Research statement

Amod Agashe

In this document, I briefly describe the main themes of my past and current research. The first section sets up some notation that is used in the rest of the article. After that, the other sections can be read more or less independently. Each of these latter sections discusses a particular aspect of my research.

1 Background and notation

Let N be a positive integer. Let $X_0(N)$ denote the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$, and let $J_0(N)$ be its Jacobian. Let $\mathbf{T}$ denote the subring of endomorphisms of $J_0(N)$ generated by the Hecke operators (usually denoted T_ℓ for $\ell \nmid N$ and U_p for $p \mid N$). Let f be a newform in $S_2(\Gamma_0(N), \mathbf{C})$. Let $I_f = \mathrm{Ann}_{\mathbf{T}} f$ and let $A = A_f$ denote associated newform quotient $J_0(N)/I_f J_0(N)$ over $\mathbf{Q}$. If f has integer Fourier coefficients, then A is just an elliptic curve, and every elliptic curve over $\mathbf{Q}$ is isogenous to some such newform quotient.

Most of my research concerns the arithmetic of newform quotients (which includes elliptic curves), especially in relation to the second part of Birch and Swinnerton-Dyer (BSD) conjecture, which I will now recall briefly. Let $L_A(s)$ denote the L-function associated to A. The *analytic rank* r of A is the order of vanishing of $L_A(s)$ at $s = 1$. Let $\mathcal{A}$ denote the Néron model of A over $\mathbf{Z}$ and let $\mathcal{A}^0$ denote the largest open subgroup scheme of $\mathcal{A}$ in which all the fibers are connected. Let $d = \dim A$, and let D be a generator of the d-th exterior power of the group of invariant differentials on $\mathcal{A}$. Let Ω_A denote the volume of $A(\mathbf{R})$ with respect to the measure given by D. If p is a prime number, then the (arithmetic) component group of A at p is the group of $\mathbf{F}_p$-valued points of the quotient $\mathcal{A}_{\mathbf{F}_p}/\mathcal{A}^0_{\mathbf{F}_p}$; its order is denoted $c_p(A)$. Let R_A denote the regulator of A. If B is an abelian variety, then we denote by $B^\vee$ the dual abelian variety of B. If B is an abelian variety over a number field F, then $Ш(B/F)$ denotes the Shafarevich-Tate group of B over F; if $F = \mathbf{Q}$, then we write just $Ш(B)$ for $Ш(B/F)$.

The *second part of the BSD conjecture* asserts the formula:

$$\frac{\lim_{s\to 1}\{(s-1)^{-r} L_A(s)\}}{\Omega_A R_A} = \frac{|Ш(A)| \cdot \prod_{p|N} c_p(A)}{|A(\mathbf{Q})_{\mathrm{tor}}| \cdot |A^\vee(\mathbf{Q})_{\mathrm{tor}}|} \tag{1}$$

I will refer to the formula above as the *BSD formula.*

In each section below, we shall continue to use the notation introduced in this section.

2 Visibility theory

Mazur introduced the notion of visibility with the idea of "visualizing" elements of the Shafarevich-Tate group, which are principal homogeneous spaces, by embedding them in some ambient abelian variety. The resulting theory has been used to prove the existence of non-trivial elements of the Shafarevich-Tate group. Roughly speaking, the idea is that if two abelian subvarieties of $J_0(N)$ intersect, then the Mordell-Weil group of one can often 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. I have been involved in these developments right from the beginning, and in joint work with Stein, we proved a theorem that makes the above idea precise [AS02] (similar theorems are proved in Cremona-Mazur's appendix in [AS05] and in [DSW03]), and investigated how much of the BSD conjectural order of the Shafarevich-Tate group of newform quotients of analytic rank zero can be explained in particular examples [AS05] (this was done earlier for elliptic curves in [CM00]). In the article [AS05], we also gave formulas and algorithms to compute quantities in the BSD formula for newform quotients of analytic rank zero (such formulas were known for elliptic curves; e.g., see [Cre97]).

