Abstracts of papers

Amod Agashe

In this document, I have assembled the abstracts of my work so far. All of the papers mentioned below are available at `http://www.math.fsu.edu/~agashe/math.html`

1) *On invisible elements of the Tate-Shafarevich group*, Comptes Rendus de l'Académie des Sciences Paris Ser. I Math., vol. 328 (1999), no. 5, 369–374.

Mazur has introduced the concept of visible elements in the Tate-Shafarevich group of optimal modular elliptic curves. We generalize this notion to arbitrary abelian subvarieties and find, based on calculations that assume the Birch and Swinnerton-Dyer conjecture, that there are elements of the Tate-Shafarevich group of certain sub-abelian varieties of $J_0(p)$ and $J_1(p)$ that are not visible.

2) (with W. Stein) Appendix on generating the Hecke algebra, in:
J.-C. Lario, R. Schoof, *Some computations with Hecke rings and deformation rings*, Experimental Mathematics, vol. 11 (2002), no. 2, 303–311.

We apply a result of Sturm to obtain a bound on the number of Hecke operators needed to generate the Hecke algebra as an abelian group.

3) (with W. Stein) *Visibility of Shafarevich-Tate Groups of Abelian Varieties*, Journal of Number Theory, vol. 97 (2002), no. 1, 171–185.

We investigate Mazur's notion of visibility of elements of Shafarevich-Tate groups of abelian varieties. We give a proof that every cohomology class is visible in a suitable abelian variety, discuss the visibility dimension, and describe a construction of visible elements of certain Shafarevich-Tate groups. This construction can be used to give some of the first evidence for the Birch and Swinnerton-Dyer Conjecture for abelian varieties of large dimension. We then give examples of visible and invisible Shafarevich-Tate groups.

4) (with K. 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 Institute Communications, vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 1–17.

In using elliptic curves for cryptography, one often needs to construct elliptic curves with a known number of points over a given prime field $\mathbf{F_n}$, where n is a prime (or a pseudo-prime). In the context of primality proving, Atkin and Morain suggested the use of the theory of complex multiplication to construct such curves. One of the steps in this method is the calculation of a root modulo n of the Hilbert class polynomial $H_D(X)$ for a fundamental discriminant D. The usual way is to compute $H_D(X)$ over the integers and then to find the root modulo n. We suggest the use of a modified version of the Chinese remainder theorem to compute $H_D(X)$ modulo n directly from the knowledge of $H_D(X)$ modulo enough small primes. Our heuristic complexity analysis suggests that our algorithm would asymptotically run better than the Atkin-Morain method or the algorithm that uses the usual Chinese remainder theorem.

5) (with W. Stein) *Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties of Analytic Rank Zero* (with an Appendix by J. Cremona and B. Mazur), Mathematics of Computation 74 (2005), no. 249, 455–484.

This paper provides evidence for the Birch and Swinnerton-Dyer conjecture for analytic rank 0 abelian varieties A_f that are optimal quotients of $J_0(N)$ attached to newforms. We prove theorems about the ratio $L(A_f, 1)/\Omega_{A_f}$, develop tools for computing with A_f, and gather data about certain arithmetic invariants of the nearly 20000 abelian varieties A_f of level ≤ 2333. Over half of these A_f have analytic rank 0, and for these we compute upper and lower bounds on the conjectural order of $Ш(A_f)$. We find that there are at least 168 such that the Birch and Swinnerton-Dyer Conjecture implies that $Ш(A_f)$ is divisible by an odd prime, and we prove for 39 of these that the odd part of the conjectural order of $Ш(A_f)$ really divides $\#Ш(A_f)$ by constructing nontrivial elements of $Ш(A_f)$ using visibility theory. We also give other evidence for the conjecture. The appendix, by Cremona and Mazur, fills in some gaps in the theoretical discussion in their paper on visibility of Shafarevich-Tate groups of elliptic curves.

6) (with K. Ribet and W. Stein) *The Manin constant*, Pure and Applied Mathematics Quarterly, 2 (2006), no. 2, 617–636 (Part II of a special issue in honor of John Coates).

The Manin constant of an elliptic curve is an invariant that arises in connection with the conjecture of Birch and Swinnerton-Dyer. One conjectures that this constant is 1; it is known to be an integer. After surveying what is known about the Manin constant, we establish a new sufficient condition that ensures that the Manin constant is an *odd* integer. Next, we generalize the notion of the Manin constant to certain abelian variety quotients of the Jacobians of modular curves; these quotients are attached to ideals of Hecke algebras. We also generalize many of the results for elliptic curves to quotients of the new part of $J_0(N)$, and conjecture that the generalized Manin constant is 1 for newform quotients. Finally an appendix by John Cremona discusses computation of the Manin constant for all elliptic curves of conductor up to 130000.

