of visibility has recently been used to give new evidence for this conjectural formula, mainly in specific examples. The PI proposes to use the theory of visibility to show theoretically that 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.

The PI will also investigate certain other arithmetic invariants appearing in the BSD formula, viz., the orders of the torsion and component groups of an abelian variety. These groups are of independent interest – 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). The PI proposes to extend techniques of Mazur and Emerton in order to characterize the primes that can divide the orders of the torsion and component groups.

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 and component groups and Sections 4–7 are devoted to 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.

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 has taught graduate courses on the topic, and served as an advisor for an undergraduate reading course as well as a Master's project in the the applications of number theory to cryptography. The PI is currently advising one graduate student in cryptography, and some of the funding will be used to support his research and provide travel money for students to attend conferences. We also plan to use the funds to invite outside speakers to the weekly Algebra seminar at Florida State University.

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 and modular abelian varieties

We recall briefly the BSD conjecture as generalized by Tate to abelian varieties (e.g., see [Lan91, III.5]). 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 finitely generated 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 $Ш_A$ or $Ш(A)$, 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, and if G is a finite group, then we use the symbol $|G|$ to denote the order of G. 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 (so $c_p(A) = 1$ for almost every prime), 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]). We will refer to the formula above as the *BSD (conjectural) formula*.

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. Suppose $L_A(1) \neq 0$. Then it follows by results of [KL89] that $A(\mathbf{Q})$ and $Ш_A$ are both finite; moreover, one can use

the theory of Euler systems to bound $|Ш_A|$ from above in terms of the order conjectured by the BSD formula, as in the work of Kolyvagin and of Kato (e.g., see [Rub98, Thm 8.6]). Also, the Eisenstein series method is being used by Skinner-Urban to show that the BSD conjectured order of $Ш_A$ divides the actual order.

2.2 Summary of the proposal

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. It is not true in general that either the torsion or component groups are explained by the divisor $(0) - (\infty)$. However, we sketch a plan to 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. This characterizes what primes can divide the torsion and component groups, and shows that the set of these primes is the same. At the same time, one expects more: there is often significant cancellation between the orders of the torsion and component groups; in particular, computational data suggests that the term $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ in the denominator of the BSD formula (1) divides the term $\prod_p c_p(A)$ in the numerator (away from 2, and perhaps 3). We sketch a plan to explain these cancellations, which involves an extension of several parts of Mazur's groundbreaking paper [Maz77] to non-prime level. Considering the important role that Mazur's paper has played (e.g., in the proof of Fermat's last theorem), we feel it is imperative to try to generalize the techniques to non-prime level, and to see to what extent they do actually generalize.

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 or one. 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.

When $L_A(1) \neq 0$, the PI and L. Merel extracted [AM05] an explicit factor F 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 used the theory of visibility to show that the odd primes that divide this factor divide $|Ш_A|$ (under certain mild hypotheses). In Section 5, we propose to extend this work to show that the *entire* factor F 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 $Ш_A$. 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 that uses 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 BSD conjecture can be accounted for.

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. In Section 7, we sketch a plan that uses visibility to show that the conjectural order of the Shafarevich-Tate group divides the actual order for quotients of analytic rank *one*. Unlike in the rank zero case, this is the only method we know that can show divisibility in the indicated direction; the theory of Euler system

gives a divisibility in the other direction (staying away from certain primes).

In Section 8, which serves as an appendix, we state a lemma about intersections of abelian subvarieties of $J_0(N)$ that is used in the earlier sections. This lemma should be useful in other areas of arithmetic geometry, and we give an application to the study of modular degrees and congruence numbers. 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. The rational divisor $(0) - (\infty)$ generates a finite subgroup of $J_0(N)(\mathbf{Q})$, which we denote C. The image of C under the quotient map $J_0(N) \to A$ is a cyclic subgroup of $A(\mathbf{Q})_{\mathrm{tor}}$; 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 $c_p(A)$.

In the landmark paper [Maz77], Mazur proved that if the level N is prime, then $C = J_0(N)(\mathbf{Q})_{\mathrm{tor}}$ and that the specialization map induces an isomorphism $C \cong \Phi_N(J_0(N))$. Building 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 significant cancellation on the right hand side of the BSD formula (1).

When the level is not prime, the situation is not so simple: the divisor $(0) - (\infty)$ does not fully explain either the torsion groups or the component groups. Let w_p denotes the eigenvalue of the Atkin-Lehner involution W_p acting on f. The product of the W_p's for $p \,|\, N$ is the Fricke involution W_N, whose eigenvalue is denoted w_N. Based on numerical data, we expect that if a prime $q > 3$ divides the order of the torsion subgroups or the component groups, then either q divides the order of the cuspidal subgroup C_A, or f is congruent modulo q to an eigenform of true level dividing N/p for some prime $p \,|\, N$ such that $w_p = -1$. As an example, for the elliptic curve $E = 66C1$ of [Cre97], the cuspidal subgroup is trivial, while $|E(\mathbf{Q})_{\mathrm{tor}}| = 10$, $c_2(E) = 10$, and $c_3(E) = 5$. One finds that for the corresponding newform f, one has $w_2 = w_3 = -1$, and that f is congruent modulo 5 to a newform at level 11 (the one associated to $11A1$). In Section 3.1, we outline a plan to prove the observation made just above, thus characterizing the primes that can divide the orders of the torsion and component groups.

The examples also suggest significant cancellation between the torsion and component groups in the BSD formula; e.g., we expect that that $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ divides $\prod_p c_p(A)$. We address this issue in Section 3.2. In order to prove these cancellations, one has to get some control on the orders of the torsion and component groups. For prime level, Mazur initiated the study of the torsion and component groups of $J_0(N)$, and Emerton used his results to deduce information for newform

quotients. The PI proposes to extend most of their results appropriately to arbitrary level, starting with square-free level. The propsed extensions of Mazur's groundbreaking paper [Maz77] should have applications beyond the BSD conjecture.