The currently available theorems on visibility (e.g., [AS02], [DSW03], and Cremona-Mazur's appendix in [AS05]) have the problem that for many applications, either the hypotheses are too restrictive (e.g., they may not hold for abelian varieties of arbitrary dimension) or the conclusion is not strong enough (e.g., the theorem may show the existence of nontrivial elements only of prime order). By combining the strategies of the articles mentioned in the previous sentence, I plan to prove a more general visibility theorem, which will work under the hypothesis of congruences between Fourier coefficients of modular forms modulo an ideal of the Hecke algebra (which need not be maximal), to give the existence of subgroups of nontrivial elements of the Shafarevich-Tate group of order equal to the norm of the ideal of congruence (subject to some mild hypotheses, no more stringent than the ones in existing theorems).

3 Visibility and the BSD formula

While much of the work on visibility has involved either proving theorems that guarantee the existence of nontrivial elements of the Shafarevich-Tate group or giving evidence for the BSD formula in particular examples, one of the long-term goals that I have been pursuing is to use the theory of visibility to directly give partial *theoretical* results towards the BSD formula.

Most of our results in this context assume the first part of the Birch and Swinnerton-Dyer conjecture (which says that order of vanishing of $L_A(s)$ at $s = 0$ is the rank of the group of rational points on A), so let us assume this in the rest of this section.

Suppose A has analytic rank zero (i.e., $L_A(1) \neq 0$). Then by [KL89], A has Mordell-Weil rank zero, and so the left side of the BSD formula (1) is $L_A(1)/\Omega_A$ (as $R_A = 1$). In [Agab], following an idea of Merel, I extracted an explicit integer factor from $L_A(1)/\Omega_A$ that is related to intersections of $A^\vee$ with abelian subvarieties of $J_0(N)$ of higher Mordell-Weil rank, and used the theory of visibility to show that if an odd prime (subject to some technical restrictions) divides this factor, then it divides $|Ш(A)| \cdot \prod_{p|N} c_p(A)$, which is the numerator of the right side of the BSD formula (1). Using the more general visibility theorem mentioned in the previous section and an observation made at the end of Section 7, I hope to prove that all of the factor mentioned above divides $|Ш(A)| \cdot \prod_{p|N} c_p(A)$ (under some mild hypotheses). The other factor in the numerator of $L_A(1)/\Omega_A$ cannot be explained by visibility in $J_0(N)$, and the hope is that it can be explained using visibility in $J_0(M)$ for some multiple M of N; I am investigating an approach to prove this using a formula of Gross [Gro87] (as generalized by Zhang [Zha01]) after base changing to a suitable quadratic imaginary field.

A similar situation arises in the case where A is an elliptic curve of analytic rank one, where by [GZ86], the BSD formula essentially says that the index of the subgroup generated by a certain Heegner point in the Mordell-Weil group of A over a suitable quadratic imaginary field K equals $|Ш(A/K)| \cdot \prod_{p|N} c_p(A)$, up to the Manin constant. In [Aga08b, Aga09b], I extracted an explicit integer factor from the Heegner index and used the theory of visibility to show that if an odd prime (subject to some mild restrictions) divides this factor, then it divides $|Ш(A/K)|$. Again the hope is that the remaining factor can can be explained using visibility in $J_0(M)$ for some multiple M of N.

In both the analytic rank zero case and the analytic rank one case, the theory of Euler systems provides upper bounds for the order of the Shafarevich-Tate group in terms of the order predicted by the BSD formula (staying away from certain primes). The theory of visibility works in the opposite direction, i.e., it gives lower bounds for the order of the Shafarevich-Tate group in terms of the order predicted by the BSD formula. For analytic rank zero, there is an approach of Skinner and Urban that also works in this opposite direction. However, for analytic rank one, as far as we know, visibility is the only technique that has given results in the direction opposite to that of Euler systems. Thus the approach using visibility may play an important role in an eventual proof of the BSD formula for analytic rank one.

