Research Summary

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, R. Taylor, and A. Wiles on Galois representations with work of J. Cremona, N. Elkies, and J.-F. Mestre on explicit computations involving modular abelian varieties. 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.

2 Objectives

The main outstanding problem in my field is the conjecture of Birch and Swinnerton-Dyer (BSD conjecture), which ties together the constellation of arithmetic invariants of an elliptic curve. There is still no general class of elliptic curves for which the full BSD conjecture is known to hold. Approaches to the BSD conjecture that rely on congruences between modular forms are likely to require a deeper understanding of the analogous conjecture for modular abelian varieties, which are higher dimensional analogues of elliptic curves.

As a first step, I have obtained theorems that make possible computation of some of the arithmetic invariants of modular abelian varieties. My objective is to find ways to explicitly compute all of the arithmetic invariants. Cremona has enumerated these invariants for the first few thousand elliptic curves, and I am working to do the same for abelian varieties. It is hoped that this work will continue to yield theoretical results. I am also writing modular forms software that I hope will be used by many mathematicians and have practical applications in the development of elliptic curve cryptosystems.

My long-range goal is to give a general hypothesis, valid for infinitely many abelian varieties, under which the full BSD conjecture holds. My approach involves combining Euler system techniques of K. Kato and K. Rubin with visibility and congruence ideas of Mazur and Ribet.

3 Modular abelian varieties

My primary objective is to verify the BSD conjecture for specific modular abelian varieties, by using the rich theory of their arithmetic.

The BSD conjecture asserts that if A is a modular abelian variety with $L(A,1) \neq 0$, then

$$\frac{L(A,1)}{\Omega_A} = \frac{\#Ш(A) \cdot \prod c_p}{\#A(\mathbf{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}}.$$

Here $A(\mathbf{Q})_{\mathrm{tor}}$ is the group of rational torsion points on A; the Shafarevich-Tate group $Ш(A)$ is a measure of the failure of the local-to-global principle; the Tamagawa numbers c_p are the orders of certain component groups associated to 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.

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

Extending Manin's work on elliptic curves, A. Agashé and I found a computable formula for the rational number $L(A,1)/\Omega_A$. Using similar techniques, I hope to find computable formulas for rational parts of special values of twists, and of L-functions attached to forms of weight greater than two. I have already computed $L(A,1)/\Omega_A$ for several thousand abelian varieties, and hope to extend these computations.

3.2 The Tamagawa numbers c_p

When A has semistable reduction at p, I have found a way to explicitly compute the number c_p, up to a power of 2. I hope to find a way to compute c_p in the remaining cases.

3.3 Bounding $\#Ш$

V. Kolyvagin and K. Kato 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.

One approach to showing that $Ш(A)$ is as large as predicted by the BSD conjecture is suggested by Mazur's notion of the visible part of $Ш(A)$. Consider an abelian variety A that sits naturally in the Jacobian $J_0(N)$ of the modular curve $X_0(N)$. The *visible part* of $Ш(A)$ is the collection of those elements of $Ш(A)$ that go to 0 under the natural map to $Ш(J_0(N))$. Cremona and Mazur observed that if an element of order p in $Ш(A)$ 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 $p \mid \#(A \cap B)$ and B has many rational points. I am trying to find the precise degree to which this observation can be turned around: if there is another abelian variety B with many rational points and $p \mid \#(A \cap B)$, then under what hypotheses is there an element of $Ш(A)$ of order p?

4 Icosahedral Galois representations

E. Artin conjectured 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.

By combining the main result of a recent paper of K. Buzzard and Taylor with a computer computation, Buzzard and I recently proved that the icosahedral Artin representations of conductor $1376 = 2^5 \cdot 43$ are modular. If I can extend a congruence result of J. Sturm, then our method will yield several more examples. These ongoing computations are laying a part of the foundation 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 in characteristic ℓ.