Research Plan

William A. Stein

October 27, 1999

1 Introduction

My research program reflects the essential interplay between abstract theory and explicit machine computation during the latter half of the twentieth century; it sits at the intersection of recent work of B. Mazur, K. Ribet, J-P. Serre, R. Taylor, and A. Wiles on Galois representations attached to modular abelian varieties (see [21, 24, 26, 28]) with work of J. Cremona, N. Elkies, and J.-F. Mestre on explicit computations involving modular forms (see [9, 11]).

In 1969 B. Birch [4] described computations that led to the most fundamental open conjecture in the theory of elliptic curves:

> I want to describe some computations undertaken by myself and Swinnerton-Dyer on EDSAC by which we have calculated the zeta-functions of certain elliptic curves. As a result of these computations we have found an analogue for an elliptic curve of the Tamagawa number of an algebraic group; and conjectures (due to ourselves, due to Tate, and due to others) have proliferated.

The rich tapestry of arithmetic conjectures and theory we enjoy today would not exist without the ground-breaking application of computing by Birch and Swinnerton-Dyer. Computations in the 1980s by Mestre were key in convincing Serre that his conjectures on modularity of odd irreducible Galois representations were worthy of serious consideration (see [24]). These conjectures have inspired much recent work; for example, Ribet's proof of the ϵ-conjecture, which played an essential role in Wiles's proof of Fermat's Last Theorem.

My work on the Birch and Swinnerton-Dyer conjecture for modular abelian varieties and search for new examples of modular icosahedral Galois representations has led me to discover and implement algorithms for explicitly computing with modular forms. My research, which involves finding ways to compute with modular forms and modular abelian varieties, is driven by outstanding conjectures in number theory.

2 Invariants of modular abelian varieties

Now that the Shimura-Taniyama conjecture has been proved, the main outstanding problem in the field is the Birch and Swinnerton-Dyer conjecture (BSD conjecture), which ties together the arithmetic invariants of an elliptic curve. There is no general class of elliptic curves for which the full BSD conjecture is known. Approaches to the BSD conjecture that rely on congruences between modular forms are likely to require a deeper understanding of the analogous conjecture for higher-dimensional abelian varieties. As a first step, I have obtained theorems that make possible explicit computation of some of the arithmetic invariants of modular abelian varieties.

2.1 The BSD conjecture

By [6] we now know that every elliptic curve over $\mathbf{Q}$ is a quotient of the curve $X_0(N)$ whose complex points are the isomorphism classes of pairs consisting of a (generalized) elliptic curve and a cyclic subgroup of order N. Let $J_0(N)$ denote the Jacobian of $X_0(N)$; this is an abelian variety of dimension equal to the genus of $X_0(N)$ whose points correspond to the degree 0 divisor classes on $X_0(N)$.

An *optimal quotient* of $J_0(N)$ is a quotient by an abelian subvariety. Consider an optimal quotient A such that $L(A,1) \neq 0$. By [13], $A(\mathbf{Q})$ and $\text{Ш}(A/\mathbf{Q})$ are both finite. The BSD conjecture asserts that

$$\frac{L(A,1)}{\Omega_A} = \frac{\#\text{Ш}(A/\mathbf{Q}) \cdot \prod_{p|N} c_p}{\#A(\mathbf{Q}) \cdot \#A^\vee(\mathbf{Q})}.$$

Here the Shafarevich-Tate group $\text{Ш}(A/\mathbf{Q})$ is a measure of the failure of the local-to-global principle; the Tamagawa numbers c_p are the orders of the component groups of A; the real number Ω_A is the volume of $A(\mathbf{R})$ with respect to a basis of differentials having everywhere nonzero good reduction; and $A^\vee$ is the dual of A. My goal is to verify the full conjecture for many specific abelian varieties on a case-by-case basis. This is the first step in a program to verify the above conjecture for an infinite family of quotients of $J_0(N)$.

2.2 The ratio $L(A,1)/\Omega_A$

Following Y. Manin's work on elliptic curves, A. Agashé and I proved the following theorem in [2].