7) *Visibility and the Birch and Swinnerton-Dyer conjecture for analytic rank one*, 16 pages, Int. Math. Res. Not. (IMRN), Vol. 2009 (2009), No. 15, pp. 2899–2913.

Let E be an optimal elliptic curve over $\mathbf{Q}$ of conductor N having analytic rank one, i.e., such that the L-function $L_E(s)$ of E vanishes to order one at $s = 1$. Let K be a quadratic imaginary field in which all the primes dividing N split and such that the L-function of E over K vanishes to order one at $s = 1$. Suppose there is another optimal elliptic curve over $\mathbf{Q}$ of the same conductor N whose Mordell-Weil rank is greater than one and whose associated newform is congruent to the newform associated to E modulo an integer r. The theory of visibility then shows that under certain additional hypotheses, r divides the order of the Shafarevich-Tate group of

E over K. We show that under somewhat similar hypotheses, r divides the order of the Shafarevich-Tate group of E over K. We show that under somewhat similar hypotheses, r also divides the Birch and Swinnerton-Dyer *conjectural* order of the Shafarevich-Tate group of E over K, which provides new theoretical evidence for the second part of the Birch and Swinnerton-Dyer conjecture in the analytic rank one case.

8) *A visible factor of the special L-value*, 29 pages, to appear in Crelle's journal (J. Reine Angew. Math.), arXiv:0810.2477.

Let A be a quotient of $J_0(N)$ associated to a newform f such that the special L-value of A (at $s = 1$) is non-zero. We extract an integer factor from the ratio of the special L-value to the real period of A; this factor is non-trivial in general and is related to certain congruences of f with eigenforms of positive analytic rank. We use the techniques of visibility to show that, under certain hypotheses (which includes the first part of the Birch and Swinnerton-Dyer conjecture on rank), if an odd prime q divides this factor, then q divides either the order of the Shafarevich-Tate group or the order of a component group of A. Suppose p is an odd prime such that p^2 does not divide N, p does not divide the order of the rational torsion subgroup of A, and f is congruent modulo a prime ideal over p to an eigenform whose associated abelian variety has positive Mordell-Weil rank. Then we show that p divides the factor mentioned above; in particular, p divides the ratio of the special L-value to the real period of A. Both of these results are as predicted by the second part of the Birch and Swinnerton-Dyer conjecture, and thus provide theoretical evidence towards it.

9) *Squareness in the special L-value and special L-values of twists*, 20 pages, Int. J. Number Theory (IJNT), to appear, arXiv:0810.5179.

Let N be a prime and let A be a quotient of $J_0(N)$ over $\mathbf{Q}$ associated to a newform such that the special L-value of A (at $s = 1$) is non-zero. Suppose that the algebraic part of the special L-value of A is divisible by an odd prime q such that q does not divide the numerator of $\frac{N-1}{12}$. Then the Birch and Swinnerton-Dyer conjecture predicts that the q-adic valuations of the algebraic part of the special L-value of A and of the order of the Shafarevich-Tate group are both positive even numbers. Under a certain mod q non-vanishing hypothesis on special L-values of twists of A, we show that the q-adic valuations of the algebraic part of the special L-value of A and of the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group of A are both positive even numbers. We also give a formula for the algebraic part of the special L-value of A over quadratic imaginary fields K in terms of the free abelian group on isomorphism classes of supersingular elliptic curves in characteristic N (equivalently, over conjugacy classes of maximal orders in the definite quaternion algebra over $\mathbf{Q}$ ramified at N and ∞) which shows that this algebraic part is a perfect square up to powers of the prime two and of primes dividing the discriminant of K. Finally, for an optimal elliptic curve E, we give a formula for the special L-value of the twist E_D of E by a negative fundamental discriminant $-D$, which shows that this special L-value is an integer up to a power of 2, under some hypotheses. In view of the second part of the Birch and Swinnerton-Dyer conjecture, this leads us to the surprising conjecture that the square of the order of the torsion subgroup of E_D divides the product of the order of the Shafarevich-Tate group of E_D and the orders of the arithmetic component groups of E_D, under certain mild hypotheses.