4 Torsion and component groups

In this section, for simplicity, we assume that A is an elliptic curve. While the Shafarevich-Tate group may be the quantity of greatest interest in the BSD formula (1), the torsion subgroup $A(\mathbf{Q})_{\mathrm{tor}}$ and the component groups of A that appear in the formula are quantities are of independent interest: the torsion subgroup addresses part of the problem of finding rational solutions to the equation defining the elliptic curve, and component groups play an important role in the study of abelian varieties (e.g., in Ribet's proof [Rib90] that the Shimura-Taniyama-Weil conjecture implies Fermat's last theorem).

The orders of the component groups appear in the numerator of the BSD formula (1), and the order of the torsion subgroup appears in the denominator. When the level N is prime, it follows by [Eme03] (which builds on [Maz77]) that the order of the torsion subgroup equals the order of the component group at N, and this results in significant cancellation in the BSD formula. While the order of the torsion subgroup need not equal the product of the orders of the component groups when N is not prime, some data of Cremona and Stein suggests that there is nevertheless some pattern. For example, when N is square-free, then for any prime $q > 3$, the order of the q-primary part of $A(\mathbf{Q})_{\mathrm{tor}}$ divides $\prod_{p|N} c_p(A)$ in the numerical data. I am investigating the data more thoroughly with W. Stein, and we are in the process of making some explicit conjectures.

The *cuspidal subgroup* C of $J_0(N)(\mathbf{C})$ is the group of degree zero divisors on $X_0(N)(\mathbf{C})$ that are supported on the cusps; it is a finite group. By dualizing the quotient map $J_0(N) \to A$, we may view A (which we are assuming is an elliptic curve) as an abelian subvariety of $J_0(N)$. Let $C_A = C \cap A(\mathbf{Q})$. When N is prime, it follows by [Maz77] that $C = J_0(N)(\mathbf{Q})_{\mathrm{tor}}$, and so $A(\mathbf{Q})_{\mathrm{tor}} = C_A$. Numerical data of Stein indicates that the last conclusion may hold in general even if N is not prime. In [Aga07], I show that if N is square-free and a prime r that does not divide $6N$ divides $|A(\mathbf{Q})_{\mathrm{tor}}|$, then r divides $|C_A|$. With more work, using some ideas from [Maz77], I plan to show that $A(\mathbf{Q})_{\mathrm{tor}} = C_A$ when N is square-free.

When N is prime, Emerton [Eme03] shows that the specialization map from C_A to the component group of A at N is an isomorphism, which is the key to proving the result mentioned two paragraphs above that the order of the torsion group equals the order of the component group at N. Thus the cuspidal subgroup is used as an intermediary to relate the torsion subgroup to the component group when N is prime. I plan to do the same for square-free level: as mentioned above, I expect to show that $A(\mathbf{Q})_{\mathrm{tor}} = C_A$, and then I hope to relate C_A to the product of the component groups, by utilizing some of the techniques of Mazur and Emerton that work even if N is not prime. Finally, I hope to generalize all of the above to the case where A need not be an elliptic curve, but any newform quotient (or its dual), to the extent possible. This would especially be useful for computing the order of the torsion subgroup of newform quotients (or bounds on this order).

While there has been much work on the Shafarevich-Tate group in the context of the BSD formula, to our knowledge, no one has undertaken a study of the torsion and component groups with regard to the BSD formula. Since a full proof of the BSD formula will likely require some knowledge of the exact cancellation between the torsion and component groups, we feel that our investigations are of vital importance.

5 The Shafarevich-Tate group and reducibility

In this section, we assume again for simplicity of exposition that A is an elliptic curve. Let p be a prime. When A has analytic rank zero or one, the theory of Euler systems gives results which say that the order of the p-primary component of the Shafarevich-Tate group of A over a suitable quadratic imaginary field is bounded above by the order predicted by the BSD formula, under certain hypotheses on p. These hypotheses usually include the hypothesis (either explicitly or implicitly) that the Galois representation $A[p]$ is irreducible.

