MR2254648 (Review) 11F67 (11G05 11G40)

Darmon, Henri (3-MGL-DM); **Pollack, Robert [Pollack, Robert[2]]** (1-BOST)

Efficient calculation of Stark-Heegner points via overconvergent modular symbols. (English summary)

Israel J. Math. **153** (2006), 319–354.

Let $E/\mathbf{Q}$ be an elliptic curve of conductor N, and let p be a prime which fully divides N. Let K be a real quadratic field in which p is inert. In [Ann. of Math. (2) **154** (2001), no. 3, 589–639; MR1884617 (2003j:11067)], the first author defined a collection of points on E over the completion K_p, and conjectured that these points are actually defined over specific ring class field extensions of K. To be more precise, let $\mathcal{H}_p := \mathbf{P}^1(\mathbf{C}_p) - \mathbf{P}^1(\mathbf{Q}_p)$ denote the p-adic upper half plane. Choose a p-adic embedding $K \subset \mathbf{C}_p$. Darmon defined a map

$$\Gamma\backslash(\mathcal{H}_p \cap K) \to E(K_p), \quad \tau \mapsto P_\tau,$$

and called the P_τ Stark-Heegner points. The set of $\alpha \in K$ such that multiplication by α sends the group $\mathbf{Z}[1/p] + \mathbf{Z}[1/p]\tau$ into itself is a $\mathbf{Z}[1/p]$-order in K, denoted $\mathcal{O}_\tau$; Darmon conjectured that $P_\tau \in E(H_\tau)$, where H_τ is the narrow ring class field attached to the order $\mathcal{O}_\tau$. As in the paper, we assume from now on that $N = p$.

The definition of P_τ starts by considering the $\mathbf{Z}$-valued modular symbol $I_f\colon \mathbf{P}^1(\mathbf{Q}) \times \mathbf{P}^1(\mathbf{Q}) \to \mathbf{Z}$ associated with the modular form f attached to E. Here we have chosen once and for all either the odd or even modular symbol. From I_f, one defines a modular symbol μ_f valued in measures on $\mathbf{P}^1(\mathbf{Q}_p)$ by requiring that its measure on $\mathbf{Z}_p$ is equal to I_f, that its total measure is 0, and by requiring a certain invariance property under $\mathrm{PGL}_2(\mathbf{Z}[1/p])$. The restriction of $\mu_f\{0 \to \infty\}$ to $\mathbf{Z}_p^\times$ is the Mazur-Swinnerton-Dyer measure associated to f, used by those authors [B. Mazur and P. Swinnerton-Dyer, Invent. Math. **25** (1974), 1–61; MR0354674 (50 #7152)] to define the p-adic L-function of f. The definition of P_τ, which we do not state precisely, is given in terms of certain integrals with respect to the measures μ_f. To compute the P_τ in practice, however, it suffices to compute integrals of the form

$$\int_{\mathbf{P}^1(\mathbf{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_f\{0 \to \infty\}(t) \in \mathbf{C}_p, \tag{1}$$

where $\log$ denotes a branch of the p-adic logarithm.

In an earlier article with P. E. Green [Experiment. Math. **11** (2002), no. 1, 37–55; MR1960299 (2004c:11112)], the first author provided computational evidence for his algebraicity conjecture by computing P_τ in various settings and showing in each case that it indeed appeared (to several p-adic digits) to be defined over the correct ring class field H_τ. The goal of the article under review is to introduce a new algorithm for these computations which is qualitatively better and indeed drastically improves the results of the experiments. The key new ingredient in these computations is the algorithm of the second author and G. Stevens to compute the moments of the Mazur-Swinnerton-Dyer measure using overconvergent modular symbols, as introduced in [R. Pollack

and G. Stevens, "Critical slope p-adic L-functions", draft, math.bu.edu/people/rpollack/Papers/critical.pdf; "Computations with overconvergent modular symbols", draft, math.bu.edu/people/rpollack/Papers/explicit.pdf].

The key difference between the Darmon-Green algorithm and the present one is in the computation of the integrals (1). To compute the integral to an accuracy of M significant p-adic digits, the former method was to partition $\mathbf{P}^1(\mathbf{Q}_p)$ into the $(p+1)p^{M-1}$ residue discs modulo p^M, and evaluate the corresponding Riemann sum. The current algorithm is to first break up the integral as the sum of two integrals: one over $\mathbf{Z}_p$, and one over $\mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p$. For the first integral, one expands the integrand of (1) as a power series in each residue disc $a + p\mathbf{Z}_p$. If we define the kth moment of μ_f on this residue disc by

$$\int_{a+p\mathbf{Z}_p} (t-a)^k d\mu_f\{0 \to \infty\}(t), \tag{2}$$

then the desired integral can be expressed as a linear combination of approximately M of these moments. The integral over $\mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p$ is transformed into one over $\mathbf{Z}_p$ via the transformation $t \mapsto -1/t$, and computed via a similar algorithm. Therefore, the new algorithm has a computational complexity which is linear in the p-adic accuracy required, whereas the Darmon-Green algorithm has an exponential complexity (viewing the prime p as fixed).