3.1 The orders of the torsion and component groups

Our first goal is the following:

Project 3.1. Show that if an odd prime ℓ divides the order of the torsion subgroup $A^\vee(\mathbf{Q})_{\rm tor}$ 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,

Suppose a prime ℓ divides the order of the torsion subgroup $A^\vee(\mathbf{Q})_{\rm tor}$. As in [Maz77, § II.14], there is a constituent V of the $(\mathbf{T}/\ell\mathbf{T})[{\rm Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module $A^\vee[\ell]$ of dimension one. Let $\mathfrak{m} = {\rm Ann}_{\mathbf{T}} V$, which is a maximal ideal with residue characteristic ℓ. Following an argument in [Maz77, § II.14], V comes from a finite flat group scheme, on which $T_r \equiv 1 + r \bmod \mathfrak{m}$ for every prime $r \nmid N$, and U_p acts as $a_p(f) = -w_p$ for every $p \,|\, N$.

Let $\mathfrak{I} = {\rm Ann}_{\mathbf{T}}((0) - (\infty))$. If r is a prime that does not divide N, then T_r acts as $1 + r$ on $(0) - (\infty)$, so $T_r - (1 + r) \in \mathfrak{I}$. Suppose N is square-free for simplicity. Then the cusps of $X_0(N)$ can be indexed by the positive divisors d of N, such that the cusp P_d is the image of a point $\frac{a}{d} \in \mathbf{P^1}(\mathbf{Q})$ with $\gcd(a, d) = 1$ (e.g., see [Dum]). Note that $P_1 = 0$ and $P_N = \infty$. A calculation shows that $(U_p - p)(P_1 - P_N) = -(p-1)(P_1 - P_p)$. We expect that the divisor $(P_1 - P_p)$ has order dividing $(p - 1)$, at least for almost every prime; for simplicity of exposition, we assume this is always so. Then U_p acts as multiplication by p on $(0) - (\infty)$. Thus $\mathfrak{I}$ is generated by the collection: $T_r - (1 + r)$ for every prime $r \nmid N$, and $U_p - p$ for every prime $p \,|\, N$.

If V arose as an image of $(0) - (\infty)$, then V is killed by $\mathfrak{I}$. Conversely, suppose all constituents V are killed by $\mathfrak{I}$. Since ℓ divides the order of $A^\vee(\mathbf{Q})_{\rm tor}$, one has a subgroup H of $A^\vee(\mathbf{Q})_{\rm tor}$ of order ℓ. Then H is killed by $\mathfrak{I}$. But if n is the order of $(0) - (\infty)$, then $n \in \mathfrak{I}$; so C is killed by multiplication by n. Thus ℓ divides the order of the cuspidal subgroup C_A. Moreover, by [Maz77, Cor. II.14.8], $J_0(N)^{\rm et}[\mathfrak{m}]$ has dimension at most one, so if every constituent V is killed by $\mathfrak{I}$, then the entire torsion is explained by $(0) - (\infty)$.

Thus the torsion is not explained by $(0) - (\infty)$ only if some constituent V is not killed by $\mathfrak{I}$. We want to see how much the action of the Hecke operators on V differs from its action on $(0) - (\infty)$; the tool to do this are certain Eisenstein series. For simplicity of exposition, we assume that $\ell \neq 2, 3$. Consider the Eisenstein series of level 1 given by: $e(q) = -1/24 + \sum_{n=1}^{\infty} \sigma(n) q^n$, where $\sigma(m)$ is the sum of the positive divisors of m. Starting with $e(q)$, we can apply the usual degeneracy operators to construct several Eisenstein series of level N that are eigenfuntions (essentially by diagonalizing the action of U_p on the p-old space for every $p \,|\, N$). For example, if N is prime, then $e(q) - Ne(q^N)$ is an Eisenstein series on $\Gamma_0(N)$, which Mazur used in his analysis when N is prime (see [Maz77, § II.5]). In particular, one can construct Eisenstein series on $\Gamma_0(N)$ that are eigenforms and whose r-th Fourier coefficient is $1 + r$ for a prime $r \nmid N$ and for a prime p that divides N, the p-th coefficient can be chosen to be either 1 or p.

A consideration of the Tate parametrization (see [Dum]) shows that if $w_p = 1$, then $\ell \,|\, (p+1) = (p + w_p)$, so $p \equiv -w_p \bmod \mathfrak{m}$, i.e., V is annihiliated by $\mathfrak{I}$ "locally" at p. Thus one only has to worry about the possibility that for some p, we have $w_p = -1$, and $p \not\equiv -w_p \bmod \mathfrak{m}$. If this happens, then we consider a suitable Eisenstein series e' whose p-th coefficient is 1 and the other prime index coefficients agree with that of f. Then $f - e'$ is a power series in q^p, and an argument similar to that in [Maz77, p.83-85] shows that the level of $f - e'$ can be lowered by p. Thus f itself is congruent modulo $\mathfrak{m}$ to a modular form of lower level. In fact, one can see that $f - e'$ is a linear

combination, under degeneracy maps, of Eisenstein series associated to the divisor $(0)-(\infty)$ at a level that divides N/p.

Thus we have a plan to achieve Project 3.1, although the details will have to be worked out, and one may have to circumvent any problems that arise (e.g., for starters, we may have to restrict to square-free level). Our argument also seems to indicate that the torsion subgroup of $J_0(N)(\mathbf{Q})$ is generated by the images of $(0)-(\infty)$ at various levels M dividing N under the degeneracy maps from level M to level N. A preliminary look at some data [Stea] seems to be in conformity with the previous statement, but a detailed check will have to be made. During our investigations, we will try to address the issue of rational torsion in the global object $J_0(N)$ as well.

Our other goal is the following:

Project 3.2. Show that if an odd prime ℓ divides $c_p(A)$, then ℓ divides the order of the cuspidal subgroup C_A or for some prime p that divides the level N, $w_p=-1$ and 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).