In [Aga09a], I show that when N is prime and p is odd, if the Galois representation $A[p]$ is reducible, then the p-primary component of $\text{Ш}(A)$ is trivial. Thus, in this case, the hypothesis in the Euler systems based results that the Galois representation $A[p]$ is irreducible is not necessary. Our proof uses a descent argument of Mazur [Maz77, III.3.6] and Emerton's result [Eme03] that the specialization map from $A(\mathbf{Q})_{\rm tor}$ to the component group at N is an isomorphism. While it is not true that the analog of our result above holds if N is not prime (there are counterexamples), I hope to use my investigations in the previous section to see to what extent the result generalizes, say when N is square-free.

6 Special L-values of twists

Let $-D$ be a negative fundamental discriminant that is coprime to N and let $\epsilon_D = (\frac{-D}{\cdot})$ denote the quadratic character associated to $-D$. If $f(q) = \sum_{n>0} a_n q^n$ is the Fourier expansion of f, then the twist $f \otimes \epsilon_D$ of f by ϵ_D is the modular form whose Fourier expansion is $\sum_{n>0} \epsilon_D(n) a_n q^n$. It is in fact a newform in $S_2(ND^2, \epsilon_D^2)$ (considering that D is coprime to N). When the newform quotient A associated to f is an elliptic curve, then the newform quotient $A_{f\otimes\epsilon_D}$ associated to $f \otimes \epsilon_D$ is isogenous to the twist of A by $-D$.

When A is an elliptic curve and its twist by $-D$ has analytic rank zero, I gave a formula [Agaa] for the left side of the BSD formula (1) for the twist which shows that this quantity, a priori a rational number, is actually an integer up to a power of 2, under certain mild hypotheses. In view of the BSD formula, this led me in [Agaa] to the surprising conjecture that for such twists, if the special L-value is nonzero, then the *square* of the order of the odd part of the torsion subgroup divides the product of the order of the Shafarevich-Tate group and the orders of the arithmetic component groups, under certain mild hypotheses (this does not hold in general if the curve is not a twist). I am now trying to prove results towards this conjecture. For example, when N is prime, as mentioned in Section 4, one knows a lot about the cancellations on the right side of the BSD formula of E; starting with this information, I plan to study how the various quantities change when one twists E by $-D$.

Another of my goals is to generalize my formula mentioned above for the left side of the BSD formula (1) for the twist of an elliptic curve to the case of the twist of a newform quotient A by any primitive Dirichlet character. It is easy to express the special L-value of the twist in terms of integrals involving f; what remains is to express the period of the twist in terms of periods of f even when A is not an elliptic curve (our proof for elliptic curves employed explicit Weierstrass equations for A and its twist).

Suppose q is an odd prime that does not divide $|E(\mathbf{Q})_{\mathrm{tor}}|$ or $\prod_p c_p(E)$. Then by the conjectural BSD formula (1), if q divides $\frac{L_E(1)}{\Omega_E}$, then q should divide $|Ш_E|$. Since $|Ш_E|$ is a perfect square, in fact q^2 should divide $|Ш_E|$, and hence under the hypotheses that q does not divide $|E(\mathbf{Q})_{\mathrm{tor}}|$ or $\prod_p c_p(E)$, if q divides $\frac{L_E(1)}{\Omega_E}$, then in fact q^2 should divide $\frac{L_E(1)}{\Omega_E}$. In [Agaa], I proved that this indeed happens when the level is prime, but under the hypothesis that q does not divide the algebraic part of the special L-value for a twist of the elliptic curve E by a quadratic character. While it is known that this hypothesis does hold for all but finitely many primes q (e.g., see [OS98, Cor. 1]), it is not clear what that finite set of primes is. In [BO03, p.167-168], one finds a criterion for how big q needs to be to satisfy the hypothesis, but the period they use (cf. [Bru99, §5]) differs from the usual period by an unknown algebraic number (cf. the discussion in [Koh85, Cor. 2]). Under certain situations, a conjecture of Prasanna [Pra08, Conj. 5.1] does imply that the hypothesis we need above is true. This conjecture asserts that the ratio of the Petersson inner product of a certain half-integral weight modular form to a certain period is q-integral. The analog of this conjecture is known to be true when the modular form has integral weight, following a result of Hida [Hid81]. I am trying to see if the work of Hida can be adapted to attack Prasanna's conjecture.