10) (with K. Ribet and W. Stein) *The modular degree, congruence primes, and multiplicity one*, 28 pages, to appear in a special volume by Springer in honor of Serge Lang.

The modular degree and congruence number are two fundamental invariants of an elliptic curve over the rational field. Frey and Müller have asked whether these invariants coincide. We find that the question has a negative answer, and show that in the counterexamples, multiplicity one (defined below) does not hold. At the same time, we prove a theorem about the relation between the two invariants: the modular degree divides the congruence number, and the ratio is divisible only by primes whose squares divide the conductor of the elliptic curve. We discuss the ratio even in the case where the square of a prime does divide the conductor, and we study analogues of the two invariants for modular abelian varieties of arbitrary dimension.

11) *A visible factor of the Heegner index*, 15 pages, submitted (2007), arXiv:0810.5177.

Let E be an optimal elliptic curve over $\mathbf{Q}$ of conductor N, such that the L-function of E vanishes to order one at $s = 1$. Let K be a quadratic imaginary field in which all the primes dividing N are split and such that the L-function of E over K also vanishes to order one at $s = 1$. In view of the Gross-Zagier theorem, the Birch and Swinnerton-Dyer conjecture says that the index in $E(K)$ of the subgroup generated by the Heegner point is equal to the product of the Manin constant of E, the Tamagawa numbers of E, and the square root of the order of the Shafarevich-Tate group of E (over K). We extract an integer factor from the index mentioned above and relate this factor to certain congruences of the newform associated to E with eigenforms of analytic rank bigger than one. We use the theory of visibility to show that, under certain hypotheses (which includes the first part of the Birch and Swinnerton-Dyer conjecture on rank), if an odd prime q divides this factor, then q divides the order of the Shafarevich-Tate group, as predicted by the Birch and Swinnerton-Dyer conjecture.

12) *Rational torsion in elliptic curves and the cuspidal subgroup*, 12 pages, submitted (2007), arXiv:0810.5181.

Let A be an elliptic curve over $\mathbf{Q}$ of square free conductor N. We prove that if A has a rational torsion point of prime order r such that r does not divide $6N$, then r divides the order of the cuspidal subgroup of $J_0(N)$.

13) *The modular number, congruence number, and multiplicity one*, 12 pages, submitted (2008), arXiv:0810.5176.

Let N be a positive integer and let f be a newform of weight 2 on $\Gamma_0(N)$. In earlier joint work with K. Ribet and W. Stein, we introduced the notions of the modular number and the congruence number of the quotient abelian variety A_f of $J_0(N)$ associated to the newform f. These invariants are analogs of the notions of the modular degree and congruence primes respectively associated to elliptic curves. We show that if p is a prime such that every maximal ideal of the Hecke algebra of characteristic p that contains the annihilator ideal of f satisfies multiplicity one, then the modular number and the congruence number have the same p-adic valuation.

14) *Mod-p reducibility, the torsion subgroup, and the Shafarevich-Tate group*, 11 pages, submitted (2009), arXiv:0905.4217.

Let E be an optimal elliptic curve over $\mathbf{Q}$ of prime conductor N. We show that if for an odd prime p, the mod p representation associated to E is reducible (in particular, if p divides the order of the torsion subgroup of $E(\mathbf{Q})$), then the p-primary component of the Shafarevich-Tate group of E is trivial. We also state a related result for more general abelian subvarieties of $J_0(N)$ and mention what to expect if N is not prime.

15) *Visibility and the Birch and Swinnerton-Dyer conjecture for analytic rank zero*, 18 pages, submitted (2009), arXiv:0908.3823.

Let E be an optimal elliptic curve over $\mathbf{Q}$ of conductor N having analytic rank zero, i.e., such that the L-function $L_E(s)$ of E does not vanish at $s = 1$. Suppose there is another optimal elliptic curve over $\mathbf{Q}$ of the same conductor N whose Mordell-Weil rank is greater than zero and whose associated newform is congruent to the newform associated to E modulo an integer r. The theory of visibility then shows that under certain additional hypotheses, r divides the product of the order of the Shafarevich-Tate group of E and the orders of the arithmetic component groups of E. We extract an explicit integer factor from the the Birch and Swinnerton-Dyer *conjectural* formula for the product mentioned above, and under some hypotheses similar to the ones made in the situation above, we show that r divides this integer factor. This provides theoretical evidence for the second part of the Birch and Swinnerton-Dyer conjecture in the analytic rank zero case.