Emerton [Eme03] shows that the geometric component group is supported at maximal ideals $\mathfrak{m}$ such that either the associated canonical Galois representation $\rho_{\mathfrak{m}}$ (e.g., see [Rib90, Prop. 5.1]) arises from a finite flat group scheme (in which case we say that $\mathfrak{m}$ is *finite*) or $\rho_{\mathfrak{m}}$ is reducible. The reducible representations correspond to rational torsion, which we have already addressed just above, and are in conformity with what we want to show. If a finite maximal ideal $\mathfrak{m}$ with irreducible $\rho_{\mathfrak{m}}$ is in the support of a component group of f, then by Ribet's level lowering criterion [Rib90], f is congruent $\bmod \mathfrak{m}$ to an eigenform of lower level. Now these congruences can contribute to the *arithmetic* component group at a prime p only if $w_p=-1$, which explains the requirement $w_p=-1$. Thus the strategy for Project 3.2 is clear.

3.2 The cancellations in the Birch and Swinnerton-Dyer formula

Suppose for the moment that $L_A(1)\neq 0$, i.e., that A has analytic rank zero. Then the PI and W. Stein [AS05, Prop. 4.6] showed that the odd part of the denominator of $\frac{L_A(1)}{\Omega_A}$ divides $|C_A|$, which in turn divides $|A(\mathbf{Q})_{\mathrm{tor}}|$ (this also follows from formula (2) in Section 5). Thus the BSD conjectural formula says that $\frac{|Ш_A|\cdot\prod_p c_p(A)}{|A(\mathbf{Q})_{\mathrm{tor}}|\cdot|A^\vee(\mathbf{Q})_{\mathrm{tor}}|}\stackrel{?}{=}\frac{x}{|C_A|}$, for some integer x. Thus one expects significant cancellation on the left side. In particular, considering that $|C_A|$ divides $|A(\mathbf{Q})_{\mathrm{tor}}|$, and that usually the torsion groups have no relation with $Ш_A$, we expect that $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ divides $\prod_p c_p(A)$. Also, the contributions to the torsion groups that are *not* explained by the cuspidal group should get cancelled by similar contributions to the arithmetic component groups. While our earlier projects show that the primes where the torsion group is supported are also in the support of the component groups, they do not explain the cancellations of actual orders.

We revert to the case where $L_A(1)$ may or may not be zero. Based on Cremona's data [Cre97], we still expect that $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ divides $\prod_p c_p(A)$. By Project 3.1, the contributions to $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ come from two sources: the divisor $(0)-(\infty)$ at level N and the divisors $(0)-(\infty)$ at lower levels, via congruences with with eigenforms of lower level.

Let us look at the second contribution first, since it is easier to explain. Suppose N is squarefree and f is congruent modulo a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ lying over a prime ℓ to an eigenform g of level dividing N/p for some prime p that divides N. Then it follows from an argument borrowed from [DSW03, § 7.4] (see [AM05, Prop. 5.3]) that if $p\not\equiv -w_p \bmod \mathfrak{m}$, $w_p=-1$, and both $A_f[\mathfrak{m}]$ and $A_g[\mathfrak{m}]$ are irreducible, then $\mathrm{ord}_{\mathfrak{m}}(c_p(A_f))>0$. The key idea in the proof is that if I_p denotes the inertia group, then one has $A_g[\mathfrak{m}]^{I_p}=A_g[\mathfrak{m}]$ since A_g has good reduction at p, and so since

$A_f[\mathfrak{m}] \cong A_g[\mathfrak{m}]$ as Galois modules (as both are irreducible), one has that $A_f[\mathfrak{m}]^{I_p}$ is also two dimensional. This latter fact essentially leads to the conclusion that $\mathrm{ord}_{\mathfrak{m}}(c_p(A_f)) > 0$. In our situation, the hypotheses $p \not\equiv -w_p \bmod \mathfrak{m}$, and $w_p = -1$ are satisfied, but the representation $A_f[\mathfrak{m}]$ is not irreducible (since there is rational ℓ-torsion). However, Lemma 8.2 of Section 8 can be used to circumvent the irreducibility hypothesis: by this lemma, it follows that $A_g^\vee \cap A_f^\vee \subseteq A_g^\vee[I_f + I_g] \subseteq A_f^\vee[I_f + I_g]$, provided certain Eisenstein ideals are Gorenstein, which requires an extension of the results of [Maz77] (we will come back to this point in the next paragraph). Thus we can replace the congruence ideal $\mathfrak{m}$ in the argument above by $[I_f + I_g]$ and expect to conclude that the order of the rational part of $A_g^\vee \cap A_f^\vee$ divides $c_p(A)$. Thus the contributions to $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ due to congruences with lower level should divide $\prod_p c_p(A)$.

It remains to explain how the contribution of $(0) - (\infty)$ to $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ cancels with its contribution to $\prod_p c_p(A)$ (both contributions are via natural projections). For this, we will try to mimic Emerton's proof [Eme03] that when N is prime, then the contributions of $(0) - (\infty)$ to $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ and $\Phi_N(A)$ have the same order. He starts with Mazur's result [Maz77] that when N is prime, the subgroup generated by $(0) - (\infty)$ is canonically isomorphic to $J_0(N)_{\mathrm{tor}}$ as well as to $\Phi_N(J_0(N))$. Emerton's key idea is to show that the quotient map $\Phi_N(J_0(N)) \to \Phi_N(A)$ on the component groups is a surjection "locally" at any maximal ideal $\mathfrak{m}$ that satisfies multiplicity one (i.e., $\dim_{\mathbf{T}/\mathfrak{m}} J_0(N)[\mathfrak{m}] = 2$) and is not finite. Note that finiteness is not a major concern at the moment, since that is related to congruences with lower level, whose contributions we have already discussed. When N is prime, the maximal ideals in the support of $(0) - (\infty)$ do satisfy multiplicity one by [Maz77, Cor II.16.3]. When the level is not prime, this need not be the case (e.g., see [CS]); however, perhaps Emerton's proof can be salvaged since it suffices that the maximal ideal is "good" in the sense of Section 8, and perhaps Mazur's techniques about the Gorenstein-ness of Eisenstein primes in [Maz77, § II.16] can be generalized sufficiently. We will do these investigations, which should show that "locally" at a maximal ideal $\mathfrak{m}$ in the support of $(0) - (\infty)$, the contribution of $(0) - (\infty)$ to $A^\vee(\mathbf{Q})_{\mathrm{tor}}$ is the same as the contribution to a suitable component group (the one that is killed by $\mathfrak{m}$). This should explain that "globally", the contribution of $(0) - (\infty)$ to $|A^\vee(\mathbf{Q})_{\mathrm{tor}}|$ divides its contribution to $\prod_p c_p(A)$.