Theorem 1. *Let m be the largest square dividing N. The ratio $L(A,1)/\Omega_A$ is a rational number that can be explicitly computed, up to a unit (conjecturally 1) in $\mathbf{Z}[1/(2m)]$.*

The proof uses modular symbols combined with an extension of the argument used by Mazur in [17] to bound the Manin constant. The ratio $L(A,1)/\Omega_A$ is expressed as the lattice index of two modules over the Hecke algebra. I expect the method to give similar results for special values of twists, and of L-functions attached to eigenforms of higher weight. I have computed $L(A,1)/\Omega_A$ for all optimal quotients of level $N \leq 1500$; this table continues to be of value to number theorists.

2.3 The torsion subgroup

I can compute upper and lower bounds on $\#A(\mathbf{Q})_{\text{tor}}$, but I can not determine $\#A(\mathbf{Q})_{\text{tor}}$ in all cases. Experimentally, the deviation between the upper and lower bound is reflected in congruences with forms of lower level; I hope to exploit this in a precise way. I also obtained the following intriguing corollary that suggests cancellation between torsion and c_p; it generalizes to higher weight forms, thus suggesting a geometric explanation for reducibility of Galois representations.

Corollary 2. *Let n be the order of the image of $(0) - (\infty)$ in $A(\mathbf{Q})$, and let m be the largest square dividing N. Then $n \cdot L(A,1)/\Omega_A$ is an integer, up to a unit in $\mathbf{Z}[1/(2m)]$.*

2.4 Tamagawa numbers

Theorem 3. *When $p^2 \nmid N$, the number c_p can be explicitly computed (up to a power of 2).*

I prove this in [25]. Several related problems remain: when $p^2 \mid N$ it may be possible to compute c_p using the Drinfeld-Katz-Mazur interpretation of $X_0(N)$; it should also be possible to use my methods to treat optimal quotients of $J_1(N)$.

I was surprised to find that systematic computations using this formula indicate the following conjectural refinement of a result of Mazur [16].

Conjecture 4. *Suppose N is prime and A is an optimal quotient of $J_0(N)$. Then $A(\mathbf{Q})_{\mathrm{tor}}$ is generated by the image of $(0)-(\infty)$ and $c_p = \#A(\mathbf{Q})_{\mathrm{tor}}$. Furthermore, the product of the c_p over all optimal factors equals the numerator of $(N-1)/12$.*

I have checked this conjecture for all $N \leq 997$ and, up to a power of 2, for all $N \leq 2113$. The first part is known when A is an elliptic curve (see [20]). Upon hearing of this conjecture, Mazur proved it when all "q-Eisenstein quotients" are simple. There are three promising approaches to finding a complete proof. One involves the explicit formula of Theorem 3; another is based on Ribet's level lowering theorem, and a third makes use of a simplicity result of Merel.

Theorem 3 also suggests a way to compute Tamagawa numbers of motives attached to eigenforms of higher weight. These numbers appear in the conjectures of Bloch and Kato, which generalize the BSD conjecture to motives (see [5]).

2.5 Upper bounds on $\#Ш$

V. Kolyvagin and K. Kato [12, 23] obtained upper bounds on $\#Ш(A)$. To verify the full BSD conjecture for certain abelian varieties, it is necessary is to make these bounds explicit. Kolyvagin's bounds involve computations with Heegner points, and Kato's involve a study of the Galois representations associated to A. I plan to carry out such computations in many specific cases.

2.6 Lower bounds on $\#Ш$

One approach to showing that Ш is as large as predicted by the BSD conjecture is suggested by Mazur's notion of the visible part of Ш (see [10, 18]). Let $A^\vee$ be the dual of A. The visible part of $Ш(A^\vee/\mathbf{Q})$ is the kernel of $Ш(A^\vee/\mathbf{Q}) \to Ш(J_0(N))$. Mazur observed that if an element of order p in $Ш(A^\vee/\mathbf{Q})$ is visible, then it is explained by a jump in the rank of Mordell-Weil in the sense that there is another abelian subvariety $B \subset J_0(N)$ such that $p \mid \#(A^\vee \cap B)$ and the rank of B is positive. I think that this observation can be turned around: if there is another abelian variety B of positive rank such that $p \mid \#(A^\vee \cap B)$, then, under mild hypotheses, there is an element of $Ш(A^\vee/\mathbf{Q})$ of order p. Thus the theory of congruences between modular forms can be used to obtain a lower bound on $\#Ш(A^\vee/\mathbf{Q})$. I am trying to use the cohomological methods of [15] and suggestions of B. Conrad and Mazur to prove the following conjecture.