The summary we have given so far occupies the introduction and first section of the paper. The second section recalls the Pollack-Stevens algorithm to compute the moments of the Mazur-Swinnerton-Dyer measure, as we now briefly summarize. Let $\mathcal{D}(\mathbf{Z}_p)$ denote the space of locally analytic $\mathbf{Q}_p$-valued distributions on $\mathbf{Z}_p$. An overconvergent modular symbol of level p is a $\Gamma_0(p)$-invariant modular symbol valued in $\mathcal{D}(\mathbf{Z}_p)$. There is a Hecke-equivariant map from the space of overconvergent modular symbols to the space of $\Gamma_0(p)$-invariant modular symbols valued in $\mathbf{Q}_p$, obtained by taking total measure (i.e. evaluating on $\mathbf{Z}_p$). Stevens ["Rigid analytic modular symbols", unpublished notes; per bibl.] proved that this map is an isomorphism when restricted to the subspaces on which U_p acts with slope less than 1. Therefore, the modular symbol I_f lifts to such an overconvergent modular symbol Φ_f. From the definitions, it is easy to see that the restriction of μ_f to $\mathbf{Z}_p$ is essentially equal to Φ_f (see Proposition 2.4); thus the evaluation of (2) is reduced to the evaluation of the same integral with μ_f replaced by Φ_f. The symbol Φ_f is efficiently computed by realizing it as the limit of a sequence of symbols obtained by repeatedly applying U_p to an initial approximation Φ. Section 2 concludes with a discussion of: (Section 2.3) how to lift I_f to an overconvergent modular symbol which is not necessarily a U_p-eigensymbol Φ, (Section 2.4) how to iterate U_p on Φ to approximate a U_p-eigensymbol Φ_f by means of a U_p-invariant filtration on $\mathcal{D}(\mathbf{Z}_p)$, and (Section 2.5) how to compute the moments of μ_f given the previous steps.

In Section 3, the authors describe how to download and execute the Magma programs that they wrote to compute Stark-Heegner points using this algorithm. In the fourth and final section, they discuss the results of their experiments. For example, for $X_0(11)$ they are able to compute Stark-Heegner points to an accuracy of 100 11-adic digits. They are pleased to report that their program can recognize the Stark-Heegner point over $K = \mathbf{Q}(\sqrt{101})$ on this curve within a few seconds, even though the point has K-rational coordinates with over 50 digits. This computation was not possible using the Darmon-Green algorithm. The authors provide several tables of data resulting from their programs, and point out that the results are publicly verifiable by downloading their

programs from the first author's Web page.

We conclude by remarking that the methods of this paper were improved upon and also generalized to the context of Shimura curves by M. Greenberg in his thesis and in [*Algorithmic number theory*, 361–376, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006; MR2282936].

Reviewed by *Samit Dasgupta*

References

1. M. Bertolini and H. Darmon, *Hida families and rational points on elliptic curves*, submitted.
2. M. Bertolini and H. Darmon, *The rationality of Stark–Heegner points over genus fields of real quadratic fields*, submitted.
3. H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics **138,** Springer-Verlag, Berlin, 1993. MR1228206 (94i:11105)
4. H. Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications*, Annals of Mathematics (2) **154** (2001), 589–639. MR1884617 (2003j:11067)
5. S. Dasgupta, *Gross–Stark units, Stark–Heegner points, and class fields of real quadratic fields*, PhD thesis, Berkeley, May 2004.
6. H. Darmon and S. Dasgupta, *Elliptic units for real quadratic fields*, Annals of Mathematics, to appear. cf. MR 2007a:11079
7. H. Darmon and P. Green, *Elliptic curves and class fields of real quadratic fields: algorithms and evidence*, Experimental Mathematics **11** (2002), 37–55. MR1960299 (2004c:11112)
8. E. de Shalit, *p-adic periods and modular symbols of elliptic curves of prime conductor*, Inventiones Mathematicae **121** (1995), 225–255. MR1346205 (96f:11074)
9. N. D. Elkies, *Heegner point computations*, in *Algorithmic Number Theory (Ithaca, NY, 1994)*, Lecture Notes in Computer Science **877,** Springer, Berlin. 1994, pp. 122–133. MR1322717 (96f:11080)
10. R. Greenberg and G. Stevens, *p-adic L-functions and p-adic periods of modular forms*, Inventiones Mathematicae **111** (1993), 407–447. MR1198816 (93m:11054)
11. D. E. Knuth, *The Art of Computer Programming*, Vol. 2, 3rd edn., Addison-Wesley, Reading, Mass, 1981. MR0633878 (83i:68003)
12. J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya **36** (1972), no. 1, 19–66. MR0314846 (47 #3396)
13. B. Mazur, J. Tate and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Inventiones Mathematicae **84** (1986), 1–48. MR0830037 (87e:11076)
14. R. Pollack and G. Stevens, *The "missing" p-adic L-function*, in preparation.
15. R. Pollack and G. Stevens, *Explicit computations with overconvergent modular symbols*, in preparation.
16. K. Rubin, *p-adic variants of the Birch and Swinnerton-Dyer conjecture* for *elliptic curves with complex multiplication*, in *p-Adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, MA, 1991)*, Contemporary Mathematics **165,** American Mathematical Society, Providence, RI, 1994, pp. 71–80. MR1279603 (95i:11065)
17. G. Stevens, *Rigid analytic modular symbols*, unpublished notes.

Note: This list reflects references listed in the original paper as accurately as possible with no attempt to correct errors.