Our ultimate goal is the following:

Project 3.3. Explain 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 $|A(\mathbf{Q})_{\mathrm{tor}}| \cdot |A^\vee(\mathbf{Q})_{\mathrm{tor}}|$.

As can be seen from our discussion above, this would be a long-term project, but we already have several leads going into it, and already significant progress can be foreseen. In addition to the papers of Mazur and Emerton, we will be studying the following articles (among others) closely:
1) The appendix by Mazur and Rapoport in [Maz77], which contains a description of the component groups of $J_0(N)$ when N is square-free.
2) Lorenzini's description [Lor95] of the torsion and component groups of $J_0(p^n)$.
3) Ligozat's formulas [Lig75] for the order of $(0) - (\infty)$ and other cuspidal divisors, and also the special case where N is product of two primes discussed in [CL97].
4) The description of the Shimura subgroup (which contributes to the Eisenstein kernel) in [LO91].
5) A detailed study of an example of failure of Gorenstein-ness in [CS].
6) Numerical data, including Stein's computation [Stea] of the order of the subgroup of $J_0(N)(\mathbf{Q})$ generated by all cuspidal divisors.

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. This notion will be used to try to show that the conjectural order of the Shafarevich-Tate group divides the actual order in the following sections. In this section, we briefly discuss the idea and propose to give an improvement to the existing main theorem on visibility.

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 (A-Stein). *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' and the orders of torsion and component groups of C and B. 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 $|Ш_C|$.*

Roughly speaking, the idea is that if two abelian varieties intersect (e.g., when the associated modular forms are congruent), then the Mordell-Weil group of one can be "transferred" to the Shafarevich-Tate group of the other, via a linking of the Selmer groups in the short exact sequences of Galois cohomology for the two abelian subvarieties. 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 certain standard maps $J_0(N) \to J_0(NM)$. 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 (see [JS]):

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 $J_0(NM)$.*

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 when A_f has analytic rank 0 or 1, assuming the first part of the BSD conjecture. Before doing that, we need to overcome a slight drawback with Theorem 4.1: the hypothesis $B[m] \subseteq C$ often does not hold (e.g., if the dimension of B is bigger than that of C). As an alternative to Theorem 4.1, one has the following theorem (see [AM05, 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. In addition, one has to assume certain mild technical hypothesis that we are skipping for simplicity. If for some prime $p|N$ such that $w_p = -1$, f is congruent* mod $\mathfrak{q}$ *to a newform of level dividing N/p, then $\mathfrak{q}$ divides $c_p(A_f)$; otherwise, $\mathfrak{q}$ divides $|Ш(A_f)|$. In any case, $\mathfrak{q}$ divides $|Ш(A_f)| \cdot \prod_{p|N} c_p(A_f)$.*

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 5.1) 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):

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 is to replace the maximal ideal $\mathfrak{q}$ in Theorem 4.3 by a "congruence ideal". In Lemma 8.2, take $B = A_g^\vee$, so that $I_B = I_g$; then we see that $A_g^\vee \cap A_f^\vee = A_g^\vee[I_f + I_g] \subseteq A_f^\vee[I_f + I_g]$, away from exceptional primes (see Section 8; these are precisely the primes that divide $2N \cdot |A_f(\mathbf{Q})_{\mathrm{tor}}|$). A closer look at the proof of Theorem 6.1 of [DSW03] (on which Theorem 4.3 is based) shows that one the condition in the previous statement is enough to transfer the Mordell-Weil group of $A_g^\vee$ to the Shafarevich-Tate group of $A_f^\vee$. As far as allowing N to be a multiple of the level of f is concerned, one has to apply the above observation to the proof of Theorem 4.1.

5 A formula for $L_A(1)/\Omega_A$ 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. In this section, 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.

We start with the definitions of some terms that will be needed to describe our formula for $L_A(1)/\Omega_A$, from which we will extract a factor that can be related to $Ш_A$ using visibility. 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 as before, let $\Im = \mathrm{Ann}_{\mathbf{T}}(0) - (\infty)$; 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,

$$\frac{L_A(1)}{\Omega_A} = \frac{\left|\pi_*\left(\frac{H^+}{\Im e}\right)\right|}{|\pi_*(\mathbf{T}e/\Im e)|} \ . \tag{2}$$

Note that the group $\pi_*(\mathbf{T}e/\Im e)$ is the subgroup C_A of $A(\mathbf{Q})_{\rm tor}$ generated by $\pi((0)-(\infty))$.

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

$$\frac{L_A(1)}{\Omega_A} = \frac{\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right| \cdot \left|\pi_*\left(\frac{H^+[I_e]}{\Im e}\right)\right|}{|\pi_*(\mathbf{T}e/\Im e)|} \ . \tag{3}$$

As mentioned above, the denominator on the left divides $|A(\mathbf{Q})_{\rm tor}|$; thus the BSD formula predicts that the numerator on the right of the formula above divides $|Ш_A| \cdot \prod_{p|N} c_p(A)$.