7 The modular degree/number, the congruence degree/number, and multiplicity one

Suppose for the moment that A is an elliptic curve. The degree of the modular parametrization of A is called the *modular degree* of A, which we will denote by δ_A. Let r_A denote the *congruence number* of A, which is the biggest integer modulo which the newform f associated to A is congruent to another cuspform in the orthogonal complement of f in $S_2(\Gamma_0(N), \mathbf{Z})$. A *congruence prime* is a prime that divides the congruence number. The modular degree and congruence primes are of great interest: Frey and Mai-Murty have observed that an appropriate asymptotic bound on the modular degree is equivalent to the *abc*-conjecture (see [Fre97, p.544] and [Mur99, p.180]), while congruence primes have been studied by Doi, Hida, Ribet, Mazur and others (see, e.g., [Rib83, §1]), and played an important role in Wiles's proof [Wil95] of Fermat's last theorem. Hence relations between the two quantities are of significant interest. Ribet showed [Zag85] that δ_A divides r_A, and Frey and Muller [FM99] asked more generally whether $\delta_A = r_A$. In [ARS], we gave examples to show that the answer to the latter question is no, but also proved that the only primes that can divide r_A/δ_A are the primes whose squares divide N. We also conjectured that if p is a prime such that $p^r \mid \frac{r_A}{\delta_A}$ for some r, then $p^{2r} \mid N$. I hope to investigate this conjecture by generalizing the techniques of [ARS] and using good models for $X_0(N)$ when N is not necessarily square free (e.g., as in [Edi89]).

Recall that a maximal ideal $\mathfrak{m}$ of the Hecke algebra $\mathbf{T}$ is said to satisfy *multiplicity one* if $J_0(N)[\mathfrak{m}]$ is two dimensional over $\mathbf{T}/\mathfrak{m}$. The multiplicity one hypothesis has played an important role in arithmetic geometry, in particular in Wiles' proof [Wil95] of Fermat's last theorem. There are theorems that guarantee multiplicity one, usually under the condition that the square of the residue characteristic of $\mathfrak{m}$ does not divide N. Our proof in [ARS] that the only primes that can divide r_A/δ_A are the primes whose squares divide N relied on a multiplicity one condition (which is satisfied if the square of the residue characteristic of $\mathfrak{m}$ does not divide N). Thus if a prime p divides r_A/δ_A, then there is a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ with residue characteristic p such that $\mathfrak{m}$ does not satisfy multiplicity one. Our examples where $\delta_A \neq r_A$ gave the first examples of failure of multiplicity one for maximal ideals of *odd* residue characteristic whose square divides N but whose cube doesn't. This shows that the hypothesis that the square of the residue characteristic of $\mathfrak{m}$

does not divide N in the current multiplicity one theorems is essential.