Conjecture 5. *Let $A^\vee$ and B be abelian subvarieties of $J_0(N)$. Suppose that $p \mid \#(A^\vee \cap B)$, that $p \nmid N$, and that p does not divide the order of any of the torsion subgroups or component groups of A or B. Then $(B(\mathbf{Q}) \oplus Ш(B/\mathbf{Q})) \otimes \mathbf{Z}/p\mathbf{Z} \cong (A^\vee(\mathbf{Q}) \oplus Ш(A^\vee/\mathbf{Q})) \otimes \mathbf{Z}/p\mathbf{Z}$.*

Unfortunately, $Ш(A^\vee/\mathbf{Q})$ can fail to be visible inside $J_0(N)$. For example, I found that the BSD conjecture predicts the existence of invisible elements of odd order in Ш for at least 15 of the 37 optimal quotients of prime level ≤ 2113. For every integer M (Ribet [22] tells us which M to choose), we can consider the images of $A^\vee$ in $J_0(NM)$. There is not yet enough evidence to conjecture the existence of an integer M such that all of $Ш(A^\vee/\mathbf{Q})$ is visible in $J_0(NM)$. I am gathering data to determine whether or not to expect the existence of such M.

2.7 Motivation for considering abelian varieties

If A is an elliptic curve, then explaining $Ш(A/\mathbf{Q})$ using only congruences between elliptic curves is bound to fail. This is because pairs of nonisogenous elliptic curves with isomorphic p-torsion are, according to E. Kani's conjecture, extremely rare. It is crucial to understand what happens in all dimensions.

Within the range accessible by computer, abelian varieties exhibit more richly textured structure than elliptic curves. For example, I discovered a visible element of prime order 83341 in the Shafarevich-Tate group of an abelian variety of prime conductor 2333; in contrast, over all optimal elliptic curves of conductor up to 5500, it appears that the largest order of an element of a Shafarevich-Tate group is 7.

3 Conjectures of Artin, Merel, and Serre

3.1 Icosahedral Galois representations

E. Artin conjectured in [3] that the L-series associated to any continuous irreducible representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_n(\mathbf{C})$, with $n > 1$, is entire. Recent exciting work of Taylor and others suggests that a complete proof of Artin's conjecture, in the case when $n = 2$ and ρ is odd, is on the horizon. This case of Artin's conjecture is known when the image of ρ in $\mathrm{PGL}_2(\mathbf{C})$ is solvable (see [27]), and in infinitely many cases when the image of ρ is not solvable (see [7]).

In 1998, K. Buzzard suggested a way to combine the main theorem of [8], along with a computer computation, to deduce modularity of certain icosahedral Galois representations. Buzzard and I recently obtained the following theorem.

Theorem 6. *The icosahedral Artin representations of conductor* $1376 = 2^5 \cdot 43$ *are modular.*

We expect our method to yield several more examples. These ongoing computations are laying a small part of the technical foundations necessary for a full proof of the Artin conjecture for odd two dimensional ρ, as well as stimulating the development of new algorithms for computing with modular forms using modular symbols in characteristic ℓ.

3.2 Cyclotomic points on modular curves

If E is an elliptic curve over $\mathbf{Q}$ and p is an odd prime, then the p-torsion on E can not all lie in $\mathbf{Q}$; because of the Weil pairing the p-torsion generates a field that contains $\mathbf{Q}(\mu_p)$. For which primes p does there exist an elliptic curve E over $\mathbf{Q}(\mu_p)$ with all of its p-torsion rational over $\mathbf{Q}(\mu_p)$? When $p = 2, 3, 5$ the corresponding moduli space has genus zero and infinitely many examples exist. Recent work of L. Merel, combined with computations he enlisted me to do, suggest that these are the only primes p for which such elliptic curves exist. In [19], Merel exploits cyclotomic analogues of the techniques used in his proof of the uniform boundedness conjecture to obtain an explicit criterion that can be used to answer the above question for many primes p, on a case-by-case basis. Theoretical work of Merel, combined with my computations of twisted L-values and character groups of tori, give the following result (see [19, §3.2]):

Theorem 7. *Let* $p \equiv 3 \pmod 4$ *be a prime satisfying* $7 \le p < 1000$. *There are no elliptic curves over* $\mathbf{Q}(\mu_p)$ *all of whose* p*-torsion is rational over* $\mathbf{Q}(\mu_p)$.