The factor $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ measures the intersection of certain abelian subvarieties; using this observation, one can show [AM05, 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 show that q divides $|Ш_A|$ (see [AM05, Thm. 5.7]). In view of this, we shall often refer to $\left|\pi_*\left(\frac{H^+}{H^+[I_e]}\right)\right|$ as the *visible factor*. Using Project 4.4 , we should be able to do more:

Project 5.1. Show that the part of the visible factor that is coprime to $2N|A(\mathbf{Q})_{\rm tor}|$ divides $|Ш(A_f)| \cdot \prod_{p|N} c_p(A_f)$ (assuming the first part of the BSD conjecture on rank).

The second factor $\left|\pi_*\left(\frac{H^+[I_e]}{\Im e}\right)\right|$ in the numerator on the right side of formula (3) is still somewhat of a mystery. In general, it cannot be explained by visibility at the same level, but we expect that it can be explained by visibility at the higher level, as we discuss next.

6 A formula of Gross and visibility at a higher level

One of the problems with formula (3) is that the first factor on the left does not completely capture the part of the Shafarevich-Tate group $Ш_A$ that can be explained by visibility at the same level, since the square of that factor is expected to divide $|Ш_A|$. This situation can be remedied by base-changing to a quadratic imaginary field, and using a formula of Gross instead of formula (2) to extract a square of a factor similar to the visible factor in the previous section. Thus we can isolate the factor that captures the contributions of visibility at the same level. By using an analog of Gross's formula coming from higher level, we sketch a plan to show that the remaining factor also divides $|Ш_A|$, using visibility at higher level. As in the previous section, f denotes a newform of weight 2 on $\Gamma_0(N)$ and $A=A_f$ is the quotient of $J=J_0(N)$ associated to f such that $L_A(1)\neq 0$.

6.1 Squareness of the special L-value

The statement of Gross's formula requires some technical definitions, which we give below briefly. For details of these definitions, 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. Let B be the definite quaternion algebra of discriminant N^-. Let $R_1, \ldots, R_t$ denote the representatives for the isomorphism classes of the oriented Eichler orders of level N^+ in B. Let $\mathcal{P}_D$ denote the free group with generators the R_i's.

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 Gross point (sometimes called Heegner 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^*. Following Gross [Gro87b], we define $e_D = \sum_{i=1}^m h_i[R_i] \in \mathcal{P}_D \otimes \mathbf{Q}$. Thus e_D is the formal sum of all Gross 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 $\mathcal{P}_D$. 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 $\langle\ ,\ \rangle : \mathcal{P}_D \times \mathcal{P}_D \to \mathbf{Z}$ by requiring that $\langle R_i, R_j \rangle = \delta_{ij} w_i$. Then Gross' formula [Gro87b, Cor. 11.6] reads: $L(f,1) \cdot L(f \otimes \varepsilon_D, 1) = \frac{(f,f)}{\sqrt{D}} \langle \pi_f(e_D), \pi_f(e_D) \rangle$, where (f,f) denotes the Petersson inner product. In [Gro87b], the formula is proved when N is prime, and the formula above should be valid following work of Zhang [Zha04] (it is stated as above in [BD97, Thm. 1.1]).

Let $\mathcal{P}_D^0$ denote the subgroup of $\mathcal{P}_D$ consisting of of divisors of degree zero (i.e., whose coefficients add to zero). Let $a_D = \sum_{i=0}^g \frac{[R_i]}{w_i}$ denote the Eisenstein element and let $e_D^0 = e_D - \frac{\deg(e_D)}{\deg(a_D)} \cdot a_D$. Let $\Im_D = \mathrm{Ann}_{\mathbf{T}} a_D$; for example, $T_\ell - (1+\ell) \in \Im_D$ for primes $\ell \nmid N$. Using some results from [RDH04], which rely on [Eme02], the PI and L. Merel [AM05, §6] show that if the level N is prime, then Gross' formula implies that up to powers of 2,

$$\frac{L_{A/K}(1)}{\Omega_{A/K}} = \frac{\left|\pi_f\left(\frac{\mathcal{P}_D^0}{\Im_D e_D^0}\right)\right|^2}{|\pi_f(\mathbf{T}/\Im_D)|^2}\ , \tag{4}$$

where the symbol $/K$ indicates that we have changed the base from $\mathbf{Q}$ to the quadratic imaginary field K. If we compare this formula to the earlier formula (2) for $L_A(1)/\Omega_A$ in Section 5, we notice that by extending our base field to K, we have obtained a square for the special L-value (up to a power of 2). 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 [AM05, Thm. 6.1]:

Theorem 6.1. *Suppose N is prime, and let $n = \mathrm{numr}(\frac{N-1}{12})$. Let q be an odd prime such that q divides $\frac{L_{A/K}(1)}{\Omega_{A/K}}$, but $q \nmid n$. Then q^2 divides the BSD conjectural value of $|Ш(A_f/K)|$.*

Under the hypothesis on q in the theorem above, it is known that q^2 divides the actual order of $Ш(A_f/K)$ (even if A is not an elliptic curve; see [AM05, Rmk. 6.3(2)]), so Theorem 6.1 provides evidence towards the BSD formula (1).

Project 6.2. Generalize formula (4) and Theorem 6.1 to the case where the level N is square-free.

In order to do this, we have to generalize to arbitrary level some of the results of [Eme02] for prime level, since they were used in deriving (4). Also, Hida [Hid04] has given different and more generalizable proofs of some of the results in [Eme02]; these should suffice for Project 6.2.

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 conjectural value of $|Ш(A/K)|$ divides the actual value, using visibility at the same and higher level and assuming the first part of the BSD conjecture.

