Sage Days 18: Computations Related to the Birch-Swinnerton-Dyer Conjecture

William Stein

December 23, 2009

The Clay Institute sponsored Sage Days 18, which took place at the Clay Mathematics Institute December 1–5, 2009, and was organized by Craig Citro, Kiran Kedlaya, Barry Mazur, and William Stein. Sage (`http://sagemath.org`) is free open source mathematical software aimed at research and education in both pure and applied mathematics. In addition to the organizers, workshop participants included Avner Ash, Salman Baig, Jen Balakrishnan, Thomas Barnet-Lamb, Joël Bellaïche, Robert Bradshaw, Mirela Ciperiani, Victoria de Quehen, Noam Elkies, Cameron Franc, Matt Greenberg, Dick Gross, David Harvey, Dimitar Jetchev, Robert Miller, Victor Miller, Robert Pollack, Bjorn Poonen, Jonathan Pottharst, Ken Ribet, David Roe, Karl Rubin, Glenn Stevens, Andrew Sutherland, John Tate, Richard Taylor, and Jared Weinstein. The main theme of the workshop was computations related to the Birch and Swinnerton-Dyer conjecture, with a particular focus on computational aspects of Heegner and Stark-Heegner points and Euler systems.

There were 12 research lectures, with several on theoretical and computational applications of Euler systems, including a proof of one of Darmon's conjectures by Mazur and Rubin, and a talk about computing Kolyvagin classes by Stein and Weinstein. Sutherland also spoke about his new highly-efficient probabilistic algorithm for computing images of Galois representations, Bradshaw about provable computation of motivic L-functions, and Baig about computational aspects of the Birch and Swinnerton-Dyer (BSD) conjecture for elliptic curves over function fields. Greenberg and Pollack gave a pair of talks about relations between p-adic modular symbols and Stark-Heegner points. Ciperiani and Jetchev rounded up the lectures with talks on applications of Heegner points. Karl-Dieter Crisman also organized a final day of the workshop on applications of Sage in undergraduate education, particularly linear algebra, calculus, and abstract algebra; this final day of the workshop was well attended by educators in the Boston area.

In addition to the 12 research lectures, Ribet organized a series of morning tutorials on how to *use* Sage. These included a tutorial by Kedlaya on Python and Sage, by Bradshaw on exact linear algebra, by Roe on Tate's algorithm, by Robert Miller on 2-descent, and by Stein and Sutherland on computings images of Galois representations.

Each evening participants also gave status updates reporting on the results of projects they carried out during the workshop. Project topics included BSD over function fields, 3-descent, images of Galois, reduction of Heegner points, anabelian invariants, and computational verification of Kolyvagin's conjecture.

Baig led a project on making systematic tables of elliptic curves over function fields, along with their BSD invariants, similar to what John Cremona has done for elliptic curves over the rational numbers. Roe worked on implementing Tate's algorithm over $\mathbf{F}_p(t)$ in Sage, by making the current implementation of Tate's algorithm over number fields (which he started at the last CMI Sage Days in 2007) more general. Victor Miller and Noam Elkies thought about techniques for enumerating elliptic curves over funtion fields, including explicit solution of S-unit equations and using that the ABC conjecture is a theorem (of Mason) over function fields. Baig and Stein looked in detail at several curves of rank 2, computing their L-functions, BSD invariants (following remarks of Tate during the status reports). Bradshaw and Roe spent substantial time writing fast compiled code in Sage for searching for rational points on elliptic curves over functions fields, thus implementing a function field analogue of Michael Stoll's ratpoints program.

Robert Miller led a project involving computation of 3-Selmer ranks of elliptic curves. He spent time explaining the general algorithms for 3-descent, then worked on implementing code in Sage for computing class groups and unit groups of quotients of univariate polynomial rings (affine algebras over $\mathbf{Q}$), building on the PARI library. Also, Jeechul Woo, a current Ph.D. student of Elkies, presented a new fast algorithm for doing 3-descent on curves that possess a rational 3-torsion point. Bradshaw, Roe, and Stein then ported Woo's GP/PARI implementation to Sage.

Andrew Sutherland's project involved making huge tables of images of Galois representations attached to elliptic curves. Each day of the workshop he improved (and recoded) his algorithm, so by the end of the workshop he had code that could compute the image for several hundred million elliptic curves in a matter of hours. Moreover, the resulting algorithm he arrived at depended mainly on lookup tables, so could likely be easily implemented from scratch again. Sutherland also restricted his computation to large collections of curves with special properties, e.g., semistable curves, and computed statistics about the image of Galois for those curves. Finally, Sutherland learned Cython and adapted his program so that it would be easy to include in Sage.

Jetchev and Stein implemented code in Sage (using theta series and rational quaternion algebras) that explicitly determined the distribution of reductions of higher Heegner points to characteristic p. In particular, they wrote code that determined the first Heegner point whose conjugates reduce to give all supersingular points in characteristic p, and gathered data using their code.

Mazur led a project to compute anabelian information about curves in characteristic p. In particular, he came up with an explicit construction that involved computing invariants of an elliptic curve over a finite field that involved point counting on certain superelliptic curves. Stein found fast code for related point counting, then Kedlaya did a direct implementation and ran it for all elliptic curves over $\mathbf{F}_p$, for very small p. The data showed that Mazur's anabelian invariant is a more refined invariant than the zeta function.

Stein led a project to verify Kolvyagin's conjecture (about nontriviality of the Euler system of Heegner points attached an elliptic curve) for a specific elliptic curve of rank 3, which had so far never been done before. Balakrishnan determined that the computation was likely feasible, and pushed several computers quite hard during the the workshop to do the computation. Stein implemented some key algorithms, and on the last day of the workshop, they were able to complete the first verification of the conjecture for a rank 3 curve. Together with Weinstein, they also computationally investigated some deeper structure of Kolyvagin's Euler system, especially for curves of rank 1 with nontrivial Shafarevich-Tate group. This all used a large package of code for computing with Heegner points and Kolyvagin classes that will soon be included in Sage.