The case in which p is congruent to 1 modulo 4 presents additional difficulties that involve showing that $Y(p)$ has no $\mathbf{Q}(\sqrt{p})$-rational points. We hope to tackle these in the near future.

3.3 Genus one curves

The index of an algebraic curve C over $\mathbf{Q}$ is the order of the cokernel of the degree map $\mathrm{Div}_{\mathbf{Q}}(C) \to \mathbf{Z}$; rationality of the canonical divisor implies that the index divides $2g-2$, where g is the genus of C. When $g=1$ this is no condition at all; Artin conjectured, and Lang and Tate [14] proved, that for every integer m there is a genus one curve of index m over some number field. Their construction yields genus one curves over $\mathbf{Q}$ only for a few values of m, and they ask whether one can find genus one curves over $\mathbf{Q}$ of every index. I have answered this question for odd m.

Theorem 8. *Let K be any number field. There are genus one curves over K of every odd index.*

The proof involves showing that enough cohomology classes in Kolyvagin's Euler system of Heegner points do not vanish combined with explicit Heegner point computations. I hope to show that curves of every index occur, and to determine the consequences of my nonvanishing result for Selmer groups. This can be viewed as a contribution to the problem of understanding $H^1(\mathbf{Q}, E)$.

3.4 Serre's conjecture modulo pq

Let p and q be primes, and consider a continuous representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(2, \mathbf{Z}/pq\mathbf{Z})$ that is irreducible in the sense that its reductions modulo p and modulo q are both irreducible. Call ρ *modular* if there is a modular form f such that a mod p representation attached to f is the mod p reduction of ρ, and ditto for q. I have carried out specific computations suggested by Mazur in hopes of determining when one should expect that such mod pq representations are modular; the computation suggests that the right conjectures are elusive. Ribet's theorem (see [22]) produces infinitely many levels $pq\ell$ at which there is a form giving rise to ρ mod p and another giving rise to ρ mod q; we hope to determine if for some ℓ there is a single form giving rise to both reductions.

References

[1] A. Agashé, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 5, 369–374.

[2] A. Agashé and W. A. Stein, *Visibility of Shafarevich-Tate groups of modular abelian varieties*, in preparation (1999).

[3] E. Artin, *Über eine neue Art von L-Reihen*, Abh. Math. Sem. in Univ. Hamburg **3** (1923), 89–108.

[4] B. J. Birch, *Elliptic curves over* **Q**: *A progress report*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 396–400.

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

[6] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* **Q**, in preparation.

[7] K. Buzzard, M. Dickinson, N. Shepherd-Barron, and R. Taylor, *On icosahedral Artin representations*, available at `http://www.math.harvard.edu/~rtaylor/`.

[8] K. Buzzard and R. Taylor, *Companion forms and weight one forms*, Annals of Math. (1999).

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

[10] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Proceedings of the Arizona Winter School (1998).

[11] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory (Chicago, IL, 1995), Amer. Math. Soc., Providence, RI, 1998, pp. 21–76.

[12] V. A. Kolyvagin, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Springer, Berlin, 1991, pp. 94–121.

[13] V. A. Kolyvagin and D. Y. Logachev, *Finiteness of* Ш *over totally real fields*, Math. USSR Izvestiya **39** (1992), no. 1, 829–853.

[14] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684.

[15] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

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

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

[18] ———, *Visualizing elements of order three in the Shafarevich-Tate group*, preprint (1999).

[19] L. Merel, *Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques*, preprint (1999).

[20] J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math. **400** (1989), 173–184.

[21] 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.

[22] ———, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Birkhäuser Boston, Boston, MA, 1990, pp. 259–271.

[23] A. J. Scholl, *An introduction to Kato's Euler systems*, Galois Representations in Arithmetic Algebraic Geometry, Cambridge University Press, 1998, pp. 379–460.

[24] J-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[25] W. A. Stein, *Component groups of optimal quotients of Jacobians*, preprint (1999).

[26] R. Taylor and A. J. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[27] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), no. 2, 173–175.

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