One can think of formula (4) as being obtained by a "parametrization at level N", and instead one can consider a formula obtained by a "parametrization at level NM" for some positive integer M, 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 (4) 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. 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 (3) in Section 5, we can rewrite equation (4) to get the following formula for "level NM" up to powers of 2:

$$\frac{L_{A/K}(1)}{\Omega_{A/K}} = \frac{\left|\pi_f\left(\frac{\mathcal{P}^0_{D,NM}}{\mathcal{P}^0_{D,NM}[I_{e^0_{D,NM}}]}\right)\right|^2 \cdot \left|\pi_f\left(\frac{\mathcal{P}^0_{D,NM}[I_{e^0_{D,NM}}]}{\Im_{D,NM}\ e^0_{D,NM}}\right)\right|^2}{|\pi_f(\mathbf{T}_{NM}/\Im_{D,NM}\ e^0_{D,NM})|^2}, \tag{5}$$

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

In formula (5), if an odd prime q divides the factor $\left|\pi_f\left(\frac{\mathcal{P}^0_{D,NM}}{\mathcal{P}^0_{D,NM}[I_{e^0_{D,NM}}]}\right)\right|$, then f is congruent modulo q to an eigenform g of level NM such that $L(g,1)=0$ (by a reasoning similar to that in Section 5), and hence using visibility, and assuming the first part of the BSD conjecture, we conclude that q divides $|Ш(A/K)|$. The term $\left|\pi_f\left(\frac{\mathcal{P}^0_{D,NM}}{\mathcal{P}^0_{D,NM}[I_{e^0_{D,NM}}]}\right)\right|^2$, being a square, usually captures *all* of the part of $Ш(A/K)$ that is visible at level NM. If we can prove the following:
(*) if a prime q (with suitable restrictions) divides $\frac{L_{A/K}(1)}{\Omega_{A/K}}$ then there exists an M such that q does not divide the second factor $\left|\pi_f\left(\frac{\mathcal{P}^0_{D,NM}[I_{e^0_{D,NM}}]}{\Im_{D,NM}\ e^0_{D,NM}}\right)\right|$ above,
then q would divide the first factor $\left|\pi_f\left(\frac{\mathcal{P}^0_{D,NM}}{\mathcal{P}^0_{D,NM}[I_{e^0_{D,NM}}]}\right)\right|$, which would imply by the argument just above that q divides $|Ш(A/K)|$ (recall that we are assuming the first part of the BSD conjecture on rank). Following Project 5.1, 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 $Ш(A/K)$ that is coprime to $2N\cdot|A(\mathbf{Q})|\cdot\prod_{p|N}c_p(A_f)$.

Note that the term $\left|\pi_f\left(\frac{\mathcal{P}^0_{D,NM}[I_{e^0_{D,NM}}]}{\Im_{D,NM}\ e^0_{D,NM}}\right)\right|$ in (*) divides the order of the torsion part of $\frac{\mathcal{P}^0_{D,NM}}{\Im_{D,NM}\ e^0_{D,NM}}$. Thus, to prove (*), it suffices to prove that
(**) for some M, q does not divide the torsion part of $\frac{\mathcal{P}^0_{D,NM}}{\Im_{D,NM}\ e^0_{D,NM}}$,
which is reasonable to expect, considering that we have a large choice of M's (and D's). In fact, D. Kohel has done some computations that give evidence towards (**). For example, there is a newform f of level $N=1283$ for which the BSD conjecture predicts that $q=5$ divides $|Ш_A|$.

The 5-torsion part of $Ш_A$ 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 $\frac{\mathcal{P}^0_{D,NM}}{\Im_{D,NM}\ e_{D,NM}}$ 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 (**).

There are two approaches that the PI plans to follow to prove (**). One approach is to write the group $\frac{\mathcal{P}^0_{D,NM}}{\Im_{D,NM}\ e^0_{D,NM}}$ 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).

7 Visibility in the analytic rank one case

In the previous two sections, we discussed how one can apply the notion of visibility to show that the conjectural order of the Shafarevich-Tate group divides the actual order when the analytic rank of A is zero. In this section, we show how these ideas can be applied in a similar manner even if the analytic rank of A is one. The main idea is to use a formula of Gross-Zagier for $L'_A(1)$ and extract a visible factor from it (just like we did in the context of $L_A(1)$, by using formulas (2) and (4) for analytic rank zero). The theory of Euler systems (e.g., see [Gro91]) bounds the actual order of the Shafarevich-Tate group in terms of the BSD conjectural order (under some hypotheses, and away from certain primes). Our project would work in the opposite direction, and thus complements the Euler system machinery. To our knowledge, this is the only known approach to show that the conjectural order of the Shafarevich-Tate group divides the actual order when the analytic rank is one (for analytic rank zero, there is the Eisenstein series method of Skinner-Urban). Thus we feel that an investigation of visibility in the context of analytic rank one is crucial.

Let f be a newform of weight 2 on $\Gamma_0(N)$, and let $A = A_f$ be the quotient of $J = J_0(N)$ associated to f such that A has analytic rank one. For simplicity, in this section, we assume that A is an elliptic curve, but the arguments should apply to higher dimensional A as well. We denote the quotient map $J \to A$ by π. Suppose $D \neq -3, -4$ is a negative fundamental discriminant, and let $K = \mathbf{Q}(\sqrt{D})$ be such that all primes dividing N split in K. Choose an ideal $\mathcal{N}$ of the ring of integers $\mathcal{O}$ of K such that $\mathcal{O}/\mathcal{N} \cong \mathbf{Z}/N\mathbf{Z}$. Then the complex tori $\mathbf{C}/\mathcal{O}$ and $\mathbf{C}/\mathcal{N}^{-1}$ define elliptic curves related by a cyclic N-isogeny, hence a complex point x of $X_0(N)$. This point, called a Heegner point, is defined over the Hilbert class field H of K. Let $P \in J(K)$ be the class of the divisor $\sum_{\sigma \in \mathrm{Gal}(H/K)}((x) - (\infty))^\sigma$, where H is the Hilbert class field of K.

