Publications

(published, accepted for publication, or submitted)

1. **Lectures on modular forms and Galois representations** (170 pages), with K. Ribet: In 1996, Ken Ribet taught an advanced course on modular forms and Galois representations. In collaboration with Ribet, I am turning my course notes into a book that has been accepted for publication in Springer-Verlag's Universitext series. The chapters are: Overview; Modular representations; Modular forms; Embedding Hecke operators in the dual; Rationality and integrality questions; Modular curves; Higher weight modular forms; Newforms; Some explicit genus computations; The field of moduli; Hecke operators as correspondences; Abelian varieties from modular forms; The Gorenstein property; Local properties of ρ_λ; Serre's conjecture; Fermat's Last Theorem; Deformations; The Hecke algebra $\mathbf{T}_\Sigma$. Though a version of the notes has been circulating for a few years, significant polishing remains to be done.

2. **HECKE: The modular forms calculator:** I wrote HECKE, a popular `C++` package for computing with spaces of modular forms and modular abelian varieties. I have been invited to visit the MAGMA group in Sydney in order to make HECKE a part of their computer algebra system, and I have already ported my code to MAGMA.

3. **Explicit approaches to modular abelian varieties** (130 pages), Ph.D. thesis under H. W. Lenstra: In the first part of my thesis, I give algorithms for computing with modular abelian varieties. These include algorithms for computing congruences between modular eigenforms, the modular degree, the rational parts of the special values of the L-function, component groups at primes of multiplicative reduction, period lattices, and the real volume.

   In the second part of my thesis, I use these algorithms to investigate several open problems. The first concerns the Birch and Swinnerton-Dyer conjecture, which ties together the constellation of invariants attached to an abelian variety; I verify this conjecture for certain specific abelian varieties of dimension greater than one. The key idea is to use B. Mazur's notion of visibility, coupled with explicit computations, to produce lower bounds on Shafarevich-Tate groups. I also describe related computations that are used in an upcoming joint paper with L. Merel on rational points of $X_0(N)$ over $\mathbf{Q}(\mu_p)$.

   E. Artin conjectured in 1924 that the L-series associated to a representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ is entire. K. Buzzard and I verify this conjecture in eight new icosahedral cases; the argument uses a theorem of K. Buzzard and R. Taylor along with a computer computation, which is used to fill in a missing mod-5 modularity result.

   Finally I turn to Serre's conjecture. I consider a family of exceptional cases, and show that the conjecture appears to fail as badly as possible. I also describe numerical experiments towards a mod-pq extension of Serre's conjecture.

   I expect to finish my thesis before May 2000.

4. **Lectures on Serre's conjectures** (77 pages), with K. Ribet: This is an expository paper based on Ken Ribet's lectures at the 1999 Park City Mathematics Institute; it will be published in the IAS/Park City Mathematics Institute Lecture Series. There are 9 lectures: Introduction to Serre's conjectures; The weak and strong conjectures; The weight in Serre's conjecture; Galois representations from modular forms; Introduction to level lowering; Approaches to level lowering; Mazur's principle; Level lowering without multiplicity one; Level lowering with multiplicity one; Other directions. We have finished all but the last three sections, and expect to finish by early December, 1999.

5. **Empirical evidence for the Birch and Swinnerton-Dyer conjecture for modular Jacobians of genus 2 curves** (22 pages), with E. V. Flynn, F. Leprévost, E. F. Schaefer, M. Stoll, J. L. Wetherell: We provide systematic numerical evidence for the BSD conjecture in the case of dimension two. This conjecture relates six quantities associated to a Jacobian over the rational numbers. One of these quantities is the size S of the Shafarevich-Tate group. Unable to compute S directly, we compute the five other quantities and solve for the conjectural value $S_?$ of S. For all 32 curves considered, the real number $S_?$ is very close to either 1, 2, or 4, and agrees with the size of the 2-torsion of the Shafarevich-Tate group, which we could compute. This paper has been submitted.

6. **Parity structures and generating functions from Boolean rings** (8 pages), with D. Moulton: Let S be a finite set and T be a subset of the power set of S. Call T a *parity structure* for S if, for each subset b of S of odd size, the number of subsets of b that lie in T is even. We classify parity structures using generating functions from a free boolean ring. We also show that if T is a parity structure, then, for each subset b of S of even size, the number of subsets of b of odd size that lie in T is even. We then give several other properties of parity structures and discuss a generalization. This paper has been submitted.

7. **Fallacies, Flaws, and Flimflam #92: An Inductive Fallacy**, (1 page) with A. Riskin: College Math. Journal 26:5 (1995), 382.

Work in progress

1. **The modular forms database:** This is an evolving collection of tables of modular eigenforms, special values of L-functions, arithmetic invariants of modular abelian varieties, and other data. These tables are available at `http://shimura.math.berkeley.edu/~was/Tables/`.

2. **Visibility of Shafarevich-Tate groups of modular abelian varieties** (20 pages), with A. Agashé: We study Mazur's notion of visibility of Shafarevich-Tate of modular abelian varieties, and use it to verify the conjecture of Birch and Swinnerton-Dyer for several specific abelian varieties. We also give evidence that visibility is rare. The computations are done, but we are still adding to the theoretical content of the paper and polishing the presentation.

3. **Component groups of optimal quotients of Jacobians** (16 pages): Let A be an optimal quotient of $J_0(N)$. The main theorem of this paper gives a relationship between the modular degree of A and the order of the component group of A. From this I deduce a computable formula for the component group of any optimal quotient of $J_0(N)$ at a prime of multiplicative reduction. I then compute over one thousand examples leading me to conjecture that the torsion and component groups of quotients of $J_0(p)$, for p prime, are as simple as possible. This paper is almost ready to be submitted.

4. **Mod** 5 **approaches to modularity of icosahedral Galois representations** (16 pages), with K. Buzzard: Consider a continuous odd irreducible representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$. A special case of a general conjecture of Artin is that the L-function $L(\rho, s)$ associated to ρ is entire. Buzzard and I give new examples of representations ρ that satisfy this conjecture. We obtained these examples by applying a recent theorem of Buzzard and Taylor to a mod 5 reduction of ρ, combined with a computational verification of modularity of a related mod 5 representation. The computations of the paper are complete, and have been mostly written up. We expect to finish the paper in time for the Hot Topics workshop at MSRI in December, 1999.

5. **Indexes of genus one curves** (10 pages): I prove results about the complexity of genus one curves. The greatest common divisor of the degrees of the fields in which a curve of genus g over $\mathbf{Q}$ has a rational point divides $2g-2$; when $g=1$ this is no condition at all. In the 1950s S. Lang and J. Tate asked whether, given a positive integer m, there exists a genus one curve so that the smallest number field in which it has a rational point is of degree m over $\mathbf{Q}$. Using Euler systems, I prove this when m is not divisible by 4. This paper is almost ready to be submitted.