In [ARS], we also generalized the notions of the modular degree and congruence number to newform quotients. Let A now be an arbitrary newform quotient. We defined the *modular number* (respectively the *modular exponent*) as the order (respectively the exponent) of the intersection of the dual of A with its complementary abelian subvariety in $J_0(N)$. If A is an elliptic curve, then the modular exponent is equal to the modular degree of A, and the modular number is the square of the modular degree. We also defined the *congruence number* (respectively the *congruence exponent*) as the order (respectively the exponent) of the quotient group

$$\frac{S_2(\Gamma_0(N), \mathbf{Z})}{S_2(\Gamma_0(N), \mathbf{Z})[I_f] + S_2(\Gamma_0(N), \mathbf{Z})[I_f]^{\perp}},$$

where $S_2(\Gamma_0(N), \mathbf{Z})[I_f]^{\perp}$ is the subgroup of elements of $S_2(\Gamma_0(N), \mathbf{Z})$ that are orthogonal to $S_2(\Gamma_0(N), \mathbf{Z})[I_f]$ with respect to the Petersson inner product. This generalizes the definition of the congruence number of an elliptic curve. In [ARS], we showed that the modular exponent equals the congruence exponent away from primes p such that $p^2 \mid N$. The modular number is a perfect square (due to the existence of a polarization) and if A is an elliptic curve, then by the discussion above, the modular number divides the square of the congruence number. While the latter may not hold if A is not an elliptic curve, I showed in [Aga08a] that the modular number equals the square of the congruence number away from primes p where multiplicity one fails. This result shows that there is a congruence of f to another cuspform modulo the order of a certain intersection (staying away from certain primes). Recall that in Section 3, we discussed a factor of $L_A(1)/\Omega_A$, for which we could show that a prime dividing it divides $|Ш(A)| \cdot \prod_{p|N} c_p(A)$, under suitable hypotheses. This factor is precisely the order of a certain intersection, and my result mentioned two sentences ago, in conjunction with the visibility theorem of [DSW03], should be useful in showing that the entire factor divides $|Ш(A)| \cdot \prod_{p|N} c_p(A)$ (staying away from certain primes).

8 The Manin constant

Suppose A is an elliptic curve. Then the pullback of the Néron differential on A to $X_0(N)$ is a multiple of the differential associated to f by a rational number; this rational number is called the Manin constant c_A of A. The Manin constant plays a role in the conjecture of Birch and Swinnerton-Dyer (see, e.g., [GZ86, p. 310] and two paragraphs below) and in work on modular parametrizations (see [Ste89, SW04, Vat05]). It is known that c_A is an integer [Edi91] and that if a prime p divides c_A, then $p^2 \,|\, 2N$ [Maz78, Cor 4.1] [AU96]. In [ARS06], we proved the new result that if p is a prime such that $p \,|\, c_A$, then $p \,|\, \delta_A N$, where recall that δ_A is the modular degree of A.

The main result of [AU96] says that if a prime divides the Manin constant of an elliptic curve, then that prime divides its conductor N. The proof involves the use of the fact that the modular degree divides the congruence number. Using my result on the modular number and the congruence number mentioned in Section 7, I hope to generalize of the result of Abbes-Ullmo to the case where A_f may have dimension bigger than one.

In [ARS06], we also generalized the notion of the Manin constant to arbitrary newform quotients A, as follows. In the BSD formula for A, the real volume Ω_A of A is calculated using Néron differentials. However, for getting a formula or for doing computations regarding the left side of the BSD formula (1), it is more convenient to compute the volume using the differentials that correspond to a basis of $S_2(\Gamma_0(N), \mathbf{Z})[I_f]$. The former volume is a multiple of the latter by a rational number c_A, which we called the *Manin constant* of A (this generalizes the definition given earlier when A is an elliptic curve). In [ARS06], we prove that the (generalized) Manin constant is an integer, and conjecture that the Manin constant is one (generalizing the conjecture for elliptic curves). We also generalized some of the results for the Manin constant known for elliptic curves to the case of arbitrary newform quotients; in particular, we showed that if $p \,|\, c_A$, then $p^2 \,|\, 4N$.