In Section 2.1, we mentioned the second part of the BSD conjecture when A has analytic rank zero. One has a similar conjecture for any analytic rank, which we do not state due to lack of space. For our purposes, what suffices is that for analytic rank one, the second part of the BSD conjecture just becomes the following (see [Gro91, Conj. 1.2]):

$$[A(K) : \mathbf{Z}\pi(P)] \stackrel{?}{=} c_A \cdot \prod_{p|N} c_p(A) \cdot |Ш(A/K)|^{1/2}, \tag{6}$$

where c_A is the Manin constant of A (conjectured to be one). Our goal is to try to show that the

left hand side divides the right hand side.

Let $B = \ker \pi$ and consider the exact sequence $0 \to B \to J \to A \to 0$. Part of the associated long exact sequence of Galois cohomology is $0 \to B(K) \to J(K) \xrightarrow{\pi} A(K) \xrightarrow{\delta} H^1(K, B) \to H^1(K, J)$, from which one can derive the following exact sequence:
$0 \to \frac{J(K)}{B(K)+\mathbf{T}P} \to \frac{A(K)}{\mathbf{Z}\pi(P)} \to \ker(H^1(K, B) \to H^1(K, J)) \to 0$. The first term can be rewritten as $\left|\pi\left(\frac{J(K)}{\mathbf{T}P}\right)\right| = \left|\pi\left(\frac{J(K)}{J(K)[I]}\right)\right| \cdot \left|\pi\left(\frac{J(K)[I]}{\mathbf{T}P}\right)\right|$, where $I = \mathrm{Ann}_{\mathbf{T}} P$. In view of all this, the BSD formula (6) just becomes:

$$\left|\pi\left(\frac{J(K)}{J(K)[I]}\right)\right| \cdot \left|\pi\left(\frac{J(K)[I]}{\mathbf{T}P}\right)\right| \cdot |\ker(H^1(K, B) \to H^1(K, J))| \stackrel{?}{=} c_A \cdot \prod_{p|N} c_p(A) \cdot |Ш(A/K)|^{1/2} . \quad (7)$$

Project 7.1. Show that the left hand side of (7) divides the right hand side, assuming the first part of the BSD conjecture.

Note that the first two terms in (7) are analogs of the numerators on the right side of (3) and (5) from the analytic rank zero case. Analogous to the rank zero situation, one can prove that if a prime q divides the first term, then f is congruent modulo an ideal over q to an eigenform g of odd analytic rank at least 3 (see [Aga05]). If one assumes the first part of the BSD conjecture, then the theory of visibility can be used to show that these primes of congruence divide $|Ш(A/K)|$ or $\prod_{p|N} c_p(A)$.

The second factor $\left|\pi\left(\frac{J(K)[I]}{\mathbf{T}P}\right)\right|$ is analogous to the second factor $\left|\pi_f\left(\frac{\mathcal{P}_D^0[I_{e_D^0}]}{\Im e_D^0}\right)\right|$ in the analytic rank zero case (Section 6.2), and similar to that case, we plan to show that this factor can be explained by visibility at higher level (and there is some experimental evidence for this), following a strategy similar to that in Section 6.2. In fact there is a striking analogy between the two cases (e.g., see [Gro87a]), which indicates a proof of one should yield a proof of the other. This also underscores the importance of undertaking the investigations in Section 6.2 – one would get two birds in one stone.

The remaining factor on the left side of (7) is the term $\ker(H^1(K, B) \to H^1(K, J))$. There was no such factor in the analytic rank one case. If p divides the order of $\ker(H^1(K, B) \to H^1(K, J))$, then either p divides some component group, or a point $Q \in A(K)$ explains a non-trivial element of $Ш(B/K)$; if we are in the latter case, we expect to show that there is a "reverse transfer" from the Mordell-Weil group of B (which has odd analytic rank, hence positive Mordell-Weil rank assuming the first part of the BSD conjecture) to $Ш(A/K)$ which would show that p divides $|Ш(A/K)|$. For either of the three terms above, to show that the entire term divide $|Ш(A/K)|^{1/2}$, we will use the generalized visibility theorem of Project 4.4.

8 Appendix: Intersections of abelian subvarieties

In this section, we discuss a lemma concerning intersections that is used in earlier sections in studying the BSD formula. This lemma should be useful in other scenarios as well, and we sketch a plan for one such application: a generalization of the result that a prime dividing the modular degree of an elliptic curve is a congruence prime.

Let f be a newform of weight 2 on $\Gamma_0(N)$, and let $A = A_f$ be the quotient of $J = J_0(N)$ associated to f. Note that there is no restriction on the analytic rank of A in this section. The dual of the quotient map $J \to A$ gives an injection $A^\vee \to J^\vee$, which when composed with the quotient map gives a polarization (in particular, an isogeny) $\phi : A^\vee \to A$. The exponent of $\ker(\phi)$

is called the *modular exponent* and the order of $\ker(\phi)$ is called the *modular number* (as in [ARS]). Since ϕ is a polarization, the modular number is a perfect square (e.g., see [AS05, Lem. 3.14]). Recall that $I_f = \mathrm{Ann}_{\mathbf{T}}(f)$, and let $I_f^\perp = \mathrm{Ann}_{\mathbf{T}} I_f$. Let $S = S_2(\Gamma_0(N), \mathbf{Z})$, and consider the group $\frac{S}{S[I_f]+S[I_f^\perp]}$, which is isomorphic to $\frac{\mathbf{T}}{I_f+I_f^\perp}$. The exponent of this group is called the *congruence exponent* and its order is called the *congruence number*. When A is an elliptic curve, the modular exponent is just the usual modular degree of A, and the congruence number is the largest integer modulo which f is congruent to another cuspform.

Ribet proved that the modular degree of an elliptic curve divides the congruence number, and in [ARS], the authors extended this result to newform quotients by showing that the modular *exponent* divides the congruence *exponent*. One may wonder if more generally, the square root of the modular *number* divides the congruence *number*. The answer is no, and a counterexample is given in [ARS]. However, this example is the only one at level < 500 in Stein's computations [Steb], and is at the same level where the first example of failure of multiplicity one (which we will recall soon) at the prime 2 was found [Kil02]. This motivates the following:

Project 8.1. Show that the square-root of the modular number divides the congruence number, "away from" primes where multiplicity one may fail (we will make this precise below).

Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ of residue characteristic p. We say that $\mathfrak{m}$ satisfies *multiplicity one* if $J_0[\mathfrak{m}]$ is two dimensional over $\mathbf{T}/\mathfrak{m}$. This is known to hold in several situations, in particular when the following conditions hold simultaneously (e.g., see [Wil95, Thm. 2.1(ii)] along with [ARS]): $p \neq 2$, $p^2 \nmid N$, the canonical semi-simple representation $\rho_{\mathfrak{m}}$ associated to $\mathfrak{m}$ (e.g., see [Rib90, Prop. 5.1]) is irreducible, and $\mathfrak{m}$ arises as a pullback from $\mathbf{T}/I_f$. If a maximal ideal fails any of the first three criteria, we will call it *exceptional*. The fourth criterion will always be met in the applications we have in mind.

Following [Eme03], we say that a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ is *good* if the $\mathfrak{m}$-adic Tate module of $J_0(N)$ is free over $\mathbf{T}_{\mathfrak{m}}$. Emerton [Eme03] shows that if $\mathfrak{m}$ is a good maximal ideal and I is any saturated ideal of $\mathbf{T}$, then the $\mathfrak{m}$-adic completion of the component group of $J_0(N)[I]$ is trivial. Note that if $\mathfrak{m}$ satisfies multiplicity one, then $\mathfrak{m}$ is good. We apply this to $I = I_f$. If $L \to M$ is a homomorphism of two $\mathbf{T}$-modules, then we say that $L = M$ *away from* a given maximal ideal $\mathfrak{m}'$ if the induced map on the $\mathfrak{m}$-adic completions is an isomorphism for all maximal ideals $\mathfrak{m}$ other than $\mathfrak{m}'$. From the discussion above, the inclusion $A^\vee \subseteq J_0(N)[I_f]$ is an isomorphism away from the exceptional ideals. Let B be an abelian subvariety of $J_0(N)$ and let $I_B = \mathrm{Ann}_{\mathbf{T}} B$. Then away from the exceptional ideals, $B \cap A^\vee = B \cap J_0(N)[I_f] = B[I_B + I_f]$. Also, $B \cap A^\vee \subseteq A^\vee \cap J_0(N)[I_B] = A^\vee[I_B + I_f]$. To summarize, we expect to prove:

Lemma 8.2. *Let A be the quotient of $J_0(N)$ associated to a newform f, and let $I_f = \mathrm{Ann}_{\mathbf{T}} f$. Let B be an abelian subvariety of $J_0(N)$ and let $I_B = \mathrm{Ann}_{\mathbf{T}} B$. Then away from exceptional maximal ideals, $B \cap A^\vee = B[I_B + I_f] \subseteq J_0(N)[I_B + I_f] = A^\vee[I_B + I_f]$.*

Now take B to be the kernel of the quotient map $J_0(N) \to A$, so that $I_B = I_f^\perp$, and the modular number is just $|\, B \cap A_f^\vee \,|$. It should be possible to show that away from exceptional maximal ideals, $J_0(N)[I_f + I_f^\perp]$ is free of rank 2 over $\frac{\mathbf{T}}{I_f+I_f^\perp}$ (this would be a sort of multiplicity one argument for ideals, as opposed to maximal ideals, e.g., as in [Rib90, Thm 5.2]); i.e., the order of $A^\vee[I_f + I_f^\perp]$ is the square of the congruence number. Thus we expect to show that if one stays away from exceptional maximal ideals, then the square root of the modular number divides the congruence number.

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.fsu.edu/~agashe/math.html`.

[Aga05] A. Agashe, *Visibility for analytic rank one*, preprint (2005), available at `http://www.math.fsu.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.

[AM05] A. Agashe and L. Merel, *A visible factor of the special L-value*, preprint (2005), available at `http://www.math.fsu.edu/~agashe/math.html`.

[ARS] A. Agashe, K. Ribet, and W. A. Stein, *The modular degree, congruence primes and multiplicity one*, submitted, available at `http://www.math.fsu.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] A. Agashe and W. A. Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484.

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

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

[CL97] S.-K. Chua and S. Ling, *On the rational cuspidal subgroup and the rational torsion points of $J_0(pq)$*, Proc. Amer. Math. Soc. **125** (1997), no. 8, 2255–2263.

[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.

[CS] F. Calegari and W. A. Stein, *A non-Gorenstein Eisenstein descent*, preprint, perhaps available at `http://modular.ucsd.edu/papers`.

[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.

[Dum] N. Dummigan, *Rational torsion on optimal curves*, to appear in Int. J. Number Theory.

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

[Gro87a] Benedict H. Gross, *Heights and L-series*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986) (Providence, RI), Amer. Math. Soc., 1987, pp. 425–433.

[Gro87b] 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.

[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.

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

[JS] D. Jetchev and W. A. Stein, *Visualizing elements of Shafarevich-Tate groups at higher level*, preprint, available at `http://modular.ucsd.edu/papers`.

[Kil02] L. J. P. Kilford, *Some non-Gorenstein Hecke algebras attached to spaces of modular forms*, J. Number Theory **97** (2002), no. 1, 157–164.

[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] G. 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.

[LO91] S. Ling and J. Oesterlé, *The Shimura subgroup of $J_0(N)$*, Astérisque (1991), no. 196-197, 6, 171–203 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[Lor95] D. J. Lorenzini, *Torsion points on the modular Jacobian $J_0(N)$*, Compositio Math. **96** (1995), no. 2, 149–172.

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

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

[Par99] P. 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.

[Stea] W. A. Stein, `http://modular.ucsd.edu/Tables/cuspgroup/index.html`.

[Steb] W. A. Stein, `http://modular.ucsd.edu/Tables/moddegcongmod-table.1-500`.

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

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

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