In [Agaa], I needed an analog of the Manin constant over a quadratic imaginary field. Such an analog is discussed in [Lan91] over an arbitrary number field F, although its relation to the Manin constant is not mentioned in loc. cit. It turns out that this analog is a fractional ideal of F, which we called the *Manin ideal* in [Agaa]. I am now trying to generalize the results of [ARS06] to the notion of the Manin ideal.

9 Real multiplication and non-commutative geometry

Loosely speaking, a quantum statistical mechanical system (which is a dynamical system) in non-commutative geometry (or operator algebras) consists of an algebra $\mathcal{A}$ of operators (usually over $\mathbf{C}$) and a time evolution, i.e., a homomorphism $\sigma : \mathbf{R} \to \mathrm{Aut}(\mathcal{A})$. A state for the system is a linear functional on $\mathcal{A}$ (usually with values in $\mathbf{C}$) satisfying certain conditions. Associated to such a system are certain naturally defined quantities, which include the partition function (similar to the one in statistical mechanics) and a set of equilibrium states (with respect to the time evolution; these are called KMS-states). One of the important problems in this area is the following: given a number field K, find a quantum statistical mechanical system such that
(i) its partition function is the Dedekind zeta function of K,
(ii) the quotient of the idèle class group C_K by its identity component D_K acts as automorphisms of the system,
(ii) there is a K-subalgebra $\mathcal{A}_0$ of $\mathcal{A}$ (called the arithmetic subalgebra) such that the values of the extremal KMS-states on elements of $\mathcal{A}_0$ are algebraic numbers that generate the maximal abelian extension K^{ab} of K, and
(iv) the induced action of C_K/D_K on the values in (iii) coincides with the action of the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ of K^{ab} over K via the class field theory isomorphism from C_K/D_K to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Thus one may say that in particular, the quantum mechanical system above provides an explicit version of class field theory over K. Such systems have been constructed when K is either $\mathbf{Q}$ [BC95], or an imaginary quadratic field [CMR05], and are amazing demonstrations of the underlying unity in mathematics across disciplines.

The next important case of K would be that of a real quadratic field. The construction of the quantum mechanical system for $K = \mathbf{Q}$ and $K = \mathbf{C}$ actually uses the explicit class field theory for these fields arising from cyclotomic fields and complex multiplication of elliptic curves respectively. Such explicit class field theory does not exist for real quadratic fields K; however, Darmon and Dasgupta have a *conjectural* description of an explicit class field theory for real quadratic fields that uses analogs of elliptic units in the p-adic setting for a suitable prime p. In collaboration with Matilde Marcolli, I am trying to see if one can construct a quantum mechanical system for K a real quadratic field satisfying conditions (i)–(iv) mentioned in the previous paragraph, by *assuming* the conjectures of Darmon and Dasgupta (for which they have extensive numerical evidence). Our approach necessitates some modification to the usual quantum mechanical system – for example, the algebra $\mathcal{A}$ is not over $\mathbf{C}$, but over the p-adic numbers for a suitable prime p. I am also hopeful that the non-commutative geometry/operator algebra approach might shed some light on the conjectures of Darmon and Dasgupta (which are purely in the number theoretic setting).

References

[Agaa] A. Agashe, *Squareness in the special L-value and special L-values of twists*, To appear in Int. J. Number Theory, available at arXiv:0810.5179 or `http://www.math.fsu.edu/~agashe/math.html`.

[Agab] A. Agashe, *A visible factor of the special L-value*, To appear in Crelle's journal (J. Reine Angew. Math.), available at arXiv:0810.2477 or `http://www.math.fsu.edu/~agashe/math.html`.

[Aga07] A. Agashe, *Rational torsion in elliptic curves and the cuspidal subgroup*, Submitted (2007), available at arXiv:0810.5181 or `http://www.math.fsu.edu/~agashe/math.html`.

[Aga08a] A. Agashe, *The modular number, congruence number, and multiplicity one*, Submitted (2008), available at arXiv:0810.5176 or `http://www.math.fsu.edu/~agashe/math.html`.

[Aga08b] A. Agashe, *A visible factor of the heenger index*, Submitted (2008), available at arXiv:0810.5177 or `http://www.math.fsu.edu/~agashe/math.html`.

[Aga09a] A. Agashe, *Mod-p reducibility, the torsion subgroup, and the Shafarevich-Tate group*, Submitted (2009), available at arXiv:0810.5176 or `http://www.math.fsu.edu/~agashe/math.html`.

[Aga09b] A. Agashe, *Visibility and the Birch and Swinnerton-dyer conjecture for analytic rank one*, Int. Math. Res. Not. (IMRN) (2009), no. 15, 2899–2913.

[ARS] A. Agashe, K. Ribet, and W. A. Stein, *The modular degree, congruence primes, and multiplicity one*, To appear in a special Springer volume in honor of Serge Lang; available at http://www.math.fsu.edu/~agashe/moddeg3.html.

[ARS06] A. Agashe, K. Ribet, and W. A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, 617–636.

[AS02] Amod Agashe and William Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185.

[AS05] Amod Agashe and William 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 (electronic), With an appendix by J. Cremona and B. Mazur.

[AU96] Ahmed Abbes and Emmanuel Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. **103** (1996), no. 3, 269–286.

[BC95] J.-B. Bost and A. Connes, *Hecke algebras, type III factors and phase transitions with spontaneous symmetry breaking in number theory*, Selecta Math. (N.S.) **1** (1995), no. 3, 411–457.

[BO03] Jan H. Bruinier and Ken Ono, *Coefficients of half-integral weight modular forms*, J. Number Theory **99** (2003), no. 1, 164–179.

[Bru99] Jan Hendrik Bruinier, *Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. **98** (1999), no. 3, 595–611.

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

[CMR05] Alain Connes, Matilde Marcolli, and Niranjan Ramachandran, *KMS states and complex multiplication*, Selecta Math. (N.S.) **11** (2005), no. 3-4, 325–347.

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

[DSW03] Neil Dummigan, William Stein, and Mark 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.

[Edi89] B. Edixhoven, *Stable models of modular curves and applications*, Thèse de doctorat à l'université d'Utrecht (1989), available at
http://www.maths.univ-rennes1.fr/~edix/publications/prschr.html.

[Edi91] B. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Birkhäuser Boston, Boston, MA, 1991, pp. 25–39.

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

[FM99] G. Frey and M. Müller, *Arithmetic of modular curves and applications*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 11–48.

[Fre97] Gerhard Frey, *On ternary equations of Fermat type and relations with elliptic curves*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 527–548.

[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.

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

[Hid81] Haruzo Hida, *Congruences of cusp forms and special values of their zeta functions*, Invent. Math. **63** (1981), no. 2, 225–261.

[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.

[Koh85] Winfried Kohnen, *Fourier coefficients of modular forms of half-integral weight*, Math. Ann. **271** (1985), no. 2, 237–268.

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

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

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

[Mur99] M. Ram Murty, *Bounds for congruence primes*, Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), Proc. Sympos. Pure Math., vol. 66, Amer. Math. Soc., Providence, RI, 1999, pp. 177–192.

[OS98] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo l*, Ann. of Math. (2) **147** (1998), no. 2, 453–470.

[Pra08] K. Prasanna, *On p-adic properties of central values of quadratic twists of an elliptic curve*, preprint (2008).

[Rib83] Kenneth A. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), no. 1, 193–205.

[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.

[Ste89] Glenn Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. **98** (1989), no. 1, 75–106.

[SW04] William Stein and Mark Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Not. (2004), no. 27, 1395–1405.

[Vat05] V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves*, J. Inst. Math. Jussieu **4** (2005), no. 2, 281–316.

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

[Zag85] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), no. 3, 372–384.

[Zha01] Shou-Wu Zhang, *Gross-Zagier formula for* GL_2, Asian J. Math. **5** (2001), no. 2, 183–290.